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

A Framework for I-Voting based on Helios and Public-Key Certificates

Un marco para I-Voting basado en Helios y certificados de clave pública

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

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

ABSTRACT/ With the development of technology, so-called electronic voting has emerged. Of particular interest to us is Internet voting (I-voting) because this method contributes to raising the percentage of voters as they can vote from anywhere and from any device, thus providing them with comfort. Indeed, the speed of counting is quick and results can be announced within a short period of time. Many voting systems have appeared in recent years but the most famous was Helios because it is open source, online available, and anyone can use it to create elections. It is a powerful and reliable system and has many features but also contains some limitations such as it is used in low coercion elections only.

In this paper, a general framework for I-voting based on the Helios voting system and public key certificates is proposed. In this framework, Helios is suggested to be linked with a certification authority to provide the necessary keys for digital signature and vote encryption. Furthermore, each voter is suggested to have the possibility to have more than one voting account, one of which is a real voting account. The others are fake accounts that might be used by the voter in case of coercion. If a voter uses the fake account to vote, her/his vote will not be counted in the final votes. We also improve the Helios interface by simplifying it, adding more explanation to each step used in voting, and adding an Arabic interface so that Arab people can use the system more easily.

Keywords: Certificate Authority; Helios; Internet Voting, Multi-Accounts; Public Key Certificates.

RESUMEN/ Con el desarrollo de la tecnología, surgió el llamado voto electrónico. De particular interés para nosotros es la votación por Internet (I-vote) porque este método contribuye a aumentar el porcentaje de votantes, ya que pueden votar desde cualquier lugar y desde cualquier dispositivo, lo que les brinda comodidad. De hecho, la velocidad de conteo es rápida y los resultados pueden anunciarse en un corto período de tiempo. Muchos sistemas de votación han aparecido en los últimos años, pero el más famoso fue Helios porque es de código abierto, está disponible en línea y cualquiera puede usarlo para crear elecciones. Es un sistema potente y confiable y tiene muchas características, pero también contiene algunas limitaciones, ya que se usa solo en elecciones de baja coerción.

En este documento, se propone un marco general para la votación I basado en el sistema de votación Helios y los certificados de clave pública. En este marco, se sugiere que Helios se vincule con una autoridad de certificación para proporcionar las claves necesarias para la firma digital y el cifrado de votos. Además, se sugiere que cada votante tenga la posibilidad de tener más de una cuenta de votación, una de las cuales es una cuenta de votación real. Las otras son cuentas falsas que el votante podría utilizar en caso de coerción. Si un votante usa la cuenta falsa para votar, su voto no se contará en los votos finales. También mejoramos la interfaz de Helios simplificándola, agregando más explicaciones a cada paso utilizado en la votación y agregando una interfaz árabe para que las personas árabes puedan usar el sistema más fácilmente.

Palabras clave: Autoridad de certificación; Helios; Votación por Internet, cuentas múltiples; Certificados de clave pública.

1. Introduction

Voting is a way for a group of people to choose one or more people to represent them and make decisions on their behalf. There are several ways to vote, most notably paper voting, a method that has some advantages, such as it can be used by all people, even those who do not have experience in technology, there is less possibility to add papers containing false or fake votes, and more

Electronic copy available at: https://ssrn.com/abstract=3459661

importantly, people trust in this kind of voting. However, paper voting has many disadvantages, like it consumes a lot of paper resulting in damage to the environment, its cost is high, and requires a lot of time to count and release the results.

There is a second way to vote which is electronic voting that uses electronic technology to vote. It has many advantages including the speed and accuracy of counting and giving results in hours or less. Also, the cost is low, and the use of cryptographic methods to store votes in an unknown location. On the other side, electronic voting can be vulnerable to penetration. Indeed, not everyone has the experience in technology and can comfortably use this type of voting. Confidence and trust is another challenging issue in this respect. If the company responsible for the voting system is corrupt and the security policies are not correctly enforced, this means giving the possibility of controlling the entire voting process such as adding or deleting votes or even modifying them.

Internet voting (I-voting) is one of the methods of electronic voting and means voting from any device and anytime and anywhere. This can result in an increase in the number of participants in the elections for those who cannot access the polling stations because of its remote location or the voter with special needs. Many I-voting schemes appeared, but few voting systems were successful. One of the most popular voting systems that have been used in real elections is the Helios voting system.

In this paper, we will propose a general framework for I-voting based on the Helios voting system and public key certificates. The main aim is to enhance security, usability, scalability, and anti-coercion aspects of I-voting. The design of the rest of the paper will be as follows: Section 2 reviews some related works. An explanation of Helios' system and steps for its use as well as weaknesses and strengths are presented in Section 3. Next, Section 4 contains a description of the Public Key Infrastructure (PKI), the public key certificates, and digital signature. The proposed framework for I-voting is presented in Section 5. Finally, the paper is concluded in Section 6.

2. Related Work

In the literature, there are many published papers that speak about the Helios voting system. Some of them made proposals and improvements in terms of security and/or the interface. Each one of these researches has its own advantages and disadvantages. In this section, some of these research papers are presented and reviewed.

In 2009, J. Weber [1] discussed the possibility of using Helios in an online election. Fake student elections were created and voters were monitored. Some minor problems related to the interface and the language used has been discovered. Indeed, problems related to educating voters and motivating them to vote, which led to half of the participants in the elections didn't complete their vote, had been reported. A set of recommendations for I-voting was also presented.

D. Bernhard et al presented a study on the security aspect of Helios and presented computational security model for ballot privacy. To avoid the imposition of restrictions required by other methods of definition of protocols, this model used encryption games. It also analyzed an abstract copy of Helios following the same basic structure instead of directly analysing the schema as it was executed. This abstract scheme was presented as a general construction of the voting scheme that has specific functionality and security characteristics [2].

F. Karayumak et al presented the use of the knowledge-based approach of security, electronic voting, and usability experts to analyse the verifiability procedures and usability of the ballot casting of the Helios open-source system. They noticed that the use of Helios in large-scale elections is only done after improvements in the possibility of verification and usability. Moreover, improvements had been proposed on the interfaces of Helios and other voting systems based on their findings [3]. M. Kauer et al presented research on the enhanced Helios interface for individual verifiability and vote casting in the previous work was applied and tested on 34 voters in a mock mayoral election. Before and after the elections voters were given instructions as well as filling out questionnaires. A helmet has been used to track eye movements and data has been collected on time and mouse movement. They argued that the interface is easy to use, while

Electronic copy available at: https://ssrn.com/abstract=3459661

some voters found it difficult to understand the motives behind individual verification [4].

In 2013, C. Loria et al [5] presented a fully distributed threshold encryption system (without a distributor) suitable for the Helios voting system and turned out to be safe under the Decisional Diffie-Hellman assumption. A different type of Helios was proposed allowing for arbitrary threshold parameters, as well as proving the privacy of the ballot when used for referenda. The first open source application for Helios was presented with a fully distributed key generation setup.

In 2014, V. Cortier et al [6] presented Helios-C which is a proposed system similar to the Helios system in its simplicity. It had strong verification capability and ballot privacy. It prevented a problem related to Helios which was the possibility of ballot stuffing. In 2015, O. Kulyk et al [7] proposed the expansion of the Helios system to ensure participation privacy for voters and universal eligibility verifiability. The scheme also improved Helios towards receipt-freeness. They claimed that their proposed system can be used as an independent system or can be used to improve other schemes such as the Estonian voting scheme [8].

M. Backes et al presented the first automated security analysis of the actual JavaScript implementation of the Helios voting client [9]. In 2016, O. Kulyk et al [10] presented an expanded Helios voting system toward proxy voting, thus providing a new type of credential, called delegation authorization data. The proposed system maintained the security requirements of the original Helios system for votes cast directly as well as proxy voting.

N. Chang-Fong et al presented a security analysis of the Helios system and they discovered a range of serious vulnerabilities that attack integrity, availability, and confidentiality. Technical details on weaknesses were provided, and they worked with Helios designers to fix them [11]. However, in 2016, M. Meyer et al [12] showed that the Helios system fails to ensure that representatives are chosen by voters because an opponent can cause a ballot other than a voter's last to be counted. They also explained how the opponent can choose the contents of these ballots, and therefore the opponent can unduly influence the selection of representatives.

D. Bernhard et al presented an extension of the Helios system, known as KTV-Helios. The search was submitted with two contributions: The first was the use of existing definitions of the privacy of the ballot and the possibility of verifying against the bulletin board. The second contribution was to provide an official definition of the receipt-freeness and the privacy of participation, which can be applied to KTV-Helios [13].

L. Panizo et al presented a work to practically and conceptually support the secure, gradual and protocolized expansion of electronic voting [14]. In 2018, B. Smyth et al [15] proved that building voting systems from non-malleable asymmetric encryption schemes suffices for ballot secrecy. They revealed that Helios does not meet the secrecy of the ballot in the presence of an opponent controlling the voting process.

As a summary, our proposed framework in this paper is another step following some of the other previous works aimed to improve Helios in various directions including usability, scalability, and/or security issues. However, it is possible to notice that several shortcoming can still been seen in Helios and its earlier improvements and variations. Therefore, following a holistic approach to enhance Helios based on sophisticated security analysis, best available cryptographic constructions, and most secure and reliable development tools can result in significant enhancement on Helios. This is the approach adopted in this work to build a secure, reliable, and flexible I-voting system framework.

3. Helios System

Helios [16] is an open-source web-based electronic voting system that was released in 2008. Due to its simplicity, availability on internet and usability by anyone, it has been used in many binding elections. It has been used in the student government elections at Princeton University since 2009. Also, it was used by the Catholic University of Louvain to elect their university president in 2009 and it has been used annually since 2010 to elect board members by the International Association of Cryptologic Research (IACR) [17], [18]. Furthermore, the Association for Computing Machinery (ACM) used Helios in the general elections in 2014 [15].

The initial version of Helios was a simple verifiable voting scheme by Benaloh [19] which was inspired by a protocol by Sako and Kilian [20]. The subsequent version of Helios used homomorphic tallying [21] instead of the mixnet-based because the homomorphic

Electronic copy available at: https://ssrn.com/abstract=3459661

tallying sequence is easier to verify when a third party writes the verification code, and also it is easier to implement. Also, to ensure that various trustees are required for decryption, Helios has added a distributed decryption, and this ensures that only the homomorphic tally of all votes is decrypted, and not individual voting at all [22].

3.1 Voting Procedure

In this subsection, the steps and method of voting followed in the Helios system are listed as below [3], [23], [24]:

1. An e-mail is sent to the voter containing the voter-ID, the assigned password, an election fingerprint, and, the URL of the election page.
2. The voter connects to the election web page through the browser. A ballot preparation system (BPS) operates as a service on the browser. The BPS permits the voter to select their choice among the valid votes set.
3. After recording the voter's selection, the BPS encrypts the answers together with some arbitrary data.
4. The voter can now select between audits the ballot or submit.
    - If she/he selects audit: key and the ciphertext are given to the voter, who can now verify if this agrees with the vote she/he wanted to cast. If everything is ok, the BPS proceeds and re-encrypts the options with new arbitrary data, again allowing the voter to select audit or submit.
    - If she/he selects submit, all but ciphertext are enduringly removed.
5. Authentication is requested from the voter, if she/he passes, the encrypted vote is recorded as the vote of the voter.
6. On the bulletin board, voter's encrypted vote is displayed. All cast votes are also shown. Every vote is either associated with the identification number or the voter's name. Anyone who has voted can see her/his encrypted voice on the bulletin board. The voter can check whether her/his vote exists or if it was indeed her/his vote.
7. After the election ends, administrators of election work together to calculate the total number of encrypted votes. This is done through the use of homomorphic encryption and secure multi-party computation.
8. The election results are announced. By using the bulletin board, anyone can verify that her/his vote has been taken into account and that adding votes has been done correctly.

3.2 Strengths and Weaknesses of Helios

The Helios voting system has many strengths that made it one of the best and most popular electronic voting programs, some of which can be mentioned as follows:

- The Helios system is fully open source and allows end-to-end verification [3].
- Using Helios does not require the existence of a physical mail address, any custom hardware, or the installation of any specific program [25].
- Trusting in the server is not required because of the nature of the Helios system where even if system administrators are completely malicious, the voting process still fully verifiable [24].
- Encryption is done using JavaScript, so the user can even disconnect the computer from the Internet after downloading all credentials, making its options, encrypting the vote, and reconnecting the Internet to the vote. So attacks, which need access to the Internet, are useless [26].
- All encrypted votes are shown on the bulletin board. Even during counting, the votes remain encrypted, so the Helios system achieves the Ballot secrecy [27].
- The bulletin board permits only one vote to link with an identity [5].

Despite the strengths of the Helios system, it also has many weaknesses, including:

- Helios does little to save voters from coercion. The coercer can dictate his orders to the voter throughout the election process and verify that the voter has complied with his orders [25].
- Helios does not do much to counteract the threat of a web browser or client-side operating system compromise. A virus can change a user's secret password and cover all checks made on the same computer to hide its paths [22].
- Helios can be accessed over the Internet, making it susceptible to attacks such as denial of service attacks [26].
- Anyone can know who has voted whether the real name or the nickname and that's because the bulletin board is public [28].
- In the future, if the encryption algorithms used in Helios broken, the attacker will be able to decrypt all votes [11].

Electronic copy available at: https://ssrn.com/abstract=3459661

- Helios only aims to achieve the privacy of the ballot and clearly, ignores the concepts of confidentiality in favour of efficiency [2].
- The system can cast votes for non-existing voters or voters who have not cast their ballots because the system cannot fully amend or remove the votes, and voters who have not voted will have to make sure that no vote has been registered by their names [24].

4. Public Key Infrastructure

Public Key Infrastructure (PKI) is a set of encryption technologies, services, and software through which organizations can maintain the security of their business transactions and their connections on the Internet. PKI provides a secure connection to users who are widely distributed and who do not know each other through the use of a common certificate commonly known as a chain of trust. Reliability, non-repudiation, and integrity of data and confidentiality are services provided by PKI to enterprises through the use of digital certificates, which are considered a digital passport containing the user name and some other data according to regulatory policies [29]. The digital signature created by public key cryptography [30], [31] can be verified by the digital certificate.

The PKI consists of the certification authority (CA), the primary part that creates certificates for users and also manages and exports public keys for data encryption as well as secure credentials. The PKI components vary according to the system used, but often consist of the following [32]:

- End Entities: It is the user or anything that needs a digital certificate to identify for any reason such as computers. The end entity uses the certificate provided by the CA in the possible PKI applications.
- Certification Authority (CA): It is an authority that establishes certificates for the end entity after the RA has reviewed their application for certification. It is a trusted authority that creates and manages public keys used to encrypt messages. The CA distributes the certificates to the end entity as well as cancels the certificate if it expires or the end entity request to cancel it or any other reason.
- Registration Authorities (RA): It is the authority that performs the administrative tasks in PKI and it is optional component. RA verifies the request of the end entity of the certificate and decides whether it is eligible to issue a certificate to it.
- Certificate Policy (CP): It is a set of guidelines and rules established by the CA to define the mechanism of work as well as determine who is entitled to obtain a digital certificate and where this certificate can be applied and determines the purpose of the PKI and the security services it supports.
- Certificate Repositories (CR): It is a system that stores digital certificates and it is an optional component in PKI. The entities that deal with are signed by the CA so it does not have to be trusted. It also stores Certificate Revocation Lists (CRL).

4.1 Public Key Certificates

A public key certificate is a digital certificate signed by the CA issued to the final entity. It is used to prove ownership of the public key of the final entity. There are many types of digital certificates approved such as Pretty Good Privacy (PGP) Certificates, X.509 Public Key Certificates, and Simple Public Key Certificates (SPKC). But here we relied on Version 3 of X.509 public key certificates because of its wide use in the PKI systems. As shown in Figure 1, the certificate consists of the following components [33]:

- Version: It distinguishes among consecutive versions of the certificate format.
- Serial number: A unique number used within the CA systems to identify the certificate.
- Signature algorithm identifier: It is defines the algorithm that used to sign the certificate with the related parameters.
- Issuer name: It is used to identify the entity that checked the information and signed the certificate.
- Period of validity: It consists of two fields not before and not after, used to determine the validity date of the certificate.
- Subject name: It is the name of the certificate holder who has the private key corresponding to the public key in this certificate.
- Subject's public-key information: The public key of the certificate holder as well as an algorithm identifier to which this key will be used.

Electronic copy available at: https://ssrn.com/abstract=3459661

- Issuer unique identifier: A unique number that is used to identify the issuing CA of the certificate in case the X.500 name has been reused for various entities, which is an optional field.
- Subject unique identifier: A unique number that is used to identify the issuing subject in case the X.500 name has been reused for various entities, which is an optional field.
- Extensions: A collection of extensions which were included in version 3.
- Signature: It is the signature of the issuing CA for the certificate. It contains a hash code for other fields that are encrypted by using the CA private key.

Helios components

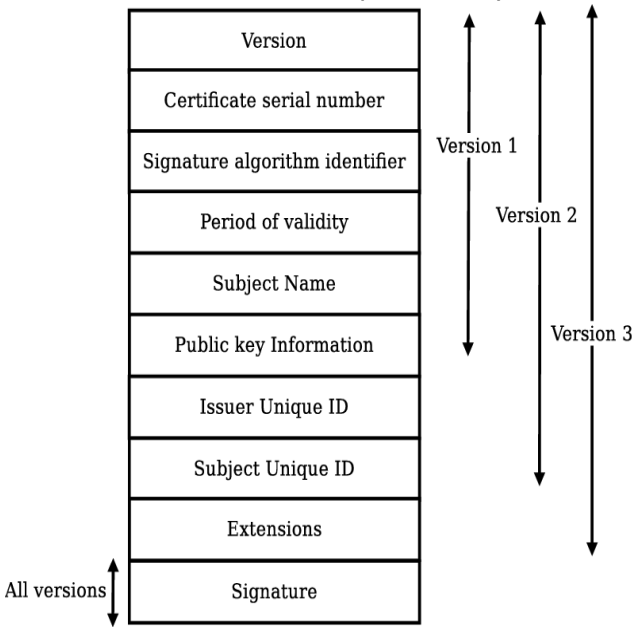

Figure 1. X.509 certificate V3 [34].

4.2 Digital Signature

The digital signature is the most important cryptographic process in the PKI systems. The digital signature provides protection if the parties exchange the digital documents between them. The recipient then can ensure that this document has not been manipulated or altered, and makes sure that the document was actually sent by the sender. This is done by creating a data element attached to the document that is uniquely linked to the sender and when the document is received by the recipient, some steps can be taken to ensure that the signature matches the sender [35].

If the digital signatures are not used, the attacker can simply intercept the document sent by the sender and change it to another document and send it to the recipient without being detected, as shown in Figure 2.

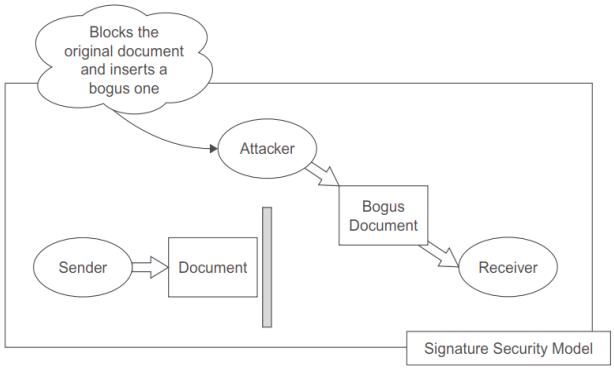

Figure 2. Block diagram of altering an unsigned document [35].

However, when the signature is attached to the document and changed by the attacker with another document, the recipient can know that the document is false and not sent by the sender, as shown in Figure 3. Secure digital signatures can be created by using suitable cryptographic algorithms.

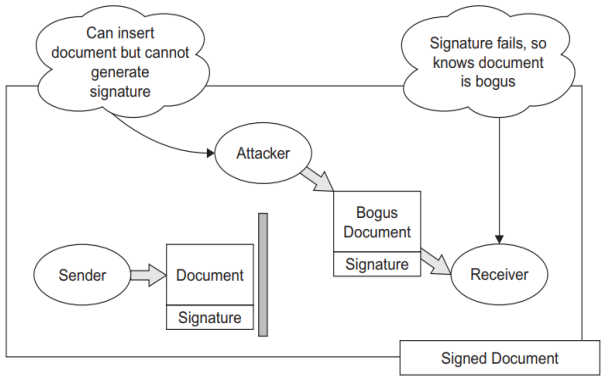

Figure 3. Block diagram showing prevention of an alteration attack via digital signature [35].

5. Proposed Framework

The proposed framework includes improvements to the Helios voting system in four main areas: Security, scalability, anti-coercion, and usability. These areas of contribution of the proposed framework are described in detail in the following subsections. Figure 4 is a block diagram that illustrates a general description of the proposed framework. The first contribution will be in the Helios interface where an Arabic interface will be added with sufficient explanation for each step in the system so as to make it easier and more attractive. The second contribution is the addition of multiple accounts to each voter who

Electronic copy available at: https://ssrn.com/abstract=3459661

uses them when subjected to coercion. Finally, and most importantly, integrating a certification authority that provides the keys needed for encryption and digital signature.

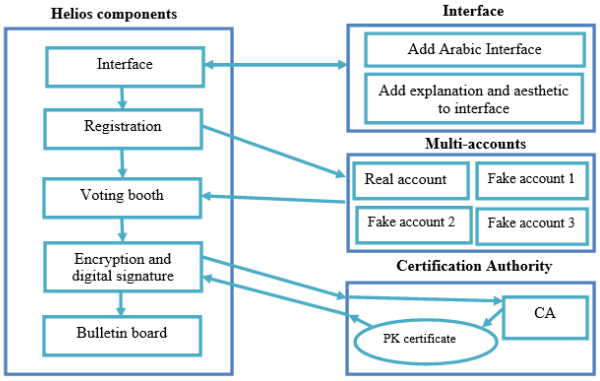

Figure 4. A general description of the proposed I-voting framework.

5.1 Security and Scalability

At first, concerning the security and scalability aspects of I-voting, we propose integrating Helios with a certification authority that creates and certifies encryption keys. The public keys are created and linked to the voter. These keys are used in digital signature and vote encryption. The addition of the certification authority to produce necessary keys for the digital signature and encryption will significantly increase system security by enabling sophisticated security services for system and data protection. Indeed, the scalability of the I-voting system can be increased to consider relatively more distributed environment compared to previous typical deployments of Helios.

The CA issues a public key certificate (one time use key) to a device in the network that can authenticate itself to the CA server. Therefore, the process of generating and distributing keys is automated. Certificates are exchanged any time a new session is negotiated, so static pre-shared keys are not configured or stored, enhancing security and reducing administration. This automated feature of secure key distribution will also highly contribute to increasing the scalability of the system by facilitating its deployment in more distributed and large scale environments. In this respect, public key certificates can be the safest and most practical forms of electronic data identification and protection in distributed environments. Figure 5 illustrates the general description of integrating the certification authority in the proposed framework.

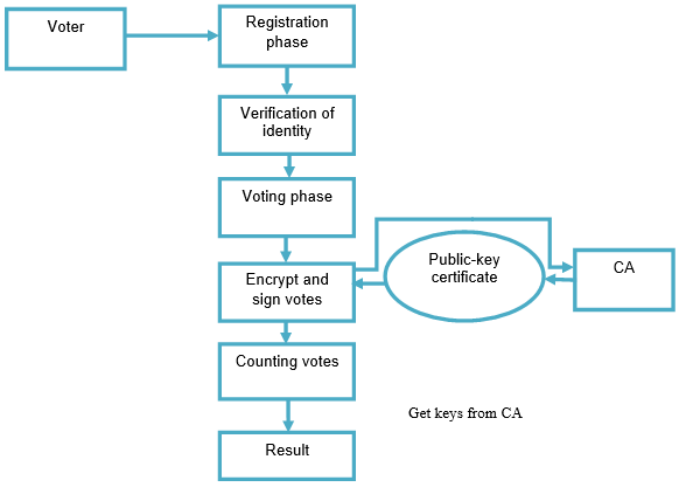

Figure 5. A block diagram showing the integration of certificate authority in the proposed framework.

The main action steps in the proposed framework can be as follows:

1. The voter registers access to the system.
2. After the identity of the voter is verified, the voter goes to the voting page to vote.
3. When entering the election web page, the voter chooses the option she/he wants from a range of options.
4. After the voter has voted, the encryption keys will be requested from the certification authority for use in voting encryption and digital signature.
5. The certification authority then verifies the request and sends the public key certificate to be used for encryption and digital signature.
6. The voter can choose to submit or audit the vote.
    - If she/he chooses to submit, her/his vote will be recorded.
    - If she/he chooses to audit: the key and ciphertext are given to her/his, who can now check whether this matches the vote she/he wanted to cast.
7. After the election ends, the system calculates final votes.
8. Finally, the system announces the election results on the bulletin board, and any voter can see the result.

5.2 Anti-Coercion

Secondly, concerning anti-coercion property, the proposed system will enable the voter to create multiple accounts during the registration stage. These multiple accounts are created for each voter where the voter will have a real account (based on her/his choice)

Electronic copy available at: https://ssrn.com/abstract=3459661

used in the elections and other (one or more) fake accounts used by the voter when subjected to coercion by the attacker. In later phases, when the voter enters the system, if she/he registers with her/his real account, she/he will be able to vote in the elections and the vote will be placed on the main database and thus calculated. In case the voter is subjected to coercion, she/he can use one of her/his fake accounts to vote as the coercer wants. In this case, the vote (unnoticeably) will be placed in the secondary database, and thus her/his vote will not count within the final result.

The coercer cannot distinguish which account is real or fake because the voter can any time choose which account to be real and the rest are fake ones. Using any fake account will cause the vote to not be counted among the final votes. When voting through the fake account, these votes will be stored in a different database than those that will be done by the real account. Thus, when counting, only votes that are in the main database will be counted. Voters can vote using their real account at any time and thus reduce the risk of coercion suffered by Helios.This is illustrates in Figure 6.

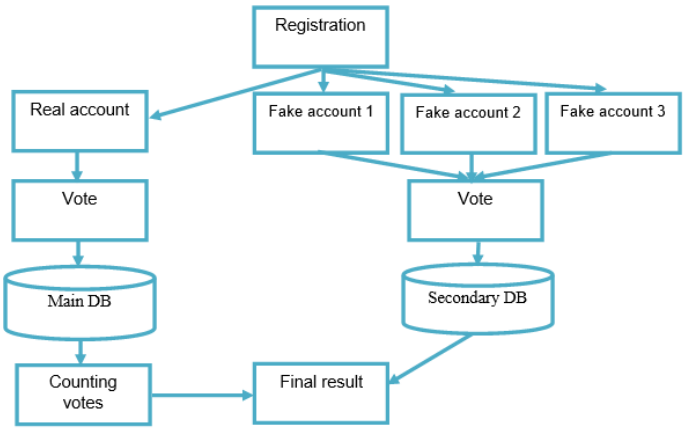

Figure 6. Block diagram shows adding multi-accounts to propose framework

5.3 Usability and Comfort

Finally, concerning the usability issue, we need improve the Helios interface as the interface is difficult to understand by people who do not have a broad knowledge of technology. There are many options that they do not understand the reason of their existence or what they should choose. Every step in the voting needs to be explained more and why the voter is doing it. So in the proposed framework, this issue need to be carefully tackled in order to increase usability and comfort. Thus, we will explain each step in the system and add a clear explanation of why this step exists and add an attractive form to the interface of the system. Hence, the contribution here will be to clarify some of the options further as well as adding aesthetic to the interface.

To use the Helios system on a larger scale, we will add an interface in Arabic. People fluent in Arabic only will use that interface. A simple button option will be added to change the language to Arabic when the system is used by the Arabs. Also, the language can be returned to English if the voter so desires. This addition will make using Helios easier and more convenient because Arab voters who do not speak English will be able to read the steps in the system and thus be able to use the system correctly.

6. Conclusion

I-voting is one of the most modern means of voting. In this work, we have proposed an I-voting framework based on Helios voting system and public key certificates. Helios has been chosen because of its popularity and wide use as well as because it is open source. We have proposed adding a certificate authority to Helios in order to obtain the public key certificate to enable using the required keys for the digital signature and for further possible encryption functionalities. Thus, better security for I-voting in more distributed environments can be achieved. Furthermore, Anti-coercion and usability aspects of I-voting have been enhanced by adding more than one account to the voter to reduce the risk of coercion and simplifying using the system by adding modifications to the Helios interface.

References

[1] J. Weber, Usability Study of the Open Audit Voting System Helios, Univ. Waterloo. (2009) 1–13.

[2] D. Bernhard, O. Pereira, B. Smyth, and B. Warinschi, Adapting Helios for provable ballot privacy, Eur. Symp. Res. Comput. Secur.. (2011) 335–354.

[3] F. Karayumak, M. M. Olembo, M. Kauer, and M. Volkamer, Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System, EVT/WOTE (2011).

[4] F. Karayumak, M. Kauer, M. M. Olembo, T. Volk, and M. Volkamer, User Study of the Improved Helios Voting System Interfaces, Socio-Technical Asp. Secur. Trust. (2011) 37–44.

[5] C. Loria, D. Galindo, C. Loria, I. N. Grand-est, and C. Loria, Distributed ElGamal ` a la

Electronic copy available at: https://ssrn.com/abstract=3459661

Pedersen - Application to Helios, Proc. 12th ACM Work. Work. Priv. Electron. Soc. (2013) 131–141.
[6] V. Cortier, D. Galindo, S. Glondu, and M. Izabachène, Election Verifiability for Helios under Weaker Trust Assumptions, Eur. Symp. Res. Comput. Secur. (2014) 327–344.
[7] O. Kulyk, V. Teague, and M. Volkamer, Extending Helios Towards Private Eligibility Verifiability, Int. Conf. E-Voting Identity. (2015) 57–73.
[8] 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.
[9] M. Backes, C. Hammer, D. Pfaff, and M. Skoruppa, Implementation-level Analysis of the JavaScript Helios Voting Client, Proc. 31st Annu. ACM Symp. Appl. Comput. (2016) 2071–2078.
[10]O. Kulyk, K. Marky, S. Neumann, and M. Volkamer, Introducing Proxy Voting to Helios, Availability, Reliab. Secur. (ARES), 2016 11th Int. Conf. on. IEEE, (2016) 98–106.
[11]N. Chang-fong, The Cloudier Side of Cryptographic End-to-end Verifiable Voting : A Security Analysis of Helios, Proc. 32nd Annu. Conf. Comput. Secur. Appl.. (2016) 324–335.
[12] 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.
[13] 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
[14]L. Panizo, M. Gascó, D. Y. Marcos, J. A. Hermida, and J. Barrat, E-voting system evaluation based on the Council of Europe recommendations : Helios Voting, IEEE Trans. Emerg. Top. Comput.. 6750 (2018) 1–13.
[15]B. Smyth, Ballot secrecy : Security definition , sufficient conditions , and analysis of Helios, Cryptology ePrint Archive, Report 2015/942. (2018).
[16]B. Adida, Helios: Web-based Open-Audit Voting., USENIX Secur. Symp. 17 (2008) 335–348.
[17]Josh Benaloh, Serge Vaudenay, and Jean-Jacques Quisquater Final Report of IACR Electronic Voting Committee. International Association for Cryptologic Research. (2010).
[18]Stuart Haber, Josh Benaloh, and Shai Halevi. The Helios e-Voting Demo for the IACR. IACR. (2010).
[19]Josh Benaloh, Simple verifiable elections, USENIX/Accurate Electronic Voting Technology Workshop, USENIX Association. (2006) 5-5.
[20]K. Sako and J. Kilian, Receipt-Free Mix-Type Voting Scheme -A practical solution t o the implementation of a voting booth-, Int. Conf. Theory Appl. Cryptogr. Tech.. (1995) 393–403.
[21]J. D. Cohen, M. J. Fischer, Y. D. C. S. Tr-, J. D. Cohen, and M. J. Fischer, Department of Computer Science (Extended Abstract) A Robust and Verifiable Cryptographically Secure Election Scheme, Yale Univ. Dep. Comput. Sci. (1985) 372–382.
[22]B. Adida and O. De Marneffe, Electing a University President using Open-Audit Voting : Analysis of real-world use of Helios, EVT/WOTE. (2009) 1–15.
[23]A. Filipiak, Design and formal analysis of security protocols , an application to electronic voting and mobile payment, PhD diss., Université de Lorraine. (2018).
[24]W. Bokslag and M. de Vries, Evaluating e-voting: theory and practice, arXiv preprint arXiv:1602.02509. (2016).
[25]O. Pereira, Internet Voting with Helios, Real-World Electron. Voting Des. Anal. Deploy. (2016) 279–310.
[26]A. Schneider, C. Meter, and P. Hagemeister, Survey on Remote Electronic Voting, arXiv preprint arXiv:1702.02798. (2017).
[27]E. A. Quaglia, B. Smyth, I. S. Group, and R. Holloway, A short introduction to secrecy and verifiability for elections, International Conference on Cryptology in Africa. Springer, Cham, (2018) 1–11.
[28]M. Volkamer, O. Spycher, and E. Dubuis, Measures to Establish Trust in Internet Voting, Proc. 5th Int. Conf. Theory Pract. Electron. Gov. (2011) 1–10.
[29]S. F. Al-janabi, Development of Certificate Authority Services for Web Applications, Futur. Commun. Networks (ICFCN), 2012 Int. Conf. (2012) 135–140.
[30]H. Ray, Technological infrastructure for PKI and digital certification, J. Computer Communications, University of Canterbury. 24 (2001).
[31] Osamah Ibrahim Khalaf, Bayan Mahdi Sabbar''An overview on wireless sensor

Electronic copy available at: https://ssrn.com/abstract=3459661

networks and finding optimal location of node'',Periodicals of Engineering and Natural Sciences, Vol 7, No 3 (2019)
[32] 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.
[33] Stallings William, Cryptography and network security: principles and practice, Sixth ed, Upper Saddle River: Pearson, 2017.
[34] Wazen M. Shbair, Service-Level Monitoring of HTTPS Traffic, Networking and Internet Architecture [cs.NI], Université de Lorraine. (2017).
[35] 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

Electronic copy available at: https://ssrn.com/abstract=3459661