Increasing public trust through technology, eVoting case Albania

Dr. Erdet KËLLIÇI
European University of Tirana

Abstract

Technology has become a mandatory tool for each of us, making everyone dependent on electronic devices and software applications to stay connected and use services. Producers, integrators and public institutions are aiming to introduce technology on a wide scale regarding country population, trying to make most of the populations part of this community. Albania has started the process of shifting form standard workflow of having service at a fix location to online services in both public and private sector. AKSHI with e-Albania platform is promoting online services to most of services offered by government institution. Still there is a gap in the targeted population to use the services due to their capabilities to use information technologies and lack of suitable devices to do so. Albanian Central Election Commission introduced for the first time in elections history countrywide electronic identification using biometric technology and piloting electronic voting. This paper aims to show the result obtained when sensitive services like election are fully supported by technology including everyone that can vote without having a targeted population. The trust of the voters, institutions, organizations and stack holders toward technology in the voting process is analyzed based on real data and facts to support the outcome of this paper.

Keywords: *electronic voting, integrity, elections, technology, biometric identification, cyber security*

Introduction

Parliament elections and local elections have been always followed by declaration regarding the secrecy and the security of the vote. Information technology or electronic systems can be utilized in the election process such as voter registration, voter authentication, granting vote, accelerate the vote counting, and provides access for voters with physical disabilities (Maurer and Barrat, 2016), A countrywide election process happens in Albania each two years but there are cases where partial elections are held more often. The institution that manages and is responsible for election is "Central Election Commission" and is dependent from the Albanian Parliament. The mission of CEC is to make sure that anyone who has the right to vote will have the possibility to do so, the vote will be secret, and each vote will be counted without changing its result. The purpose of this paper is to identify the benefits and the weakness of the usage of technology in election process with the focus on Electronic Voting and counting. In Albania now we have the possibility to evaluate the impact of the technology in voting process because of the use with success of this technology during parliamentary election of 25 April 2021 and partial election for municipality Mayer of 6 March 2022. The information technology approach will increase the participation of the citizen to democracy in the developing countries and it is called e-democracy Amelin et al. (2016). Furthermore, the hybrid e-voting also supports vote verification Ben-Nun et al. (2012). In both of this elections CEC implemented electronic voting in both rural and metropolitan areas for testing the capacity of voters to use this modern device for electronic voting and furthermore identify any obstacles that may be present in the field for this modernization in election processes. The use of technology in elections must address these key elements as listed below:

- Everyone that has the voting right must be able to vote independently without being blocked by technology. This includes the voters with special needs.
- Each vote must be secret and there won't be any possibility to connect the vote with the voter.
- The device used for the voting process must have the ability to be simple to use, simple to install and with an intuitive interface to facilitate the voting process.
- The counting process should be auditable, and any ballot can be investigated accordingly in case an audit is needed.
- Cyber security issues must be addressed and mitigated prior, during and after the voting processes.
- The project should be economically feasible and must last at list for 5 years.

Due to the importance of the processes all these issues should be accordingly addressed, and the solution must fulfill fully each element so the process of voting and counting will be transparent, trustable and at any time auditable.

Literature review

Voting is a very delicate process, and its accuracy identifies the level of the democracy a state has reached so far. Electronic voting poses a great challenge to the authority that organize and implement this kind of voting especially which level of security these systems could provide and how it offers and protects the privacy of its users (Khan et al., 2015) and (Wang et al., 2013). There are a lot of studies that analyze the security of the votes and state that the integrity of the ballot is very critical (Bernhard et al. 2017). When we analyze the electronic voting system and electronic voting devices the first thing that is required to do is to store them in patterns in a safe way which are required for better investigations (Yahyaoui et al., 2020) that may help to increase the credibility of the electronic device and electronic systems. By doing so the trust toward technology will be increased for both users and stack holders of the process. Security of the device and securing access to it that can use a secure method like two ways authentication method using a password and a device that can be a mobile device, a token key or a card. Furthermore, the information located in the device must be encrypted to disallow access of unauthorized persons or organizations. Encryption is a reversible method of encrypting data that requires a key to decrypt. Encryption can be used in conjunction with encryption, which provides another level of confidentiality (Sun et al., 2018)

Methodology

My approach to identify the effect of technology implementation in election process is by taking several variable data before the implementation of the technology and comparing them with the variables produced after the implementation of this technology. These data are measured again and the comparison between them shows the real effect this technology has on the process of the elections. The data are analyzed based on the publications that CEC has on its website and data taken from IT directorate for this research.

In this study I focus on analyzing intangible and tangible benefits of the use of technology in election projects. I have studied and collected data from CEC that is the responsible entity for each election process in Albania. I have taken in

the consideration the technical details of the solution implemented in Albania. A general overview for the use of technologies in the election process is made for the countries of the region and worldwide.

Analyzing the security techniques implemented to secure device information toward cyber security threats is an important aspect that is taken in consideration by this paper.

Institution Challenge

CEC is responsible for organizing the election processes in Albania according to the election code that is subject to change time to time. CEC has 84 full time employees that are responsible for preparing and organizing each election process. During the election period from 3-6 months CEC hire part time employs to help the institution during the election process. CEC hire about 280 part time employees during election time. CEC successfully introduced technology in the election for biometric identification and electronic voting and counting in 2021 parliamentary elections. This countrywide implementation of technology in elections challenged ICT Directorate that is the responsible for the implementation of technology in election process and election data processing and publication. Before the implementation of the biometric identification the voters were identified using printed lists and they signed beside their name in this list. This process was manual and not the best way to identify the real identity of the voter.

The identification though a printed voter list had several problems to be addressed:

- The process was manual, and the identification of the voter identity was made by the commission by examining its id card or passport. This is not an accurate way to identify the identity of a person. Nowadays technology allows the correct identification of the identity of a person.
- One of the most important data that is processed and displayed publicly during an election process is the percentage of participation in election. The processing of this data is preferable in real time or as often as possible. By using voter list the reporting of the number of voting participation was impossible to be communicated automatically and periodically.
- Processing the data in real time was impossible.
- Process of finding and identifying the voter was time consuming.

Regarding the voting process some findings are as follows:
Depending on the ballot complexity the voter may not fully understand how to

fill in the ballot paper and doing so the vote will not express his will or me become an invalid vote.

A lot of effort is made to input security elements including paper quality, special marks, hidden marks, special ink and other elements to increase the security of each ballot paper so no false ballots can be produced. This increase of ballot complexity increases the price of the ballot paper and overall value of the election process costs.

Mistakes during the printing of the ballot cannot be unmade by doing so in some areas the voting process cannot take place until the mistake is fixed.

Ink stamps for each ballot are needed in each polling center, increasing operative costs and delaying the voting sessions.

Each vote should be counted by a counting commission in a secure and surveyed area. During this process human interpretation of the vote is done. This way of counting each vote brings to argues regarding signs used to vote, place of signs and writing inside the voting ballot. This delays the numbering process and increases tensions between members of the counting group.

After each ballot box is counted the result of the count is written on a designed paper and handed out to the operator to enter the figure into the system. This process may contain human errors during entering or writing the figures.

Due to these reasons CEC and political parties agreed on modernizing the voting system by introducing electronic technology to modernize the process. The modernization of the use of the technology in the election process should be done carefully selecting appropriate device with an eye to operational and fixed costs. Technology should address all security issues especially concerning cyber security issues that may happen during the voting and counting process.

Technical Solution

The prerequisite of implementing electronic voting and counting to satisfy all parties are as follows:

- The voting process will be done through a touch screen with suitable dimensions for the voting process based on the voting ballot configuration that will be like the paper ballot.
- Electronic Voting and Counting Devices (EVCD) shall provide electronic voting as well as the calculation of the result at the level of one Polling Station after the closing of the voting process in each PS respectively.
- Securely and anonymously store the votes but simultaneously reproduce the hard copy confirmation/in paper for the vote of each voter by making it available respectively for personal verification.

- Establish the auxiliary technological infrastructure to document/audit the security and accuracy of the vote at each Polling Station.

To fulfil the first request, the company that have offered the solution has produced industrial device using a tablet with 17" touch screen embedded in a suitable form for easier installation as shown in figure 1.

FIGURE 1

Source: www.kqz.gov.al

The device has an android operating system installed in it. This system is modified from the factory to fulfil the security requirements needed for the device. Based on the size of the screen a ballot can designed easily and can be like the voting paper as shown in figure 2.

FIGURE 2

Source: www.kqz.gov.al

To fulfil the second request, the company that have offered the solution has created a software to calculate each electronic vote during the voting process and print a detailed report with the result of voting immediately after the closing of the

election. The result is printed in clear text, and it also has a QR code that can be scan for future use. The QR code is encrypted to secure no change in result during transmission of the data through an encrypted QR code.

To fulfil the third request, the company that have offered the solution implemented a mixing system of each electronic vote stored into the device memory. This system changed the datetime of all electronic votes each time a voting session ended and furthermore it used a random name for the vote file. By doing so all the files had the same timestamp as the last electronic vote. In this way is impossible to check the ordering of the file based on name or timestamp. At the end of each voting session a printer prints the vote in hard copy and cast it into a ballot box as shown in figure 3.

FIGURE 3

Source: www.kqz.gov.al

An audit can be performed by counting the votes into the ballot box that are in hard copy version to be sur that the electronic result match the result of the printed votes that are into the ballot box. This ensure that the machine cannot produce fake reports with wrong results other than what is voted.

To fulfil the fourth request, the company that have offered the solution implemented a logging system that write each event into a log file. This log can be analysed and can be treated as audit log for identifying every event produced by the device.

As already mentioned above the proposed device is classified as modified tabled with a modified android system according (Agasi, O. 2015) stated that there is no complete solution to prevent mobile security problems. This brings a big challenge toward the successful implementation of the solution that will satisfy all security requirements.

Data Analyses

Electronic voting was implanted during parliamentary election on 24 April 2021 in Administrative Zone 40 corresponding to the administrative unit nr. 10 of Tirana. This administrative unit has 32 polling stations grouped into 5 polling stations in the territory of the administrative zone. CEC decided to put two voting machines in each PS to minimize the technical problems that may happened due to electronic device functionality and availability. Table 1 shows a comparison of data between previous elections that were conducted using the traditional way through paper and the data that are provided using electronic voting for the same ZAZ.

TABLE 1

	Parliamentary Elections 2017	Parliamentary Elections 2021	Difference %
Participation in election	12428	12096	2.6%
Valid Votes	12171	11976	1.6%
Blank/Invalid votes	255	120	53%

Source: https://kqz.gov.al/zgjedhje-per-kuvendin/

From the data above provided for the same ZAZ is clear that the new way of voting from traditional to electronic voting did not impact the participation of the voters in the voting process for parliamentary election. The difference is insufficient only 2.6%, so we can conclude that the technology did not pose any barrier to the voters. The age of voters is between the range of the 18-100 year old and their education varies from basic primary school to heigh education level. Based on this data we can conclude that the technology used is easy to use and the way that the information is displayed is intuitive. The equipment is easy to use for a wide age range and for a wide range of education.

Analyzing data regarding invalid votes or blank votes we can conclude that during the electronic voting we have only blank votes that are the votes that the voter intentionally wants to leave blank. Meanwhile in traditional voting we don't know if the voter left them intentionally blank, voted wrong making the vote invalid or the counting commission somehow classified this vote as invalid or blank. The difference is 53% leads to arguments why this difference is so big. Maybe the voting during the parliamentary election of 2017 was more complicated and harder to fill than the one of 2021 parliamentary election. In this case I made another research analyzing the percentage overall blank/invalid votes in all Albanian territory during the elections of 2021 with the ones in ZAZ 40 to see if there is any difference. The result is shown in table 2.

TABLE 2

Parliamentary Elections 2017	Total Voters	Blank/Invalid votes	%
Countrywide	1662274	83059	5
ZAZ 40	12096	120	1

Source: https://kqz.gov.al/results/results2021/results2021.htm

Based on table 2 information is clear that the electronic voting is more accurate and expresses better the intension of the voter enabling him not to mismatch the vote or make mistakes that may invalidate the ballot itself. The electronic voting method removes the "middlemen" from the process. There is no more need for counting groups to count the ballots and decide the validity of them.

Conclusions

Electronic voting is a good solution especially for the counties that have issues with voting processes and yang democracies. This way of voting can help produce accurate results electronically and immediately after finishing the voting process. This will bring into elimination of human errors or human prediction of the ballot.

In many cases the technology is seen as a barrier to access information and services from part of the population mainly older people but from this paper I have identified that when the product is easy and intuitive to use than the technology can help offering a secure and convenient service.

Since the process and result depends totally on the electronic systems security of the devices and system itself must be taken in consideration, any data breach can lead to the loss of the credibility of the system and in loss of invested money for purchasing the system.

The user interface must be simple, intuitive and with further possibilities to offer voting for people with special needs. The device itself must be easy to install for facilitating the setup of the voting center during the voting day.

Specialized and trained personnel must be available at each voting place to help in case of any technical issue. This also includes some contingency devices that must be located near to the voting places.

To avoid cyber-attacks the devices must operate without being connected to the internet, however at the closing of the voting center the device can connect just for transmitting the voting results. The transmission must be encrypted and through a secure network, preferable private APN to avoid transmission of data through public internet or access points.

For this specific case logistics plays a special role because there is a need to deliver the devices to several locations that are in different geographic areas.

References

Maurer, A. D. and Barrat, J. (2016). E-voting case law: A comparative analysis. Routledge.

Amelin, R., Channov, S., and Polyakova, T. (2016). Direct democracy: Prospects for the use of information technology. In First International Conference on Digital Transformation and Global Society, pages 258–268.

Ben-Nun, J., Farhi, N., Llewellyn, M., and Riva, B. (2012). A new implementation of a dual (paper and cryptographic) voting system. In Fifth International Conference on Electronic Voting, pages 315–329.

Agasi, O. (2015). Encapsulating mobile security. Computer Fraud & Security, 2015(6), 10-12.

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. Procedia Computer Science, 56, 376-383.

Wang, C., Chow, S. S., Wang, Q., Ren, K. & Lou, W. (2013), 'Privacy-preserving public auditing for secure cloud storage', IEEE transactions on computers 62(2), 362–375.

Yahyaoui, H., El-Qurna, J.&Almulla, M.(2020), 'Specification and recognition of service trust behaviors', Kuwait Journal of Science 47(1).

Sun, C.-C., Hahn, A., Liu, C.-C., 2018. Cyber security of a power grid: State-of-the-art. Int. J. Electr. Power Energy Syst. 99, 45–56.