EXPLORING THE SECURITY CHALLENGES OF AN E-VOTING SYSTEM (EVS). A CASE STUDY IN THE BOLGATANGA SENIOR HIGH SCHOOL (BIGBOSS)

ABSTRACT

The integration of electronic voting systems (EVS) into electoral processes promises increased efficiency, speed, and transparency. However, this technology also introduces a variety of security challenges that must be addressed to ensure the integrity of the voting process. This study explores the security vulnerabilities of an EVS, focusing on its implementation at Bolgatanga Senior High School (BIGBOSS). Through a case study approach, this research examines the potential threats to the EVS, including issues related to data privacy, system integrity, authentication protocols, and susceptibility to cyber-attacks. A mixed-methods strategy was employed, utilizing surveys, interviews, and system tests to assess both technical vulnerabilities and user experiences. Key findings reveal concerns over data breaches, weak encryption methods, and unauthorized access, alongside challenges in user trust and system adoption. Recommendations include strengthening encryption protocols, improving user authentication measures, and enhancing cyber security awareness among stakeholders. These findings contribute to the ongoing discourse on EVS security, providing insights into practical measures for improving the reliability and safety of electronic voting systems in educational institutions and beyond.

Keywords: electronic voting system, security challenges, data privacy, encryption, cyber-attacks, Bolgatanga Senior High School, system integrity

INTRODUCTION

In every democratic context where individuals hold varying and often conflicting viewpoints, the necessity arises to choose among multiple alternatives. According to [1], this dynamic unfolds in various settings, including the corporate world, educational institutions, social organizations, and most prominently, in the realm of government. One established method for arriving at decisions amidst such diversity is the practice of voting [2]. Therefore, the electronic voting (E-voting) represents the advancement of modernizing the electoral process by ushering it into the digital era. This transition holds paramount

importance in terms of minimizing paperwork, enhancing efficiency in terms of time, and yielding cost-effectiveness [3]. As we move into this digital age, it is of utmost significance to maintain the trust of the populace by ensuring the comprehensive security of the entire process. This way, voters can readily grasp and accept the changes with confidence and ease [4]. [5]assert that electoral integrity is essential not just for democratic nations but also for state voter's trust and liability. Political voting methods are crucial in this respect. From a government standpoint, electronic voting technologies can boost voter participation and confidence and rekindle interest in the voting system. As an effective means of making democratic decisions, elections have long been a social concern[6]. As the number of votes cast in real life increases, citizens are becoming more aware of the significance of the electoral system. Further, voting represents a formal procedure for individuals to express their individual opinions, whether in favour of or against a specific proposal [7]

LITERATURE REVIEW

According to [8]constitutes a pivotal element of the democratic process, where qualified individuals convey their preferences or selections by submitting a ballot in support of a candidate, a political party, or a specific matter within the context of an election or a formal decision-making procedure. [9]Voting serves as a means for citizens to actively engage in the administration of their nation or locality, enabling them to exert influence in shaping the results of elections, referendums, or other significant determinations. Voting

plays a central role in democratic societies, as it allows citizens to have a voice in selecting their leaders and influencing government policies [10]. It is a cornerstone of representative democracy and is used to make decisions on a wide range of issues, from electing political leaders to approving or rejecting legislation and policies.

According to [11], an electronic voting system comprises mechanical, electromechanical, and electrical components, along with software that manages device control, ballot definition, vote casting and counting, and result calculation and display. [12]the primary functions of e-voting systems include registering voters in a list or registry, verifying their legitimacy, authenticating and authorizing users, enabling the casting of votes, displaying electronic ballots for anonymous citizen voting, gathering cast votes through a central server, processing votes, and ultimately calculating and presenting election results. E-voting systems evolved from mechanical voting machines in the late 19th century to the development of internet voting today. Innovations like punch card voting, optical scan systems, and direct-recording electronic (DRE) machines have shaped modern voting. Internet voting has also emerged, offering convenience but posing significant security challenges [13]. E-voting makes voting more accessible, especially for individuals with disabilities, offering features like screen readers and voice commands [14]. However, robust security measures are essential to protect the integrity of the system. Encryption, multi-factor authentication, and regular security audits are critical to ensure secure elections [15]. SaproSoft E-voting System, myBallotBox e-voting system allows voters to cast their votes securely using personal devices. It offers features such as voter registration, secure login with OTP verification, and a voter-verified audit trail (VVAT) for transparency. The system ensures that elections are conducted efficiently, minimizing errors and enhancing voter confidence [16]. However, the faces several security challenges, including potential attacks on DRE systems, which may involve unauthorized software modifications and a lack of voter-verifiable audit trails [17]. Additionally, internet voting systems are vulnerable to denial-of-service attacks, malware, and man-in-the-middle attacks, compromising the election's fairness and integrity [18].

METHODOLOGY

A research design is procedural plan that is adopted in a study to answer questions validly, objectively, accurately and economically[19]. This study is a qualitative study and uses an exploratory research

methodology. This is a research methodology that is used to investigate a problem which is not clearly defined. Therefore, this research methodology was adopted and used to unravel an unclearly defined problem of the security challenges of an E-voting system (Saprosoft E-voting system) at the Bolgatanga Senior High School, Ghana.

RESULTS AND FINDINGS

MyBallotBox(E-voting system)

MyBallotBox is a web-based voting system that will helps you manage elections. This voting system is used for casting votes during the elections held in senior high schools and other institutions . In this system there is a database which is maintained in which all the name of the voters with their complete information is stored. The System Administrator registers the voters by simply filling a registration form to register the voters. After registration, the voter is assigned a secret voter ID and password with which he/she can use to login to the system and cast his/her vote

The components of the evoting system

Dashboard

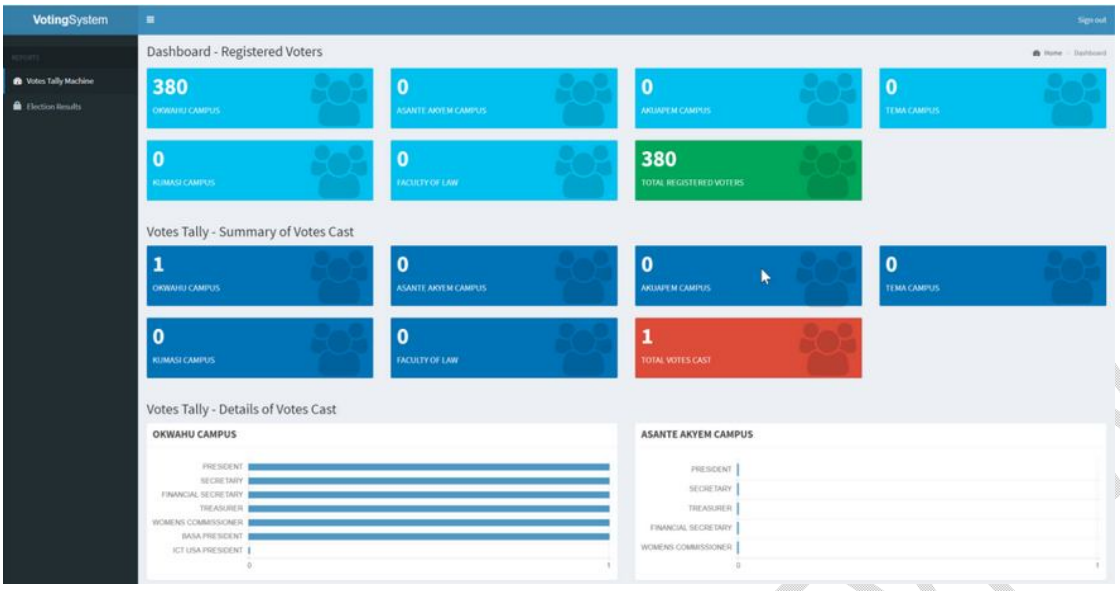

Figure 1: Saprosoft E-voting System interface

Voter Login

A student is required to key in a system generated Voter ID and password to have access to the portal.

Figure 2. Voter login

Electronic Ballot Paper

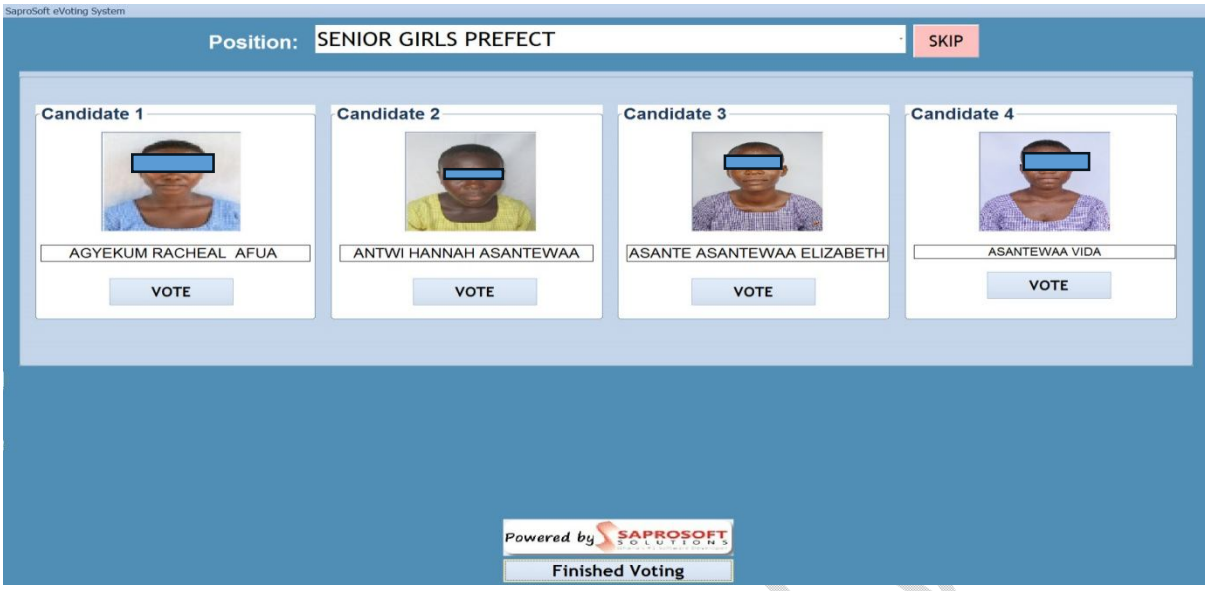

Figure 3: Electronic Ballot paper

Once the system validates the login credentials provided, the various positions declared will appear with the candidates.

1. A voter is required to select one candidate from the list of candidates by clicking on the 'VOTE' button.
2. Once the vote is confirmed, the system automatically takes the voter to the next position and repeats step 1 above until all position are voted for.
3. In the event that a voter decides not to vote for any of the candidates, voter can click on 'skip' button on top of the screen.

The methods to identify and analyse the security challenges of an e-voting system.

Experts in this study cited that security is important in an E-voting system (myBallotBox). Experts believe that, "*End-to-End Encryption technology is employed to ensure that data, including votes, is encrypted from the voter's device to the central server. Only authorized parties can decrypt and access the information*"**.** Trust in the electoral process is fundamental to the functioning of a democracy. If voters and stakeholders doubt the security and integrity of the voting system, it can erode trust in the entire democratic system. Security breaches or vulnerabilities in e-voting systems can lead to allegations of

fraud and a loss of confidence in election outcomes. Also, expert B says that, "*Security measures in e-voting systems are essential to guarantee that elections are conducted fairly and transparently"*. Expert C believe that, "*Robust authentication mechanisms, such as biometrics, smart cards, or multi-factor authentication, are employed to verify the identity of voters and prevent unauthorized access*. However, the SaproSoft E-voting system does not use the biometric and smart card technology that is making it a challenge for voter because they have to still come to the voting centre in other to cast their votes.

Further, some common security challenges that e-voting systems face according to experts, "*E-voting systems rely on networked infrastructure for communication, making them susceptible to network-based attacks such as DDoS attacks or hacking."* Example: In 2016, the Democratic National Committee (DNC) in the United States fell victim to a cyber-attack attributed to Russian hackers, leading to the release of sensitive emails.

Expert D says, "*Insiders with access to e-voting systems may pose a threat by abusing their privileges or leaking sensitive information"*. Example: In 2014, a technician with insider access was arrested for allegedly tampering with e-voting machines in Virginia, USA. While no actual tampering was confirmed, it raised concerns about insider threats. More so, ensuring that voters are who they claim to be is critical to prevent voter impersonation and identity theft. Expert D revealed that, *"in some cases, voters have reported instances of identity theft where their votes were cast by someone else without their consent".* These jeopardies the authenticity of the election process.

Expert E also believe that, E-voting machines can become infected with malware or viruses, potentially altering votes or disrupting the election. He further cites that, "*in 2010, researchers demonstrated that they could infect a widely used e-voting machine with a virus that could spread between machines and manipulate votes".*

Ensuring the integrity of the supply chain for e-voting machines and software is essential to prevent tampering during production or distribution, according to experts D, "*Concerns have been raised about the security of the supply chain for e-voting machines, particularly those manufactured overseas".*

According to the students, failing to conduct independent security audits can leave vulnerabilities undiscovered. For instance, various jurisdictions have faced criticism for not conducting thorough security assessments of their e-voting systems, which can lead to concerns about their reliability.

Additionally, when conducting a security assessment of an e-voting system, the steps or methodologies would you follow to identify potential security vulnerabilities or weaknesses. Gathering of information and documentation about the E-voting system is the number one task to consider.

For instance, the respondent's expert E, "*collect all available documentation about the e-voting system, including system architecture, source code, design documents, user manuals, and any security-related documentation"*

Consider managing the risk identified by evaluating the potential impact and likelihood of each identified threat. Expert D says, "*Prioritize them based on risk, focusing on those with the highest impact and likelihood".*

Conduct penetration testing to simulate attacks and vulnerabilities exploitation. Expert A highlighted this process; *vulnerability scanning and assessment, network penetration testing, application testing, social engineering assessments, and wireless network testing (if applicable).*

Authentication and Authorization Assessment is very crucial in any E-voting system. Examine the authentication and authorization mechanisms within the system. Expert D, says *"Check for weak password policies, inadequate session management, and unauthorized access issues"*

Based on their responses, security assessments should be conducted by experienced professionals who are well-versed in cybersecurity practices and have a deep understanding of e-voting systems. Additionally, ensure that the assessment is conducted with the utmost care to maintain the integrity and confidentiality of the voting process.

Security challenges of the SaproSoft E-voting system used in Bolgatanga Senior High School.

Describing the specific security features and protocols implemented in the SaproSoft E-voting system to ensure the integrity and confidentiality of the voting process in Bolgatanga Senior High School. Expert A says, "*the software is on web and all device connected to the software must be on the same network before the can function"*. Any device on a different network cannot access the software. "*This prevent hackers from hacking into the system because they are not on the same network and cannot see the IP address of the programme"*. However, it possesses a challenge for voters because as it is design to serve a convened way to vote, voters still have to form a long queue to cast their vote which can lead to physical security breach of the system.

Measures in place to authenticate and verify the identity of voters in the system and how the system prevent unauthorized individuals from casting vote. "*Expert B say, password and user name are generated by the system. The challenge here is that anybody can pick the password and user name and use it to cast a vote".* Also, students can use their friend's user name and password to cast a vote. Also, he revealed an insider lets out the IP address by abusing his or her privileges can lead to hacking of the system.

How is the secrecy of the ballot ensured within the system? What safeguards are in place to prevent votes from being traced back to individual voters? According to expert C "*the secrecy of the ballot is aimed at ensuring that a vote is anonymous and cannot be traced back to the person who cast it"*. All votes mixed randomly in the system with and end-to-end encryption and cannot trace back. According to expect E, "*the user name that are generated by the system are unique to everyone and does not use any personal information by the voter"*.

Physical security measures in place to protect the hardware components of the e-voting system, such as voting machines or servers, from tampering or unauthorized access. According to expert B, "*one of the greatest security challenges is the physical attack on the E-voting system. Because is a web software and all devices must be on the same network before it can work, the machines are exposed to physical attack*

”

What innovative solutions are there to enhance the security of E-voting System.

Enhancing the security of e-voting systems is crucial to ensure the integrity, confidentiality, and trustworthiness of the electoral process. Here are some innovative solutions according to experts to enhance the security of e-voting systems:

According to expert A “*implementing a blockchain-based e-voting system where each vote is recorded as a transaction in a tamper-resistant and transparent ledger will go a long way to improve the security of the E-voting system”*. Blockchain enhances the integrity and auditability of the voting process. Also, the utilize homomorphic encryption to allow votes to be encrypted in a way that they can be counted without decryption, preserving voter privacy while ensuring the accuracy of the count.

Moreso, according to expert B “*the implementation and use biometric verification to ensure the identity of voters”*. Biometrics like fingerprint and facial recognition can enhance security and prevent impersonation. Further, use secure hardware modules, such as trusted platform modules (TPMs), to protect critical components of the e-voting system against physical attacks.

Furthermore, expert C said “*the use digital signatures to verify the authenticity of electronic ballots and ensure that they haven't been altered during transmission”*. This prevents doubt about the authenticity of the vote cast. Besides, develop secure mobile apps for remote voting, Expert E says, there should be an “*incorporating robust security features and encryption to protect votes cast via mobile devices and not necessarily depending of the same network to function properly”*. This will reduce the crowd at the voting centre, thereby preventing physical attack and securing the votes through a robust security protection.

Expert D suggests that there should be the “*implementation of real-time monitoring of the e-voting system to detect and respond to security threats promptly”* and also provide ongoing cybersecurity education and training to election officials, staff, and voters to raise awareness and reduce the risk of human error.

CONCLUSION AND RECOMMENDATION

Through several reviews and observation of the Saprosoft e-voting system offer numerous benefits. However, it's important to implement them with strong security measures and transparency to address potential concerns and ensure the integrity of the electoral process. Public trust in the technology and processes used is essential for the success of e-voting systems. To address these challenges, e-voting systems must undergo rigorous security assessments, adhere to best practices, and be subject to independent scrutiny and auditing. Additionally, collaboration with cybersecurity experts, election officials, and stakeholders is essential in designing and implementing secure e-voting systems. The recommends that security assessments should be conducted by experienced professionals who are well-versed in cybersecurity practices and have a deep understanding of e-voting systems. Also, E-voting system such myBallotBox should incorporate the biometric verification technology in other to secure the votes and the identity of the voter. myBallotBox should be able to generate unique user name and password which cannot be used by anybody except that unique person. Also, the E-voting system should ensure that all its device should not necessarily be no the same network or connected to one sever in other to avoid overload. Whereas there are still security measures to ensure that hacker do not penetrate into the system.

CONSENT

In accordance with international or university standards, the author(s) have obtained and retained written consent from the respondents.

ETHICAL APPROVAL

In compliance with international or university standards, the author(s) have obtained and retained written ethical approval.

REFERENCES

[1] S. S. Chaeikar, A. Jolfaei, N. Mohammad, and P. Ostovari, “Security Principles and Challenges in Electronic Voting,” in *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW*, 2021. doi: 10.1109/EDOCW52865.2021.00030.

[2] J. Díaz-Santiso and P. Fraga-Lamas, “E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts †,” *Eng. Proc.*, vol. 7, no. 1, 2021, doi: 10.3390/engproc2021007011.

[3] U. Jafar, M. J. A. Aziz, and Z. Shukur, “Blockchain for electronic voting system—review and open research challenges,” *Sensors*, vol. 21, no. 17. 2021. doi: 10.3390/s21175874.

[4] E. de las M. Zurita Meza and D. S. Ramírez Supe, “Vulnerabilities and securities in the electronic voting: a review,” *Rev. ODIGOS*, vol. 2, no. 1, 2021, doi: 10.35290/ro.v2n1.2021.405.

[5] M. A. Javaid, “Electronic Voting System Security,” *SSRN Electron. J.*, 2014, doi: 10.2139/ssrn.2393158.

[6] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, “Analysis of an electronic voting system,” in *Proceedings - IEEE Symposium on Security and Privacy*, 2004. doi: 10.1109/SECPRI.2004.1301313.

[7] C. Vancouver, “Security Principles and Challenges in Electronic Voting,” *J. Intell. Conflict, Warf.*, vol. 1, no. 3, 2019, doi: 10.21810/jicw.v1i3.821.

[8] S. Nissen, “Political Participation: Inclusion of Citizens in Democratic Opinion-Forming and Decision-Making Processes,” 2021. doi: 10.1007/978-3-319-95960-3_42.

[9] S. Nissen, “Political Participation: Inclusion of Citizens in Democratic Opinion-forming and Decision-Making Processes,” 2021. doi: 10.1007/978-3-319-71066-2_42-1.

[10] A. Turska-Kawa and W. Wojtasik, “Communication Function of Elections,” *Commun. Today*, vol. 4, no. 1, 2013.

[11] Y. M. Wahab *et al.*, “A Framework for Blockchain Based E-Voting System for Iraq,” *Int. J. Interact. Mob. Technol.*, vol. 16, no. 10, 2022, doi: 10.3991/ijim.v16i10.30045.

[12] M. A. Dorantes Gonzalez, M. R. Cordero Lopez, and J. B. Silva Gonzalez, “Official Voting System for Electronic Voting : E-Vote,” 2014. doi: 10.5121/csit.2014.4508.

[13] A. Le Bellec, “Toward a Gender-Sensitive Securitization of the Common European Asylum System,” *Front. Hum. Dyn.*, vol. 3, 2021, doi: 10.3389/fhumd.2021.635809.

[14] M. K. Alomari and H. U. Khan, “Toward a Significant E-Voting Adoption Model,” *Int. J. Technol. Hum. Interact.*, vol. 18, no. 1, 2022, doi: 10.4018/ijthi.300283.

[15] A. Seth, D. S. Narang, A. Sagar, and S. Jain, “SoulBound E-Voting System,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 3, 2023, doi: 10.22214/ijraset.2023.48548.

[16] A. Sarker, S. Byun, W. Fan, M. Psarakis, and S. Y. Chang, “Voting Credential Management System for Electronic Voting Privacy,” in *IFIP Networking 2020 Conference and Workshops, Networking 2020*, 2020.

[17] B. Collier, D. R. Thomas, R. Clayton, A. Hutchings, and Y. T. Chua, “Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services,” *Polic. Soc.*, vol. 32, no. 1, 2022, doi: 10.1080/10439463.2021.1883608.

[18] H. Sandberg, V. Gupta, and K. H. Johansson, “Secure Networked Control Systems,” *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 5. 2022. doi: 10.1146/annurev-control-072921-075953.

[19] &Na; *et al.*, “How to Critique Research,” *Assess. Eval. High. Educ.*, vol. 31, no. 2, 2011.