Open Access Library Journal
2024, Volume 11, e12166
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Security Challenges around the Student Representative Council's e-Voting System at Public-Funded University in the Western Cape

Joel Chigada[1*], Dion Steven Tawanda Mazhawidza[2]

[1]School of Computing, Department of Information Systems, College of Science, Engineering & Technology, University of South Africa, Roodepoort, South Africa
[2]Department of Information Systems, University of the Western Cape, Bellville, South Africa
Email: *jchigada@iwc.ac.za

How to cite this paper: Chigada, J. and Mazhawidza, D.S.T. (2024) Security Challenges around the Student Representative Council's e-Voting System at Public-Funded University in the Western Cape. *Open Access Library Journal*, **11**: e12166.
https://doi.org/10.4236/oalib.1112166

Received: August 26, 2023
Accepted: September 22, 2023
Published: September 25, 2024

Abstract

This study examines the security challenges around the Student Representative Council (SRC)'s electronic voting systems at a public-funded university in the Western Cape province. Given the emergence of the global Corona Virus Disease (COVID-19) pandemic and South Africa's national energy crisis, universities have reconfigured their business models including the SRC voting system. The objective of this paper was to conduct a credible and preserve the SRC voting process. In addition, the study examined the security challenges brought about by the electronic voting system with the aim of suggesting appropriate interventions that could deter would be perpetrators. A qualitative research methodology was used to gather data from members of the SRC, students and student administration. Data were collected through a semi-structured interview, in a face-to-face environment. The study established user mistakes, technical errors and unacceptable user behaviour as the root causes of security vulnerabilities in the e-Voting system. Furthermore, the paper revealed that students voted for the SRC using their student numbers, thus, exposing the identities of voters. The recommendations were to generate numbers, allocate them to registered voters, and use them for voting. Election Officers were required to attend Information Security awareness training programmes in order to exercise due handling of people's information. The use of biometrics authentication was suggested to improve the security of information.

Keywords

Biometrics Authentication, Information Security, e-Voting, Student Representative Council, Security Vulnerabilities

1. Introduction

Electronic voting (e-voting) means an electronic ballot conducted through remote voting on the internet. This has been practiced in Estonia ("I-Voting"), and according to the Estonian government, I-Voting allows voters to cast their ballots from any internet-connected computer/mobile phone anywhere in the world [1]. After the Estonian government, many institutions began adopting the new online voting system. Since the 1980s, Internet voting has been a topic of interest when [2] proposed the use of mixed nets to ensure the secrecy of the vote. Today, the interest in Internet voting continues to grow constantly, with its increasing adoption in legally binding elections ranging from universities [3] [4]. The increase in the adoption of e-voting came from benefits such as voters' ability to cast ballots using their own devices and the fact that there is no time wasted in long queues. Voters do not travel long distances, thus, reducing transportation costs, and can do other business chores [4]. The system allows for inclusivity as people living with disabilities or serious medical conditions can exercise their democratic rights without transporting themselves to the polling station to cast ballots. In addition, Internet voting allows those people who will be traveling or will be on duty during election day to cast their ballots anywhere in the world [5] [6].

With an increase in institutions and countries adopting new ways of voting, there is a high chance that cyber attackers are likely to counterattack the voting systems. The computer security community has looked at online voting systems for decades and considers it an open problem [6]. This implies that electronic voting is an open book that can be explored by cyber attackers and tampered with for malicious reasons; hence security and privacy issues in (e-voting) have been receiving extensive attention recently [7] [8]. Many researchers believe paperless electronic voting machines are inherently insecure because they lack the transparency or verifiability necessary to prevent attacks by dishonest insiders [1] [6] [9]. Election boards overestimate the reliability of technology assume it will solve existing problems and ignore the potential for anticipated consequences and new vulnerabilities.

This study focused on the public university that has initiated the use of internet voting to elect its respective student representative council or political organisation. The greatest challenge with Internet voting arises from the fact that electoral authorities do not have control over all the equipment used by voters [10] and who cast their votes. The potential for former students accessing the system and casting their votes is very high. The checks and balances to verify are minimal and in many instances unavailable.

1.1. Overview of Electronic Voting (e-Voting)

The shift from computers to smart devices, the automation changes of computers connecting via wireless devices, and the use of these devices to produce information for humans to use in production and processing are termed Industry 4.0 (I4.0) [11]. Industry 4.0 comprises technologies that can be incorporated into voting.

Particularly cost-effective in voter authentication and identification, vote counting, publication of results, and voting and recording of votes cast [12] [13]. The electronic voting system uses Identity Document (ID) /Staff /Student numbers as voter authentication. At universities, student numbers are used as voter authentication. Some electronic voting systems allow electronic IDs either by way of a smart card or cell phone with a public key infrastructure capable of SIM-card, to authenticate themselves [7]. Electronic voting can also be described as the use of electronic devices over the internet to cast ballots at home or possibly at work [11]. These electronic devices are smart computers, mobile phones, or anything that can be connected to a server.

Electronic voting protocols have been implemented in different elections, ranging from university to government-based or political party elections [12]. The United States of America (US) is utilizing electronic voting during their government–based elections. The e-voting system involves several types of machines, touch screens for voters to mark choices, scanners to read paper ballots, and web servers to display results to the public. However, [4] advocates that the term e-voting is being used from casting votes by electronic means to asking the Internet community for an opinion on a political issue, to the publication of election results. According to [14], electronic voting is a more encompassing initiative than Internet voting since it can represent any means of electronic voting, including kiosks, Internet, telephones, punch cards, or optical scans. There are four types of electronic voting systems namely Computer Counting, Direct-recording electronic voting machines, Online voting, Poll site and Kiosk voting systems. However, the two main types of e-voting systems, remote voting and direct-recording electronic voting machines will be discussed in this paper because of their relevance to the SRC e-voting system used at the research site.

1.1.1. Direct-Recording Electronic Voting System

There has been extensive adoption of Direct-Recording Electronic (DRE) devices for voting at polling stations around the world [9]. The system was used by Brazil in the 2022 elections, and voters had to dial a number that corresponds to the desired candidate or party, which shows the name and photo of the candidate or party on the screen. After that process the voter would press a specific button to confirm the vote or cancel the vote and retry. [6] emphasize that this system requires voters to use a keyboard or touch screen to mark their votes on a computer terminal, directly connected to a stand-alone, polling-station-located computer. When the candidate selection procedure is completed, DRE systems present the final selection to the voter before ballot casting is completed [15]. This system is similar to a computer machine located inside the university library which is used by students to purchase printing and scanning credits. The system requires students to key in their student numbers for student identification. In contrast, researchers have identified security challenges with the DRE system that of manipulation of hardware and software by individuals [16]. Hardware can be manipulated to cause system failures during votes

or software can be manipulated with a malware virus to tamper with votes. [17] point out that could insert hidden computer code that would add, subtract, or change votes. In the best-known potential exploit, the hidden code would cause the DRE to record a different vote from what the voter sees on the face of the machine. Another possibility is that the malware could change vote totals after they had been recorded but before they were downloaded for tallying.

1.1.2. Remote Voting

This type of voting system allows voters to cast their votes from any computer or digital device connected to the Internet or to a private network, typically from home or at work. Devices such as personal digital assistance, mobile phones and even game machines may access these systems [6]. According to [18], remote electronic voting is a practice where voters are able to vote from a location unsupervised by election officials. The system is different from the Direct-Recording Electronic system because with the DRE system voters need to vote where the electronic device system is located meaning voters still need to queue to utilize the system, however with the remote system voters do not have to travel where the system is located, any electronic device can be utilized to vote. Remoting voting can be described as the voting system used in a remote, non-controlled environment, through electronic means, in which the vote is sent partially or totally via an Internet connection from a personal computer or mobile device which has not been specially designed as a specialized electronic voting machine [19]. The remote Voting system can be identified as a voting system that is utilized by the publicly funded university in the Western Cape. The system shares a website platform that allows students to vote through any electronic means in a non–controlled environment. Voters can vote wherever they are geographically located as long they have an Internet connection. A remote voting system is an entirely automated electronic voting environment that uses computers and telecommunication technologies for remote access [13]. However, the authors argue that with these types of electronic voting systems, there is a high chance that these systems can be breached and tempered if not secured accordingly [20].

Both e-Voting systems are confronted with a plethora of challenges that lead to security compromises and data breaches and these are discussed in section 1.2 to propose reasonable countermeasures.

1.2. Security Challenges Facing e-Voting Systems

1.2.1 Voter Identification and Voter Authentication

Voter identification is required during two phases of the electoral process: first, for registration to establish the right to vote, and afterward, at voting time, to allow a citizen or student to exercise their right to vote by verifying that the person satisfies all the requirements needed to vote. Voter identification would have to occur with some other types of credentials. This includes Social Security Numbers, dates of birth, driver's licenses, or some other unique identifier [3]. With the system utilized at the publicly funded university in the Western Cape, Student numbers,

dates of birth, and Identification Numbers (ID) are used as forms of voter identification.

Lack of voter identification can be a security challenge to the voting system because hackers or adversaries can acquire the voter's identification to register and vote for unknown voters, leading to fraudulent activities of votes. At universities, hackers and adversaries can acquire student numbers and Identification Numbers (ID). Especially nowadays where such important details are now linked to social media accounts or anywhere on the internet web for easy access to accounts [21]. In addition, students that are no longer studying at the university can still access the student system with ease, thus, another free passage of ghost voters.

As stated by [10] within most e-voting systems there is no way for a voter to verify that the vote recorded inside the voting machines/systems is the same as the vote he or she entered and displayed on the machine and system. Hence other researchers suggested that the electronic voting system must ensure, at every stage, the voting procedure of the vote is protected [22]. Various methods have been adopted to acquire voter identification; however, many challenges still arise on this issue.

1.2.2. Control over Equipment

Perhaps the greatest challenge with Internet voting arises from the fact that electoral authorities do not have control over the equipment used by voters [10] [22]. This can be a major threat, especially with the use of remoting voting whereby voters are voting from the comfort of their homes, using a certain website. Lack of control over equipment can provide room for hackers to hack voting software or systems especially personal devices connecting through unsecured public WiFi. Furthermore, voters cannot be assisted when faced with security challenges during the voting process, because the person who may be able to assist will illegally access personal information and use it unethically [8]. This is evident at the publicly funded university in the Western Cape where there are no interventions put in place when student voters are faced with security challenges such as software malfunctioning. The challenge with remote voting is that some of the electronic devices that are used by individuals might have malware viruses which might affect the voting website platform to function properly.

1.2.3. Denial-of-Service Attacks (DoS)

One of the security threats to electronic voting is susceptible to denial-of-service attacks. Denial-of-Service is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to a network [23]. DoS is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. This kind of attack is common on most software or website platforms especially when people are using URL links to connect to the service provider because many individuals can use the link at the same

time to connect to the site which may result in delays in connecting to the system [8] [21]. According to [24] election or government official can have knowledge of the inner working of an electronic voting system, and they can deliberately manipulate the system for either personal gain, or to change the election outcome. Hence it is crucial to have an independent third party to conduct audit checks of the electronic voting infrastructure and control voting equipment during election process.

1.2.4. Malware

Malware is software intentionally designed to cause disruption to computer, server, client or computer network to leak information, gain unauthorized access to information or systems [2]. The programs are mainly used broadly against government or corporate websites to gather information. For example, an election electronic voting system. Attackers can tamper with the software of voting machines to illegally access voting information by designing a program to erase voting data or edit vote data. In the 2014 Ukrainian presidential elections were hacked by a malicious code which deleted key files and made the vote tallying system inoperable, however the issue was quickly resolved before extensive damages were encountered. This malicious code can disrupt the voting system by not allowing the voters to vote for their desired election party [21] [25]. There are two threats of malicious code. The first one looks to plant malicious software into the election web server by attackers.

At the public funded university attackers can plant malicious software on the voting web server to destroy the student vote data. The second threat is the distribution of malicious software in voter computers thus affecting the election process [26]. For example, attackers can install malicious software, such as a vote–stealing program or denial-of-service attack on all computers at the university to prevent students from using computers on campus to vote during the election process, thus affecting the election process. Furthermore, the use of One Time Password was regarded as insecure measure as an authentication method because hackers nowadays deploy ways to have access to One Time Passwords. As stated by [17] [27] attackers can develop mobile phone and email malware especially Trojans, that are designed to intercept SMS messages containing OTPs. The virus can receive, alter, delete, and forward SMS or email messages without user interaction.

1.2.5. Spoofing Attacks

Another security issue of using electronic voting systems is Man-in-the-middle attacks. A man-in-the-middle attack is a type of cryptographic attack over a communication channel by a malicious third party where a person takes over a confidential communication channel between two or legitimate communicative points. The attacker can control the communication channel [28]. According to [26], there are several methods for an adversary to become a Man-in-the-middle and one of them is spoofing attacks, which deceive voters that they are communicating with the election web server. For instance, at universities, student voters during the SRC and

CHC election can be redirected from an official election website to a fake election web server, which allows exploitation and tampering of votes, because student votes have been misled that they are at a real voting website. Furthermore, a spoofing attack could result in an invasion of personal privacy which includes the personal information of voters. For instance, at universities, this can consist of student numbers, date of birth, and Identification Numbers [28].

1.2.6. Ransomware

A ransomware is the control of data or a system which restricts access of user interaction with the devices or system [7] [27]. Ransom attackers usually ask for hefty sums of money which called a ransom and data can only be released to users only after successful payment. Ransom is a "go-to-method of attack" for cybercriminals (Sausalito, 2020). In some worst scenarios, if the ransom is not paid the stolen data can be deleted from the devices or system resulting in financial and information losses. [29] states that ransomware attack may affect an entire landscape of security services, such as confidentiality, integrity, and availably (CIA Triad), which may not result in financial losses but may also result in important information. For example, a Texas company in United States that sells software that cities and states to display results on election night was hit by ransomware in November 2020. The ransomware required public officials to pay certain amount in order to decrypt the data to the Texas government officials.

Ransomware has affected a broad spectrum of industries like transport, telecommunications, financial companies, public law enforcement and health services. According to [30] when electronic voting system is targeted by this attack it renders the data hosted on the election servers (such as the votes cast) unavailable and therefore the election would have to stop. In some cases, the attackers could even disclose the data to the public (so-called "double or multiple extortions"). To illustrate, at a public-funded university, attackers can disclose confidential students' information details such as their student numbers and identification numbers, Furthermore, as mentioned by [31] "*Ransomware attacks frequently begin through email as typical phishing message purporting to be from someone the potential victim trusts, such as a co-worker or friend*".

To illustrate, an attacker portrayed as the student can send a fake voting website link via the student's email accounts to gain voting data details from students and use them for beneficial gains.

1.2.7. Social Engineering

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information [25] [32]. Social engineers take advantage of victims to get sensitive information, which can be used for specific purposes. For example, in the context of the public funded university electronic voting system, this sensitive information can be student numbers and identification numbers which can be used to register and vote without student knowledge. According to [32], there are two categories of social engineering, human-based or

computer-based. Within the human-based attack, the attacker executes the attack in person by interacting with the target to gather desired information. Students at universities can create relationships with other students in order to gain access of their partners confidential information. The second category is a software-based attack that is performed using devices such as computers or mobile phones to get information from the targets, and one of the attacks is spear phishing emails. Attackers can be a call or an email that directs individuals to fake website, at the research site context that would be an email that directs students to a fake electronic voting website [33] [34].

Some of the countermeasures that can be implemented to safeguard e-Voting systems are described in section 3 below.

2. Countermeasures to Safeguard e-Voting Systems

2.1. End-to-End Verification and Encryption

A properly designed vote verification process can allow a voter to perform end-to-end verification allowing checks indicating that votes have been recorded as cost and counted as recorded. In this paper the authors deploy vote verification methods, such as end-to-end verification which is a method that enables a voter to have an encrypted copy of the vote store in systems. End-to-end verification, cryptographic, or open–audit voting systems are systems which have been used to preserve ballot secrecy [35]. Furthermore, voters should not be allowed to vote twice, on an electronic system and this can be achieved by a proper authentication method. As illustrated by [18] a good authentication must be provided so that voters should have unambiguous regarding the security of electronic voting systems, and this can be achieved by the combined usage of visual cryptography and anti-phishing process. For instance, using a visual cryptography technique, voters can be able to identify whether they are utilizing a phishing web server or original site.

Apart from visual cryptography, voters can make use of biometric-based authentication method which allows the use of fingerprints, face recognition. [35] believe that biometric-based authentication will increase the security level of electronic voting systems because biometrics have personal characteristics different from one another, cannot be stolen or used by someone else. Universities must have this kind of authentication to secure the information of students which is regarded as highly confidential.

2.2. Blockchain-Based e-Voting Systems

After the rising popularity of Bitcoin, blockchain technology gained popularity in numerous sectors. The same technology is now being used in electronic voting systems. Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network [36]. This system can help voters' information to be secured because with a blockchain system every move and transaction is monitored and checked before being executed [35]. In addition, with the blockchain system, authorized viewers can view the voters'

information meaning access is blocked for unauthorized viewers. [35] [36] suggested that to ensure that the system is secure, during the electronic voting process, the block will contain the previous voter's information, so that if any of the blocks are compromised, then it would be easy to find out since all blocks will be connected to each other. This process prevents the duplication of multiple votes because it can detect if the number of votes is greater than the number of people who showed up to vote. For instance, if 1000 voters are registered in the blockchain and 1500 voters are detected in the system. The system can send an error message to the back-end of the system regarding the additional 500 votes in the blockchain system which provides an awareness of possible security breaches in the electronic voting system.

Blockchain technology generates cryptographically secure voting records. Votes are recorded accurately, permanently, securely, and transparently [35]. Permissions and cryptography prevent unauthorized access to the network and ensure that participants are who they claim to be. Furthermore, [18] [35] stated that Blockchain distributes individual voting information across thousands of computers globally making it impossible to alter or delete votes once they have been cast. These contribute to trust between voters, by protecting their data and privacy Data and privacy are important in terms of voting and with the use of blockchain technology data, votes can be secured from malicious attacks.

2.3. Anti-Virus Software and Firewall

Antivirus software protects computers from viruses, malware, spyware, worms and trojan horses easily. There are various antivirus software available in the market. This software protects our computer from viruses, updating virus definitions, block viruses, and prevents infections from virus [20]. As illustrated before, how malicious code can affect the votes in the system, anti-virus software can be a good intervention to prevent these malicious codes. Anti-virus software and Firewall can be used to protect computer where election ballot or data stored from viruses, worms, and firewalls can protect the electronic voting system from illegal access by blocking attackers from disrupting the private network. [5] [24] believe that the entire E-Voting System and the E-Voter database would be operating using the Internet services which make them more susceptible to online threats. Therefore, multiple layers of security would be implemented through the use of firewall and anti-virus to ensure highest levels of security for the web portal and mobile applications.

3. Methodology

The interpretivism paradigm was used to guide this qualitative research study. According to [37], interpretivists go into the real world, collect data on a particular research phenomenon, in this case on public-funded universities' electronic voting system from the user perspective. Interpretivism was utilized in qualitative research studies because the authors wanted to interpret what they got from the real world, that is from the students using the electronic voting system. In

qualitative research studies, non-numerical data is used to answer/solve a particular research question [38]. The qualitative research method was used in the research because the authors interacted with the student voters at the university to understand their perception of the established electronic voting system. In order to understand participant' lived experiences in a social environment, it was imperative to conduct semi-structured interviews [39]. A case study design was used because it provided the authors with an in-depth description of sample elements [40] [41]. [41] states that a case study allows investigators to retain the holistic and meaningful characteristics of real-life events, such as individual life cycles, small group behaviour, organizational and managerial processes, neighbourhood change and school performance. In addition, [42] states that despite the existence of many innovative designs and approaches for applied research, careful consideration should be given. It is vital for researchers to avoid using weak designs or with methodological flaws [42]. The authors of this paper used a case study design because of its strengths and wide use in qualitative research.

Primary data were collected using in-depth interviews from students who voted in 2021 and 2022 election of the SRC. A total of fifteen (15) participants were selected for this study. The Each interview was conducted for not more than15 minutes using a mobile voice recorder. Each interview was saved separately on the software. The interviews were saved as, '*Interview* 1, *Interview* 2...*Interview* 15'. The interview recordings were uploaded in ATLAS.TI version 9. ATLAS. TI version 9 is a qualitative data analysis program used by researchers to analyse qualitative data [39]. The authors used ATLAS. TI to organise, structure and be systematic with the data. The data that were aligned to the current electronic voting system, which cannot be found using secondary data [43].

4. Discussion of Findings

The study examined security challenges around the student representative council e-voting system at public—a funded university in the Western Cape. This section presents and discusses the findings from the 15 interviews.

4.1. Demographics of Participates

A total of 15 participants were selected for the study. The sample was based on individuals who reside on campus at the public-funded university in the Western Cape. The participants were mainly students who were part of political parties. Eight participants were males and seven were female. The majority (8) of the representative were between the ages of 24 - 44 males doing their post-graduate programs in Business Administration and Politics. The minority (7) were females between the ages of 18 - 24 third-year students studying Bachelor of Commerce. Furthermore, majority (10) of the respondents were student politicians from different political parties. This is a suitable sample as it was based on individuals who resided on campus with most of them having participated in the 2021 and 2022 SRC elections.

Table 1. Demographics of participants.

Gender	Age cohorts		Degree/Qualification of study		Frequency
	18 - 23	24 - 44	Postgraduate bus. admin & politics	BCom	
Male	3	5	8	-	8 (53.3%)
Female	5	2	-	7	7 (46.7%)
TOTAL					**100**

4.2. Challenges on the e-Voting System in the SRC/CHC Student Elections

In this research, the influences of student/ ID number, exclusion of other political parties, and the approval of OTP on the online voting system SRC/CHC student elections security challenges was analysed.

4.2.1. Student Number/ID Number

The use of ID numbers was identified as a determining factor across all the participants in all age groups. This was due to the lack of privacy and safety of information of other participants when using their student email accounts. One participant stated that:

> "Student numbers and numbers are no longer private information because nowadays everyone can have access to that information easily just pay certain people". This is a contributing factor because individuals can know other students' ID numbers and student numbers. Participant D states that "He can vote for his partner/friend without her knowledge because he knows his partner/friend's student number and ID number".

This information is confidential since it is required for voter authentication as illustrated by [3] in the literature review about voter identification such as social security numbers, dates of birth, driver's licenses, or some other unique identifier. However, this voter identification is not confidential at a public funded university in the Western Cape, student numbers and Identification numbers are recorded almost everywhere around the institution and this kind of information can be captured and tempered for beneficial gains.

Participant C mentioned that:

> "Student personal details are not safe because the information is recorded in open books everywhere around campus, especially at residential entrances where almost everyone can see other student personal details".

The disclosure of student information can lead individuals to steal the information for the purpose of gaining access to student email details and details needed to vote during the election process. In contrast, the findings from the study provided the view that individuals perceive the use of face recognition and fingerprints as good methods of identification. Participant Z mentioned the use of face

recognition or fingerprints as a method of identification prevents fraudulent activities on a large scale because it prevents inside attack activities and hacking of student information. Participant Z said:

> "Fingerprints can be ideal because it truly identifies the voter because you cannot be forced to use your fingerprint to identify yourself". Some respondents advocate the use of online voting and suggest going back to the traditional way "We should drop the online voting system until there are definite secure methods".

The utilization of fingerprints as an intervention was supported by researchers [44] when they illustrated that an effective tool to uniquely identify voters and prevent voters from re-voting is to use each voter's fingerprint as a form of biometric identification. Since each fingerprint is unique to a person, there will not be an opportunity to fake your eligibility or your name when voting. Moreover, a One Time Password is used as an identification key to connect to a server which can only be used once for security measures. The use of the receiving OTP code for voter confirmation via student email was disliked because most of the student email accounts are connected/linked to their student numbers and ID number. Participant D mentioned:

> "If I can access your email account then I can receive the OTP on your behalf".

The security issue of OTP authentication is supported by [17] in the literature review when the author illustrated that the use of One Time Password was regarded as insecure measure in term of authentication method because hackers nowadays have deployed ways to have access to One Time Passwords. This shows that receiving OTP passwords as a security measure is still a pending issue because there are no authentication methods put in place to secure the code once received on mobile numbers or email address.

Participant E mentioned she received an OTP code via email without her knowledge. In addition, participate B said:

> "Received an OTP notification before voting".

This implies that there are possibilities that a certain individual used the participant's student email account without the participant's knowledge, thereby if the student email accounts are linked to the student number and ID number individuals can get access to other student email accounts by using the user's student number as username and ID number as a password. In contrast, participants A and B mentioned that they prefer a link to receive an OTP in order to eliminate the process of receiving an OTP code via student email accounts. Especially participant B said:

> "I prefer receiving the OTP via my cell phone number because it is more convenient than via my student email account"

4.2.2. Exclusion of Other Political Parties/Management

The danger of interference by someone else in proximity to a voter (for example,

at home or at work) during the process of remote Internet voting in order to control the voting decisions through intimidation, fraud, and forced to vote sell. The involvement of political parties/members during the student voting process was identified as a challenge. Participant F mentioned that the involvement of political parties during the voting process affects the decision-making of the voters and said that:

"Political leaders can intimidate voters or buy votes from individuals".

One of the researchers agrees with respondent F when [2] illustrated that people intent on selling their vote by giving out their card IDs in electronic voting systems. With online voting, voters can sell their votes to different political parties. Furthermore, this inclusion of political parties/ institution management in the voting process may result in unfair activities from political parties/ management. Participant Y mentioned that:

"The involvement of management/political parties may result in fraudulent activities, especially when the institution does not want certain political parties involved in the institution's management. Management can assist in inside attacks to promote their agenda or propaganda".

[33] supports participant Y that the system is vulnerable to inside attacks when the author illustrated that inside attacks from system administrators can contribute to temper around election outcomes to favour candidates. In addition, other participants believed there was an inside attack involved during the elections, according to voters' stats, more than 1000 students voted from 3 am to 6 am on the last day of voting. In contrast, this can be biased information because students can vote during that time because the system was available 24/7. The inclusion of political members during the voting process can be relevant to support other voters who do not have the technical skills to access the website or server during the voting process or voters who face system challenges during the voting process. Findings from the study suggested that political parties and institution management must not be involved during the election process. Participant X mentioned involving a different group of control that does know anything about the political parties and institutions "*Inclusion of a special group can prevent fraudulent activities because they have only one job which is to monitor the election process*".

4.2.3. System Failure

The possibility of system attacks or breakdowns, or connection failure. **Table 1** shows some of the numbers of voters who were logged on the system and did not complete casting their votes. This incompletion could have been caused by the system taking a long to respond, which is related to connection failure. In addition to this connection failure, the system could have experienced bottlenecks where there is an overload of users using the system. For instance, more than 1000 students would want to vote on the system simultaneously, which may result in system breakdowns. Some participants stated that the system would have some

periods where voters struggled to vote, delaying them to cast from casting votes and forfeiting their votes. With these system breakdowns and connection failures mentioned and experienced by student voters, there was no intervention to mitigate the problems. Participant N stated that:

> "When the system was experiencing these challenges, they would try again until the system began responding."

[10] support participant N when the author illustrated in the literature review that electrical authorities do not have control over the equipment used by voters, this equipment can be the system that the voters utilized during the voting system. Another researcher in the literature [27] also support respondent N regarding the issue of system lags which can be caused by malicious code that can be installed on the Web server or system to disrupt the voting process. Furthermore, other researchers also support the response when [9] illustrated that malware may prevent casting votes (potentially stealthily, leading voters to believe they did cast votes), deceive voters about any aspect of the voting process, publicly expose voters' choices, or degrade the experience to deter voters from voting at all.

5. Conclusions

The study examined the security challenges around the Student Representative Council electronic voting system at the public-funded university in the Western Cape. Relevant literature on electronic voting systems and the types of electronic voting systems, namely, direct recording electronic voting systems and remote voting, were discussed. The study outlined the security challenges and interventions that are put in place to mitigate these types of voting systems. The study revealed that current security challenges include the use of student numbers and identification numbers as voter identification and authentication and the inclusion of other political parties/management during the voting process. The overall results of this study recommended the use of biometric authentication fingerprints or face recognition for voter identification which makes the student information private and secure from other individuals. The study suggested that the electronic voting system should be monitored and protected by system administrators to prevent denial of service attacks and the installation of malicious software being installed in the voting system from outsiders. To prevent outsiders from having access to student email accounts when receiving their One Time Passwords, students should change their passwords or use multi-authentication factors so that no attackers can predict their login details. Lastly, the authors advise that web servers and systems utilized for the voting processes should be protected from malware infections with the use of antivirus and firewall programs. However, the findings provide room for research to be conducted as only front-end users of the voting system were used for analysis. With more information, more findings can be drawn to counter the challenges.

Acknowledgements

I acknowledge Professor Joel Chigada, the academic supervisor for his scientific contribution during the time of this study. A special thank you and appreciation to the Department of Information Systems at the University Western Cape for allowing Deon to conduct this study during the COVID-19 pandemic. Joel Chigada acknowledges Dion Mazhawidza's contribution in conceptualizing this paper and agreeing to publish it.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Madheswari, N.S.A.N. (2016) Secured Authentication for Internet Voting in Corporate Companies to Prevent Phishing Attacks. *International Journal of Emerging Technology in Computer Science & Electronics* (*IJETCSE*), **22**, 976-1353.

[2] Birch, S., Cockshott, P. and Renaud, K. (2014) Putting Electronic Voting under the Microscope. *The Political Quarterly*, **85**, 187-194. https://doi.org/10.1111/1467-923x.12071

[3] Batt, S. (2019) How Electronic Voting Works: Pros and Cons vs. Paper Voting. https://www.makeuseof.com/tag/how-electronic-voting-works/

[4] Buchsbaum, T.M. (2004) E-Voting: International Developments and Lessons Learnt. 31-42. http://dl.gi.de/handle/20.500.12116/29127

[5] Matharu, G.S., Mishra, A. and Chaudhary, L. (2014). Integrated Election Voting System: A Model for Leveraging ICT in the Indian Election Scenario. *Proceedings of the* 2014 *International Conference on Information and Communication Technology for Competitive Strategies*, Udaipur, 14-16 November 2014, 1-7. https://doi.org/10.1145/2677855.2677944

[6] Qadah, G.Z. and Taha, R. (2007) Electronic Voting Systems: Requirements, Design, and Implementation. *Computer Standards & Interfaces*, **29**, 376-386. https://doi.org/10.1016/j.csi.2006.06.001

[7] Chigada, J.M. (2020) A Qualitative Analysis of the Feasibility of Deploying Biometric Authentication Systems to Augment Security Protocols of Bank Card Transactions. *SA Journal of Information Management*, **22**, a1194. https://doi.org/10.4102/sajim.v22i1.1194

[8] Chigada, J. and Daniels, N. (2021) Exploring Information Systems Security Implications Posed by BYOD in a Financial Services Firm. *Business Information Review*, **2**, 1-12.

[9] Park, S., Specter, M., Narula, N. and Rivest, R.L. (2020) Going from Bad to Worse: From Internet Voting to Blockchain Voting. Oxford University Press, 2-12.

[10] Jefferson, D., Rubin, A.D., Simons, B. and Wagner, D. (2004) Analyzing Internet Voting Security. *Communications of the ACM*, **47**, 59-64. https://doi.org/10.1145/1022594.1022624

[11] Ajish, S. and AnilKumar, K.S. (2021) Secure Mobile Internet Voting System Using Biometric Authentication and Wavelet Based AES. *Journal of Information Security and Applications*, **61**, Article ID: 102908. https://doi.org/10.1016/j.jisa.2021.102908

[12] Tarasov, P. and Tewari, H. (2017) The Future of E-Voting. *IADIS International Journal on Computer Science and Information Systems*, **12**, 148-165.

[13] Unt, T., Solvak, M. and Vassil, K. (2017) Does Internet Voting Make Elections Less Social? Group Voting Patterns in Estonian E-Voting Log Files (2013-2015). *PLOS ONE*, **12**, e0177864. https://doi.org/10.1371/journal.pone.0177864

[14] Carter, L. and Bélanger, F. (2012) Internet Voting and Political Participation. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, **43**, 26-46. https://doi.org/10.1145/2351848.2351851

[15] Khan, K.M., Arshad, J. and Khan, M.M. (2020) Investigating Performance Constraints for Blockchain Based Secure E-Voting System. *Future Generation Computer Systems*, **105**, 13-26. https://doi.org/10.1016/j.future.2019.11.005

[16] Yao, Y. and Murphy, L. (2007) Remote Electronic Voting Systems: An Exploration of Voters' Perceptions and Intention to Use. *European Journal of Information Systems*, **16**, 106-120. https://doi.org/10.1057/palgrave.ejis.3000672

[17] Mulliner, C., Borgaonkar, R., Stewin, P. and Seifert, J.P. (2013) SMS-Based One-Time Passwords: Attacks and Defense (Short Paper). 1-10. https://www.semanticscholar.org/paper/SMS-Based-One-Time-Passwords%3A-Attacks-and-Defense-Mulliner-Borgaonkar/a925a0f165c82b01c587215dcd66e06a7b10dcdf

[18] Abu-Shanab, E., Khasawneh, R. and Alsmadi, I. (2013) Authentication Mechanisms for E-voting. In: Saeed, S. and Reddick, C.G., Eds., *Human-Centered System Design for Electronic Governance*, IGI Global, 71-86. https://doi.org/10.4018/978-1-4666-3640-8.ch006

[19] Marcos del Blanco, D.Y., Panizo Alonso, L. and Hermida Alonso, J.A. (2018) Review of Cryptographic Schemes Applied to Remote Electronic Voting Systems: Remaining Challenges and the Upcoming Post-Quantum Paradigm. *Open Mathematics*, **16**, 95-112. https://doi.org/10.1515/math-2018-0013

[20] Kumar, V. and Kumra, S. (2016) Computer Systems Security and Support for Internet Voting System. *International Journal of Engineering Applied Sciences and Technology*, **1**, 50-53. http://www.ijeast.com

[21] Sausalito, C. (2020) Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[22] Mahr, J. (2021) What Are the Security Requirements for Online Voting? EDGE Elections. https://medium.com/edge-elections/what-are-the-security-requirements-for-online-voting-9fafa67892ab

[23] Chigada, J. (2023) Towards an Aligned South African National Cybersecurity Policy Framework. Ph.D. Thesis, University of Cape Town.

[24] Ravi, D. (2020) Part 1: Security Vulnerabilities of e-Voting—Keesing Platform. https://platform.keesingtechnologies.com/evoting-security-vulnerabilities/

[25] Salahdine, F. and Kaabouch, N. (2019) Social Engineering Attacks: A Survey. *Future Internet*, **11**, Article No. 89. https://doi.org/10.3390/fi11040089

[26] Javaid, M.A. (2014) Electronic Voting System Security. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2393158

[27] Zhong, F., Chen, Z., Xu, M., Zhang, G., Yu, D. and Cheng, X. (2023) Malware-on-the-Brain: Illuminating Malware Byte Codes with Images for Malware Classification. *IEEE Transactions on Computers*, **72**, 438-451.

https://doi.org/10.1109/tc.2022.3160357

[28] Mallik, A. (2019) Man-in-the-Middle-Attack: Understanding in Simple Words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, **2**, 109-134. https://doi.org/10.22373/cj.v2i2.3453

[29] Reshmi, T.R. (2021) Information Security Breaches Due to Ransomware Attacks—A Systematic Literature Review. *International Journal of Information Management Data Insights*, **1**, Article ID: 100013. https://doi.org/10.1016/j.jjimei.2021.100013

[30] Rodriguez-Perez, A. (2021) Five Common Attacks Against Online Voting. https://medium.com/edge-elections/five-common-attacks-against-online-voting-599036eb3e80

[31] Yaqoob, I., Ahmed, E., Rehman, M.H.U., Ahmed, A.I.A., Al-garadi, M.A., Imran, M., *et al.* (2017) The Rise of Ransomware and Emerging Security Challenges in the Internet of Things. *Computer Networks*, **129**, 444-458. https://doi.org/10.1016/j.comnet.2017.09.003

[32] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015) Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, **22**, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

[33] Halderman, J.A. (2019) Practical Attacks on Real-World E-Voting. University of Michigan. In: Hao, F. and Ryan, P.Y.A., (Eds.), *Real-World Electronic Voting: Design, Analysis and Deployment*, Auerbach Publications, 143-170.

[34] Nyasvisvo, B. and Chigada, J. (2023) Phishing Attacks: A security Challenge for University Students Studying Remotely. *The African Journal of Information Systems*, **15**, 1-27.

[35] Ben Ayed, A. (2017) A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications*, **9**, 1-9. https://doi.org/10.5121/ijnsa.2017.9301

[36] Panja, S. and Roy, B. (2021) A Secure End-to-End Verifiable E-Voting System Using Blockchain and Cloud Server. *Journal of Information Security and Applications*, **59**, Article ID: 102815. https://doi.org/10.1016/j.jisa.2021.102815

[37] Bryman, A. (2016) Social Research Methods. 5th Edition, Oxford University Press. https://ktpu.kpi.ua/wp-content/uploads/2014/02/social-research-methods-alan-bryman.pdf

[38] Creswell, J.W. and Creswell, J.D. (2018) Mixed Methods Procedures. In: Creswell, J.W., Ed., *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, SAGE Publications, Inc., 418.

[39] Babbie, E. (2010). The Practice of Social Research. 12th Edition, Wadsworth.

[40] Gill, S.L. (2020) Qualitative Sampling Methods. *Journal of Human Lactation*, **36**, 579-581. https://doi.org/10.1177/0890334420949218

[41] Yin, R.K. (2009) Case Study Research: Design and Methods (Fourth, vol. 5). SAGE Ltd. https://books.google.co.za/books?id=FzawI-AdilHkC&printsec=frontcover&dq=yin++case+study+4th+edition&hl=en&sa=X&redir_esc=y#v=onepage&q=yin%20%20case%20study%204th%20edition&f=false

[42] Arthur, P.B. (2018) Caregiving in Alzheimer's Disease: Research Designs & Considerations. *Advances in Alzheimer's Disease*, **7**, 36-49. https://doi.org/10.4236/aad.2018.72003

[43] Sutton, J. and Austin, Z. (2015) Qualitative Research: Data Collection, Analysis, and Management. *The Canadian Journal of Hospital Pharmacy*, **68**, 226-231. https://doi.org/10.4212/cjhp.v68i3.1456

[44] Dandapani, A., Hartigan, B. and Kennedy, J. (2021) Fingerprint Protected Voting Machine. https://courses.grainger.illinois.edu/ece445/getfile.asp?id=18903