UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Secure e-Voting in Smart Communities

Article

Accepted version

V. Agate, M. Curaba, P. Ferraro, G. Lo Re, M. Morana

In Proceeding of the Fourth Italian Conference on Cyber Security (ITASEC 2020)

Publisher: CEUR-WS

Secure e-Voting in Smart Communities

Vincenzo Agate[1], Marco Curaba[1], Pierluca Ferraro[1], Giuseppe Lo Re[1], and Marco Morana[1]

University of Palermo
Department of Engineering
Viale delle Scienze, ed. 6
90128 Palermo, Italy
{firstname.lastname}@unipa.it

Abstract

Nowadays, digital voting systems are growing in importance. This is an especially sensitive area, because elections can directly affect democratic life of many smart communities. The goal of digital voting systems is to exploit ICT technologies to improve the security and usability of traditional electoral systems. In this work we present a secure electronic voting system that guarantees the secrecy, anonymity, integrity, uniqueness and authenticity of votes, while offering a user-friendly experience to voters, putting them at ease through the use of technologies familiar to them. To ensure these fundamental security requirements, the system fully separates the registration and voting phases and does not collect information on users, making it impossible to determine the identity of whoever cast each vote. Only the electoral supervisor, during the tallying phase, can decipher the electronic ballot papers, which are also totally anonymous. We consider universities to be one of the most representative smart communities, and for this reason we used the case study of university elections held on our campus to test the system. The experiments carried out tested the system in increasingly challenging scenarios, and were carried out by volunteer students and university staff members.

1 Motivations and Related Work

Elections are a fundamental mechanism for maintaining democratic life in many countries around the world. In this respect, cyber security techniques can be very helpful, ensuring that the entire electoral process is transparent and verifiable, as well as accelerating tallying procedures, guaranteeing user privacy and the integrity of votes.

However, digital voting systems have not yet taken over, and their role is still controversial. This is due to doubts regarding both the security and fairness of the elections, and the possibility that they could create a gap between participants who know and trust the technologies involved and those who do not trust electronic voting systems in sensitive operations such as electoral procedures [9].

The electronic voting system that we present in this work aims to address both of these issues. Our system uses advanced cryptographic techniques to protect the privacy of the participants and guarantee the secrecy, anonymity, and authenticity of the votes. At the same time, all technologies and devices involved should be familiar to voters, increasing their sense of confidence in the system itself.

Indeed, our goal is creating an electronic voting system that retains the security features of traditional voting systems, such as the need for physical identification of voters by staff members. As in traditional systems, the presence of election officers ensures that elections are conducted properly, without anomalies.

In fact, election officers are involved in various phases of electoral procedures: they are responsible for preliminary operations, such as creating ballot papers and voter lists; they oversee

the voter registration phase and the actual voting operations; finally, an *election supervisor* is the only person who has the credentials to carry out the tallying of votes at the end of elections.

Guaranteeing the proper conduct of the elections poses several research challenges. In particular, the biggest problems are related to: (i) maintaining voter privacy; (ii) gaining users' confidence in the voting system; (iii) ensuring that voting takes place in complete freedom, without constrictions or attempts to influence it.

Indeed, a difficult problem in designing electronic voting systems is the need to authenticate users, to prevent unauthorized people from voting and, conversely, to guarantee their privacy when actually voting by not storing any information about them. To solve this issue, our system completely decouples the registration and voting phases, thus ensuring both authentication and privacy, as will be shown in the following sections.

Obviously, the level of security required for holding the elections depends on the type and complexity of the election itself. For example, the security requirements for national parliamentary elections are certainly different from those for the election of university students' representatives. For this reason, digital voting systems must be flexible and re-configurable to adequately manage elections of any kind and complexity.

For example, in certain contexts it is possible to relax some of the security policies and use web-based systems that allow remote voting. In some works such as [1, 14, 15], for example, the authors present new electronic voting schemes that allow voters to participate remotely in elections over the Internet.

This is obviously very convenient for voters, who do not need to physically go to the polling station, but it does involve security problems. In particular, the absence of physical booths and controls by the election staff makes it impossible to verify with certainty that the user is actually alone at the time of voting, and that he is not threatened or spied on. That is, the requirement of non-coercibility cannot be enforced.

Such solutions can only be applied in particular contexts where privacy and non-coercibility are not the main requirements. For this reason, supervised voting systems are often the most appropriate choice. In this context, two different types of systems are frequently used: direct voting machines and computerized voting systems [12].

Over the last few years, digital voting systems have gained more and more interest, both from public and political authorities and from the scientific community [5, 10]. In the literature there are several e-Voting systems that offer a user experience similar to that of traditional systems. This allows for a high level of user satisfaction, increasing voters' confidence in the overall system [2, 3, 4, 8, 17]. For example, the authors of [13] present a detailed analysis of the elements that most influence voter trust, such as the overall usability of the system and the reliability and competence of staff members.

The privacy and security criteria that all e-voting systems should comply with have been rigorously defined by several studies, including [7, 11, 16]. The standardization of these criteria is a fundamental step to design systems that can be actually used in a real-world context.

In this work we present the case study of elections in a university setting. Several evaluations of the proposed system were carried out, involving an increasing number of volunteer students and university staff members, in progressively more complex scenarios.

The remainder of the paper is organized as follows. Section 2 presents an architecture overview of the proposed e-Voting system. The security requirements that are met by our system are described in Section 3. Section 4 analyzes in detail the data flow of electoral procedures, describing the encryption and decryption operations needed to ensure the secrecy of votes. Our case study is presented in Section 5, and we draw our conclusions in Section 6.

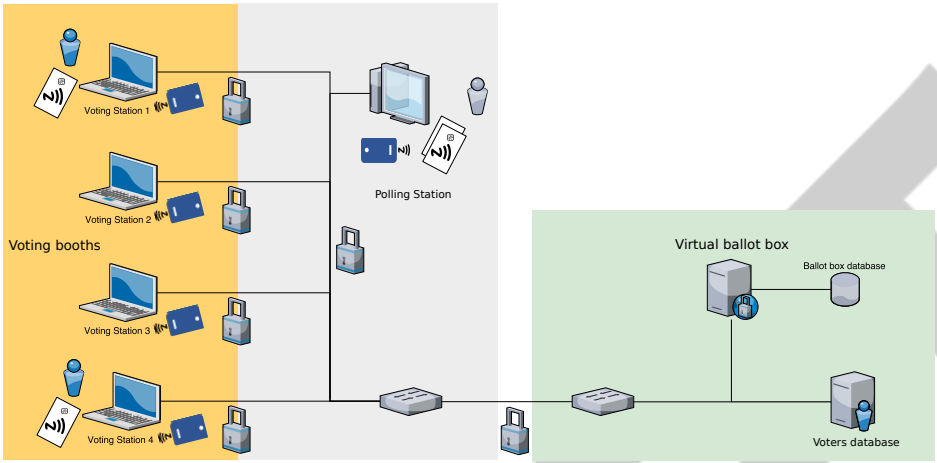

Figure 1: Hardware architecture overview.

2 Architecture overview

In this section we present the hardware and software components necessary for the operation of the proposed system. Our e-Voting system belongs to the category of electronic voting machines which are installed in public polling stations and are connected to a centralized server (virtual ballot box) that securely collects and stores the votes cast. Voting procedures are supervised by staff members who act as election officers, ensuring the proper running of elections. The term *staff members* refers to all representatives of electoral authorities who work together to ensure the proper and secure running of the elections. We divide staff members into two categories, according to the stages of the electoral process in which they are involved:

- staff members who, on election day, activate the voting stations with the appropriate passcodes, as well as overseeing the registration and voting operations (we assume that such staff members are trusted);
- an *election supervisor*, who is the only one who has the credentials to decrypt the voting cards and carry out the counting, after the end of the election, and then publish the results; in particular, the election supervisor's credentials are kept by a notary until the end of the election, when votes are counted.

To reduce organizational costs, the proposed solution does not require expensive dedicated hardware. On the contrary, it allows reusing existing PCs, laptops and tablets. These devices are preventively configured by installing software specifically developed for our e-Voting system.

The whole system is based on an architecture that includes several software applications running concurrently on multiple physical machines, as shown in Figure 1. Specifically, the system consists of three categories of software applications:

- a centralized software that acts as a virtual ballot box, with the task of collecting and securely storing encrypted votes;
- a software installed in all voting stations, which allows users to express their preferences;
- a software used by electoral officers to manage polling stations, register users and check whether they are actually entitled to vote.

To allow multiple users to vote simultaneously, these software components are continuously interacting with each other. To increase communication security, all devices involved are connected to a single VPN. In addition, all data exchanges take place via SSL/TLS connections.

The right side of the Figure 1 shows the virtual ballot box and the two databases used by the system, i.e. the one in which the encrypted votes are stored and the one containing the centralized list of voters. These components collectively form the back end of our e-Voting system.

It is very important to guarantee the security of the virtual ballot box, since it plays a major role. In fact, the entire integrity of the elections depends on it, given that the virtual ballot box is responsible for receiving and storing encrypted votes prior to the tallying phase.

The security protocol used by the system to ensure data integrity will be described in detail in Section 4, showing all cryptographic encryption and decryption operations that are performed on the voting packets. It is important to point out that the virtual ballot box does not know any information about the voters, who are therefore completely anonymous. In fact, the only information managed by the virtual ballot box is that relating to voting packages, which are ciphered by asymmetric encryption and can only be deciphered using a private key in possession of the election supervisor at the end of the election. All RSA keys in our system are generated according to the recommendations of [6] to ensure necessary randomness requirements.

The purpose of the centralized database that manages the list of voters is to ensure consistency between different polling stations, preventing the same person from voting multiple times. Since users can choose the polling station where they want to vote, it is necessary to maintain a unified and up-to-date list that keeps track of who has the right to vote and who has already voted.

Devices used as polling stations and voting stations are shown on the left side of Figure 1. Particular attention should be paid to the configuration and security of voting stations, as they are used directly by users during elections. The software installed on these devices must therefore be easy to use and error-proof. The purpose of voting stations is clearly to make users vote as easily, quickly and safely as possible. Polling stations, on the other hand, are used by staff members to manage the pre-vote operations and the user registration phase. Again, the software installed on these devices must be easy to use, intuitive and error-proof, as staff members may not be IT experts.

3 Security requirements

In this section we describe nine security requirements that are enforced by our e-Voting system, thus guaranteeing the integrity of elections as suggested in [7, 16]: secrecy, possibility of expressing only one vote, authenticity, integrity of the vote, non-coercibility, validity, ensuring the right of vote, transparency, losless.

Secrecy: the requirement of secrecy is one of the most important constraints of the system. In a distributed ICT system, this task is not trivial, but there are several security technologies, such as encryption, that can help accomplishing it. Even if adversaries are able to intercept the communications payload exchanged between different parts of the system, it should be impossible to understand which candidates or preferences a voter expressed. For these reasons we use a two step encryption process which entails both symmetric and public key cryptography.

Possibility of expressing only one vote: each person entitled to vote may do so only once. In our system, each user can vote indifferently in any of the electoral polling stations. If the system has recorded the expression of a voter's preference through a polling station, any other

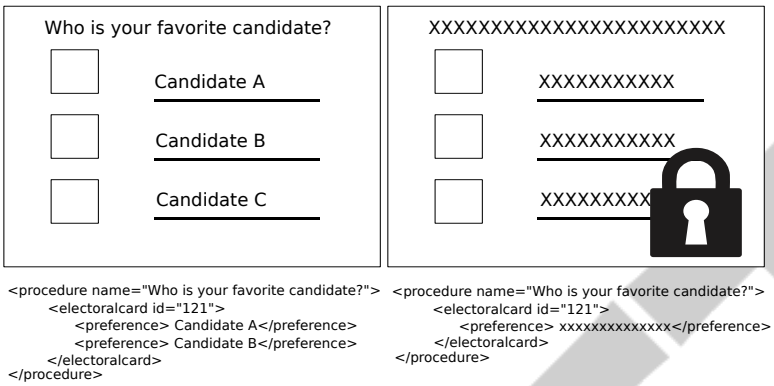

Figure 2: Digital ballot card before and after encryption.

polling station will immediately be able to verify the impossibility of casting another vote. While the system is capable of registering those who have already voted, no information that can link the voter to their expressed preference is stored.

Authenticity: a vote is authentic if it comes from a reliable source or, in other words, if it comes from one of the known polling stations. In order to establish whether a vote has actually been cast in one of the booths, the voting station uses a Message Authentication Code (MAC) before sending it. Once the virtual ballot box receives the vote package, it verifies the MAC code attached, discarding or storing the secret vote. To ensure the authenticity of votes until the tallying phase, the virtual ballot box signs the vote package, making it resistant to tampering.

Integrity of the vote: we ensure the integrity of votes and electoral procedures at different levels of our architecture. The integrity at the communication level (above TCP) of the data transmitted from the voting station to virtual ballot box is guaranteed by SSL/TLS. The digital signature of the voting station and that of the virtual ballot box are used to ensure both the integrity of the voting packages during the transmission from a voting station to virtual ballot box, and the integrity inside the database after receiving it.

Non-coercibility: the impossibility of forcing a voter to express a preference is guaranteed by using voting booths. Each voting station is placed inside a voting booth where voters can enter one at a time, and only if they have the authentication token received during the registration phase. This solution, although more expensive compared to web-based e-voting ones, guarantees privacy and secrecy, which is impossible to guarantee in web based systems.

Validity: one of the most insidious problems during the counting phase in conventional paper-based voting systems is the management of invalid votes, which inevitably can be produced due to negligence of the voters. Our system allows users to fill in the voting form in a valid and unequivocal manner. The voter also has the option of completing the ballot by expressing the number of preferences or leaving the ballot deliberately empty.

Ensuring the right to vote: the voting system we propose is supervised, so the right to vote is guaranteed by the staff authorized to carry out the preliminary activities of voters' identification. To enable users to vote, staff members provide them with authentication tokens (such as NFC tags) after the registration phase.

Transparency: one of the most sensitive responsibilities of the system is that of maintaining transparency during voting operations. This means that the voter and staff members must

have a clear and unequivocal confirmation that the vote expressed has been successfully and securely stored in the virtual ballot box. The system will communicate the completion of the operation, through a message displayed on the voting station and on the polling station.

Lossless: There must be no possibility of losing the voting packages after users express their preferences. To ensure this requirement, the system is equipped with mechanisms that groups all the functionalities into database transactions.

Verifiability: Individual verifiability (i.e., a way for each voter to gain confidence that their own vote was correctly recorded and counted) is guaranteed by the fullfillment "transparency" and "lossless" requirements. Global verifiability (i.e., a way for everyone to gain confidence that all votes were correctly counted and that only eligible voters cast a ballot) is guaranteed by the fullfillment of three other requirements, namely "possibility of expressing only one vote", "transparency" and "lossless". Note that, deliberately, our system does not give voters the opportunity to demonstrate their vote to others, because that would go against the principle of non-coercibility.

4 Proposed system

This section will describe the proposed system, analyzing the data flow before, during and after voting procedures. Our e-Voting system is a distributed application consisting of several software and hardware components with different roles in the voting process.

The characteristics of electoral procedures can vary widely. Some of the possible differences may concern the type and number of elected representatives, the number of preferences that can be expressed by the voter, the subdivision of candidates into parties and electoral groups.

To handle these different demands in a flexible way, the voting card is electronic in our system. Using the XML format guarantees that the voting station does not have to be specifically configured to handle different types of elections. All voting cards are automatically generated during the *preparatory phase*, on the basis of the data provided by the election officers.

When the voter expresses his preference, the XML file is filled in by the system with the vote cast. Before the voting card is sent to the virtual ballot box, the file is digitally signed and encrypted. Figure 2 shows the voting card before and after the voter has filled it out and it has been encrypted.

4.1 Voting phase data flow

Voter identification and registration, carried out by election officers, is a key operation to ensure the security of the system. After this phase, election officers use the GUI provided by the polling station to connect to the central database with the list of voters and check if the user is actually entitled to vote and has not already done so.

Once it is determined that the user can vote, it is no longer necessary to maintain other information about him. Indeed, from this point on, votes must become completely anonymous, to ensure their privacy and the secrecy of the votes.

For this reason, our system introduces the idea of *virtual users*. The polling station software randomly assigns such a temporary identity to the voter, allowing him to vote in an available voting booth, which is also randomly chosen. As a result, the voting station system does not receive any personal information about the person who is going to cast his vote. The only information that the voting station system has to know is that the virtual user v_i, which is in

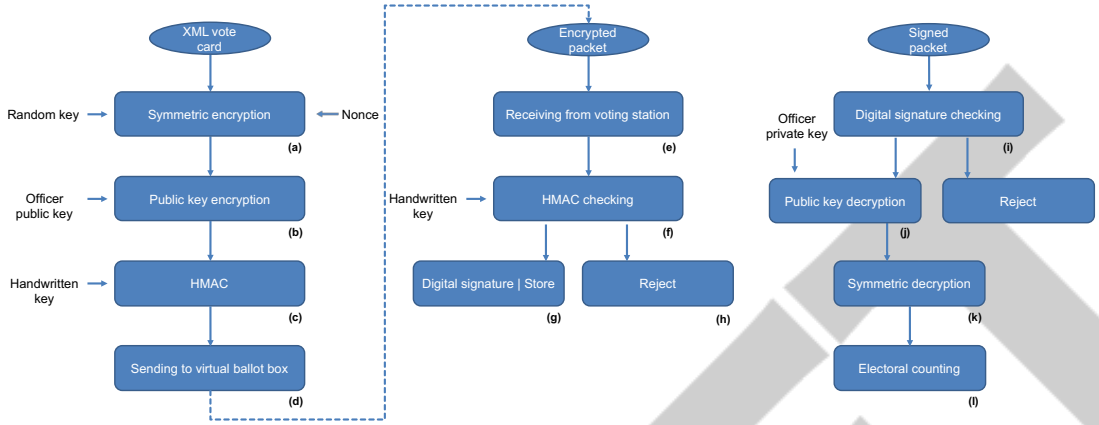

Figure 3: Voting operations data flow.

possession of the token t_k, can express a single vote. Virtual users are constantly reused for different voters, thus ensuring their privacy.

The user casts his vote in a voting booth, which guarantees his privacy, and interacts with the system of the voting station, installed on a computer located inside the booth. To be enabled, the voting station requires the user to hold the identification token he received near the token reader. If the token is correctly recognized, the voting station is enabled and the user can express his vote; the appropriate voting card, depending on the user's group, is then shown on the screen and allows the user to make his choice. When the user confirms his preference and decides to send the voting card, the system starts the encryption process, which guarantees the secrecy and authenticity properties described in Section 3.

The voting station generates a symmetric key, K_i, and uses it to encrypt individual fields that need to be kept secret until the end of the electoral procedure (Figure 3-a). This key, in turn, is encrypted with an asymmetric encryption algorithm, using a public key associated with the private key of the election supervisor. In this way, only he will be able to decrypt the K_i key, and therefore the secret fields of the ballot, and that will happen only during the tallying phase (Figure 3-b).

The encrypted voting package, as well as the asymmetrically encrypted key and a *nonce*, are sent to the HMAC algorithm, so as to ensure integrity and authenticity (Figure 3-c). The secret key needed by the HMAC algorithm to authenticate the message is derived from a passcode manually entered by the election staff when activating each voting station on election day. The recourse to paper-based codes guarantees an additional layer of security, which is necessary given the particular importance of these procedures to guarantee the overall security of the system and of the voting operations.

The encrypted voting package, together with the key, the *nonce* and the digest produced by HMAC are sent to the central ballot box by using SSL/TLS, as shown in Figure 3-d and 3-e.

An additional layer of security is provided, at the application level, by the verification of the HMAC digest of the voting package received from the virtual ballot box, which confirms that the ballot is intact, authentic and, therefore, valid (Figure 3-f). To protect the system against *replay attacks*, the central ballot box maintains a database of previously received HMAC digests. If the received digest is the same as any other already known, the package is rejected (Figure 3-h), and the voting station must send it again, after generating a new *nonce* and computing the new HMAC digest. If, instead, the received package is valid and has a unique HMAC digest,

the central ballot box saves it in a relational database, after having digitally signed it, as shown in Figure 3-g.

The tallying phase, which only takes place when the elections are over, starts by requesting the election supervisor to enter his credentials. Using these credentials, his private key is retrieved and deciphered (Figure 3-j). Then, for each voting packet, the system checks the corresponding digital signature (3-i) that was added by the system when the packet was saved in the database, as described above. This is to ensure that the voting package has not been altered in any way. The supervisor's private key is used to decrypt the symmetric K_i key which encrypted that specific voting packet (Figure 3-k). Once the packet has been decrypted, the system automatically updates the total vote count, based on the preferences stated on the ballot, as shown in Figure 3-l. The result of the tallying phase is also digitally signed, to prevent any tampering with the outcome of the vote and ensure its authenticity and integrity. Even after the tallying phase, the votes are only stored in encrypted form. Subsequent counting operations for verification purposes are carried out following the same procedure described above. At all times, the private key of the supervisor is always required to decipher the votes.

5 Case study

In this section, we will present a case study that we have used to test the proposed system on several occasions, allowing a growing number of users to try it out in increasingly challenging situations. In particular, the scenario considered is that of university elections. We believe universities are well suited to the adoption of digital voting systems, since potential users (e.g., students, professors, researchers, staff members) are accustomed to using ICT tools to carry out their daily activities. In practical terms, a university campus provides easy access to the required technological infrastructure, such as wireless connections, printers and PCs that can be easily leveraged for electoral purposes. Alternatively, if it is necessary to purchase some of these resources, they can be reused by students or staff members for other activities, in between votes.

It is important to note that for political electoral procedures, there are dedicated agencies that deal with elections both in economic and organizational terms. On the contrary, in a university context elections are seen as a secondary activity. However, expenses related to software development and provision of the necessary tools for the adoption of an electronic voting system can be amortized in the course of several elections.

In universities, various collegiate bodies have to be renewed periodically and, for this reason, elections of various sizes are often held. Indeed, university elections can be varied, with different categories of interested voters (e.g., students or staff members), and thus the number of participants is highly variable. Our goal is to create a platform for digital voting that minimizes resources wasted by using paper-based systems. This is reflected in the replacement of paper voting ballots with digital ones, eliminating slow manual vote counting by adopting an automated tallying process that is significantly faster and more secure.

We use secure contactless smartcards with NFC technology as authentication tokens to enable voting stations. These NFC tags are handed over to users by staff members during the identification phase. After voting, users return the NFC tags to staff members, who will then hand them over to new users.

In our tests, we used MIFARE Plus products, but the system is compatible with other products that use AES security for authentication, data integrity and encryption based on open and global standards. Each polling station is equipped with an NFC writer used by staff members, and each voting stations is equipped with an NFC reader. The voter, once registered,

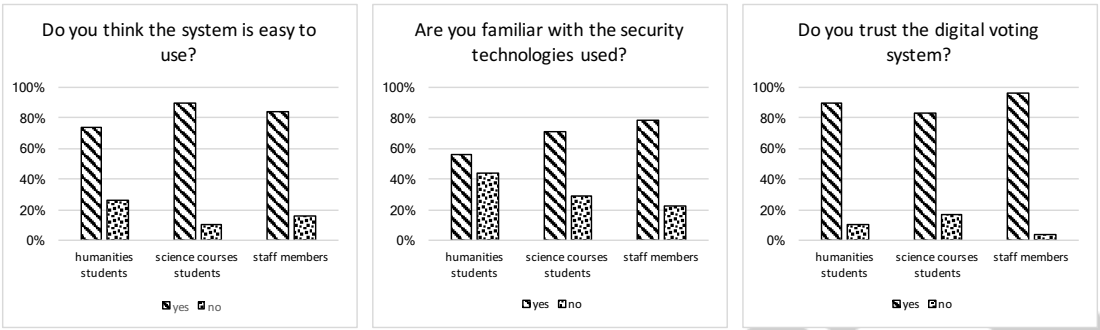

Figure 4: Questionnaire results.

receives one of the NFC tags with a new code written by the NFC writer. Each tag will only enable the voting station indicated by the system.

5.1 Testing phase

To evaluate and refine the system, we have carried out several tests over the course of six months, at the University of Palermo. The various trials carried out were intended to test different functions of the system in increasingly challenging scenarios, starting from a basic trial up to extensive tests with several hundred voters and multiple polling stations. The tests were conducted with volunteer students and university staff, and involved mock elections with fictional candidates. At the end of the voting process, we presented a questionnaire to each of the participants, inquiring about their satisfaction when using the system and asking for suggestions to improve it. The questionnaires we presented to users are similar to those proposed in numerous works in literature in the field of e-Voting systems, such as [12, 13]. In each test, we noticed a steady increase in user satisfaction, compared to previous versions of the system. Most of the changes requested were related to user interface and bug fixes.

We present the results obtained from the questionnaires of the last test carried out. The test involved the use of two polling stations with two voting stations each, and about five hundred volunteer participants among students and university staff members. This test simulated the election of two typical university organizations: student committee and academic senate.

Voting students were asked to indicate whether they were from humanities or science courses. The survey revealed that about 90% of students in scientific courses consider the new voting system easy to use, as shown in Figure 4. Among humanities students, the percentage is slightly lower with a preference of about 75%. This difference is justifiable given the greater familiarity of students from scientific courses with new technologies such as NFC tags. However, as expected, the satisfaction level is still very high, since the students belong to the generation of digital natives.

Voters belonging to university staff have a very positive perception of the new electronic voting system, so much so that about 84% of respondents approve it. This is to be expected, given the extensive use of innovative information technology in their daily work.

Another question asked to participants was their level of trust in the system. Perhaps surprisingly, humanities students, who are less familiar with the security technologies used, tend to have more confidence in the new voting system than their colleagues. In any case, it is worth noting that the university setting is comprised of people with a good level of computerization and acceptance of new technologies, so it is not surprising that there is such a high degree of

appreciation about the proposed system.

After having extensively tested the system with mock elections, we used it in a real university election. Out of a total of 416 people who were entitled to vote, 297 voters actually participated in the election. All participants used our voting system. According to the election rules, voters were divided into six categories, based on their role within the university, and each type of voter was shown a different voting card, with candidates belonging to the same category as the voter. Also in accordance with regulations, the election was run in a single location, in the course of a morning. Two registration posts and two voting stations were deployed, alongside appropriately trained staff members ready to answer users' questions.

6 Conclusions

In this work we have presented a new electronic voting system that is particularly suited to the context of university elections. This type of election poses interesting challenges because of the various types of elections possible and, therefore, the high degree of reconfigurability that voting systems must exhibit in order to adapt to all situations. At the same time, the university environment has proved to be well suited to our purposes, as it has allowed us to carry out multiple tests of our system.

We have shown how the use of electronic voting systems can make electoral procedures more cost-effective in terms of resources and personnel involved, saving both time and money. In fact, the use of an electronic system as the one proposed here ensures that the costs incurred can be amortized in tens or hundreds of elections, incurring a minimum cost of reconfiguration for each new one. On the other hand, the time gains are substantial given the speed with which tallying phase takes place and the reduced number of staff members required.

In order to guarantee the necessary requirements of privacy, secrecy and authenticity, the system completely decouples the registration and voting phases, not collecting any information about users, so that it is not possible in any way to trace the identity of the person who expressed each vote. To this end, the content of the voting packages, in addition to being completely anonymous, can only be decrypted by the election supervisor, and only during the tallying phase, when the election is over.

The use of known and proven cryptographic technologies guarantees the security of the system. In particular, the adoption of techniques that are familiar to most users results in a high degree of user satisfaction and trust, as shown in the case study section.

Ultimately, the role of electronic voting systems is still under debate today because it can create a divide between digital natives and participants who may not have confidence in computer systems. At the same time, though, results reported in this work show that the university community seems ready to finally adopt a system like the one we have proposed.

References

[1] H. Agarwal and G. N. Pandey. A secure e-election system. In *2014 International Conference on Information Science Applications (ICISA)*, pages 1–4, May 2014.

[2] Athanasios Antoniou, C Korakas, Christos Manolopoulos, Anastasia Panagiotaki, Dimitris Sofotassios, P Spirakis, and Yannis C Stamatiou. A trust-centered approach for building e-voting systems. In *International Conference on Electronic Government*, pages 366–377. Springer, 2007.

[3] Chrisanthi Avgerou, Silvia Masiero, and Angeliki Poulymenakou. Trusting e-voting amid experiences of electoral malpractice: The case of indian elections. *Journal of Information Technology*, page 0268396218816199, 2019.

[4] France Bélanger and Lemuria Carter. Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2):165–176, 2008.

[5] Lemuria Carter and France Bélanger. The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information systems journal*, 15(1):5–25, 2005.

[6] Henry Corrigan-Gibbs, Wendy Mu, Dan Boneh, and Bryan Ford. Ensuring high-quality randomness in cryptographic key generation. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 685–696, 2013.

[7] Dimitris A Gritzalis. Principles and requirements for a secure e-voting system. *Computers & Security*, 21(6):539–556, 2002.

[8] Ildar M Khamitov, Victor Dostov, and Pavel Shoust. Secret voting: Knowledge vs trust. In *International Conference on Computational Science and Its Applications*, pages 577–586. Springer, 2019.

[9] A. Meier. *eDemocracy & eGovernment: Stages of a Democratic Knowledge Society*. Springer Berlin Heidelberg, 2012.

[10] Donald P Moynihan. Building secure elections: e-voting, security, and systems theory. *Public administration review*, 64(5):515–528, 2004.

[11] Peter G Neumann. Security criteria for electronic voting. In *16th National Computer Security Conference*, volume 29, 1993.

[12] X. Ochoa and E. Peláez. Affordable and secure electronic voting for university elections: The save case study. In *2017 Fourth International Conference on eDemocracy eGovernment (ICEDEG)*, pages 110–117, April 2017.

[13] J. Pomares, I. Levin, R. M. Alvarez, G. L. Mirau, and T. Ovejero. From piloting to roll-out: voting experience and trust in the first full e-election in argentina. In *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, pages 1–10, Oct 2014.

[14] M. Rezvani and S. M. H. Hamidi. Mizan: A secure e-voting schema with vote changeability. In *2010 International Conference on Information Society*, pages 548–552, June 2010.

[15] J. L. Tornos, J. L. Salazar, and J. J. Piles. An evoting platform for qoe evaluation. In *2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013)*, pages 1346–1351, May 2013.

[16] M. Volkamer and M. McGaley. Requirements and evaluation procedures for evoting. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, pages 895–902, April 2007.

[17] Yurong Yao and Lisa Murphy. Remote electronic voting systems: an exploration of voters' perceptions and intention to use. *European Journal of Information Systems*, 16(2):106–120, 2007.