- Recepción/ 27 junio 2019
- Aceptación/ 25 agosto 2019

Security of Internet Voting Schemes: A Survey

Seguridad de los esquemas de votación por Internet: una encuesta

Sufyan T. Faraj Al-Janabi
College of Computer Science and IT
University of Anbar, Ramadi, Iraq
saljanabi@fulbrightmail.org

Noor Hamad Abid
College of Computer Science and IT
University of Anbar, Ramadi, Iraq
hopingsmile9@gmail.com

ABSTRACT/ Voting is the process through which representatives of the country are chosen. Everyone has the right to elect candidates who he deems fit to lead the country. It must be ensured that the elections are fair and that votes are not manipulated, deleted or changed, or even that voters are forced to vote for candidates who do not want them. Some voters do not go to the polls to vote for personal or public reasons. One solution to this problem is Internet voting (I-voting) where it can be voted from anywhere and anytime.

Internet voting has many advantages and certainly, there are disadvantages. Many I-voting systems have been proposed, but their use is low and not widespread in the world. This is due to the lack of confidence on the Internet among voters because it is possible that the system is being attacked from anywhere in the world and also not everyone in the world uses the Internet. This paper includes an up to date survey on I-voting systems and their related security characteristics and concerns. In accordance, it can be concluded that when designing an I-voting system, the most important thing to be considered is voter confidence in the system by proving to them that the system is safe and can withstand any attack and should also be transparent, accurate and better than traditional voting.

Keywords: Blind signature, electronic voting, internet voting, homomorphic encryption, security

RESUMEN/ Votar es el proceso a través del cual se eligen representantes del país. Toda persona tiene derecho a elegir candidatos que considere adecuados para liderar el país. Debe garantizarse que las elecciones sean justas y que los votos no sean manipulados, eliminados o modificados, o incluso que los votantes se vean obligados a votar por los candidatos que no los quieren. Algunos votantes no acuden a las urnas para votar por razones personales o públicas. Una solución a este problema es la votación por Internet (I-vote) donde se puede votar desde cualquier lugar y en cualquier momento.La votación por Internet tiene muchas ventajas y, ciertamente, hay desventajas. Se han propuesto muchos sistemas de votación I, pero su uso es bajo y no está muy extendido en el mundo. Esto se debe a la falta de confianza en Internet entre los votantes porque es posible que el sistema esté siendo atacado desde cualquier parte del mundo y que no todos en el mundo usen Internet. Este documento incluye una encuesta actualizada sobre los sistemas de votación I y sus características y preocupaciones de seguridad relacionadas. De acuerdo con esto, se puede concluir que al diseñar un sistema de votación I, lo más importante a considerar es la confianza de los votantes en el sistema al demostrarles que el sistema es seguro y puede resistir cualquier ataque y también debe ser transparente y preciso. y mejor que la votación tradicional.Palabras clave: firma ciega, votación electrónica, votación por internet, encriptación homomórfica, seguridad

1. Introduction

Voting is one form of democracy that ensures that people choose a person to rule or make decisions instead of them. Therefore, the vote is very important and there must be fair elections that are not manipulated so as not to choose a corrupt person. At first, a paper voting appeared, which used paper to vote, this method is expensive and requires voters to come to the ballot stations, but also have advantages such as transparency and secrecy. This system is acceptable and is used today in many countries.

As technology has grown and entered almost everywhere, the electronic voting system has emerged, which in turn has facilitated many things, including ease of use, the speed of counting and low cost. One form of electronic voting is Internet voting (I-voting), which means that elections are held from anywhere, at any time and on any device. This procedure provides many facilities to ensure the participation of the largest segment of people in the elections, such as the participation of people with special needs or if the polling stations are far from voters and many problems.

Despite the many benefits of the I-voting, it is not widespread in the world, and there are few countries that use it like Estonia and Switzerland. Building an I-voting system is not easy. The security level must be high, transparent, easy to use and, most importantly, voters must trust it and use it instead of the paper ballot. At present, the paper voting process cannot be cancelled and replaced by an I-voting due to the digital divide, but it needs more time to ensure its effectiveness and voters confidence in this system. It is therefore used in some countries as a supplement to a paper ballot.

In this paper, an up to date survey of I-voting schemes is presented. Various security aspects, constructions, and concerns are considered. The remaining of this paper is organized as follows: Section 2 reviews some important literature. The I-voting basic model, characteristics, and requirements for I-voting are introduced in Section 3. Next, Section 4 presents the strengths and weaknesses of I-Voting. The primary cryptographic techniques used in I-voting systems are considered in Section 5. Then, Section 6 explores some important I-voting schemes. Some final issues are discussed in Section 7 before concluding the paper in Section 8.

2. Related work

In the literature, it is possible to many papers talking about I-voting. Some of them considered specific I-voting proposals and implementations. Others have focused on security aspects and/or cryptographic constructions. Moreover, few survey and review papers have been published. However, each of these has its own interesting aspects and limitations. In this section, some of these papers are reviewed. Others will be mentioned in respective sections.

In 2008, Helios was proposed as the first open voting system on the Internet. Any person can set up and hold an election and any observer can review the whole process. It has been claimed to be ideal for online software communities, local clubs, student government and other environments that require secret and credible elections [1].

Some researchers suggested an I-voting plan that allows voters to vote using cloud computing to meet the security requirements. The advantage of this proposal is that it consumes less time and results in faster voting and less spending [2]. Another I-voting system had been proposed based on reliable web services. It was designed with reliability block diagrams and reward Petri nets. Voting requirements such as confidentiality, mobility, accuracy, uniqueness, and safety were considered. The system is assumed to remain functioning even if some components fail [3].

In order to achieve the principles of democratic voting, the use of an anonymous channel protocol based on the blind signature with certain strengthening elements was also proposed. These elements included smart cards for networks, adaptive interfaces for voters, inspector agents at server side, and vote proof protection for secure receipt usage [4].

Pretty Understandable Democracy (PUD) is a voting system that was suggested to meet security requirements and provide some possibility of verification as two integrity sub-criteria are provided without posing restrictions on the adversary [5]. Other people proposed the use of optical encryption to supply mutual authentication to servers of election and voters. They suggested to use their system by corporate companies to hold elections to fill various positions like manager elections, presidential elections and so on [6].

An extension of Estonia's electronic voting protocol had been introduced allowing voters to verify the cast-as-intended and recorded-as-cast properties of their vote by using a mobile device. The scheme was used during the 2013 Estonian local municipal elections and the 2014 European Parliament elections [7].

An earlier work proposed an algorithm to generate unique and unknown identifiers based on the Chinese Remainder Theorem. This had extended the functionality of an election to allow for races with multiple winners. The prototype of this voting system was implemented as a multiplatform web application [8]. Yet, another work introduced a voting system that was assumed to allow voters to verify their vote as tallied-as-intended without the assistance of special software or trusted devices. Additionally, the system aimed to allow voters to delegate auditing to a third party auditor, without sacrificing their privacy [9].

A group of researchers described the implementation aspects, the main challenges and the adopted solutions for an I-voting system designed for specific elections a Land Reclamation Authority in Italian Emilia Romagna region [10]. Another group considered an I-voting portal including server and database execution in India. They analyzed the portal and discussed various types of problems with voting systems over the Internet [11].

However, the issue of assessing the risk of any I-voting system is crucial. One approach in this respect is to generate and validate the general threat tree facing I-voting systems. Indeed, the test has to achieved by a committee of election officials, security experts, and academics, electoral law attorneys, voting equipment vendors and testing equipment testing equipment [12].

It is prudent to assume that any I-voting scheme proposal should present many advantages including greater accuracy, better access, lower cost, minimizing human and mechanical errors, and faster classification of results [13]. Some researchers analyzed electronic voting systems and found many problems related to integrity and voter privacy. They also identified the relevant advantages such as accuracy and flexibility against corruption and power against unauthorized voting [14]. Others studied the issue of providing security against all types of attacks when the vote moves from client to server [15].

3. I-Voting Basic Mode, Characteristics, and Requirements

The basic participants in the elections are the voters and the authorities. Thus, it is possible to consider the following terms [16]:

- *Votes:* Voting is the process of answering questions in elections and selecting candidates. The structure of votes depends on the type of election.
- *Voters:* Voters do not want to annoy themselves with a complex election process so it should be easy and simple. Voters can abstain if they want. Also, all information about voting must be confidential and no one can access it.
- *Authorities:* The authorities are the people who run the election process and are keen to protect it from attacks and they are also voters who are sometimes entitled to vote.

Typically, the main phases of I-voting consists of [16]:

- *Initialization phase:* In the first phase of the elections, the system is established, the secret and public keys are set up, the persons eligible to vote are declared, and the questions and answers are formulated. All this is done by the authorities.
- *Voting phase:* In the second stage, eligible voters will have access to a system to vote, and the votes will be sent to the relevant authorities for the next stage.
- *Counting phase:* In the last stage, the authorities reach the votes using secret and general keys, and then these votes are counted and the final result is published where the voters can make sure that their votes have been counted.

The main characteristics of I-voting are [17]:

- Providing an easy-to-use environment that for Internet-based systems is reachable through a traditional WWW browser.
- Counting the final vote tally after the end of the election automatically.
- Supporting all the required services for conducting and organizing the process of opinion expressing. Relying on the process of election these services may be registration of the voter, authentication of the voter, casting the vote, calculation of the vote tally and verification the result of the election.
- Assisting the voter by supporting collaborative techniques, and all relevant behavioural and social aspects must be taken into account.
- Supporting the active participation in the elections, including representatives of parties, voters, candidates, election organizers, and administrators (monitoring voting centres, managing eligible voters and voting areas, ballot generation and management, remote voting areas, etc.)

However, there are many opportunities for corruption while performing these tasks. Election organizers may permit the registration of unqualified voters or allow voters to vote more than once. Achieving privacy and security is not easy if the system is not properly built and is easily hacked. This could corrupt the voting process and violates the privacy of the voter. A secure and efficient voting protocol for the voting system should be implemented to prevent fraud and violation of voter privacy. In this respect, it can be shown that I-voting needs the following requirements [2],[13],[18]:

- *Accuracy:* Votes must be recorded in the system and only valid votes are counted.
- *Eligibility:* Only eligible voters have the right to vote.
- *Reliability:* Even if the system encounters a failure it must be able to continue working.
- *Coercion-Resistance:* The voter must not be forced to choose a candidate he/she doesn't want. There must be no proof of how voters voted.
- *Privacy:* The voter's vote must not be known by anyone and remains hidden.
- *Flexibility:* The system must accept different formats used.
- *Receipt-Freeness:* The voter must not be given anything that proves his/her vote to a particular person because it can be used by the coercer against him.
- *Completeness:* Calculating all valid votes correctly.
- *Auditability:* Election records must be reliable.
- *Integrity:* After the election, there must be no deletion, replacement or removal of votes.
- *Uniqueness (Unreusability):* Each voter is entitled to vote once.
- *Verifiability:* After the election is over, there must be a possibility to verify the election and that the votes have been counted correctly.
- *Anonymity:* No one should know who voted in the elections.
- *Secrecy:* No one can know how voters voted in elections.
- *Fairness:* Only the final result is announced and there are no partial results.

4. Strengths and Weaknesses of I-Voting

On one hand, I-voting has many advantages. These include a potential for competent authorities, better accessibility, transparent results, and strong credentials. These can be described as follows:

- *Qualification of Authorities:* Usually, I-voting requires a small number of employees. I-voting system is monitored by specialized and competent people. It also requires fewer resources than traditional voting, which requires more resources, more voting staff, and security personnel to protect the voting process [19].
- *Accessibility:* I-voting is done from anywhere and from any device, so it provides voters with comfort and also increases voter turnout because, in the traditional vote, voters must go to polling stations that may be far from them and difficult to reach, especially by people with special needs or the elderly [20].
- *Transparent Results:* I-voting allows voters to verify the election results after the results are announced and to ensure that their votes are counted correctly, using encryption techniques, thus making the elections transparent and visible to the voters, without revealing the identity of voters. On the contrary, in the traditional elections, voters have to accept the final result without verifying it or knowing how votes have been counted [21].
- *Strength of Credentials:* In I-voting, secure authentication systems are used, so only qualified people are entitled to vote for one time only, and this reduces the sale of votes. In traditional elections, credentials used for the purpose of voting are not sufficiently secure and can be easily falsified and used by impostors [14].

On the other hand, there are many weaknesses in I-voting systems. The existence of data on the Internet itself puts it at risk. It can be attacked from anywhere and at any time. Many believe that an online voting system is unsafe and cannot be useful, but if the system is built properly, weaknesses can be overcome. The attacks on an I-voting system can generally be categorized into two types:

- *Client-side attacks:* Client-side attacks include counterfeit sites used for election or harmful technical support. Voters can be intimidated and forced to vote for a particular person, their credentials may be stolen, and unscrupulous voters sometimes sell their votes for money. A large group of people do not care about the elections. People can be taught how to use websites to counter malicious web attacks, as well as using methods to prevent coercers from forcing voters to vote for them, but selling votes is extremely dangerous and difficult to prevent [12].
- *Server-side attacks:* The attack on the server is more dangerous since one problem can lead to a complete system crash. If the attacker breaks the voting system, he/she can manipulate the election and its results. This can be avoided by providing strong system protection as well as sound management. In fact, there is nothing to guarantee the security of I-voting, but it can be more efficient than traditional voting since the latter is not safe either because ballot boxes are placed in places that are not safe enough and can easily be accessed, stolen or burned [14].

One of the serious attacks on I- voting systems is the denial of service attack (DoS). This attack can affect voting in two different ways. The first is when the attacker changes the network connection to a particular Web site to non-important data that prevents the user from accessing the site and casting her/his vote. What makes this attack serious is that it can be operated automatically by the computer (or cooperated computers). The second is that the attacker places irrelevant information on useless tasks at the election site so that the server remains busy and this may prevent voters from voting [22].

5. Primary Cryptographic Techniques

Some of the primary cryptography techniques typically used in I-voting systems are: homomorphic encryption, mixnets, and blind signature. The relevant I-voting schemes are described in the following subsections.

5.1 Homomorphic Encryption Based Schemes

There are many I-voting schemes hiding the contents of the ballot instead of hiding the identity of the voter. These cards are traceable and linked to the identity of the voter so that the possibility of verification can be achieved. But sometimes voter privacy can violate that when calculating election results the ballot is decrypted. The ballot is encrypted with a homomorphic encryption function to avoid this. A cryptographic function E is called ($\otimes$, $\oplus$)-homomorphic if the following equation holds for any two plaintext T_1,T_2:

$$E\ (T_1) \otimes E\ (T_2) = E\ (T_1 \oplus T_2) \qquad (1)$$

Usually, but not necessarily, the operator's $\otimes$ and $\oplus$ represent modular multiplication and addition, respectively. Encrypted ballots are multiplied together and the result is a result of the encrypted election. I.e. can calculate the result without decoding the ballot. But the addition restricts the votes by yes or no (1 for yes and 0 for no), while it is necessary to prove that the encrypted ballot paper actually includes such a ballot and not an arbitrarily large value [17].

The encrypted result can be distributed to several authorities so that it can only be decrypted when there are coalitions of a certain size because if the system is under corrupt authority it will fail. One of the advantages of homomorphic encryption based schemes is that votes cannot be counted before they are cast. Indeed, counting steps are unpretentious. On the negative side, there is a worry about the use of a zero-knowledge proof in the I-voting schemes. Furthermore, these schemes are vulnerable to attacks like RSA blinding attack.

5.2 Mixnet Based Schemes

Mixnets are based on public key cryptography, thus providing the non-tracking and hide identity. Mixnet is a multi-party communication protocol that takes input messages and arranges them randomly. None of these parties knows anything about the mixing algorithm, but only know that it has been mixed [23].

Mixnet uses anonymous channels to communicate where the sender's information is hidden, and no one even the recipient can find out or back to the sender's address. This is done through nodes that take the message and return it in random order. The sender sends the message and passes it through the node. This node switches the order of the contents of the message and sends it to the second node, and so on. When the message reaches the last node, it sends it to the recipient. If one node works correctly, it is possible to make sure that the sender's identity is hidden [16]. There are two main categories of Mixnet [24]:

- *Decryption Mixnet:* The contract in this category contains a pair of public and private keys. The keys are distributed by the public key infrastructure. Let pub_i be the public key and $priv_i$ the private key for the *i*-th node, and r_i be a random padding. The encryption protocol works as follows if a voter sends a message *m* through five nodes:

$$m_{enc}= E_{pub1}(r_1, E_{pub2}(r_2, E_{pub3}(r_3, E_{pub4}(r_4, E_{pub5}(r_5, m))))) \qquad (2)$$

The message will be encrypted in layers, and in the correct order, the encrypted message will be passed, the message is decrypted through the nodes and the last node delivers the message. When using private keys, the protocol works the same way.

- *Re-encryption Mixnet:* It is also made up of several nodes and mixes messages and passes them. In this category, the message is re-encrypt in each node and sent to the next node instead of decrypting it when it is received from the previous node. For this, it can be guaranteed hide identity if only one node has its work properly. ElGamal is one example of a re-encryption Mixnet deployment.

The advantages of these schemes are that they do not require that the phases to be sequential and the use of mixing makes votes not tied to voters. There disadvantages are that their accommodation of large messages is inefficient and the input needs multiple encryptions.

5.3 Blind Signature Based Schemes

Blind signature [25] is a type of digital signature and is used in many I-voting schemes, where the message is signed without disclosing its contents and thus achieve privacy. It will not be known whom the voter votes for because the authorities blindly signed the voter's vote.

Presently, blind key signature schemes exist with many public key protocols. One of these is the use of traditional RSA with the blind RSA Scheme. Let (*N, e*) be the public key of authority and (*N, d)* be his private key where *d* is the inverse of *e* mod ϕ(*N*). The voter need to select a random number *r* such that gcd (r, N) = 1, and sends the following to the authority:

$$v' = v \cdot r^e \ mod \ N \qquad (3)$$

The random number *r* is used to hide the ballot *v* from the authority. Next, the authority signs the blinded ballot after verification and sends back S'.

$$S' = (v')^d = v^d \cdot (r^e)^d = v^d \cdot r \ mod \ N \qquad (4)$$

After receiving S', the voter now can unblind it to get the true signature *S* since she/he knows *r*.

$$S = S' \cdot r^{-1} = v^d \cdot r \cdot r^{-1} = v^d \ mod \ N \qquad (5)$$

To achieve more privacy anonymous channels can be used. The voter will submit a vote to Mixnet after signing it. At the end of the ballot, Mixnet will process the encrypted votes. Votes are decrypted by the authorities and the voting results are then published [18]. Blind signature based schemes are simple and can be efficiently implemented. However, universal verifiability is difficult to carry out and the signer controls only the features associated with the public key.

6. I-Voting Schemes

In this section, some important I-voting schemes are reviewed with a summary of their analysis.

- *Helios:* Helios is a web-based voting system [1]. Voters use the browser to run it and send their votes. Its protocol is comparable to Benaloh's simple verifiable voting protocol [26]. It uses Mixnet to hide the identity of the voter. It provides individual verifiability and universal verifiability so voters can make sure that their vote has been received. Voters can verify the validity of votes without any credentials. But it is not suitable for high-coercion elections.
- *VoteBox:* VoteBox [27] is a system that provides auditability and robustness in the case of faulty initialization, manipulation or failure because it uses frequent logs and a distributed broadcast network. Vote decryption keys can be distributed to mutable unreliable parties. In order for the voter to ensure that his or her vote has been received as intended, the system uses an immediate challenge to vote. The system provides receipt-freeness. Privacy and coercion-resistance are also achieved because it is assumed that there is a voting booth.
- *Civitas:* Civitas [28] uses a digital signature to preserve the integrity, as well as uses a publicly viewable record service like a bulletin board. Through many cases of zero-knowledge proof (ZKP), protocol compliance is enforced. The voter creates false credentials by using his private key and running an algorithm and these cards

are used to resist coercion. All votes adopted on false credentials are excluded. In this scheme, the resistance of coercion is achieved through false credentials, as well as verifiable through the bulletin boards. Figure 1 shows the Civitas architecture.

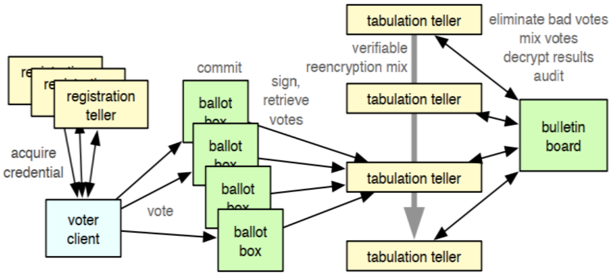

Figure 1. Civitas architecture [28].

- *Prêt á Voter:* Prêt á Voter [29] uses a random candidate list to encode the voter's voice. Confidentiality is guaranteed by randomization. The voter ensures that his vote has been received after voting at the voting booth by giving him a receipt. By using encrypted receipt, voters can re-vote. Secret cryptographic keys are shared over multiple tellers. Voters check their votes after it has been posted on the bulletin board. All voter receipts are taken by tellers and decrypted, and then calculated after application of the mix network. This scheme offers the possibility of resisting coercion and privacy because it assumes the existence of the voting booth and also provides the receipt-freeness and end-to-end verifiability.
- *Multi-Authority E-voting System:* This scheme overcomes conspiracy and ensures privacy because elections are controlled by multiple parties [30]. It uses homomorphic encryption. Using the ElGamal Digital Signature Algorithm (DSA), the voter's ballot is signed and encrypted with the additive ElGamal scheme. Completeness and fairness are ensured. Voters are allowed to vote only once, but opponents can use these votes in their favour, and voters do not have a means of defence against coercion. This schema uses ZKP. The architecture of this system is shown in Figure 2.

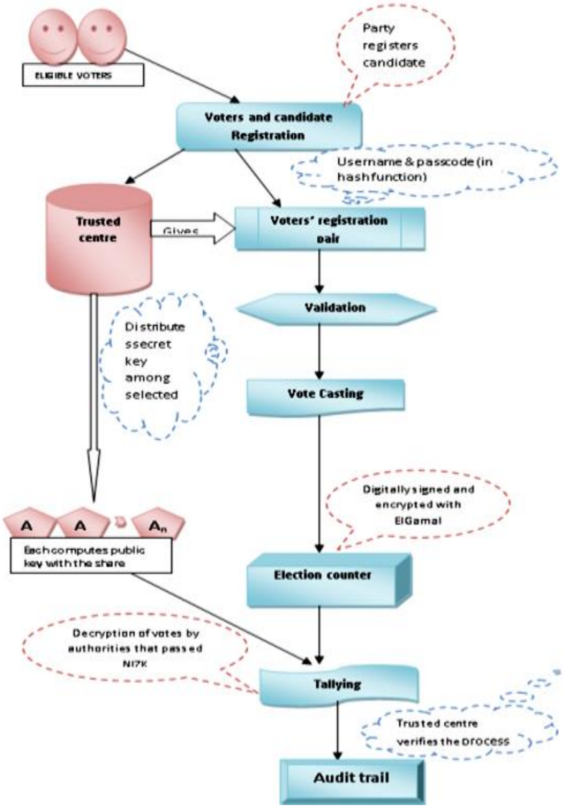
ELIGIBLE VOTERS
Party registers candidate
Voters and candidate Registration
Username & passcode (in hashfunction)
Trusted centre
Gives
Voters' registration pair
Validation
Distribute ssecret key among selected
Vote Casting
Digitally signed and encrypted with ElGamal
A
A
An
Each computes public key with the share
Election counter
Decryption of votes by authorities that passed NIZK
Tallying
Trusted centre verifies the process
Audit trail

Figure 2. Multi-Authority E-voting System architecture [30].

- *Secure Internet Voting Using DSA Public Keys:* By mixing the DSA public keys, this scheme hides the identity of the voter [31]. Credentials of votes consist of a simple DSA public keys. As a result of mixing, a list of anonymous keys that the voter can use to verify his signature is created, but these keys cannot be assigned to individual voters. Receipt-freeness and universal verifiability are provided in this scheme, but resistance to coercion is dubitable.
- *E-NOTE:* E-NOTE [32] is a scheme that prevents the collusion of the authorities and also Leaks privacy through the use of two levels of security measures. E-NOTE is an improved version of NOTE (Name and vOte separaTed E-voting scheme) [33], where privacy concern can be wiped out while calculating votes by separating votes from names on the ballot. To eliminate fraud all voting transactions are registered. Registration is done by the authorities and a certificate is given to voters. Voters receive a ballot through this certificate. There is no correlation between the voter's certificate and his identity, so this scheme guarantees confidentiality. The electronic ballot made up of three

sections. The votes are sent to vote counting committee (VCC) but can only decrypt one section of the voting data. Voters can be protected from enemies, also the privacy is achieved because evaluation is done without matching the vote with the voter. To achieve confidentiality each voter is given a watchdog by the election commission. Receipt-freeness is not carried out because the voter gets a receipt to track and review his vote. Also, coercion resistance is not achieved.

- *UVote:* At this scheme [34] voters register in advance and can vote more than once but give priority to voting from the polling station or the last vote. When voters vote from polling stations, this prevents coercion. Because the voter can vote again, this prevents the sale of votes. The voter creates the main account by his e-mail or his phone number to register and also can create other accounts later. To resist coercion, the voter uses his or her main account. The account is verified by sending messages and alerts to the main account and can't be deleted. Each voter receives a unique identification number to access the election site and also receives a public and private key for encryption and decryption. In this scheme, universal and individual verification is achieved, also fairness is achieved because partial results are not announced. The voter is given a receipt and thus receipt-freeness is not achieved (See Figure 3).
- *Cobra:* Cobra [35] is a scheme where voters must register by constructing and presenting encrypted credential. These credentials are added to the encrypted Bloom filter [36], [37] homomorphically. A voter chooses a password to register from among several candidate passwords. The votes are encrypted and by using the password, the voter re-produce the credential. When the voter is subjected to coercion, he can give the imposter a false password, so this scheme is coercion resistant. Anonymous channels are used to send votes. Authorities count the votes. Homomorphically, the credentials are added and decrypted, and the results are announced. Final results can be verified.
- *Zeus:* Zeus [38] is a web-based system, where voters register their private and public keys by visiting the website. The recorded key is compared with the hash value by the browser. This scheme is similar to Helios and uses the same encryption techniques. The mixing process is carried out by external authorities and the Zeus system. When the mixing process is completed, trustees are notified for decryption. Encryptions are collected by Zeus and the results are announced. External algorithms can be used to advertise results. In this scheme, universal verification is achieved because the results are published on the bulletin board. Because the voter gives an encrypted receipt, it does not achieve receipt-freeness.

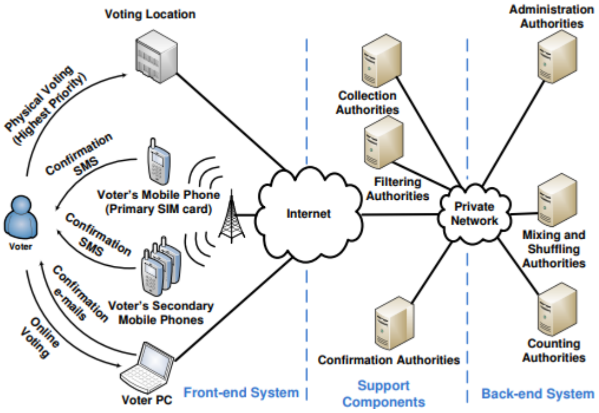

Figure 3. UVote architecture [34].

7. Discussion

After presenting this survey in the field of I-voting, one can conclude that despite the development in technology, there are still many challenges faced by I-voting such as voter confidence, confidentiality, transparency, privacy, and the authorities that monitor the whole election process. Hence, solutions must be found for all or most of these challenges in order to make people move to use I-voting in elections instead of traditional voting.

Voters' Confidence in I-Voting: Confidence in the voting system is essential for elections, but this is a complicated issue since not all voters have full knowledge of the Internet or know how to use it. Indeed, there are a few of them who trust in the Internet. Some measures must be taken so that everyone can trust the Internet. Some independent institutions and experts can play an important role in this because voters trust them. One way to make voters trust the system is to make public information available to the public. And that this system is reliable and there are certificates proving its effectiveness and security against attacks and cannot be manipulated.

Privacy and confidentiality of voting: Conducting elections in non-supervised environments increases the violation of privacy of the voter and there is nothing to prove that the voter was alone when he voted and this increases the fears of I-voting. This can be reduced by allowing the voter to vote more than once and count his last vote or by forming false election cards used by the voter if he/she is forced to vote by the abusers.

Access to the Internet: This point is referred to as a point of strength for I-voting because access to the voting system is from anywhere and from any device, which increases the participation of voters with disabilities, elders, or even ordinary voters who are living or working away from polling stations. However, not all voters have reliable Internet access and/or Internet devices that can be used whenever needed. Thus, the digital divide must be taken into account (not all voters have knowledge of the computer). Also, building a system that works on all different operating systems is difficult. This can be solved or mitigated by putting computers in remote areas that voters can use at the time of elections. Training courses can also be held to teach people who do not have Internet knowledge before the elections and teach them how to use the voting system.

The role of the authorities in the elections: The role of the authorities is an important thing in the voting process as they run the election process and they can do anything. If the authorities are corrupt this means that they can manipulate the election results and make them in favor of any candidate they want. Therefore, they must be fair, independent, transparent, and not affiliated to any party. The authorities must somehow be monitored during the elections and during counting and announcement of the results to ascertain their work. Building an I-voting system that meets all these requirements is difficult but not impossible, as the world is constantly evolving and it makes no sense for the vote to remain the same. Some countries have already started using this system as long ago as Estonia and Switzerland. Other countries may use it in the future.

8. Conclusion

I-voting is an important step in the development of this world and it is natural to replace traditional voting or at least be complementary to it. Therefore, it is necessary to build strong systems that are secure, safe, reliable, transparent, and which voters can trust and use comfortably. In previous years and so far, many I-voting systems have been proposed and each has its own advantages and disadvantages. In this survey paper, we have reviewed some of these systems in addition to their characteristics, requirements, strengths, and weaknesses. Our next step is to develop an I-voting system with enhanced security features and usability requirements that can be proposed for wide range of election tasks.

References:

[1] B. Adida, Helios: Web-based Open-Audit Voting, USENIX Secur. Symp. 17 (2008) 335–348.

[2] S. Ramesh, V. Muralibhaskaran, Internet voting using cloud computing, Sustain. Energy Intell. Syst. (SEISCON 2011), Int. Conf. (2011) 799–802.

[3] A. Omidi, Modeling and Quantitative Evaluation of an Internet Voting System Based on Dependable WebServices, International Conference on Computer and Communication Engineering (ICCCE) (2012) 3–5.

[4] M. Huarte, I. Goirizelaia, J.J. Unzilla, J. Matías, J.J. Igarza, A new fully auditable proposal for an Internet voting system with secure individual verification and complaining capabilities, Secur. Cryptogr. (SECRYPT), 2013 Int. Conf. (2013) 1–8.

[5] M.F.M. Mursi, G.M.R. Assassa, A.A. Abdelhafez, K.M. Abosamra, A Secure and Auditable Cryptographic-Based e-Voting Scheme, Proc. - 2015 2nd Int. Conf. Math. Comput. Sci. Ind. MCSI 2015. (2016) 253–262.

[6] A.B. Rajendra, H.S. Sheshadri, Visual Cryptography in Internet Voting System, Third Int. Conf. Innov. Comput. Technol. (INTECH 2013). (2013) 60–64.

[7] S. Heiberg, j. Willemson, Verifiable Internet Voting in Estonia, 2014 6th Int. Conf. Electron. Voting Verif. Vote. (2009) 1–7.

[8] K. Butterfield, H. Li, X. Zou, F. Li, Enhancing and implementing fully transparent internet voting, Proc. - Int. Conf. Comput. Commun. Networks, ICCCN. (2015) 0–5.

[9] N. Chondros, B. Zhang, T. Zacharias, P. Diamantopoulos, S. Maneas, C. Patsonakis, A. Delis, A. Kiayias, M. Roussopoulos, D-DEMOS: A Distributed, End-to-End Verifiable, Internet Voting System, Proc. - Int. Conf. Distrib. Comput. Syst. (2016) 711–720.

[10] C. Taddia, D. Ferraretti, M. Pastorelli, S. Nanni, G. Mazzini, Secure Management of an Internet Voting System: A Case Study for Land Reclamation Authority, 2017 25th Int. Conf. Software, Telecommun. Comput. Networks. (2017) 1–5.

[11]V.P. Singh, H. Pasupuleti, N.S.C. Babu, Analysis of internet voting in India, Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017. (2018) 1–6.

[12]Harold Pardue, Alec Yasinsac, and Jeffrey Landry, Towards internet voting security: A threat tree for risk assessment, 2010 Fifth International Conference on Risks and Security of Internet and Systems (CRiSIS). IEEE, (2010).

[13]M.I. Ahmed, M. Abo-Rizka, Remote Internet Voting: Security and Performance Issues, World Congress on Internet Security. IEEE (2013) 56–64.

[14] K. Butterfield, X. Zou, Analysis and implementation of internet based remote voting, Proc. - 11th IEEE Int. Conf. Mob. Ad Hoc Sens. Syst. MASS 2014. (2015) 714–719.

[15]S.M. Jambhulkar, J.B. Chakole, P.R. Pardhi, A secure approach for web based internet voting system using multiple encryption, Proc. - Int. Conf. Electron. Syst. Signal Process. Comput. Technol. ICESC 2014. (2014) 371–375.

[16]Z. Rjašková, Electronic voting schemes, PhD thesis, Comenius University, Bratislava, (2002).

[17]C. Lambrinoudakis, V. Tsoumas, M. Karyda, S. Ikonomopoulos, Secure Electronic Voting: The Current Landscape, Advances in Information Security book series (ADIS), 7 (2003) 101–122.

[18]A. Schneider, C. Meter, and P. Hagemeister, Survey on Remote Electronic Voting, arXiv preprint arXiv:1702.02798. (2017).

[19]Nevo, Saggi, and Henry Kim. How to compare and analyse risks of internet voting versus other modes of voting. EG 3.1 (2006): 105-112.

[20]W. Bokslag, M. de Vries, Evaluating e-voting: Theory and practice, arXiv preprint arXiv:1602.02509 (2016).

[21]S. Mudana, Security Flaws in Internet Voting, Report, Computer Science Department, University of Auckland. 1-11.

[22] R. Aditya, B. Lee, C. Boyd, E. Dawson, An Efficient Mixnet-Based Voting Scheme Providing Receipt-Freeness, Trust Priv. Digit. Bus. (2004) 152–161.

[23] Ogudo, K.A.; Muwawa Jean Nestor, D.; Ibrahim Khalaf, O.; Daei Kasmaei, H. A Device Performance and Data Analytics Concept for Smartphones' IoT Services and Machine-Type Communication in Cellular Networks. *Symmetry* **2019**, *11*, 593.

[24] Ayman Dawood Salman1, Osamah Ibrahim Khalaf and Ghaida Muttashar Abdulsahib, 2019. An adaptive intelligent alarm system for wireless sensor network. Indonesian Journal of Electrical Engineering and Computer Science, Vol. 15, No. 1, July 2019, pp. 142~147

[25]D. Chaum, Blind Signatures for Untraceable Payments, Advances in Cryptology, Springer, Boston, MA. (1983) 199–203.

[26]R. Küsters, T. Truderung, An epistemic approach to coercion-resistance for electronic voting protocols, Proc. - IEEE Symp. Secur. Priv. (2009) 251–266.

[27] Osamah Ibrahem Khalaf, Ghaidaa Muttasher et al., "Improving video Transmission Over Heterogeneous Network by Using ARQ and FEC Error Correction Algorithm‟, vol. 30, no.8, pp.24-27, Nov 2015

[28]M.R. Clarkson, S. Chong, A.C. Myers, Civitas: Toward a secure voting system, Proc. - IEEE Symp. Secur. Priv. (2008) 354–368.

[29] GHAIDA MUTTASHAR ABDULSAHIB and OSAMAH IBRAHIM KHALAF, 2018. AN IMPROVED ALGORITHM TO FIRE DETECTION IN FOREST BY USING WIRELESS SENSOR NETWORKS.International Journal of Civil Engineering & Technology (IJCIET) - Scopus Indexed.Volume:9,Issue:11,Pages:369-377.

[30]A.A. Philip, S.A. Simon, A Receipt-free Multi-Authority E-Voting System, Int. J. Comput. Appl. 30 (2011) 15–23.

[31]R. Haenni and O. Spycher, Secure internet voting on limited devices with anonymized DSA public keys, 2011 Electron. Voting Technol. Work. / Work. Trust. Elections, EVT/WOTE '11, San Fr. (2011).

[32]H. Pan, E. Hou, N. Ansari, E-NOTE: An E-voting System That Ensures Voter Confidentiality and Voting Accuracy, 2012 IEEE Int. Conf. Commun. (2012) 825–829.

[33] Osamah Ibrahim Khalaf, Bayan Mahdi Sabbar''An overview on wireless sensor networks and finding optimal location of node'',Periodicals of Engineering and Natural Sciences, Vol 7, No 3 (2019)

[34]R. Abdelkader, M. Youssef, UVote: A ubiquitous e-voting system, Proc. - 2012 3rd

FTRA Int. Conf. Mobile, Ubiquitous, Intell. Comput. Music 2012. (2012) 72–77.

[35]A. Essex, J. Clark, U. Hengartner, Cobra: Toward concurrent ballot authorization for internet voting, Proc. 2012 Int. Conf. Electron. Voting Technol. Trust. Elections, EVT/WOTE. (2012) 3.

[36]W. Itani, C. Ghali, A. El Hajj, A. Kayssi, A. Chehab, SinPack: A security protocol for preventing pollution attacks in network-coded content distribution networks, GLOBECOM - IEEE Glob. Telecommun. Conf. (2010) 1 - 6.

[37]H. Perl, Y. Mohammed, M. Brenner, M. Smith, Fast confidential search for bio-medical data using bloom filters and homomorphic cryptography, 2012 IEEE 8th Int. Conf. E-Science. (2012) 1 - 8.

[38]Osamah Ibrahim Khalaf, Ghaida Muttashar Abdulsahib and Muayed Sadik, 2018. A Modified Algorithm for Improving Lifetime WSN. Journal of Engineering and Applied Sciences, 13: 9277-9282