UNIVERSITE IBN KHALDOUN - TIARET

MEMORY

Introduced to:

FACULTY OF MATHEMATICES AND COMPUTER SCIENCE

DEPARTMENT OF COMPUTR SCIENCE

For the graduation of:

MASTER

Specialty: Software engineering

Through:

- DJAAD Fatima

- KHARACHI Azhar

On the subject:

───

➤ The Voting System: From Electronic Voting To Internet Voting

───

Soutenu publiquement le 18/ 09 / 2022 à Tiaret devant le jury composé de :

Mr MOKHTARI Ahmed	MAA	Tiaret	Président
Mr DAHMANI Youcef	Grade	University PB	Encadreur
Mr BENATHMANE Lalia	Grade	Université Xxxxxx	Examinateur

Acknowledgements

First of all, we thank the Almighty God who gave the strength, the patience and the courage to

Can accomplish this work.

It is with great humility and gratitude to deeply acknowledge all those who helped us put these ideas, above the level of simplicity, into something concrete.

We would like to express our special thanks and gratitude

To Dr. Dahmani who gave us the golden opportunity to do this wonderful project, who also helped us do a lot of research and got to know a lot of new things. We are really grateful to them.

No attempt at any level can be satisfactorily completed without the support and guidance of our parents and friends.

Last but not least, we would like to thank everyone who helped and motivated us to work on this project.

DEDICATION

«وما توفيقي إلا بالله عليه توكلت وإليه أنيب»

I dedicate this success in my life to the most

precious thing I own in this world, my support and

help in my life and it was a gift from God to me

« *My family* **».**

I thank them so much for being in my life

And I wanted to say that you mean

Everything to me.

I sincerely thank Mr.DAHMANI Youcef,

Mr.Mokhtari Ahmed, Ms.BENATHMANE

Lalia

Finally, I thank the wonderful people Ihave,

My friends and everyone who Shares me

And who have supported and

Helped me from near or far during my Journey

Djaad.fatima

dedication

I would like to tell my dear parents that no dedication expresses my respect, my undying love and my consideration for the sacrifices they have made for my education and my well being. Thank you for all the support and love you have given me since my childhood and I hope your blessing is always with me , All my gratitude and thanks and love to my dear sisters and my friends as well as my classmates and my teachers during these amazing five years

Kh. Azhar

Abstract

The interconnectedness of networks and the rapid expansion of the Web have allowed the development of a large number of applications that can be used. And it became necessary to contribute to the creation of a website or application that could help the Electoral Commission to people in a much better way.

That is why we pose the following problem: Why is it not currently expected the electronic voting system or the online voting system, will benefit from these technological developments?

In this current technological world it was necessary to build a way in which elections could be conducted through the Internet by every citizen in the society. This project is a contribution from our side where the Electoral Commission can help the people in a much better way.

Also, electronic or online voting has multiple advantages, which translate into the availability of a greater number of participants thanks to its ease of use. The process involved is immobility and simplicity of the process, automatic counting and therefore faster, and it is also easier for the user (administrator, candidate and voter) to participate in voting via Internet because it contains a simple and interactive user interface.

The proposed portal is secured and has a unique security feature such as creating a unique identifier that adds another layer of security (except for login ID and password) and gives the administrator the ability to verify user information and determine whether or not he is eligible. Electronic voting with defining the list of accepted candidates. It provides tools for retaining the votes of voters in municipal elections and calculating the total number of votes (candidates) and age groups for each municipality.

It also creates and manages voting and election details where all users have to login by username and password and click on the candidates to register the vote, this helps and facilitates the voting process for the users.

Keywords: Voting system, Electronic voting, online voting, technological developments, Electoral Commission, build, automatic counting, voter, candidate, eligible to vote, security, manages voting, register the vote, voting process.

Résumé

L'interconnexion des réseaux et l'expansion rapide du Web ont permis le développement d'un grand nombre d'applications utilisables. Et il est devenu nécessaire de contribuer à la création d'un site Web ou d'une application qui pourrait aider la Commission électorale aux gens d'une bien meilleure façon.

C'est pourquoi nous posons le problème suivant : Pourquoi n'est-il pas prévu actuellement système de vote électronique ou le système de vote en ligne, bénéficie de ces évolutions technologiques ?

Dans ce monde technologique actuel, il était nécessaire de construire un moyen par lequel les élections pourraient être menées via Internet par chaque citoyen de la société. Ce projet est une contribution de notre côté où la Commission électorale peut aider le peuple d'une bien meilleure façon.

Aussi, le vote électronique ou en ligne présente de multiples avantages, qui se traduisent par la disponibilité d'un plus grand nombre de participants grâce à sa facilité d'utilisation. Le processus impliqué est l'immobilité et la simplicité du processus, le comptage automatique et donc plus rapide, et il est également plus facile pour l'utilisateur (administrateur, candidat et électeur) de participer au vote via Internet car il contient une interface utilisateur simple et interactive.

Le portail proposé est sécurisé et possède une fonction de sécurité unique telle que la création d'un identifiant unique qui ajoute une autre couche de sécurité (à l'exception de l'identifiant de connexion et du mot de passe) et donne à l'administrateur la possibilité de vérifier les informations de l'utilisateur et de déterminer s'il est éligible ou non. Vote électronique avec définition de la liste des candidats acceptés. Il fournit des outils pour retenir les voix des électeurs aux élections municipales et calculer le nombre total de voix (candidats) et les tranches d'âge pour chaque municipalité.

Il crée et gère également les détails de vote et d'élection où tous les utilisateurs doivent se connecter avec un nom d'utilisateur et un mot de passe et cliquer sur les candidats pour enregistrer le vote, cela aide et facilite le processus de vote pour les utilisateurs.

Mots-clés: système de vote, vote électronique, vote en ligne, développements technologiques, commission électorale, construction, dépouillement automatisé, électeur, candidat, habilité à voter, sécurité, gestion du vote, enregistrement des votes, processus de vote.

مــلخص

سمح الترابط بين الشبكات والتوسع السريع للويب بتطوير عدد كبير من التطبيقات التي يمكن استخدامها. وأصبح من الضروري المساهمة في إنشاء موقع على شبكة الإنترنت أو تطبيق يمكن أن يساعد مفوضية الانتخابات الناس بطريقة أفضل بكثير.

ولهاذا نطرح الإشكال التالي : لماذا لا يُتوقع حاليًا أن يستفيد نظام التصويت الإلكتروني أو التصويت عبر الإنترنت من هذه التطورات التكنولوجية ؟

في هذا العالم التكنولوجي الحالي كان لابد من بناء طريقة يمكن من خلالها إجراء الانتخابات من خلال الإنترنت من قبل كل مواطن في المجتمع. هذا المشروع هو مساهمة من جانبنا حيث يصبح من الممكن أن تساعد مفوضية الانتخابات الناس بطريقة أفضل بكثير.

أيضًا، يتمتع التصويت الإلكتروني أو عبر الإنترنت بمزايا متعددة، والتي تُترجم إلى توفر عدد أكبر من المشاركين بفضل سهولة استخدامه العملية المتضمنة هي عدم الحركة وبساطة العملية، والعد التلقائي وبالتالي أسرع، كما يسهل على المستخدم (المسؤول ،المترشح و الناخب) المشاركة في التصويت عبر الإنترنت لاحتوائه على واجهة مستخدم بسيطة وتفاعلية.

البوابة الإلكترونية المقترحة مؤمنة ولديها ميزة أمان فريدة مثل إنشاء معرف فريد يضيف طبقة أخرى من الأمان (باستثناء معرف تسجيل الدخول وكلمة المرور) ويمنح المسؤول القدرة على التحقق من معلومات المستخدم وتحديد ما إذا كان مؤهلاً أم لا .يتم رفض أي مترشح لا يتطابق مع قوانين نظام التصويت الالكتروني مع تحديد قائمة المترشحين المقبولين. و يوفر أدوات للاحتفاظ بأصوات الناخبين في الانتخابات البلدية وحساب العدد الإجمالي للأصوات (المرشحين) والفئات العمرية لكل بلدية..

كما أنه ينشئ ويدير تفاصيل التصويت والانتخاب حيث يتعين على جميع المستخدمين تسجيل الدخول باسم المستخدم وكلمة المرور والنقر على المرشحين لتسجيل التصويت ، وهذا يساعد ويسهل عملية التصويت للمستخدمين..

الكلمات المفتاحية: نظام التصويت ، التصويت الإلكتروني ، التصويت عبر الإنترنت ، التطورات التكنولوجية ، مفوضية الانتخابات ، البناء ، العد الآلي ، الناخب ، المرشح ، مؤهل للتصويت ، الأمن ، يدير التصويت ، تسجيل التصويت ، عملية التصويت.

Table of contents

List of figures

Liste of tables

Glossary of Acronyms and Abbreviations:

E-voting: Electronic Voting.

I-voting: Internet Voting.

EVM: Electronic voting machines.

ACL: Access Control List.

HRD: Human Resources Department.

UML: Unified Modeling Language.

ERD: Entity relationship diagrams.

An overview of the topic

Challenges and working hypothesis

Online voting in elections might seem like a logical step forward considering the many other daily activities, like banking and shopping, that we complete online. However, voting online does present unique challenges that usually don't apply to other internet-based processes. These challenges are related to a variety of factors, including the security required for online voting, legal requirements and frameworks, public opinion, and investment.

- ❖ Security
- ❖ Voter Verification and Privacy
- ❖ Election Verifiability
- ❖ Legal Frameworks

Thesis Overview:

In this letter, we suggest an electronic or online voting system (Supervisors, candidates, voters) are registered and their information is sent and processed directly to the official website of the elections, instead of going to the election center, in addition to defining the list of those accepted in the electoral campaign and the election results and providing a platform via the website to see everything related to the elections.

Objectives and Advantages of the new system

- Faster counting and delivering of election results.
- Increased trust in elections as human error is avoided.
- Increased voter turnout, especially when internet voting is involved.
- Cost reduction when applying e-Voting on multiple electoral events.
- Reduced ballot waste.

Improved convenience for voters

- Easier vote marking and casting as the voting experience helps to avoid errors, in particular when over-voting, under-voting or making incorrect selections.
- Ballots available in multiple languages.
- Vote remotely from home or other locations using internet voting.

Improved Accessibility

- People with disabilities are able to vote thanks to audio voting.
- Online voting allows people who are unable to reach the polling places to vote.

Fraud Prevention

- E-Voting reduces the chances of accidental or intentional variations in vote counts by reducing poll worker direct interaction with ballots or counts.
- E-Voting and online voting reduce voter errors and the chances of voter fraud, increasing electoral integrity.

Subject delimitation:

Any developer or researcher strives to exploit the best possibilities to make the work perfect. Despite this, any scientific research work is limited in many respects due to the continuous development of technology and scientific research.

We wanted to take a step in the field of information technology so that we worked in the field of electronic voting, in addition to services that provide electoral rights to candidates and voters at the same time to provide a safe and more transparent space.

The methods and procedures followed:

In the context of this project, we used the UML method to model our new system.

We focused on software engineering to build the system, by building an effective system for determining electoral lists in municipalities according to the laws stipulated by the states, and this online voting system works by managing voter information through which the voter can log in and use his data. Voting rights and provides them with a secure network.

In addition to providing voting statistics (supervisor, candidate and voter) in each municipality in order to facilitate knowing the number of interested segments of society and participating in the electronic or online voting system.

Scope of Project

As this website provides better way of election between persons and political parties, hence we suppose that this project has a greater scope and is important requirement is to provide a compact, stable system of voting with a facility to be at home.

GENERAL INTRODUCTION:

GENERAL INTRODUCTION:

The interconnection of networks and the rapid expansion of the Web have allowed the development of à large number of applications that the user can run remotely without physically moving. One of the applications currently expected to benefit from these technological advances is voting.

In fact, traditional elections and referendums require all those participating in the vote to travel, but it is difficult to convince everyone to make the trip when it would be so easy to vote from home, electronically or via the Internet.

The advantages would be multiple: a greater number of participants thanks to the ease of this operation implied by the non-displacement and the simplicity of the process, the automated counting and therefore faster and more secure.

Then, voting by internet seems to go without saying. It is not difficult to add voices, and many banking or commercial transactions take place via this new medium. But this operation presents unprecedented characteristics in the computer field.

First of all, the secrecy of the vote prohibits observing the procedure during its unfolding.
- In this thesis, we will learn more about electronic voting:

- ➢ **The first chapter:** presents a general overview of the voting system: From electronic voting to internet voting.
- ➢ **The second chapter:** presents the analysis and specification of our voting system, in particular its design based on UML diagrams.
- ➢ **The third chapter:** is dedicated to the presentation of the different tools used for the realization of our project. It then gives addresses the realization side of our project, with examples of the most important interfaces.

- Our report consists of three chapters listed below as illustrated by figure1:
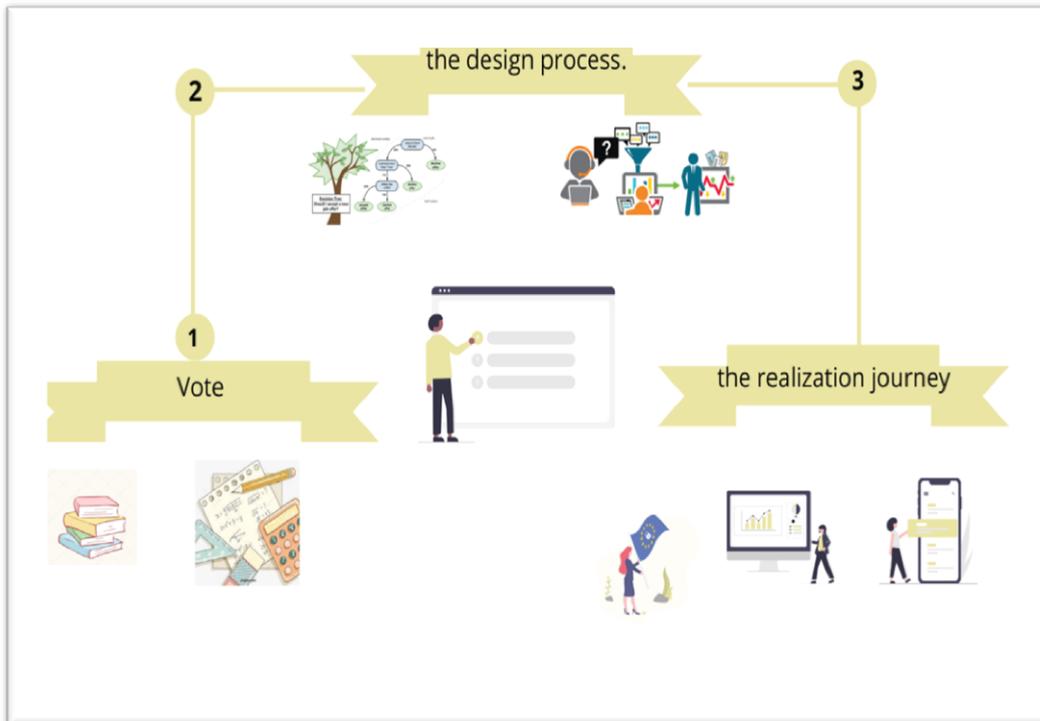
Figure 1: Project Graduation structure
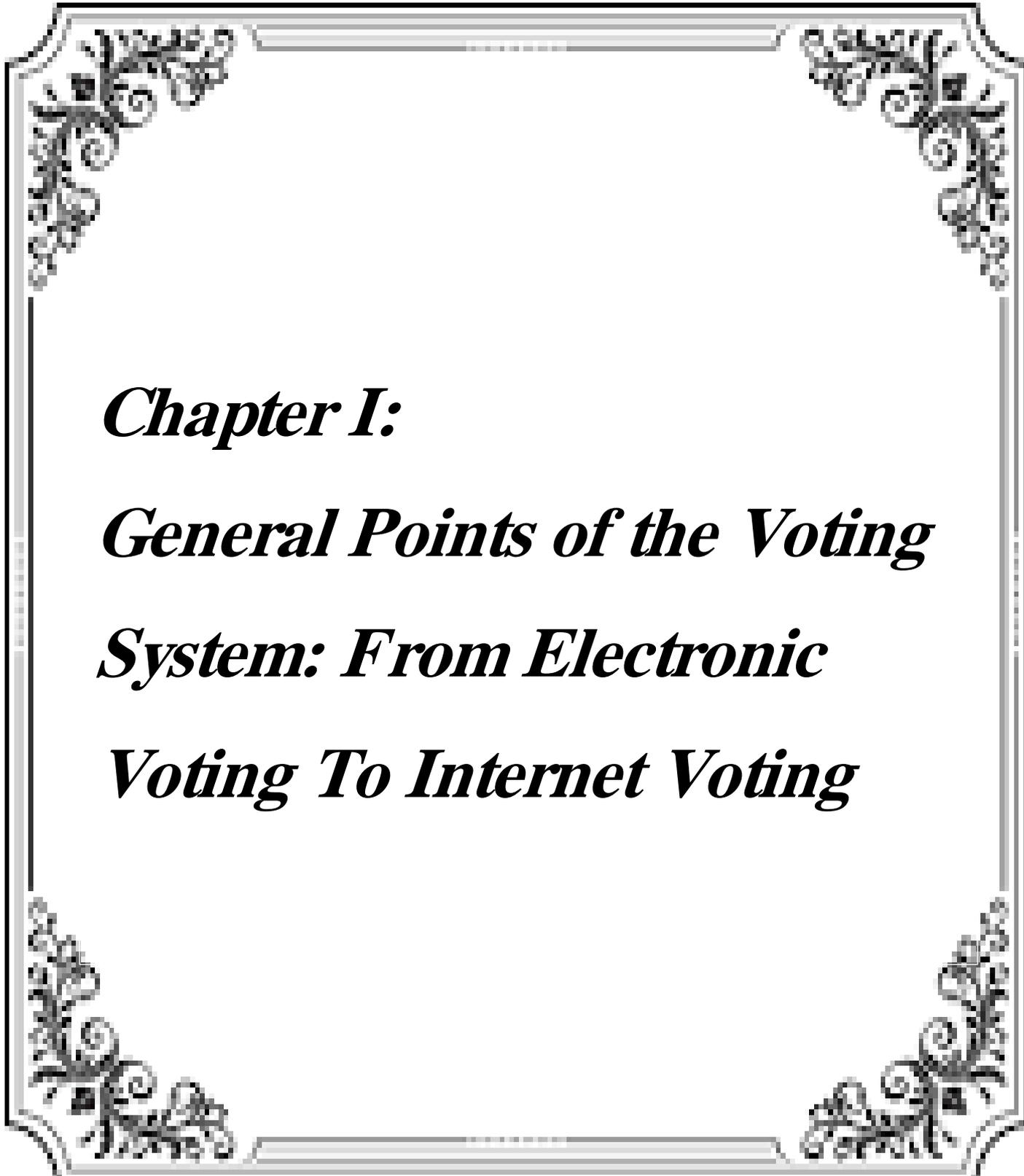
Chapter I:

General Points of the Voting System: From Electronic Voting To Internet Voting

I.1.Introduction

Eectronic voting is an example of decentralized application that can hold elections over an open computer network.

Electronic voting, a form of computer-mediated voting in which voters make their selections with the aid of a computer. The voter usually chooses with the aid of a touch-screen display, although audio interfaces can be made available for voters with visual disabilities.

To understand electronic voting, it is helpful to consider the four basic steps of the election process. Assembling ballots for voters to choose. Voting, where voters vote. Ballot recording, where the system records ballots. Aggregation where votes are counted. Voting, recording, and ballot aggregation are routinely performed by computers, even in strictly non-electronic voting systems. Electronic voting, in its strictest sense, is a system in which the first step, voting (or selection), is done with the help of a computer.

There are two quite different types of electronic voting technologies: those that use the Internet (I-voting) and those that do not (e-voting). These two types are described in this chapter.

I.2. Electronic voting:

Electronic voting (also known as e-voting) is voting that uses electronic means to either aid or take care of casting and counting ballots.

Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet.

Eectronic voting is an example of a decentralized application that can hold elections over an open computer network, In this application, a group of voters send ballots over the network to the Virtual Count Center. The Virtual Count Center is responsible for receiving, validating, and sorting ballots. Participants involved in electronic elections are usually a group of voters and a group of voters. The number and usefulness of these authorities depends on the voting scheme under consideration [1]. Electronic voting scenarios can be divided into three phases:

➢ **Registration Phase:** In this first phase, the Election Commission edits the voter list of all voters registered for this election process and publishes it on the Internet.

➢ **Voting Phase:** In this phase, voters can submit ballots using the communication options provided by the network.

➢ **Counting Phase:** At the end of the voting phase, authorities will stop accepting ballots and start counting results. Finally, the results will be published and made available to voters over the network.

I.2.1. Electronic voting properties:

Voting applications are intended to run on the network, so a good electronic voting system needs to ensure some properties that define security and implementation requirements [2, 3].

Below, you define the security requirements to consider when designing your system.

Accuracy: The choice is correct if the following requirements are met:

Voting cannot be changed. That is, you cannot change the voting results by adding invalid votes or changing the content of the ballot (consistency).You need to count valid votes. Invalid votes are not counted.

Democracy: This property is guaranteed if Only voters are eligible to vote.

Each voter can only vote once. Democratic ownership is basically related to the integrity of the electoral list (the list of voters). To do this, you need to add some mechanism to prevent the administrator of this list from breaking this property.

Confidentiality: Confidentiality voting is called voting in the following cases:

Neither the electoral authorities nor anyone else can link voters to their votes (anonymity): Anonymity is probably the basis of any voting system Electronics [4].

Voters cannot prove that they have voted in a particular way. It is also important to prevent the purchase of votes, as voters can only sell votes if they can prove to the buyer that they have actually made a choice their wish

Verifiability: This property has two definitions: universal verifiability and individual verifiability. The voting system can be universally verified if each person can do it independently.

Make sure all ballots are counted correctly. The voting system can be individually verified (weakly defined) if each voter can independently verify that his ballot was counted correctly [5]. Before explaining the proposed voting scheme and how it attempts to meet the above security requirements, I will briefly introduce the main types of voting protocols described in the literature.

I.3. Synthesis and critiques of electronic voting protocols

Early electronic voting records did not use encryption technology. These protocols are usually based on two electoral authorities. One is responsible for authenticating registered voters and the other is responsible for collecting ballots and counting results. Despite their simplicity, these protocols have major drawbacks. In fact, they do not meet most of the above characteristics.

As a result, a protocol using an encryption mechanism was proposed. The latter introduces encryption to ensure the confidentiality of the vote and a digital signature to ensure that the voter is authenticated, thus ensuring that the voter cannot vote more than once. To ensure voter anonymity, some of these protocols rely on using two permissions to separate the two tasks of voter authentication and ballot counting. However, anonymity issues are constantly occurring because of the risk of two authorities colluding to determine who voted for [6].

I.4.Electronic voting in five steps:

I.4.1. Use the data to register with the system

Access to the online voting system is obtained by entering two access data: an employee ID and a **one-time-valid password.**

I.4.2. Confirmation of registration:

Anonymization voting system checks if the data is available in List of voters. Only if the data is available in you can use the list to access the system. At this point, the internal system will generate a token (voting key) that will allow you to vote. This prevents voters from being tracked for voting and guarantees the confidentiality of ballots.

I.4.3. Online electronic voting:

How to express your preference the ballot is displayed and you can express your preference. You can choose them.

. Cancel your vote with your favorite list or candidate, or with just one click.

I.4.4. Confirm your selection:

After clicking your preference on the ballot, you can double-check your ballot to confirm your selection before sending it to the digital ballot box.

I.4.5. vote registered:

Finally, the vote is finally registered and the token is removed from the system only when you log out. Thus, a ballot without l Ability to edit it.

I.5. Internet voting:

The online voting system is a software platform that allows groups to vote and vote safely. A high-quality online voting system balances voting security, accessibility, and general requirements for an organization's voting event.

Basically, the online voting system protects the integrity of the vote by preventing voters from voting multiple times. As a digital platform, it eliminates the need for direct collection, paper voting, or other means (email, insecure research software, etc.).

You may hear an online voting system called an online voting system, an electronic online voting system, or an electronic voting system. This is all the same. A safe vote tool to collect comments from the group to the group and check the real-time results correctly.

Continue reading to access the most complete introduction of online voting systems. Good Internet Voting Systems need to ensure some essential properties that define requirements.

If polling contains a long shift, online voting may have advantages such as survey adjustment. Therefore, the adjustment of people living abroad is traditionally embassy, sometimes far away. This is a few countries like Australia, and it is in spacious. Online voting also allows you to consult with voters more often. This is one of the reasons Switzerland wants to expand electronic voting. However, it is clear that online voting poses potential security issues. This is for three main reasons. Voters, on the other hand, no longer had a polling place with a polling place. Therefore, it is difficult to verify the identity of a voter and ensure that this person is free to vote without restrictions. Meanwhile, computers use many malware that can not be controlled. Finally, voters do not control the selected voting method, and there is no opportunity to ensure that voters are not manipulated by a malicious actor or by election authority. Of these observations.

I.5.1. Internet voting properties:

Two types of security elements that are essential for voting are anonymity and validity.

Anonymity: Most elections require anonymity to vote. This means that it should not be possible to know how a particular voter voted, unless disclosed by the results (for example, if the vote is unanimous). Anonymity alone may not be enough, depending on what is at stake in the election. It is also important that the protocol resists coercion to avoid coercion and voting purchases. It must be impossible to record information that could convince a third party of the value of the vote.

Guarantee of Correction: Of course, it is imperative that the published results correspond to voters' voting intent. For traditional surveys, the observer can comply with the voters themselves, and to ensure their enthusiasm and their credibility, it is the honestness of the vote. In online voting, make sure that the results are correct. For example, how do you know that the program that runs on the Kurfürster PC is correct? The system may be an error victim or a different program may be running for bulky viruses and software.

So make sure that the volume saved on the election server is not forged. Furthermore, higher verification fluctuation characteristics are desirable: The protocol must provide mathematical evidence for the validity of the result. This eleger needs to be able to see if his newsletter is on the ballot paper. This is called the possibility of individual reviews. On the other hand, complete verification potential ensures that the result of the election was properly calculated by the individual votes in a manner that each observer can confirm. Finally, it is essential to ensure that the newspaper comes only from the legitimate voter. Then we talk about the possibility of confirming approval. These opinions are irrelevant to the software used for adjustment and planning. Therefore, it allows problems with bugs and malware.

Safe Electronic Voting System Development is a sensitive process. In particular, verification and forced resistance are antagonistic properties. A certain sound must be recorded in the score and that it does not show one third to sound. Protocols created to meet these two functions with great use of encryption are some protocols. Thus, the system needs to implement one of the only protocols for both checks and resistors. However, implementation is complicated. Verification and anonymity system must also be included. And ease of use.

I.6. Defrence between electronic and internet voting (Advantages / Disadvantage):

Can facilitate voting, whether your personal or public access can be accessible to 24/24 hours voters from smartphones, tablets and browsers from computers (POST,) Town Hall And so on, a significant reduction in voting costs is voted on the Internet, but the voting machine's electronic vote is available from the election station at a specific time.One percentage of cost.

An electronic vote that realizes the security of the electronic voting causes the system to be developed for the public and civil collaboration, specialized order, political parties, and domestic legal elections, and also in some National Arbitral Elections, The system can secure each person's confidentiality and sincerity. Trusting the sincerity of the vote, electronic voting has maintained a lot of sensitive points of our fellow to ensure that the election vote could be reviewed in the election.Therefore, the only online vote solution that integrates the possibility of checking the vote.

Votes are also widely developed in public and private agencies, specialized foundations, political parties, political parties, and legal elections of a particular state, but the conflict of voting integrity is a lot of sensitive points of our national brother.

Online tuning allows you to check your voter's vote.

Currently, electronic voting on voting machines (censored voting machines) is a far superior guarantee than the confidentiality and transparency of all electronic voting solutions. Online voting also raises new technical challenges from a security perspective, but solution suggestions are complex and accessible only to experts in this area. It seems impossible to achieve the simplicity of voting on a voting machine. For all these reasons, it seems premature to rely on online voting for high stakes and important political elections, even for the safest and auditable systems required by verification mechanisms. On the other hand, it's not easy to believe that online voting is more dangerous than other popular voting systems. Online voting is often used in place of electronic voting, which has many weaknesses. Unlike voting at polling stations, few people can see a mail ballot. Voters need to be completely confident in the election organizers. In addition to electronic voting, it can be sensitive to ballot boxes, as indicated by certain attacks [7].

-**W**e have summarized the difference in some points in the following table:

	Electronic voting	Online voting
Advantages	(+) The system Can Secure Confidentiality and honesty	(+) The possibility of voting remotely and from anywhere, as it is available for 24/24 hours of smartphones, browsers, etc,..
	(+) vote can be reviewed in the elections	(+) Not consuming time and workload
	(+) The Most Secure and auditable systems that verification mechanisms require	(+) It greatly reduces the costs and facilitation of voting as it is more convenient
	(+) is a much higher guarantee than the confidentiality and transparency of all electronic voting solutions.	(+) the only solution that integrates the possibility of voting verification. Votes are also widely developed.,
	(+) Provides high level of security, authentication, reliability	(+) allows you to check your voter's vote.
Disadvantages	(-) Voters must go to a polling station at a specific time	(-) complexity security issues
	(-) Time Consuming and work load	(-) The most dangerous involves many attacks and weaknesses
	(-) It is less suitable and more expensive	(-) Its opaque character cannot be verified.

Table I.1: *Defrence between electronic and internet voting.*

I.7. Types of voting systems

Today, there are numerous possible voting systems around the world, some of which are currently in use, while others are purely theoretical.

These different systems can be divided into three "family". A semi-proportional system and a proportional majority system. Voting systems within a particular "family" tend to produce similar results and are similar in pros and cons. Therefore, the main difference is not within the family, but between the families. The following links give you access to a description of these three "family" of voting systems, including sample ballots.

I.7.1. Majority System:

The win-win system is widespread. These include common multiple systems such as winner general elections and general districts, as well as less common majority voting systems.

I.7.2. Proportional Electoral System:

These electoral systems are used in most other advanced western democracies so that political parties are proportionally represented (based on vote rate) in parliamentary parliament. Is designed for. These include party-list proportional systems, mixed-member proportional voting, and individual transferable voting.

I.7.3. Semi-proportional systems:

These systems are used in some local elections. They tend to produce results that are more proportional than the majority system, but less proportional than the fully proportional system. These include cumulative voting and limited voting.

I.8. Diagram of the voting process:

The voting protocol envisioned in the previous section forms the platform on which the vote architecture is built. The following describes the voting scheme by detailing the exchange of messages between the different authorities involved in the different phases of the voting process.

I.8.1. Voter registration phase:

This phase consists of editing and viewing a list of voters who wish to participate in the organized voting process prior to the actual voting process. To do this, the organization outsourced to this task must first have a list of people allowed to register. There are two reasons to introduce this step into your voting system:

1. There is no need to contact in advance (as part of the voting operation) between the voter and the voting organization to improve the agility of the system. Therefore, at this stage, you need to provide voter authentication using information obtained from voters, such as: Resident registration number and password. This information may be disclosed when a voter becomes a member of the organization that organizes the vote. For example, company members can: After joining the company, you will receive it by email.

2. The registration step also allows you to know the number of voters who have abstained, reducing the chances of a registration authority sending fraudulent votes on their behalf.

The main issue that arises during this phase is how to authenticate eligible persons on the list. To provide this critical service, we chose the challenge-response authentication mechanism for the following reasons: ChallengeResponse is an authentication mechanism based on the use of a strong password mechanism.

The key-based signing mechanism cannot be used because these keys cannot be used before the tuning process is organized. ChallengeResponse handles large-scale attacks that can occur during an authentication session, especially replay attacks [8], with minimal limits (such as synchronization) and an acceptable level of complexity and implementability. ..

To complete the registration procedure, each authenticated voter uses a password and identification number to generate a private / public key pair and sends the public key to the registration authority for the next phase. Used to verify the signature during registration vote.

I.8.2. Voting phase:

This phase includes two essential steps:

I.8.2.1. Ballot Verification Procedure

This includes symmetric encryption, hashing, masking, and ballot signatures, and sends the vote to the agency responsible for verification (blind signature).
This will return the confirmed vote to the voter. A message is displayed.

I.8.2.2. Collection phase during this voter phase

Starts removing masking elements from approved ballots. This vote must be sent to the aggregator. The aggregator must check for validity and integrity before decrypting using the voter's private key received over a secure channel.

I.8.3. Count Phase:

This is the final step in the voting process, where the vote is decrypted and stored in a dedicated database using the appropriate decryption key.

I.9. Implementation

To implement the above scheme, we used a Java development environment that provides a solution that allows you to embed an executable program in a web page. These programs, called applets, are used by the system to ensure voter registration, mail-in ballots, and results are obtained, and can run without compromising the security of the client's system, In addition, applets can connect to the server and make remote procedure calls [9].

I.9.1. Voting system module

Internet voting uses four modules (ACL, ACD), each representing a voter, one module representing an election organizer, performing election processes, automating registration procedures, and running ballots Generated.

I.9.1.1. Organizer module

The Organizer module is called from the Voting Task Manager. In the latter case, you will be prompted to enter a password to be able to run it.

In addition to the voter registration phase, the Organizer module is responsible for the preparation required for voting. His role can basically be summarized as follows.

Ballot Creation: Using HTML as the creation language, ballot managers define the ballot model used during elections. This model depends on the details of each voting process, including: Its nature (elections, referendums, etc.), the number of options proposed for voting, etc…

The Organizer module is also used to create a population list and trigger and stop various phases of organized elections.

I.9.1.2. LCD module

The ACL module is responsible for completing the validation phase and validates only one of them.votes are checked for each registered voter.

I.9.1.3. ACD module

The ACD module is responsible for collecting ballots and counting results. And its publications.

I.9.1.4. Voting module

This module acts like a voting agent. He needs to be able to:

- Capture voters' votes.
- Performs all cryptographic operations that voters need to perform.
- Get and get the required validation and receipt confirmation.
- Delivery of ballots to various authorities (ACL, ACD).
- Check the election results and protest if you make a mistake.

I.10. Conclusion

This chapter present the Electronic and the Internet voting, Recall the definitions and attributes, give an overview and review of the electronic voting protocol, and then submit the electronic ballot. Focus on the type of voting system in the implemented voting system.

The following chapters provide a description of the existing operating system in your company's Customer Service Center "Voting System: From Electronic Voting to Internet Voting".

Then, we conducted an investigation at the operational level of the existing system and analyzed the progress of the agent's work. This allows us to propose a fully computerized solution for improving quality of service. Designing a voting system to find the is a very important step in setting up your application. It cites the UML model, various use case diagrams and class diagrams, and sequences.
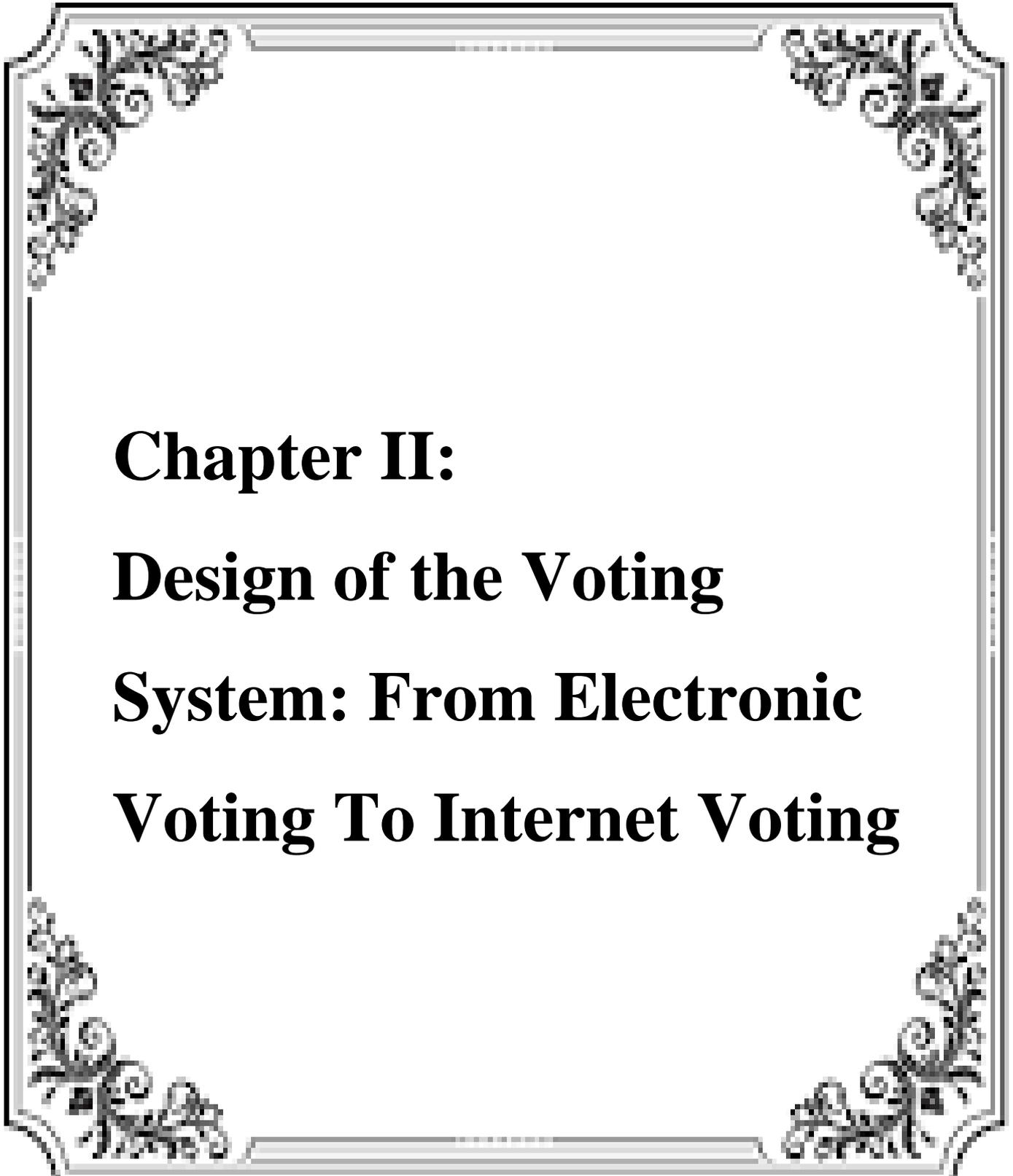
Chapter II:

Design of the Voting System: From Electronic Voting To Internet Voting

II.1.Introduction:

The development of any information system requires a very important step in the life cycle of software, and modeling in practice is important in software development, in our project we choose the UML modeling language which we will exhibit,

In this chapter we propose the most important design diagrams, see how they are used in the modeling of an IS (information system), throughout this chapter UML diagrams facilitating the study of processes from different perspectives:

- ➤ A use case diagram is used to analyze and organize the needs and behavior of a System.
- ➤ A UML class diagram to define the order of execution of the different services in order to achieve a business objective.
- ➤ A sequence diagram makes it possible to represent the interactions between objects according to a temporal point of view.

II.2. General

This guide is available on the website of the services of the representative of the State as well as on the website of the Ministry of the Interior: www.interieur.gouv.fr. Unless otherwise specified, the articles cited are those of the electoral code in their version applicable to the general renewal of the municipal councils of March 2020.

II.3. Provisions relating to the preparation of municipal electoral operations

II.3.1 Election Candidates: What Candidates Should Know?

II.3.1.1. Eligibility criteria

Candidates for local or state people's conferences must meet the following conditions:

Item No. 01: Participate in the electoral rolls he runs.

Item No. 02: He must enjoy his civil and political rights and does not exist in any of the disqualifications established by current law.

Item No. 03: Must be at least 23 years old on Election Day.

Item No. 04: Have Algerian citizenship,

Item No. 05: Prove that he has completed or is exempt from military service,

Item No. 06: He should not have been convicted of a felony or detention crime and was not considered rehabilitated except for an unintended crime.

II.3.2 Election List

II.3.2.1. Conditions for registration in the electoral list

Item No. 53: Under the responsibility of an independent body, create and manage a national electoral list consisting of all local voter lists and foreign diplomatic and consular missions in accordance with the law in force.Increase.

Independent agencies regularly check the electoral rolls and confirm in each election consultation or referendum, in accordance with applicable law. The conditions for maintaining a national electoral list and its use are determined by the decision of the president of an independent body.

Item No. 54: Registration on the Electoral Roll is mandatory for all citizens who meet the statutory requirements.

Item No. 55: All Algerian men and women who enjoy civil and political rights and have never been on the electoral list are required to apply for registration.

Item No. 56: No one can participate in multiple electoral rolls.

ItemNo.56: Notwithstanding the provisions of Articles 55 and 56 of this Basic Law, Algerians residing abroad and registered with Algerian diplomacy and consulates may apply for registration:

1- Regarding the electoral list of one of the following commune in connection with the elections of the Joint People's Assembly and the Wilayah People's Assembly:

- A commune for the birth of stakeholders.

- The commune of the person's last place of residence.

- The birthplace of one of the person's ancestors.

2- Electoral rolls of Algerian diplomacy and consulates in the country of residence of voters for presidential elections, parliamentary elections, referendum consultations.

ItemNo.59 : Toute personne ayant recouvré sa capacité électorale à la suite d`une réhabilitation, d`une levée d`interdiction ou d`internement ou d`une mesure d`amnistie, est inscrite sur la liste électorale, conformément aux dispositions de la présente loi organique.

ItemNo. 60: During a change of residence, the voter registered on an electoral list must request, within three (3) months following this change, his deletion from this list and his registration on the list of his new commune of residence.

II.3.3. Elector:

II.3.3.1. Qualifications required to become a voter:

Item No 50: All Algerian men and women who are 18 years old on the day of the election are voters who enjoy civil and political rights, as stipulated by the laws in force, and the electoral list

Item NO 51: Within the meaning of Article 36 of the Civil Code, no one can vote if they are not on the electoral list in which they live.

Item NO 52: Anyone:

- Engaged in actions against the interests of the motherland during the National Liberation Revolution.
- Convicted of a crime and not rehabilitated.
- He was sentenced to imprisonment for the period specified by the application of violations of Articles 9 to 1 and 14 of the Penal Code, with the prohibition of voting and candidacy.
- It has been declared bankrupt and has not been rehabilitated.
- A judicial detainee or detainee. The Prosecutor's Office will also notify the City Commission of legally validating the electoral rolls and will send a list of the persons mentioned in Section 2 as soon as the electoral roll verification period begins. And. 3, 4, 5 above.

II.4 Election Organizing:

Electronic and Internet Voting systems consist of two main components.

1. A voter registration system owned and operated by the Election Commission and hosted by a third party provider.

2. Internet voting system itself. This includes the voting platform and voting verification platform, which will be deployed to servers from other providers.

Registration. Because the use of Internet Voting is restricted to a relatively small population (hundreds of thousands based on certain conditions), voters wishing to vote by Internet Voting Should apply to the Election Commission for registration.

Must be submitted. With this registration, voters will also choose the password (or PIN code) used to identify them. Once the voter's registration is approved, the voter will receive a voting ID ("Vote number via the Internet"). This ID can be sent by the Election Commission through various channels such as SMS, email, mail and phone. The voter ID and voter password are also used to protect the signing key that voters use to sign ballots.

Preparing for electronic voting. Before the election begins, the election office is stored on a

smart card and generates a set of keys to ensure the confidentiality of the vote. Ballots are also defined in the form of voting files.

The voters whose registration has been confirmed can vote through the election website. Authenticate yourself using the username and password generated during registration, make sure you haven't voted else where, and use the key that corresponds to the private key generated and signed by the election office. And publish the encrypted vote. Voters then receive a receipt from the ballot and the QR code used on the ballot.

II.5. Needs specifications and analysis

II.5.1. Requirement Specification

In this part, it is necessary to divide the context of the subject by conducting functional research of future systems. Therefore, it is important to show all the actors acting in our system and identify specific use cases.

II.5.1.1. Actor identification

Actors are prototypes of users (people, external processes, etc.) that interact with the system. By default, this is the main actor. H. It acts directly on the system and expects results from it, or it can be a secondary actor who often seeks additional information. In our case, the table below shows all the actors that act on the system.

Actors	Descriptions	Roles
Administrator	He can be the HRD or any other qualified person	He manages the administration part of the platform
Supervisor	The supervisor is part of the electoral commission, depending on the type of election. Municipal elections	He oversees the election. He starts and finishes submitting candidates. Publish a list of candidates and a report on voting results. He can configure elections, but he can also send notices about specific elections.
candidate	For each type of election, or specific type of candidate.	He can modify his information or withdraw his candidacy.
Elector	Voters can be members	He can submit his candidacy for a given election; he can also vote for the candidate of his choice

Table II. 1: Identification of Actors.

II.5.1.2. Feature Identification

Features are actions or services that the system can provide at the request of the actors involved. These services can be external (requires actors) or internal (that is, internal). He it

doesn't show up, but it works internally when a particular process is started. In our research, we were able to list some of the features that can perform the process of organizing and coordinating in our system. The following table shows the scope of functionality.

Actor(s)	Features
Admin,Candidate, Elector, Supervisor	- Authenticate
Admin	- Create an election and election-related positions - Manage users (add, edit, delete) - Assign an election to a supervisor - Manage Municipal and services
Supervisor	- Publish information note on the opening of the ballot by e-mail - See the list of candidates registered for an election - See the list of voters for an election - View the progress of the vote (view electors voting and electors not voting) and the provisional results. - Publish the results with printing of the minutes
Elector	- Apply
Candidate	- Modify your information - Withdraw his application
Elector, Candidate	- Cast a vote
Supervisor	- Open an election - Validate an application - With draw a candidate

Table II. 2*: Feature identification*

II.5.2. Needs Analysis:

The purpose of the analysis is to understand the needs and requirements of supervisors and e-learning development. Analyze business needs and workplaces and create specifications for designing solutions.

II.5.2.1. Analysis of functional requirements:

The functionality of the client is described in detail by the product structure. That we worked. Functional needs are expressed as we've covered the details in the project management part of the user story, the graceful Scrum methodology material used to manage projects, this methodology, and the usage report for product builds.

The following functional requirements describe which different representatives interact with the application and why. We have identified three types of application users. Public users represent the concept of user abstraction with general needs, voice, and voting behavior. They are important users who have the same needs as public users, but also have specific needs. For example, an officer may want to be able to handle votes and votes.

You can vote. In this way, we analyzed and identified the functional requirements of the user story that represent the enhancement.

Determine who the requester is, what the request is, and what the purpose of the request is. Therefore, we propose career needs as follows. Therefore, it presents functional needs as follows:

II.5.2.2. Analysis of non-functional requirements:

Non-functional requirements refer to the needs of the development team to design and build applications. We also used the same formula to define our functional needs.

Helps define non-functional needs called technical stories within the framework of the SCRUM approach. It does not represent a functional increment of the customer, but it is necessary to meet the customer's needs and in this case run the project. For example, we implemented the public key cryptosystem described in the technical report section to ensure voting confidentiality standards. Previously, to implement this technique, you had to develop a method that used modular arithmetic. If you want to use the voting app, you need 3 actors.

First, an administrator who can't vote and manages both the voter and the voter.

Next, a few voters on behalf of the customer.

Finally, the actions that can be performed by the latter two are performed by the General user, Learn more about the various actions these actors can perform:

Administrator:

➤ Manage Voters: Delete or create new voters and update the database.

➤ Calculate Results: Closes the vote and allows voters to view the results.

➤ Referendum Reset: You can reset the votes of all voters and create a new ballot. Voter:

➤ Voting: Voters choose from two answers. Often "yes" or "no". (1 or 0 in our case) Answer the survey questions. This vote   It is then encrypted on the client side and stored in the database as follows Waiting for the result to be calculated.

User:

➤ Show encrypted voice: Shows how the application works also, to ensure reliability, users can see how the vote was recorded in the database.

➤ View result: The final result will be decrypted. After this action voters have access to election results.

➤ Connection: Allows users to send their identifiers for access go to different features of the application, depending on the role of voter or administrator.

➤ Check Connection: The protocol run by the server to check the connection check voter credentials or admin credentials. As you can see in the attachment, there is a final use case diagram slightly modified compared to the original prototype. Changes were made during the project.

➤ Initially, the administrator was also a voter, but to separate it A role determined for a single administrator with a specific task.

➤ I also considered creating statistics and graphs for explanation various aspects of tuning, over time we I realized that this wasn't the focus of the project, so I decided not to implement such a feature.

➤ Finally, I wanted to allow voters to change their address. Emails or their passwords, but after some consideration, it made little sense to focus on them.

II.6. UML Modeling:

UML is an abbreviation for "Unified Modeling Language" and is a unified language for modeling. UML is a set of tools to support modeling future computing applications. UML is a graphical way to create object-oriented models for the design and modeling of object-oriented software.

II.6.1. Use Case Diagram

Allows users to express the functionality they need. You can create use case diagrams for the entire software or for each package. This figure clarifies how external users (actors) interact with these use cases [10].

II.6.1.1. Use case diagram of the "Administrator, Elector, Voting candidate" case:

The following figure represents use case diagram Elector and condidat:
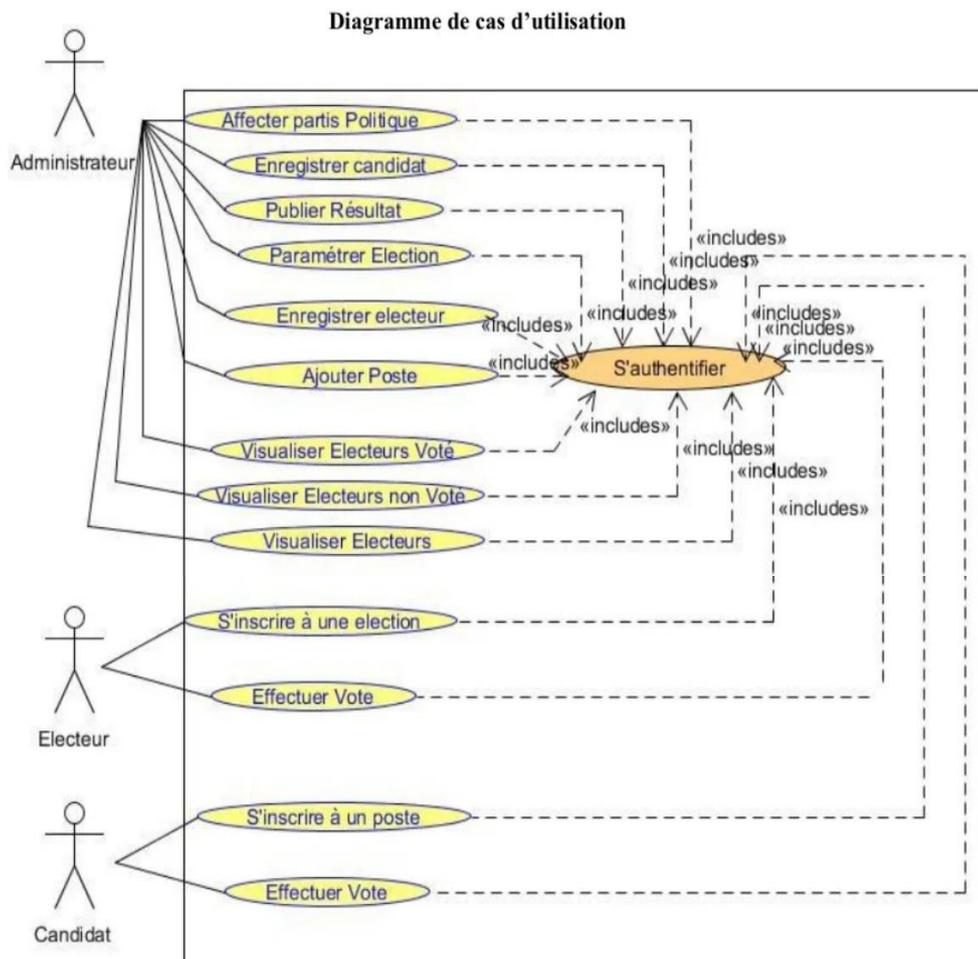
Figure II. 1 Represent Use case diagram of the "Elector and candidate Vating"
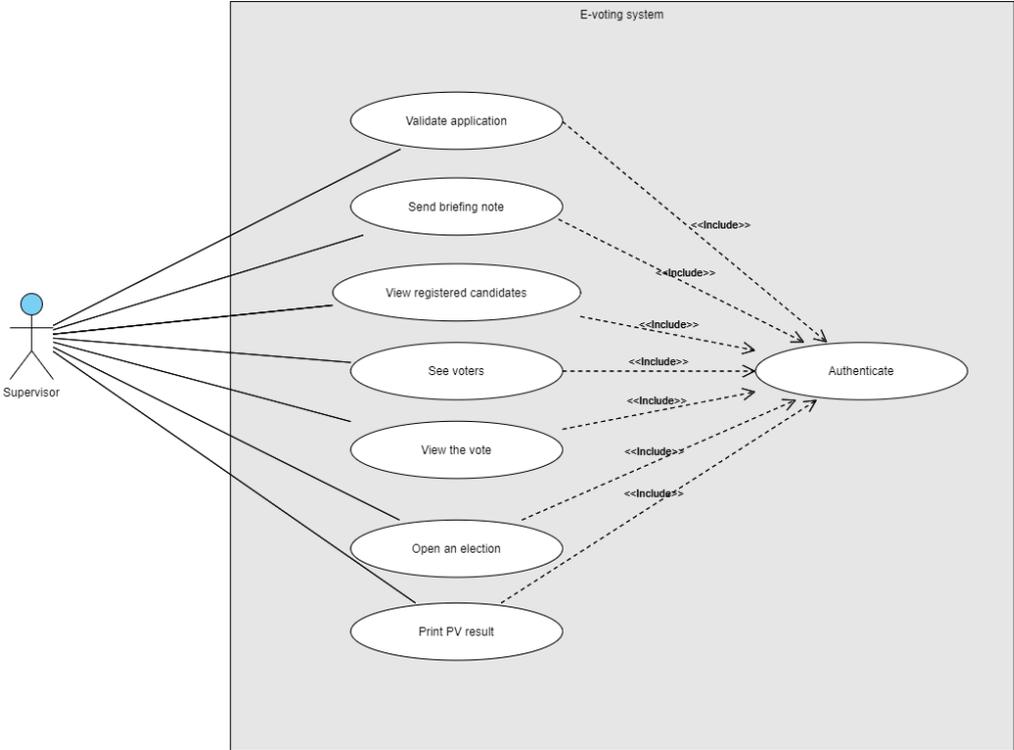
Figure II. 2: Represent Use case diagram of the "Supervisor Voting"

II.6.1.2. Use case diagram of the "Vote registration" case:
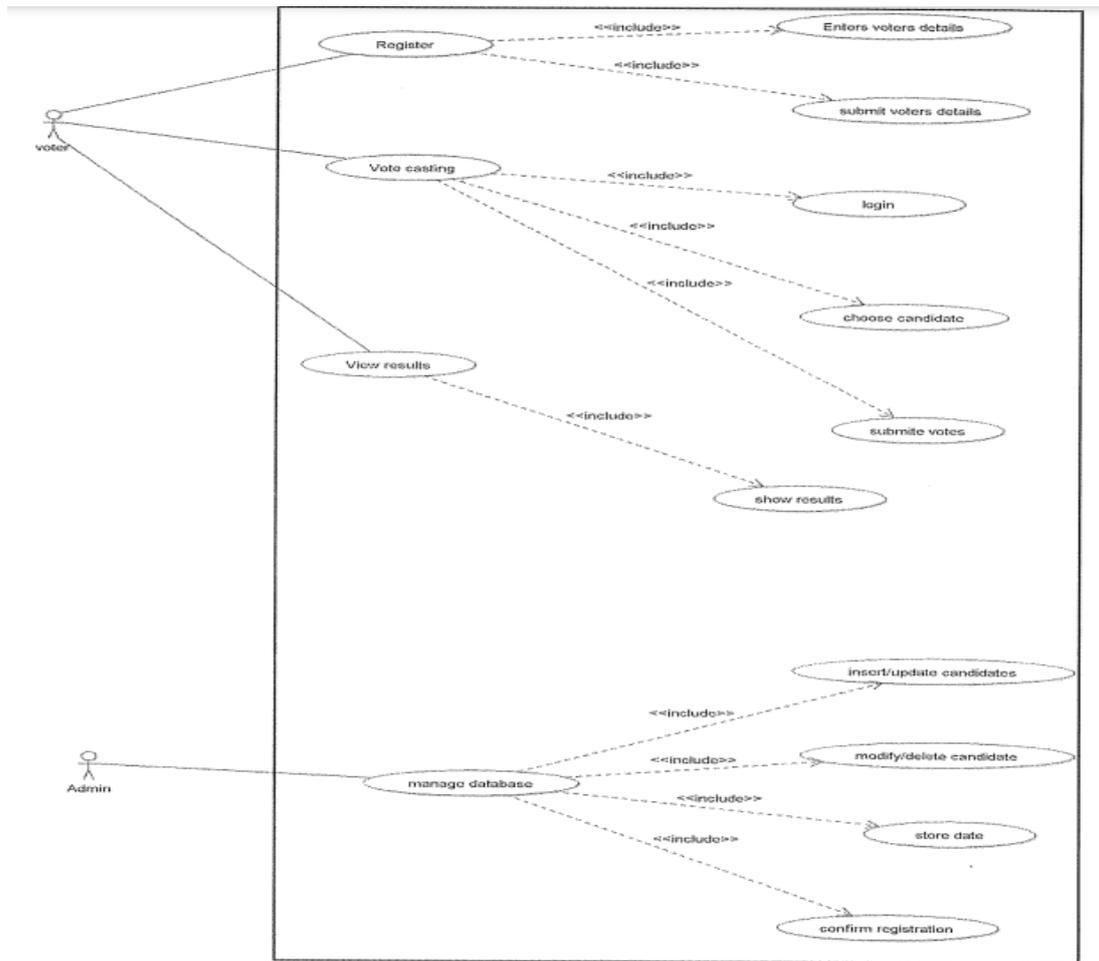
Figure II. 3: Represent Use case diagram of the "registration Voting Systems"

II.6.2. Entity-Relationship Diagram:

Entity relationship diagrams (ERD) are used in software engineering during the planning stages of a software project. They help define the different elements of the system and their relationships with each other. It is often used as the basis for data flow diagrams, or DFDs as they are commonly known.

Or as it can be said that it is a visual representation of the different entities within the system and how they are related to each other.

Here is the ER diagram that represents the voting system we have relied on:

Figure II. 4: Represent ER diagram of the "Voting Systems"

II.6.3. Class diagram

The class diagram represents a user-controlled entity. This is the focus of object-oriented development and is the most commonly used diagram.

Represents the relationship between the type of object and aux [11].

II.6.3. 1.Voting class diagram of the "voting systems" case:
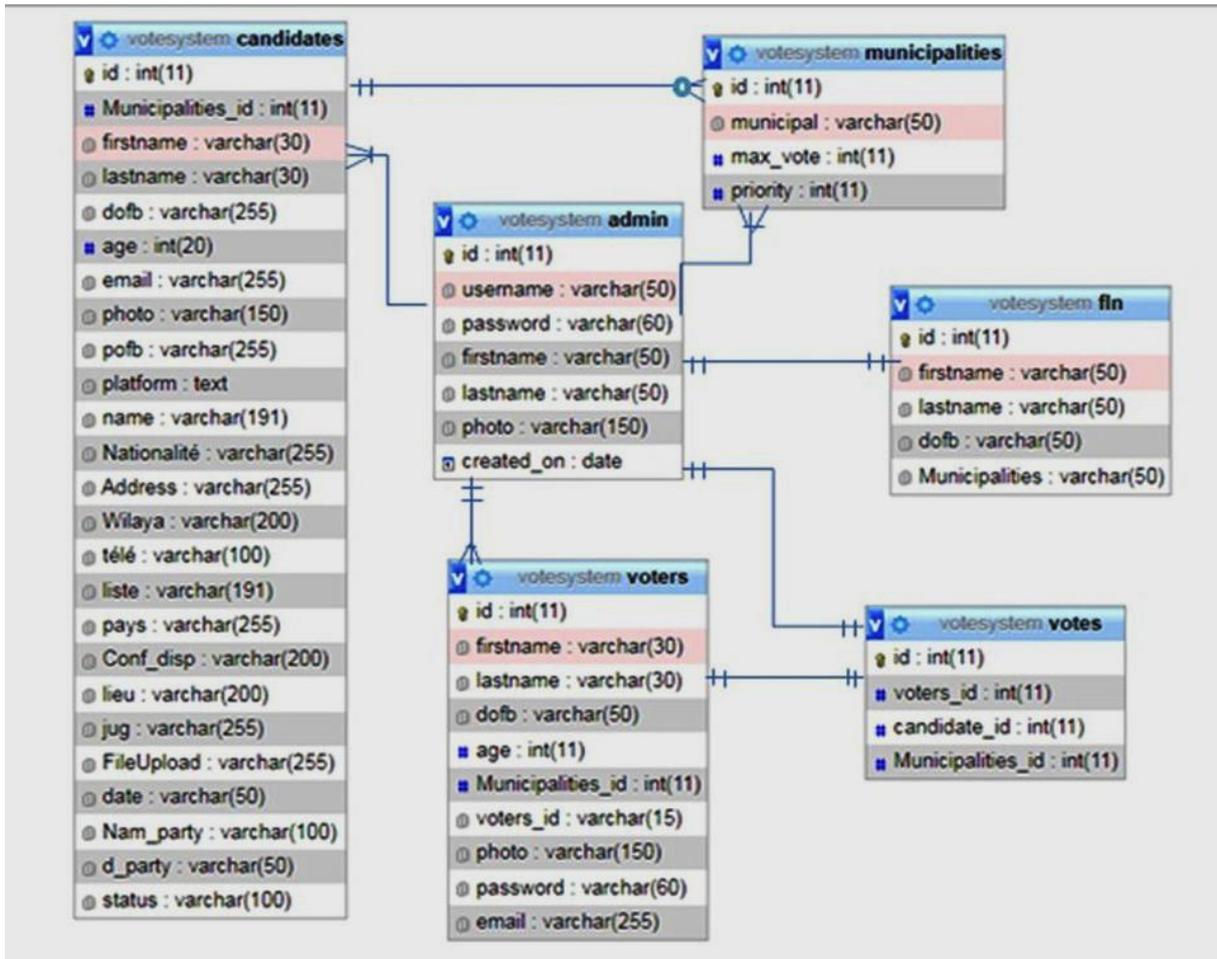
Figure II. 5: Represent class diagram of the "Voting Systems"

II.6.4. Sequence Diagram

Allows you to explain the interactions between objects in your system on a schedule. This interaction occurs by sending a message that calls the method (synchronous or asynchronous message).

II.6.4.1.Sequence diagram of the "vote" case:
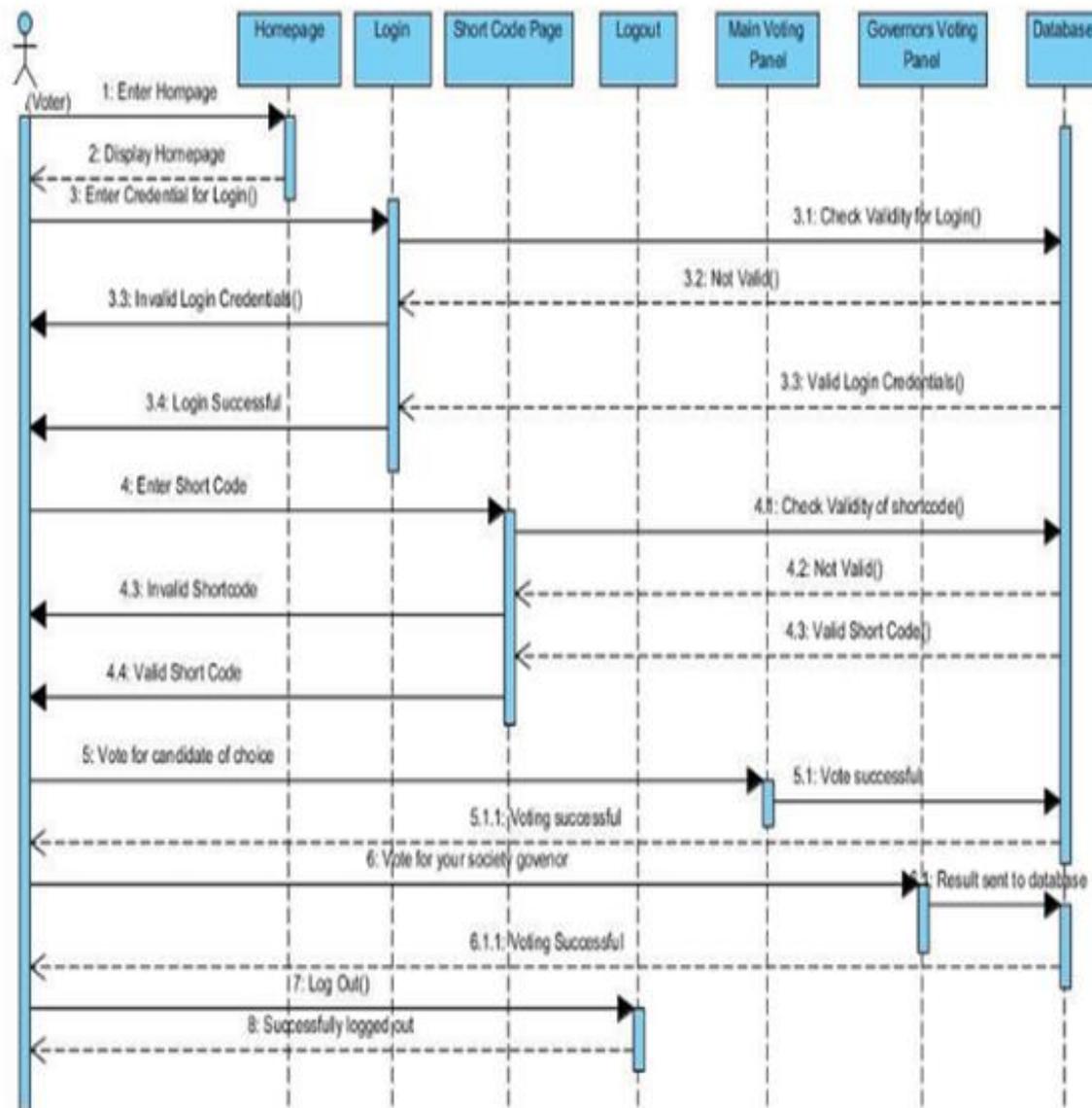
Figure II. 6: Represent Sequence diagram of the "Vote"

II.6.4.2.Sequence diagram of the "Elector to Vote" case:
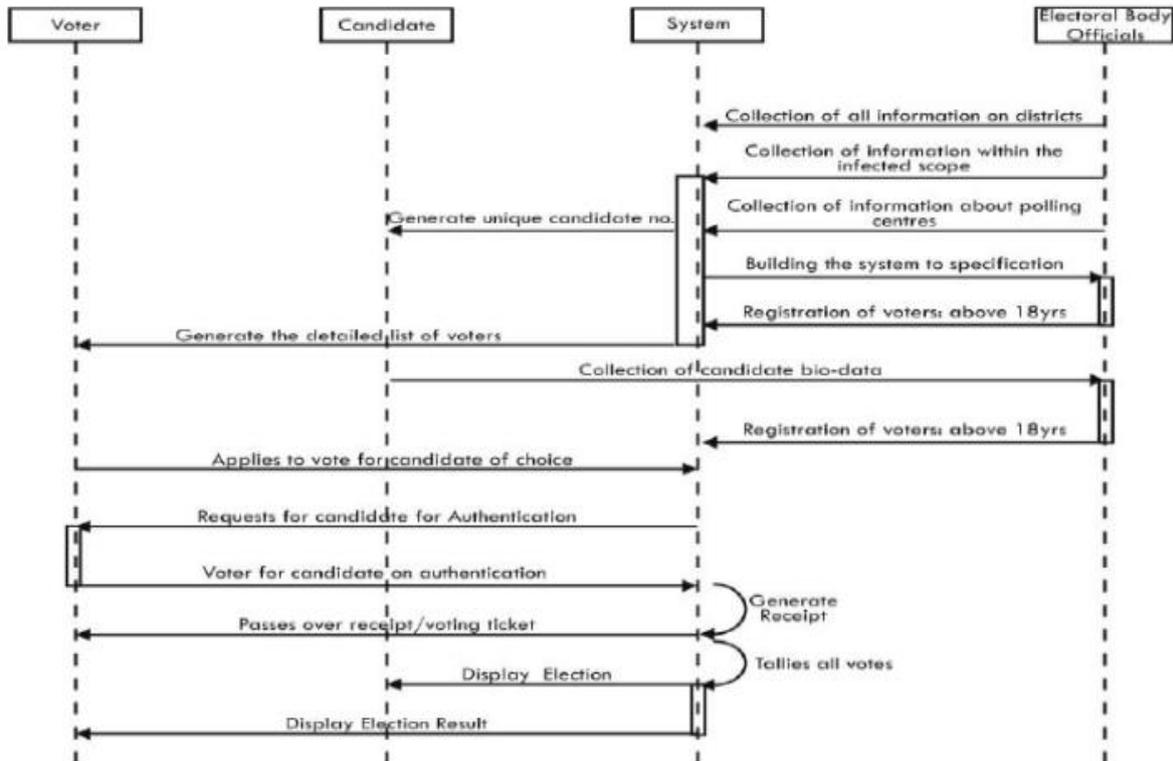
Figure II. 7: Represent Sequence diagramof the "Elector Vating"

II.6.4.3.Sequence diagram of the "candidacy" case:
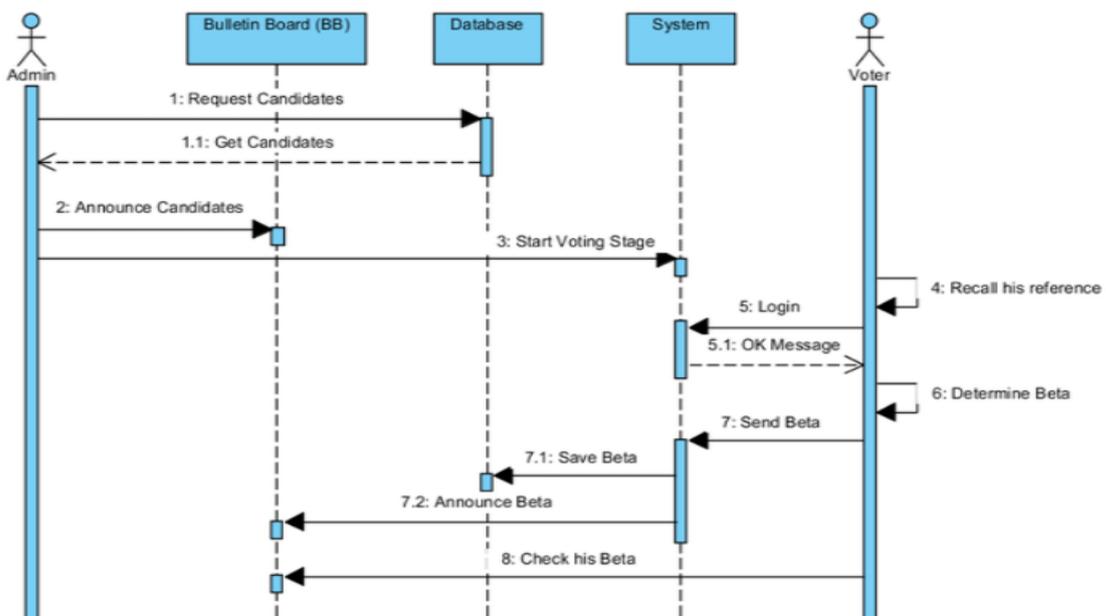
Figure II. 8: Represent Sequence diagram of the "Candidacy Vating"

II.7. Conclusion

In this chapter, we reviewed surveys at the level of existing operations at the core of needs analysis and specifications, and customer service, as well as the in-house 4334 agent Voting System: Electronic Voting Internet Voting. When implemented, it reveals some performance issues and finds an acceptable solution to the functional requirements of the new system.

Therefore, this design for UML modeling of voting systems. Various diagrams are shown, including use case diagrams and class and sequence diagrams.

The next chapter will show us how to do this and shows a clearer picture of our application by displaying screenshots of the main page of it, in addition to the application development tools.
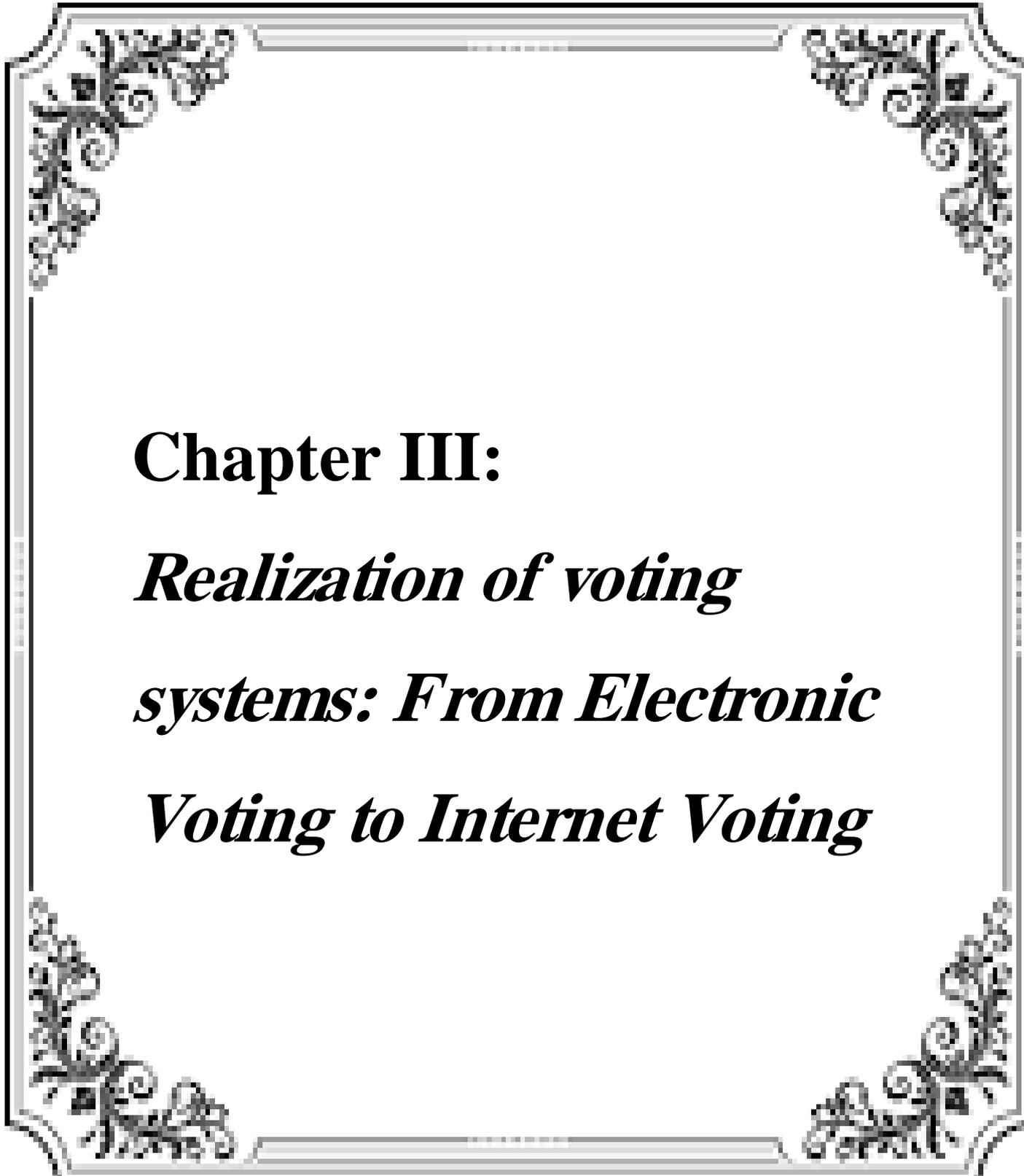
Chapter III:

Realization of voting systems: From Electronic Voting to Internet Voting

III.1.Introduction

After having presented, the general concepts of Image Processing and Digital image and the techniques of Deep Learning and search image, this chapter is devoted to present the tools and libraries used in our experiments and a humble discussion about the results.

III.2. Development environment:

In this part, we will introduce the various programming software, programming languages and image processing software that we use for the operating system

III.2.1.Operating system:

The basic environment for this work is Windows 7 operating system, to achieve performance in a simpler way, it is machine dependent. Windows 7 ensures more efficient work, ensuring reliability and efficiency. - In this part we give some definitions of programming languages

III.2.1.1. PHP (Hypertext Preprocessor):

Better known as PHP, it is a WEB programming language primarily used to create dynamic web pages (client/server) through HTTP servers such as Apache. PHP is sometimes referred to as a platform rather than a simple language. PHP code is called a "script" and is contained within HTML code. Example (script):

Official website: https://www.php.net/

III.2.1.2. HTML (HyperText Markup Language)

It is a beacon language that allows coding of web pages. HTML can also semantically structure and format website surfaces for the integration of multimedia resources such as images, input forms, and computer programs. It supports the creation of documents that are interoperable with various devices and meet web accessibility requirements. It is often used in conjunction with programming languages and presentation formats (Cascading Style Sheets). HTML was originally derived from Standard Generalized Markup Language (SGML)

Official website: https://developer.mozilla.org/fr/docs/Web/HTML

III.2.1.3. JavaScript

JavaScript is a pc language used on web pages.This language has the particularity of being activated on the client computer, in different words it's far your computer so that it will get hold of the code and with the intention to need to execute it. This is in evaluation to other languages which can be server-side enabled. The execution of the code is performed via your net browser inclusive of firefox or google chrome.

Official website: https://developer.mozilla.org/fr/docs/Web/JavaScript

III.2.1.4. CSS

CSS stands for Cascading Style Sheet, is a design language Simple intended to simplify the method of providing net pages , consequently used on the Internet to format HTML or XML documents, So this code to manipulate the designates of an internet page.

Official website: https://www.w3schools.com/css/

III.2.2. Development tools:
III.2.2.1. XAMPP:

XAMPP stands for Cross-Platform (X), Apache (A), MySQL (M), PHP (P) and Perl (P).A web server and an FTP server. It is a distribution ofUnfastened software program (X Apache MySQL Perl PHP) clean to put in offering an excellent flexibility of use permit the exploitation of an Apache server, the MySQL DBMS and the PHP interpreter. XAMPP is likewise cross-platform, meaning it works equally well on Linux, Mac, and Windows.

Official website: https://www.apachefriends.org/fr/index.html

III.2.2.2. Apache server:

Apache is loose and open-source net server software that Powers approximately forty six% of websites international. The name Official is Apache HTTP Server and it is maintained and advanced by means of Apache Software Foundation. Specially used on Internet website hosting in Linux, Despite the fact that it's also usable in Windows.

Official website: https://www.hostinger.fr/tutoriels/quest-ce-quapache-serveur-web-apache

III.2.2.3. MySQL :

Is a database control device (DBMS). As Open Source Relational Database Server, Based On Structured Query Language (SQL). Also MySQL is the maximum often associated with net-based applications

Official website: https://www.mysql.com/fr/

III.2.2.4. Bootstrap :

Is a set of equipment useful for creating the design (portraits, animation and interactions with the page inside the browser, and so forth.) of net websites and applications. It is a fixed that consists of HTML and CSS codes, forms, buttons, navigation gear and different interactive elements, as well as non-compulsory JavaScript extensions. It is one of the most popular projects on the GitHub development control platform.

Official website: https://getbootstrap.com/

III.2.2.5. A Visual Studio Code editor:

Lighting fast, unfastened, and extensible code editor from Microsoft, based totally on open supply, that runs on Windows, macOS, and Linux. Built-in rich language assist for web development: HTML, JavaScript, TypeScript, CSS, SCSS, Less, Markdown, and so on. Out of the field support for multicursor, Emmet, split view, formatting, code folding, and plenty of greater code enhancing functions.

Rich atmosphere of extensions for all principal languages, network themes, services, and Functions.

Official website: https://code.visualstudio.com/migrate-from-brackets/

III.2.2.6. HTML Sublime editor:

Is a helper software for growing and designing HTML pages.

In Our case we used a function-wealthy editor
Many specialists use this editor to
All programming languages. It is the editor
"Sublime Text".

Official website: https://www.sublimetext.com/download/
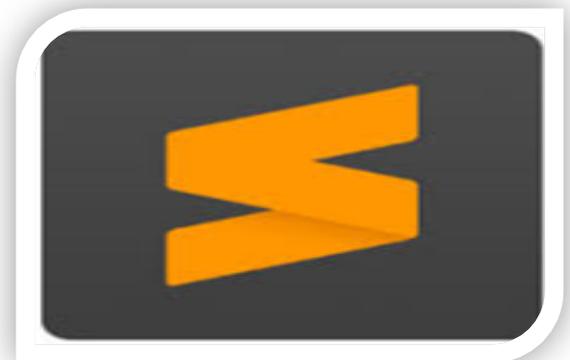
III.3.Overview of the applicaion

Through the diverse have a look at phases completed, we were capable of expand an electronic voting utility. This website is a prototype and covers the whole method of an election. The website has a fixed of capabilities and get entry to is authorized to 4 styles of person (administrator, supervisor(s), electorate and candidate(s)). The main capabilities of the website are presented in the following sections. But earlier than that, we gift a top level view of the software within the following determine.

III.3.1.System Architectour:
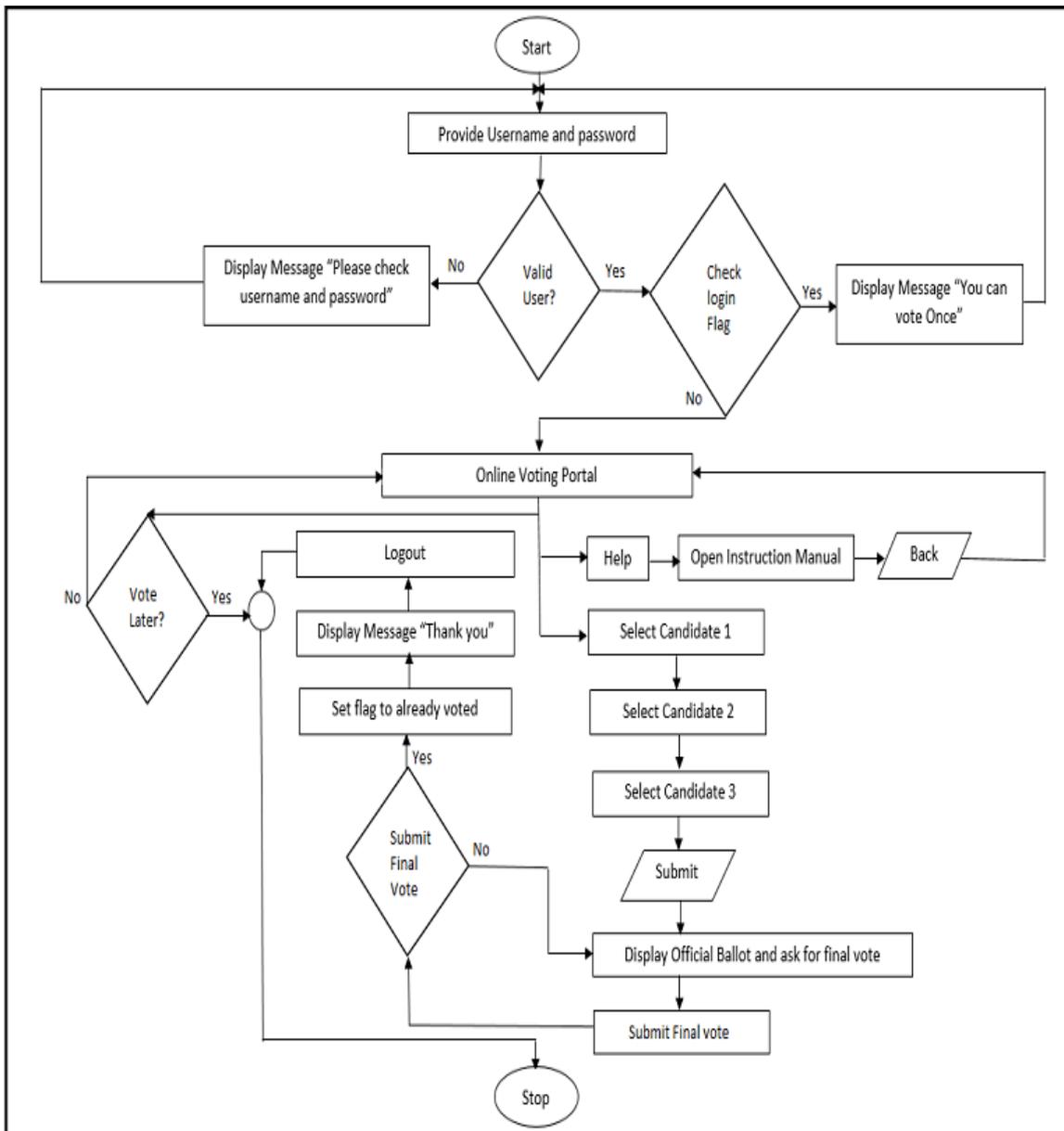
Figure III. 1: Results and discussion.

III.3.2. Authentication:
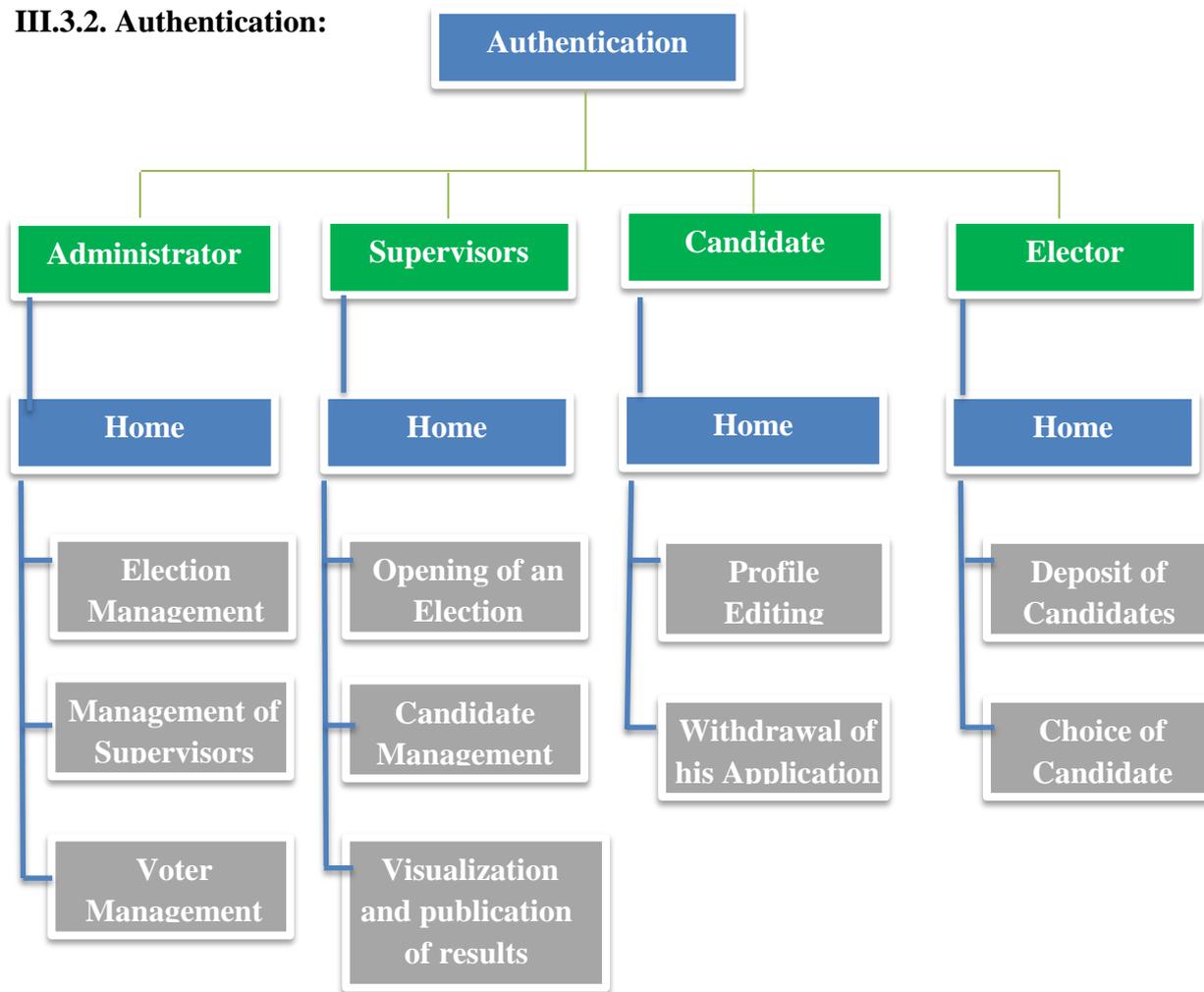
Figure III. 2: The authentication of system voting.

III.3.2.1. Authentication page: *In* this page the learner or the administrator can be diagnosed by way of typing his call and password. If the statistics Authentication are wrong, the system displays a brand new page Identification with a warning message.

Figure III. 3: Voting system authentication login page to Admin.

To maintain security, no other user is registered unless he is registered in the server system by the original site controller. Only the username and password will be submitted.

He is only given the ability to change his profile:

Figure III. 4: Register "sign in" page to Admin.of the voting system.

The password_hash () function creates a new hash using a strong and irreversible hashing algorithm.

The following algorithms are currently supported:

- o PASSWORD_DEFAULT - Use of the bcrypt algorithm (default since PHP 5.5.0). Note that this constant is designed to change over time as newer and stronger algorithms are added to PHP. For this reason, the length of the result from this algorithm can change over time, so it is recommended to store the result in a database column that can contain at least 60 characters (255 characters can be a very good choice).

- o PASSWORD_BCRYPT - Using the CRYPT_BLOWFISH algorithm to create the hash key. This will create a standard crypt () hash key using the identifier "$2y$". The result will always be a 60 character string,

Code source to Cryptage:

```
17
18    $password = password_hash($_POST['password'], PASSWORD_DEFAULT);
19    //generate voters id
```

III.3.2.2. Home: This page is the home web page. It includes the primary Content material of your web site.

Figure III. 5: Home page of the online voting

Home page of the e-voting "Admin": Appears on the Count page = (Municipalities / Candidates / Total Voters / Voters), It also displays vote statistics:
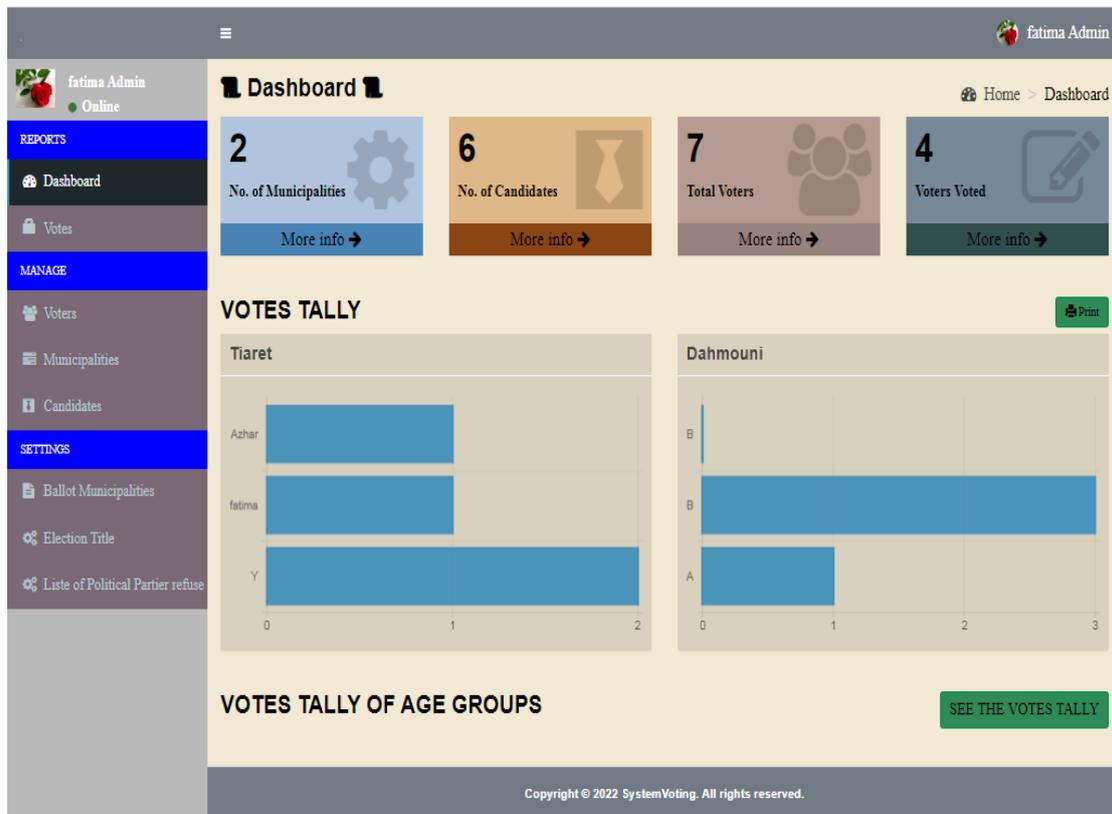
Figure III. 6: Home page of the e-voting "Admin"

III.3.2.3. Registration: If the person traveling the website is invited (i.E. Does not having a user account), so the consumer have to register at the website, via clicking on the hyperlink "Registration" he'll discover a shape to fill in the Registration web page.

III.3.2.3.1.Registration of the voter consumer:

After authentication the learner or administrator on the profile page   which incorporates the personal statistics of Candidat

1. Registration from online voting:

External => online voting (website)
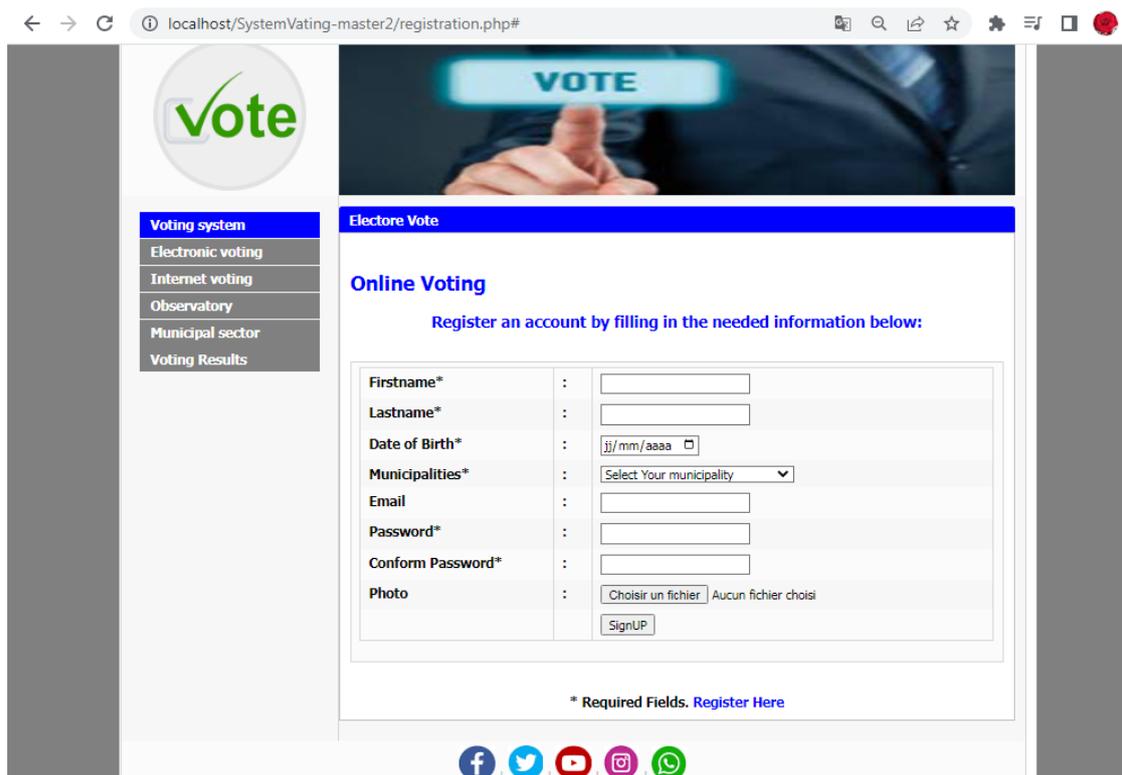
Figure III. 7: Page sensor Register External "sign in" of the cerate vote.

2. Registration from Electronic Voting:

Interned => admin (polling station).
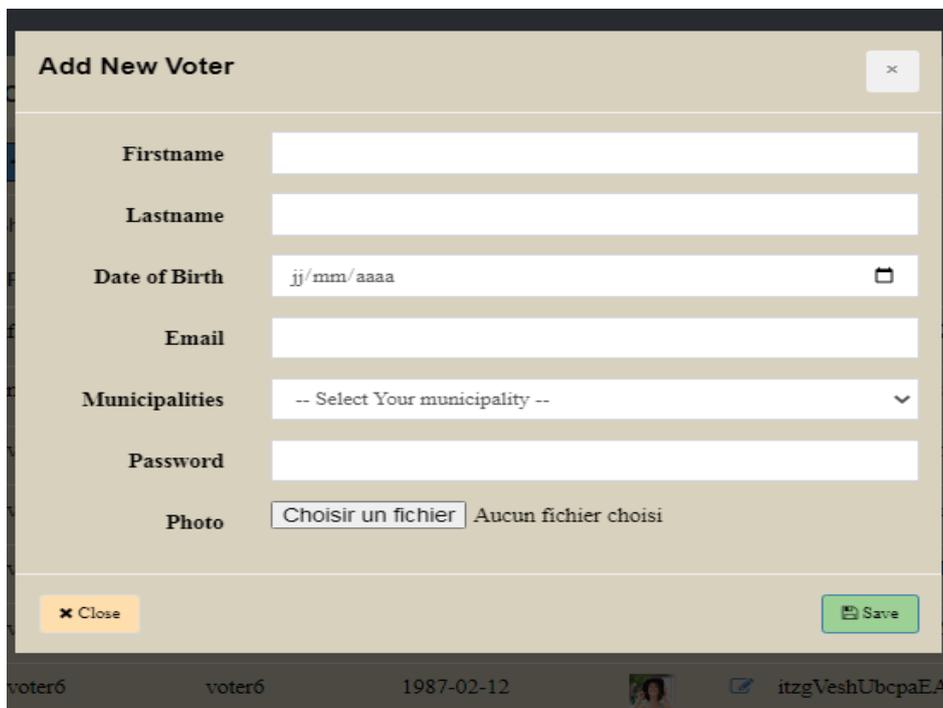
Figure III. 8: The registration External of Voter
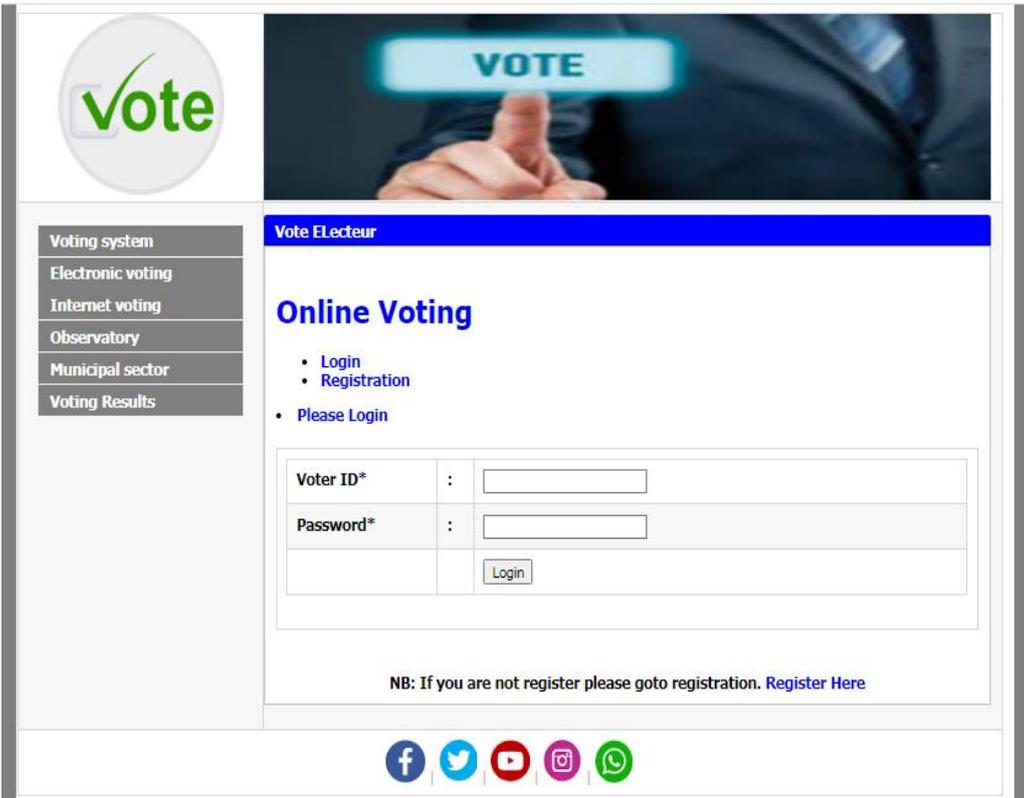
Figure III. 9: Page sensor Vating system authentication login to Voter.

III.3.2.3.2.Registration of the condidat:
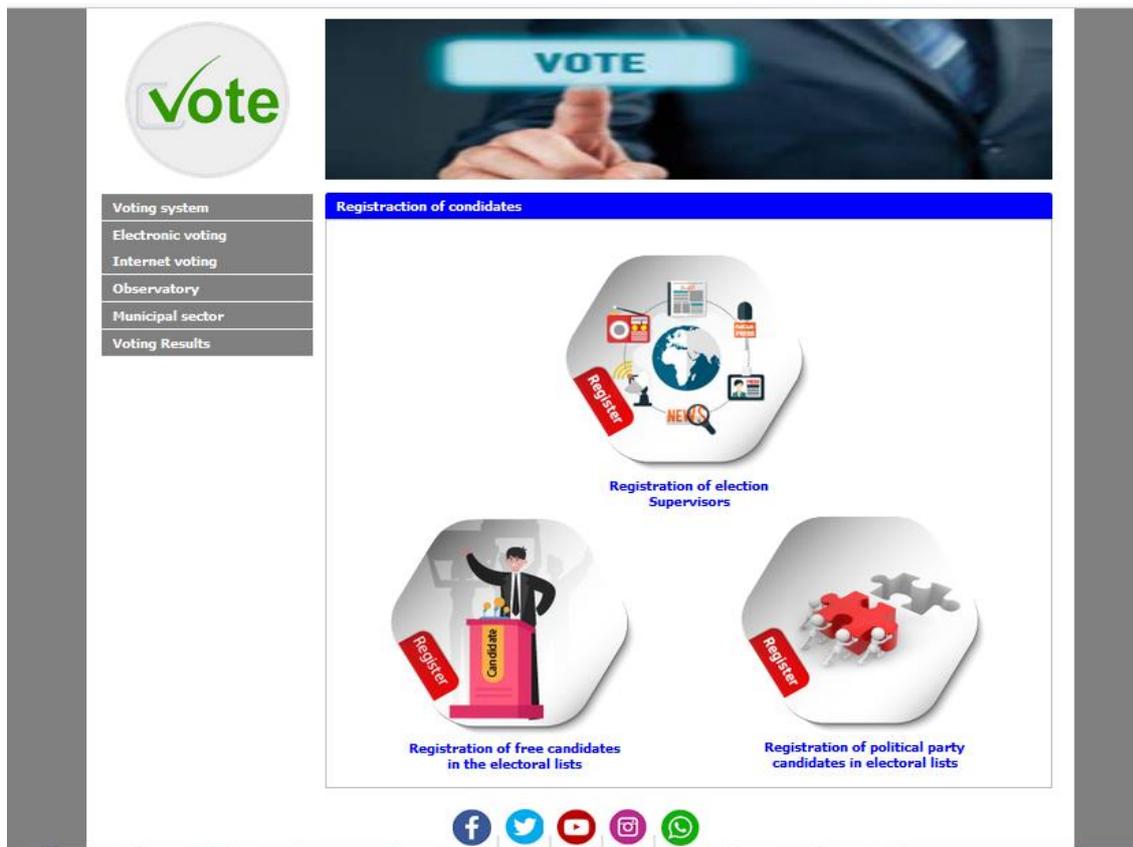
Figure III. 10: The registration Condidate of lists election

III.3.2.3.2.1.Registration of the supervisor vote:

In this component, the supervisor can be responsible for holding the elections by deciding when the packets will be submitted, as well as the date of the polls. The election supervisor must also be voted on by a specialized committee if he fulfills the conditions through the following registration:

1. Registration from online voting:

External => online voting (website)

Figure III. 11: The registration External of Supervisors

2. Registration from Electronic Voting:

Interned => admin (polling station).

Figure III. 12: The registration interned of Supervisors

III.3.2.3.2.2.Registration of Candidate consumer vote: After the authentication the learner or the administrator on the profile page which contains the private data of Candidat.

1. Registration from online voting:

External => online voting (website)

Figure III. 13: The registration External of Political party Condidate.
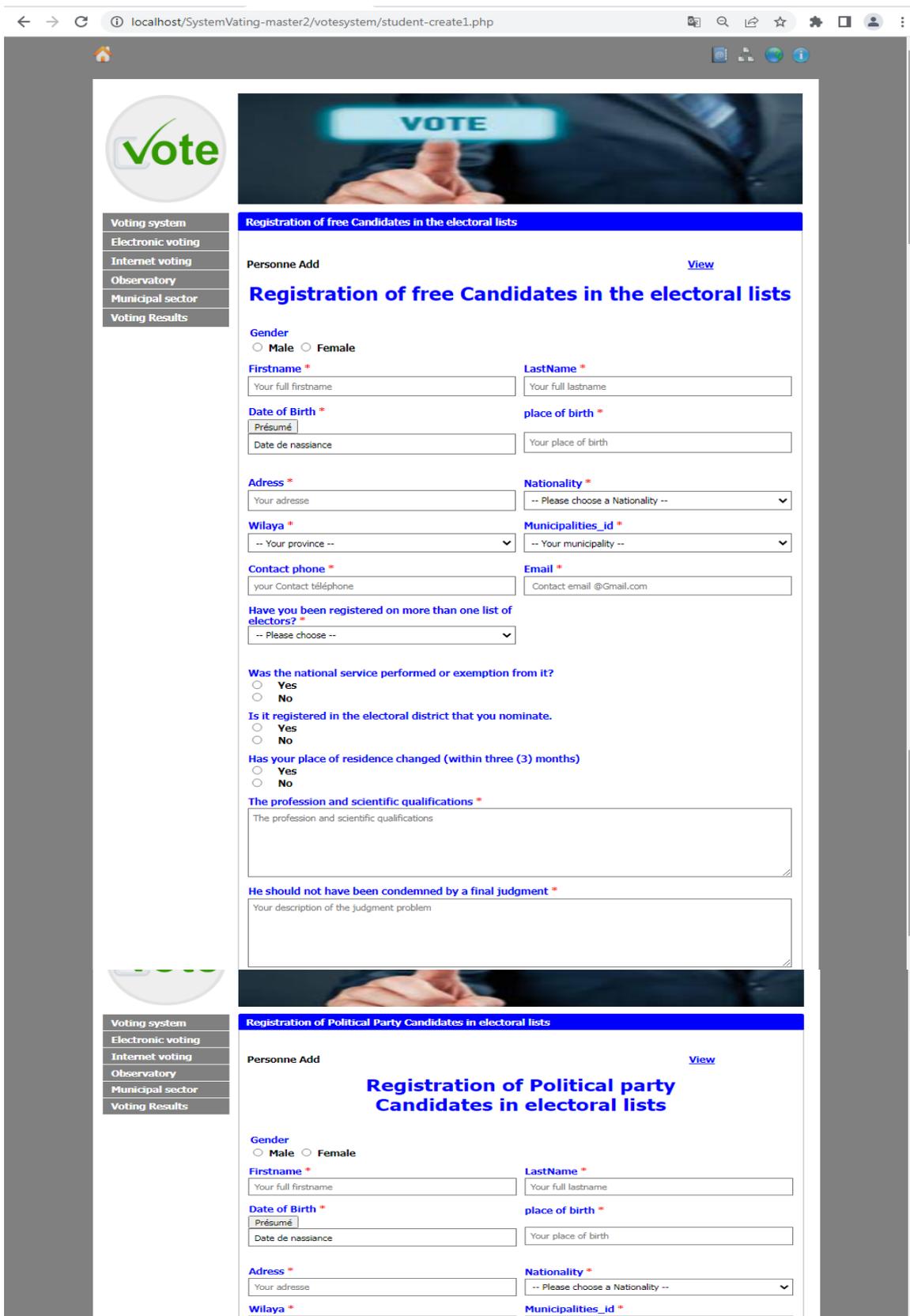
Figure III. 14: The registration External of Free Condidate.

2. Registration from Electronic Voting

Interned => admin (polling station).

*Figure III. 15: The registration **interned** of Condidate*

III.4. User control for the administrator:
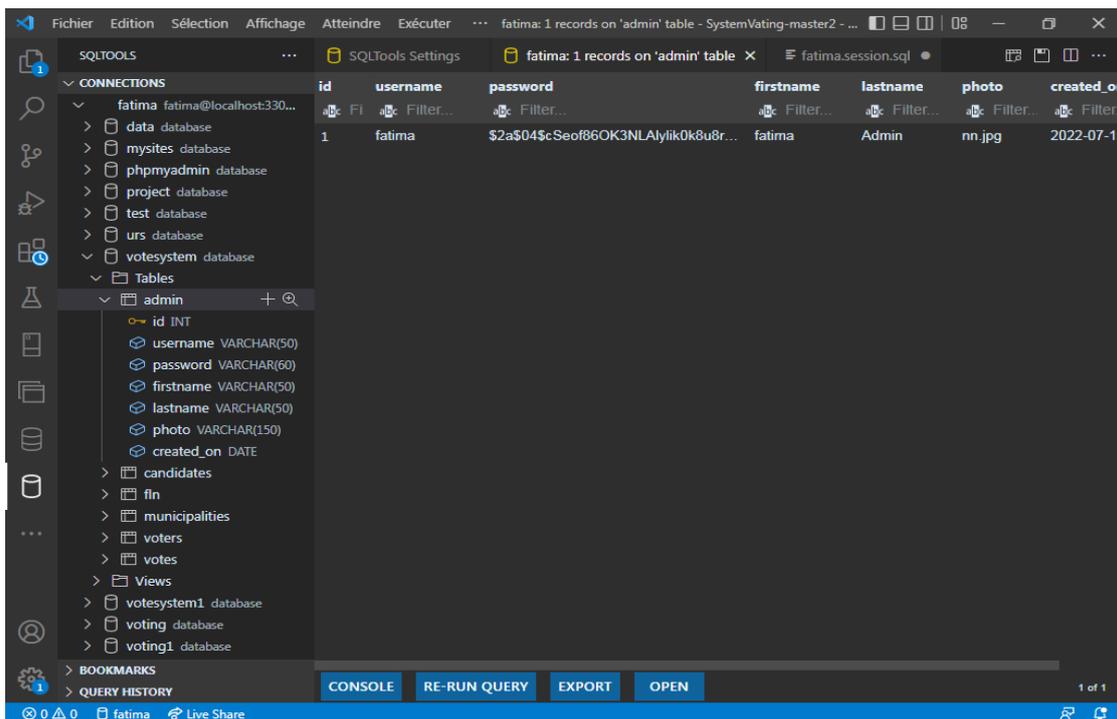
Figure III. 16: Manage users login page

This part is vital to add, alter or delete beginner, that is to say to manipulate the machine.

III.4.1. User control for the Voter:
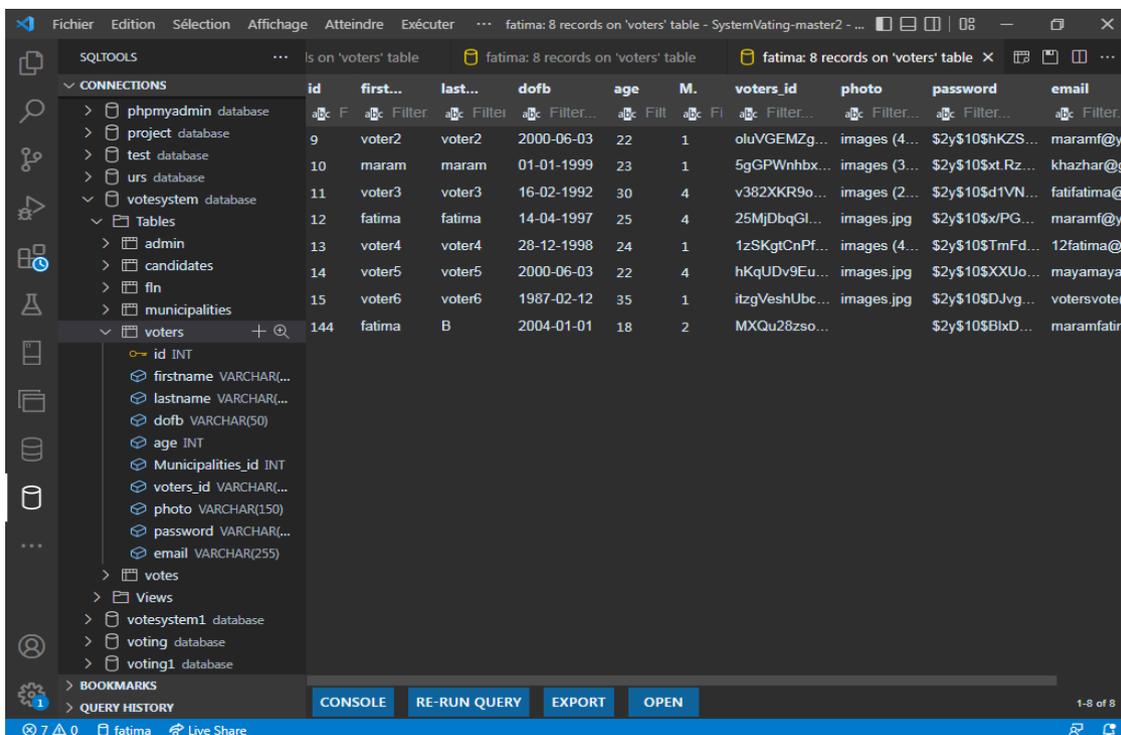
Figure III. 17: Manage Voter by the database.

III.4.1.1. Crypt candidate:

Figure III. 18: Manage Crypt"Candidat" of Voter by the database.

Encrypt candidate by md5:

Definition: The password MD5 function is a hash function, it is also the name given to the result of this function. The MD5 hash of a piece of data matches it with a 32-character fingerprint, which makes it possible to identify the initial piece of data. Hash functions are widely used in computer science and cryptography.

Principle of encryption: How to encode in MD5?
The MD5 hash calculates from computer data a digital fingerprint of 32 hexadecimal characters. The algorithm uses non-linear functions,

III.4.1.2. Crypt Password and Voters_id:
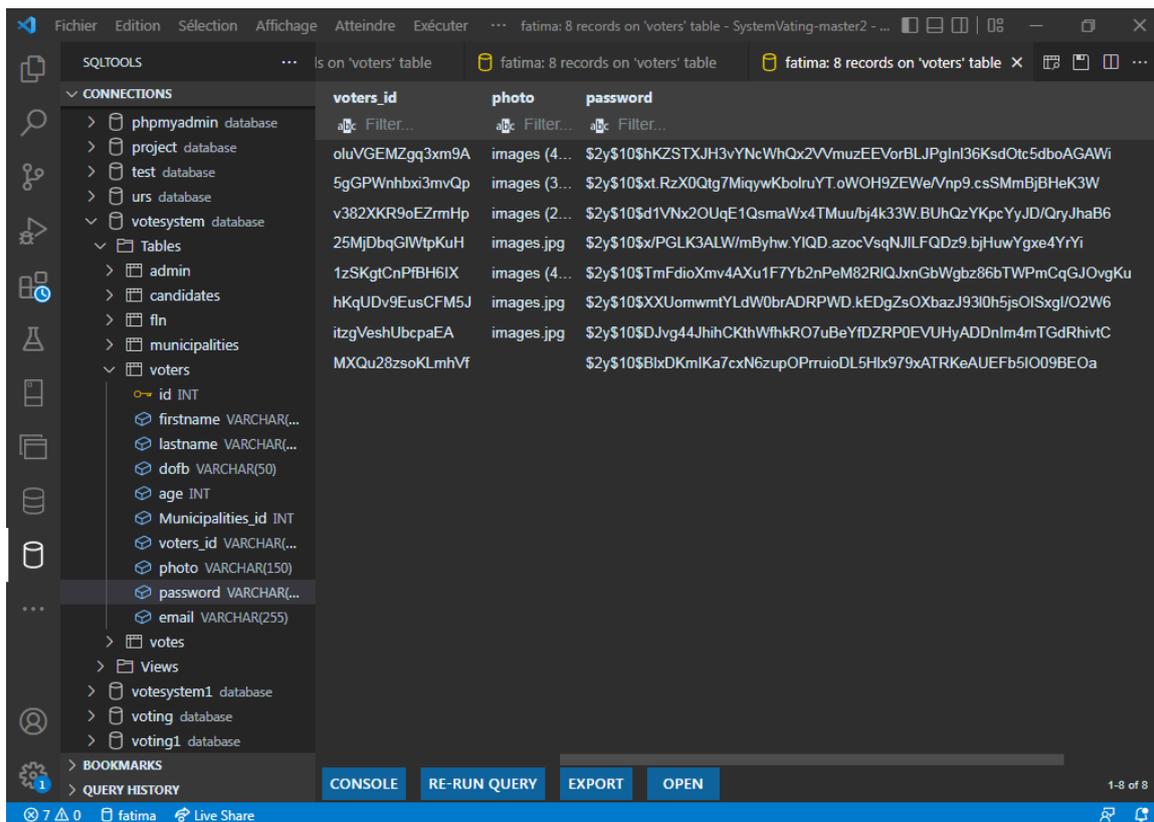
Figure III. 19: Manage Crypt "Password and Voter_id" of Voter by the database.

Cryptage password:

$password = password_hash ($_POST ['password'], PASSWORD_DEFAULT);

Cryptage voter id: substr (str_shuffle)

The str_shuffle () function randomly shuffles all characters in a string.

str_shuffle () shuffles characters in a string. A permutation among all possible ones is created.

```
17
18        $password = password_hash($_POST['password'], PASSWORD_DEFAULT);
19        //generate voters id
20        $set = '123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
21        $voter = substr(str_shuffle($set), 0, 15);
22
```

III.4.2. User control for the Candidates vote:
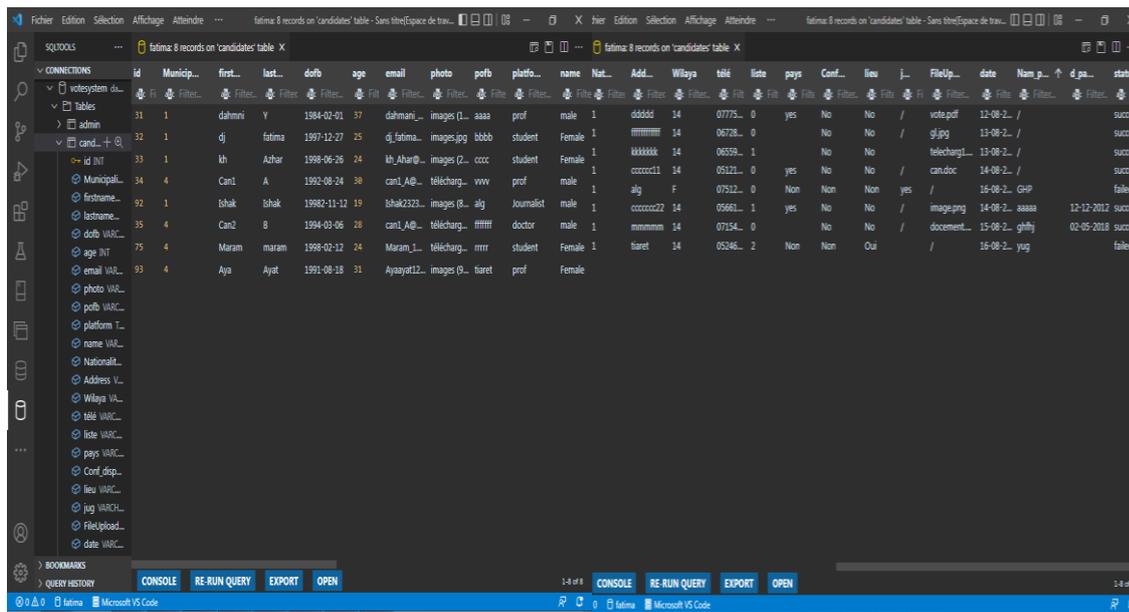
Figure III. 20: Manage the Candidate registration database.

III.4.2.1.Manage the candidat registration database:

The database through which the user controls is dealt with through the process of listing, editing, deleting and seeing candidates, whether for the supervisor or the voter, through which they are added to the electoral list as candidates

An example of Manage the candidat registration database:

Figure III. 21: Manage of created the candidate registration database.

View the candidate's personal data:

Figure III. 22: Manage of View the candidate's created the candidate registration.

III.4.3. User control View for the list «accepted» of electoral candidates:
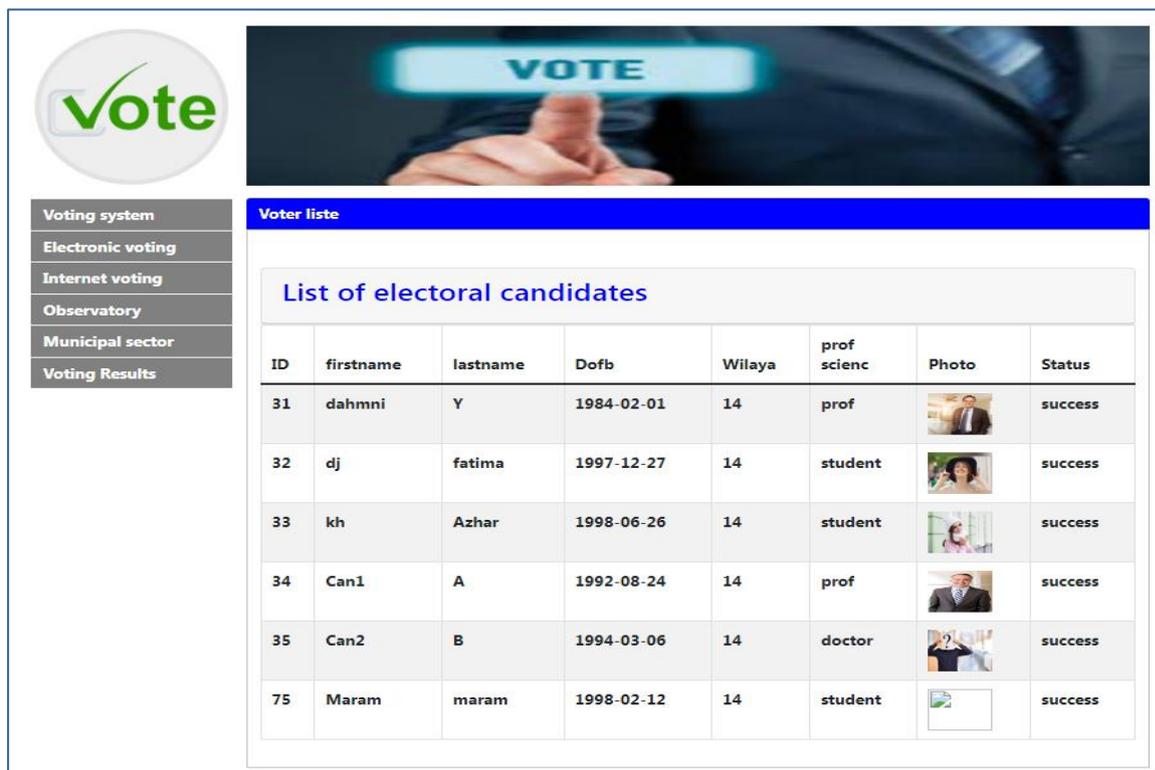
Figure III. 23: List of election candidates.
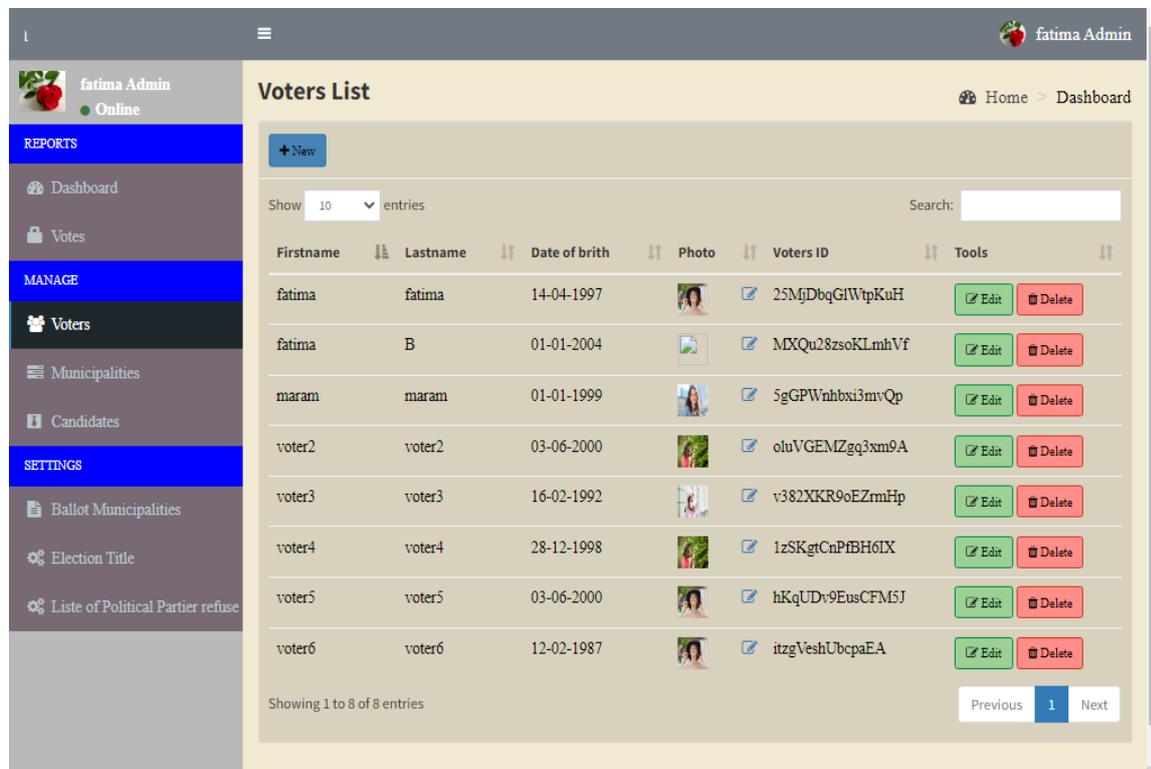
Figure III. 24: *List of voter*

III.5. Home Page of the Online voting Interface:

On this page, we have introduced the user interface for onling voting, which is represented in:

III.5.1.Home Page of the Candidate voting Interface:

Login voter

Submit voter

Success Ballot

Figure III. 25: Page sensor your candidate vote.

III.6.OnlineVoting Results:

From here, we presented the election results for both the supervisor and the candidat who were represented as follows:

III.6.1. Candidate Voting Results:

Figure III. 26: Page Sensor See candidate voting results.

III.6.2. Results Voting statistics:

III.6.2.1. Voting statistics of candidates for each municipality:
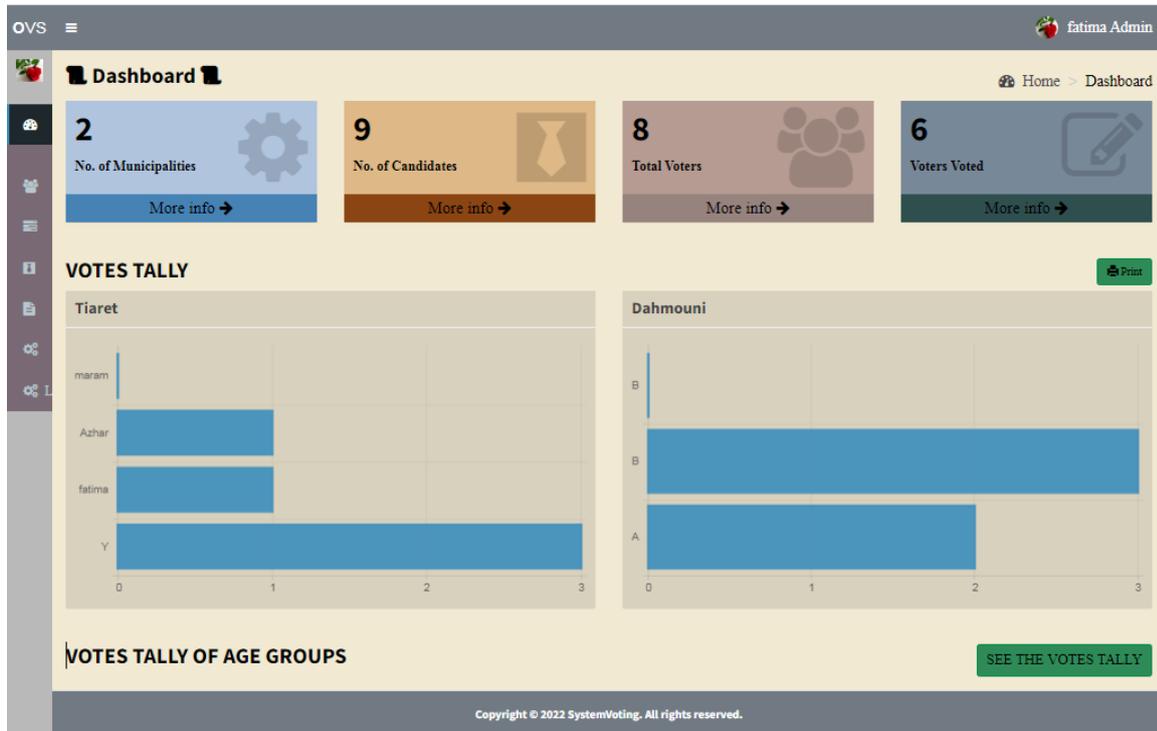
Figure III. 27 : Page sensor your Voting statistics of candidates for each municipality.

III.6.2.2. Age groups that voted in the election for each Municipality:
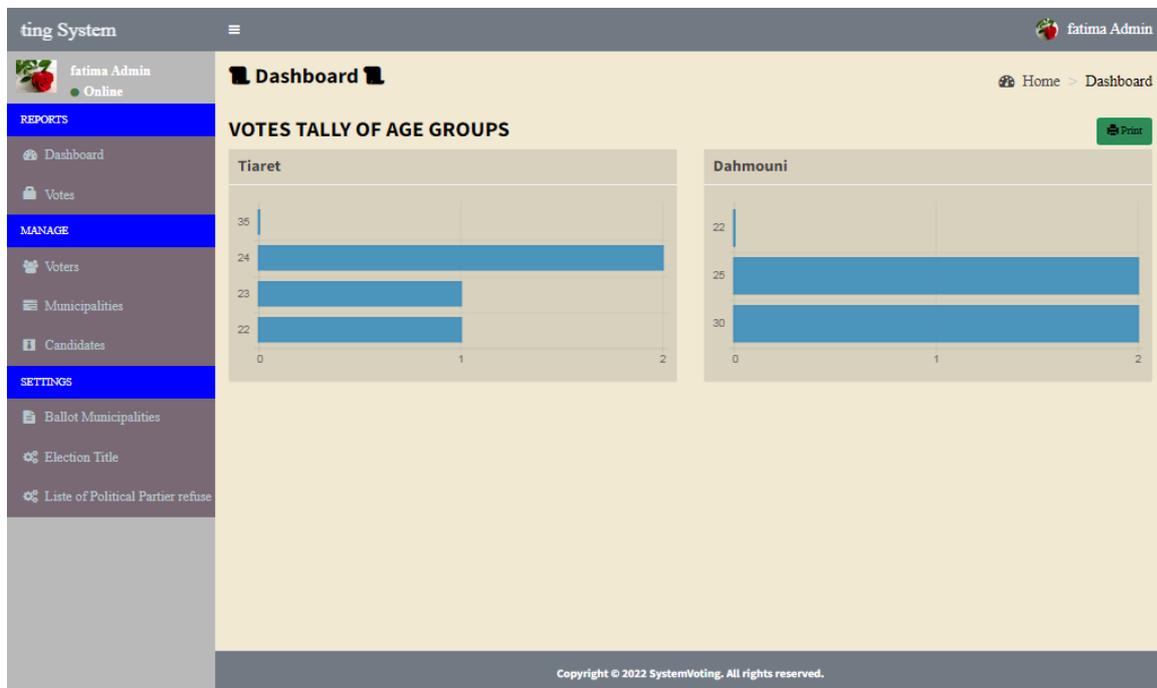
Figure III. 28: Page sensor your Age groups that voted in the election for each Municipality.

III.7.Code Source PHP:

III.7.1. The PHP of Home Page by voting:

```
C:\xampp1\htdocs\Online-Voting-System-main\Online Voting System\voting management system\votesystem\votesystem\home.php • (Online-Voting-System-main)...
File   Edit   Selection   Find   View   Goto   Tools   Project   Preferences   Help

index.php  ×    votes.php  •     home.php  •    candidates_modal.php  ×    candidates_add.php  ×    view.php  ×    control.php  ×

69    <!-- Voting Ballot -->
70        <form method="POST" id="ballotForm" action="submit_ballot.php">
71            <?php  include 'includes/slugify.php';
72                $candidate = '';
73                $sql = "SELECT * FROM municipalities ORDER BY priority ASC";
74                $query = $conn->query($sql);
75                while($row = $query->fetch_assoc()){
76                $sql = "SELECT * FROM candidates WHERE municipalities_id='".$row['id']."'";
77                $cquery = $conn->query($sql);
78                    while($crow = $cquery->fetch_assoc()){ $slug = slugify($row['municipal']);
79                                        $checked = '';
80                    if(isset($_SESSION['post'][$slug])){
81                        $value = $_SESSION['post'][$slug];
82                    if(is_array($value)){
83                        foreach($value as $val){ if($val == $crow['id']){
84                                    $checked = 'checked';}
85                                        }}
86                    else{ if($value == $crow['id']){ $checked = 'checked';}
87                                }}
88                $input = ($row['max_vote'] > 1) ? '<input type="checkbox" class="flat-red '.$slug
                        .'" name="'.$slug."[]".'" value="'.$crow['id'].'" '.$checked.'>' : '<input
                        type="radio" class="flat-red '.$slug.'" name="'.slugify($row['municipal']).'
                        " value="'.$crow['id'].'" '.$checked.'>';
89                $image = (!empty($crow['photo'])) ? 'images/'.$crow['photo'] : 'images/
                        profile.jpg';
90                $candidate .= '<li>'.$input.'<button type="button" class="btn btn-primary btn-sm
                        btn-curve clist platform" style="background-color: #4682B4 ;color:black ;
                        font-size: 12px; font-family:Times" data-platform="'.$crow['platform'].'"
                        data-fullname="'.$crow['firstname'].' '.$crow['lastname'].'"><i class="fa
                        fa-search"></i> Platform</button><img src="'.$image.'" height="100px"
                        width="100px" class="clist"><span class="cname clist">'.$crow['firstname'].'
                        '.$crow['lastname'].'</span></li>'; }
91                $instruct = ($row['max_vote'] > 1) ? 'You may select up to '.$row['max_vote'].'
                        candidates' : 'Select only one candidate';
92                    echo '<div class="row"> <div class="col-xs-12">
93                        <div class="box box-solid" style="background-color: #d8d1bd" id="'.$row['id']
                            .'"> <div class="box-header with-border" style="background-color:
                            #d8d1bd">
94                        <h3 class="box-title"><b>'.$row['municipal'].'</b></h3>
95                                        </div>
96                        <div class="box-body" ><p>'.$instruct.' <span class="pull-right">
97                        <button type="button" class="btn btn-success btn-sm btn-curve reset"
                            style="background-color:#9CD095 ;color:black ; font-size: 12px;
                            font-family:Times"  data-desc="'.slugify($row['municipal']).'"><i
                            class="fa fa-refresh"></i> Reset</button>
98                                        </span></p>
99                        <div id="candidate_list"><ul>'.$candidate.'
100                                       </ul>
101                                  </div>
102                                </div>
103                            </div>
104                        </div>
105                    </div> ';
106
107                $candidate = '';}
108                    ?>
109            <div class="text-center">
110                    <button type="button" class="btn btn-success btn-curve" style
                        ='background-color: #9CD095 ;color:black ; font-size: 12px;
                            font-family:Times' id="preview"  ><i herf="preview.php"
                        class="fa fa-file-text"></i> Preview</button>
111                    <button type="submit" class="btn btn-primary btn-curve" style
                        ='background-color: #4682B4 ;color:black ; font-size: 12px;
                            font-family:Times'name="vote"><i class="fa
                        fa-check-square-o"></i> Submit</button>
112                </div>
113            </form>
114
115            <!-- End Voting Ballot -->

Line 113, Column 37                                                    Tab Size: 4          PHP
```

Figure III. 29: Page to code source by vote.

III.7.2. The PHP login and registration of Candidat the voters:

III.7.2.1. The PHP of Registration:

Figure III. 30: Source code capture for login of the Registration vote.

III.7.2.2. The PHP of Registration:

Figure III. 31: Source code capture for Register "sign in" of the cerate vote.

III.7.3. The PHP Code of Managed candidate of Election List by the database:


```php
<?php
session_start();
require 'dbcon1.php';

if(isset($_POST['delete_candidates']))
{
    $candidates_id = mysqli_real_escape_string($con, $_POST['delete_candidates']);

    $query = "DELETE FROM candidates WHERE id='$candidates_id' ";
    $query_run = mysqli_query($con, $query);

    if($query_run)
    {
        $_SESSION['message'] = "Personne Deleted Successfully";
        header("Location: index1.php");
        exit(0);
    }
    else
    {
        $_SESSION['message'] = "Personne Not Deleted";
        header("Location: index1.php");
        exit(0);
    }
}
```

Figure III. 32: Source code capture for Delete in the database.

```
26
27   if(isset($_POST['update_candidates']))
28   {
29       $candidates_id = mysqli_real_escape_string($con, $_POST['candidates_id']);
30       $name = mysqli_real_escape_string($con, $_POST['name']);
31       $firstname = mysqli_real_escape_string($db, $_POST['firstname']);
32       $lastname = mysqli_real_escape_string($db, $_POST['lastname']);
33       $pofb = mysqli_real_escape_string($con, $_POST['pofb']);
34       $dofb = mysqli_real_escape_string($con, $_POST['dofb']);
35       $Age = mysqli_real_escape_string($con, $_POST['Age']);
36       $Nationalité = mysqli_real_escape_string($con, $_POST['Nationalité']);
37       $Address = mysqli_real_escape_string($con, $_POST['Address']);
38       $Wilaya = mysqli_real_escape_string($con, $_POST['Wilaya']);
39       $Municipalities_id = mysqli_real_escape_string($con,
40           $_POST['Municipalities_id']);
41       $télé = mysqli_real_escape_string($con, $_POST['télé']);
42       $Email = mysqli_real_escape_string($con, $_POST['Email']);
43       $liste = mysqli_real_escape_string($db, $_POST['liste']);
44       $Nam_party = mysqli_real_escape_string($db, $_POST['Nam_party']);
45       $pays = mysqli_real_escape_string($db, $_POST['pays']);
46       $Conf_disp = mysqli_real_escape_string($db, $_POST['Conf_disp']);
47       $lieu = mysqli_real_escape_string($db, $_POST['lieu']);
48       $platform = mysqli_real_escape_string($con, $_POST['platform']);
49       $jug = mysqli_real_escape_string($con, $_POST['jug']);
50       $FileUpload = mysqli_real_escape_string($con, $_POST['FileUpload']);
51       $Photo = mysqli_real_escape_string($con, $_POST['Photo']);
52       $date = mysqli_real_escape_string($con, $_POST['date']);
53
54       $query = "UPDATE candidates SET name='$name', firstname='$firstname', lastname=
             '$lastname' , dofb='$dofb' ,pofb='$pofb' , Age='$Age' , Nationalité='$
             Nationalité' , Address='$Address' , $Wilaya='$Wilaya' , Municipalities_id='
             $Municipalities_id' , télé='$télé' , Email='$Email' , liste='$liste'
             ,Nam_party='$Nam_party' , pays='$pays' , Conf_disp='$Conf_disp' , lieu='$
             lieu' ,platform='$platform' , jug='$jug' , FileUpload='$FileUpload' , Photo
             ='$Photo', date='$date' WHERE id='$candidates_id'";
55
56
57       $query_run = mysqli_query($con, $query);
58
59       if($query_run)
60       {
61           $_SESSION['message'] = "Personne Updated Successfully";
62           header("Location: index1.php");
63           exit(0);
64       }
65       else
66       {
67           $_SESSION['message'] = "Personne Not Updated";
68           header("Location: index1.php");
69           exit(0);
70       }
71
72   }
73
```

Figure III. 33: Source code capture for Update in the database

```
74
75   if(isset($_POST['save_candidates']))
76   {
77       $candidates_id = mysqli_real_escape_string($con, $_POST['candidates_id']);
78       $name = mysqli_real_escape_string($con, $_POST['name']);
79       $firstname = mysqli_real_escape_string($db, $_POST['firstname']);
80       $lastname = mysqli_real_escape_string($db, $_POST['lastname']);
81       $pofb = mysqli_real_escape_string($con, $_POST['pofb']);
82       $dofb = mysqli_real_escape_string($con, $_POST['dofb']);
83       $Age = mysqli_real_escape_string($con, $_POST['Age']);
84       $Nationalité = mysqli_real_escape_string($con, $_POST['Nationalité']);
85       $Address = mysqli_real_escape_string($con, $_POST['Address']);
86       $Wilaya = mysqli_real_escape_string($con, $_POST['Wilaya']);
87       $Municipalities_id = mysqli_real_escape_string($con,
88           $_POST['Municipalities_id']);
89       $télé = mysqli_real_escape_string($con, $_POST['télé']);
90       $Email = mysqli_real_escape_string($con, $_POST['Email']);
91       $liste = mysqli_real_escape_string($db, $_POST['liste']);
92       $Nam_party = mysqli_real_escape_string($db, $_POST['Nam_party']);
93       $pays = mysqli_real_escape_string($db, $_POST['pays']);
94       $Conf_disp = mysqli_real_escape_string($db, $_POST['Conf_disp']);
95       $lieu = mysqli_real_escape_string($db, $_POST['lieu']);
96       $platform = mysqli_real_escape_string($con, $_POST['platform']);
97       $jug = mysqli_real_escape_string($con, $_POST['jug']);
98       $FileUpload = mysqli_real_escape_string($con, $_POST['FileUpload']);
99       $Photo = mysqli_real_escape_string($con, $_POST['Photo']);
100      $date = mysqli_real_escape_string($con, $_POST['date']);

100      $query = "INSERT INTO candidates (name, firstname, lastname,pofb, dofb, Age,
             Nationalité, Address, Wilaya, Municipalities_id, télé, Email,
             liste,Nam_party, pays, Conf_disp, lieu,platform, jug, FileUpload,Photo,
101          date) VALUES ('$name','$firstname','$lastname' ,'$pofb','$dofb','$Age',
102          '$Nationalité' ,'$Address' ,'$Wilaya','$Municipalities_id' ,'$télé' ,'
103          $Email' ,'$liste','$Nam_party','$pays','$Conf_disp','$lieu','$platform',
104          '$jug','$FileUpload','$Photo','$date')";
105
106
107      $query_run = mysqli_query($con, $query);
108      if($query_run)
109      {
110          $_SESSION['message'] = "Personne Created Successfully";
111          header("Location: student-create1.php");
112          exit(0);
113      }
114      else
115
116      {
117          $_SESSION['message'] = "Personne Not Created";
118          header("Location: student-create1.php");
119          exit(0);
120      }
121  }
122
123  ?>
124
125
```

Figure III. 34: Source code capture for Save in the database.

III.7.4. the PHP of Results Voting statistics:


```php
<?php include 'includes/scripts.php'; ?>
<?php
  $sql = "SELECT * FROM Municipalities ORDER BY priority ASC";
  $query = $conn->query($sql);
  while($row = $query->fetch_assoc()){
    $sql = "SELECT * FROM candidates WHERE Municipalities_id = '".$row['id']."'";
    $cquery = $conn->query($sql);
    $carray = array();
    $varray = array();
    while($crow = $cquery->fetch_assoc()){
      array_push($carray, $crow['lastname']);
      $sql = "SELECT * FROM votes WHERE candidate_id = '".$crow['id']."'";
      $vquery = $conn->query($sql);
      array_push($varray, $vquery->num_rows);
    }
    $carray = json_encode($carray);
    $varray = json_encode($varray);
    ?>
    <script>
    $(function(){
      var rowid = '<?php echo $row['id']; ?>';
      var municipal = '<?php echo slugify($row['municipal']); ?>';
      var barChartCanvas = $('#'+municipal).get(0).getContext('2d')
      var barChart = new Chart(barChartCanvas)

      var barChartData = {
        labels  : <?php echo $carray; ?>,

        datasets: [

          {
            label             : 'Votes',

            fillColor         : 'rgba(60,141,188,0.9)',
            strokeColor       : 'rgba(60,141,188,0.8)',
            pointColor        : '#3b8bba',
            pointStrokeColor  : 'rgba(60,141,188,1)',
            pointHighlightFill  : '#fff',
            pointHighlightStroke: 'rgba(60,141,188,1)',
            data              : <?php echo $varray; ?>
          }
        ]
      }
      var barChartOptions              = {
        //Boolean - Whether the scale should start at zero, or an order of magnitude down from
        the lowest value
        scaleBeginAtZero      : true,
        //Boolean - Whether grid lines are shown across the chart
        scaleShowGridLines    : true,
        //Number - Width of the grid lines
        scaleGridLineWidth    : 1,
        //Boolean - Whether to show horizontal lines (except X axis)
        scaleShowHorizontalLines: true,
        //Boolean - Whether to show vertical lines (except Y axis)
        scaleShowVerticalLines  : true,
        //Boolean - If there is a stroke on each bar
        barShowStroke         : true,
        //Number - Pixel width of the bar stroke
        barStrokeWidth        : 2,
        //Number - Spacing between each of the X value sets
        barValueSpacing       : 5,
        //Number - Spacing between data sets within X values
        barDatasetSpacing     : 1,
        //String - A legend template
        legendTemplate        : '<ul class="<%=name.toLowerCase()%>-legend"><% for (var i=0;
          i<datasets.length; i++){%><li><span style="background-color:<%=datasets[
          i].fillColor%>"></span><%if(datasets[i].label){%><%=datasets[
          i].label%><%}%></li><%}%></ul>',
        //Boolean - whether to make the chart responsive
        responsive            : true,
        maintainAspectRatio   : true
      }

      barChartOptions.datasetFill = false
      var myChart = barChart.HorizontalBar(barChartData, barChartOptions)
      //document.getElementById('legend_'+rowid).innerHTML = myChart.generateLegend();
    });
    </script>
    <?php
  }
?>
```

Figure III. 35: Source codes capture Voting statistics the vote.

III.8.Conclusion:

In this chapter, we've got provided the equipment and programs which have been worked on in our undertaking and we've chosen a language TO USED together with personal home page, EX: PHP, Mysql and therefore XAMPP as a improvement tool and database

We additionally touched on providing the maximum crucial interfaces on the site and offering the most crucial functions which have been labored directly to permit the citizen to check in online effectively and luxury.
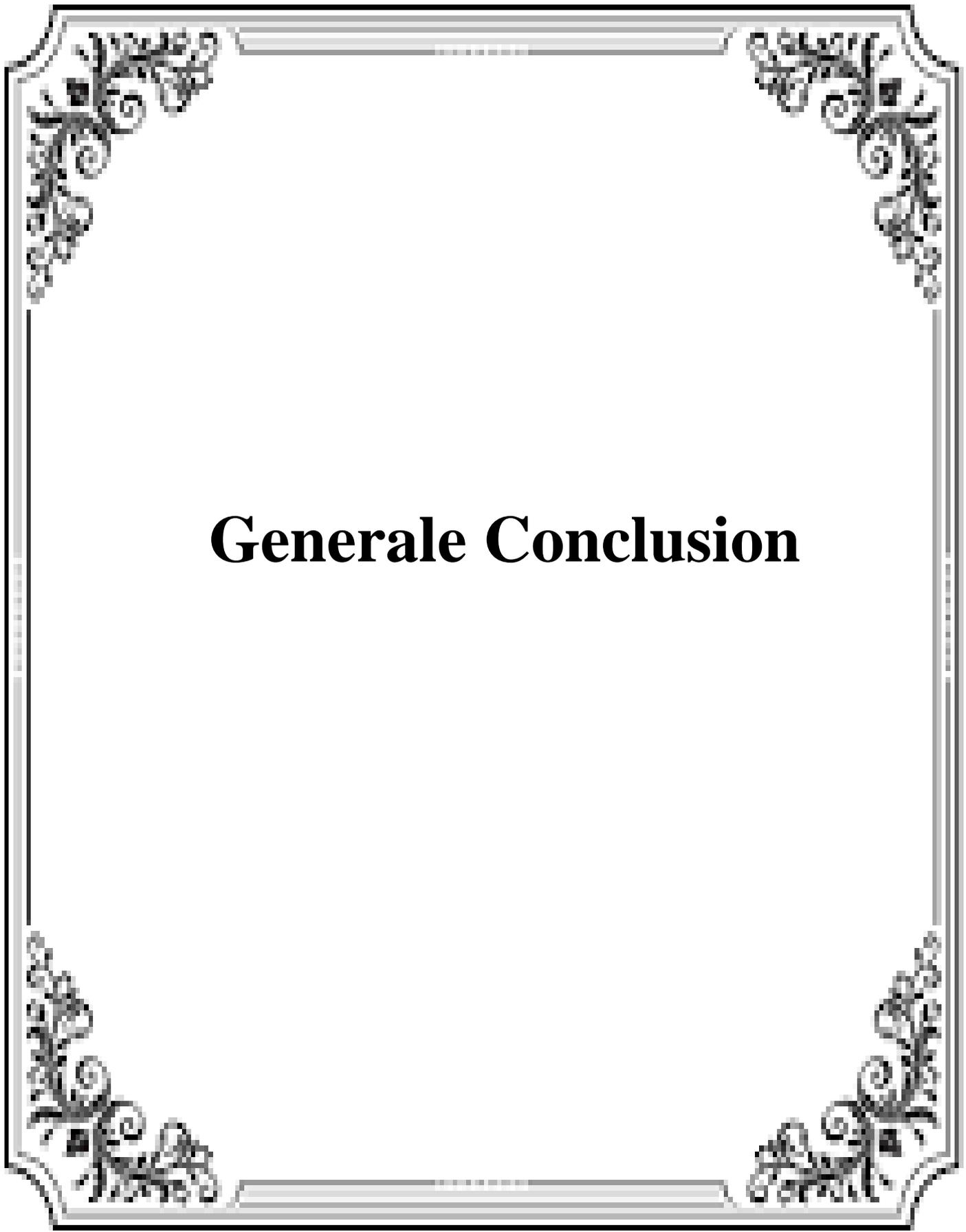
Generale Conclusion

GENERAL Conclusion

In this project, we treated the subject "Design and implementation of a system Electronic or online voting.

Our current work aims to develop the voting system and information management for all candidates and voters remotely by providing full coverage of the work systems we have relied on such as "UML", as well as the transparency of the system in enabling candidates and voters to preserve their electoral rights and trying to improve their credibility as much as possible, in addition to Facilitating the counting of elections and determining the total number of votes.

At first, we covered a general knowledge of electronic voting and electronic voting, and then we Present some of the previous work and explain some of their systems to provide system we made.

We used UML to model our system to give an idea how to build the application and how it works.

This online voting system works by managing voter information with which a voter can log in and use his or her voting rights.

The system will include all the features of the voting system. Provides tools to keep the electorate voting for municipal elections and calculates the total number of votes (candidates) for each municipality.

There is a database maintained by the Electoral Commission where all voters' names are stored with complete information.

References

BIBLIOGRAPHIC REFERENCES

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

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

[3] 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`.

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

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

[6] 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.

[7] S. Benmeziane. Mécanismes d'authentification. Rapport interne, CERIST, 2001.

[8] L. Khelladi et K. Bouguessa. Conception et réalisation d'un système de vote électronique en Java. Mémoire de fin d'étude, novembre 2001.

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

[10] Joseph Garby & David Garby, UML 2 ANALYSE ET CONCEPTION,Dunod Paris,2008, ISBN 978-2-10-053567-5

[11] https://openclassrooms.com/courses/debutez-l-analyse-logicielle-avec-uml/les-differentstypes- de-diagrammes