IMPROVEMENT OF VOTING SYSTEM THROUGH VISUAL CRYPTOGRAPHY AND MULTI-FACTOR AUTHENTICATION TO FURTHER MITIGATE CLONE PHISHING ATTACK

Abstract

Background: The growing concern over phishing attacks on voting systems, particularly with the rise of online voting, has highlighted vulnerabilities in elections. The convenience of internet voting has led to security risks like clone phishing attacks. While online voting offers accessibility benefits, security, privacy, and usability issues have arisen. Multi-factor authentication (MFA) has been proposed to enhance security in mobile internet voting systems. Visual cryptography, dividing images into shares for decentralized data storage, is suggested to counter clone phishing. MFA's effectiveness in various sectors is established, and secure voting systems combining visual cryptography and blockchain have been proposed. Challenges remain for visual cryptography, making additional security measures crucial. This research sought to bolster the security of the voting system using visual cryptography and multi-factor authentication (MFA), with the goal of increasing voter trust and the reliability of the voting procedure, by designing a secure system and evaluating its performance, accuracy, and accessibility.

Methodology: The researcher developed an improved voting system using visual cryptography and multi-factor authentication, assessed its performance against Eligo and Voxvote, utilized Java for programming, MYSQL via XAMPP for the database, HTML, CSS, JavaScript, and PHP (Laravel) for client-server sides. The Scrum agile methodology was followed, employing brief sprints for adaptive development. Evaluation was done through web tools and benchmarks. The system's architecture and flowchart were presented, featuring an interactive GUI, Java 2 platform, MySQL, PHP 7, and specific hardware/software requirements. System setup included database and server configuration, fingerprint scanner installation, and Java runtime setup. Deployment involved executing a built Java program, and system testing was conducted on Windows 10, utilizing the Apache server and initiating the "ElectronicVoting" program for online multi-factor authentication.

Results: Achieving a performance rate of 92%, the developed system surpassed its competitors Eligo and Voxvote, which achieved scores of 15% and 33% correspondingly, as indicated by the data. Eligo and Voxvote attained scores of 88% and 80% individually, whereas the newly designed system obtained a rating of 93% in terms of accessibility. Nonetheless, the research also highlighted specific downsides, encompassing intricacy, reluctance to embrace change, and technological barriers. To tackle these issues and enhance the adoption of such systems, these limitations underscore the necessity for further investigation and advancement.

Conclusion: The study demonstrates that integrating multi-factor authentication and visual cryptography significantly enhances voting system security, reducing clone phishing risks. Visual cryptography secures decryption keys, preserving voting integrity, while multi-factor authentication adds defense against unauthorized access. The researcher's online voting system outperforms competitors in performance metrics and accessibility. The study underscores the importance of combining these techniques for improved voting system reliability and security.

Enhancing voters' confidence in the election process will involve raising awareness among voters and stakeholders about the importance of multi-factor authentication and visual cryptography within the voting process, while involving key parties like electoral commissions, political entities, and civil society organizations is essential for successful deployment. Therefore, the system is recommended for adoption by the Nigerian electoral commission and similar bodies to improve electoral processes and outcomes.

Key words: Improvement of Voting System, Visual Cryptography, Multi-factor authentication, Clone phishing attack

Introduction

In recent times, the escalating concern about phishing attacks impacting voting systems, particularly with the rise of electronic and online voting methods, has underscored the vulnerability of elections to compromise. The acceptance of internet voting platforms due to their convenience and accessibility, exemplified by systems like Integrated Real-time Electronic Voting (IREV), has coincided with an increase in security risks, with clone phishing attacks being a notable threat (Sulaiman & Abdullah, 2019). While online voting offers advantages in accessibility and cost-effectiveness, questions about security, privacy, and verifiability have arisen (Kulyk et al., 2018). Usability is another crucial aspect, prompting the proposal of a multi-factor authentication technique to increase the safety and security of mobile internet voting systems (Kim et al., 2021).

Research has highlighted various security threats, including clone phishing attacks, prompting a focus on these assaults (Finkenzeller et al., 2016). These attacks aim to obtain sensitive data by imitating legitimate websites, raising significant concerns for the overall security of voting systems (Sulaiman & Abdullah, 2019). To counteract this, the implementation of visual cryptography, which divides secret images into shares to prevent centralized data storage, has been suggested as a defense mechanism(Möller &Poddebniak, 2016). However, the application of visual cryptography to combat clone phishing in online voting systems, specifically IREV, remains relatively unexplored(Möller &Poddebniak, 2016). Multi-factor authentication (MFA) emerges as a pivotal security approach, mandating users to provide multiple authentication factors, with support from different categories, to access systems or data.

MFA's effectiveness in mitigating identity theft and cyber threats has been established in various industries and studies, with regulatory bodies like PCI DSS and GDPR endorsing its adoption. Notably, research indicates MFA's ability to prevent a significant portion of account compromises and data breaches (Microsoft, 2019; Verizon, 2020).In 2020,Alvi et al. proposed a secure online voting system combining visual cryptography and blockchain technology, encrypting votes with visual cryptography and storing them on a blockchain to ensure anonymity and tamper-proof verification.

Conversely, Pereira et al. (2023) suggested a similar approach, utilizing visual cryptography and blockchain to encrypt and securely store votes, protecting anonymity and enhancing resistance against various attacks like vote fraud and tampering (Alvi et al., 2022).Makki et al. (2018) also proposed a visual cryptography method to protect electronic voting systems from phishing attacks, using cover images and steganography to conceal original vote images. Among other types of attacks, this method was found to resist phishing attempts. Nevertheless, visual cryptography still faces challenges including scalability issues with

participant numbers (Das et al., 2020; Shih et al., 2020), alignment requirements for share recreation (Yang et al., 2019), potential information leakage (Gope & Naskar, 2019; Tseng et al., 2021), and inefficiency with dynamic data (Zhang et al., 2019). To enhance its deployment, additional security measures must be considered (Das et al., 2020; Shih et al., 2020; Yang et al., 2019).

Hence this study was carried out to develop a secure, robust voting system withstanding attacks like clone phishing using visual cryptography and multi-factor authentication,this, in turn, enhances the integrity of the voting process, improves the security of the voting system, and increases voter confidence.

Methodology

Utilizing visual cryptography and multifactor authentication, the researcher designed and developed a voting system to additionally counter clone phishing attacks. The designed system was then evaluated through benchmarking based on accessibility, performance, and accuracy. This was achieved using the Java programming language. MYSQL database was chosen and implemented through the XAMPP database management system. The client side was constructed using HTML, CSS, and JavaScript, while the server side was built with the Hypertext Pre-processor (PHP) framework, specifically Laravel.

The project adopted the Scrum agile methodology, involving small self-organizing teams gradually delivering a product, focusing on customer value, and adapting to changing requirements (Schwaber & Sutherland, 2020). It followed brief time-boxed sprints spanning one to four weeks, allowing the team to organize, implement, and assess work to ensure progress towards the project's overarching goal (Schwaber & Sutherland, 2020). The developed system was benchmarked using Eligo and Voxvote to assess accessibility, performance, and accuracy. For the evaluation, the webpage test (www.webpagetest.org), a tool available under the polyform shield license, was employed in conjunction with the Google Lighthouse tool for auditing web applications.

The figure below illustrates the system architecture for the enhanced voting system employing visual cryptography and multifactor authentication

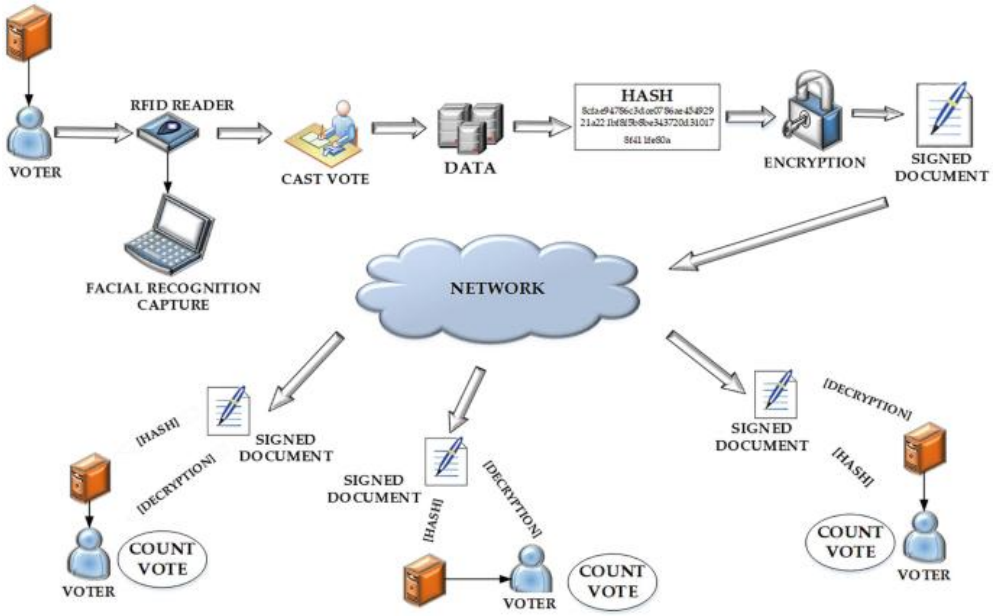

Figure 1: Illustration of the System Architecture

The figure below is an illustration of the system flowchart

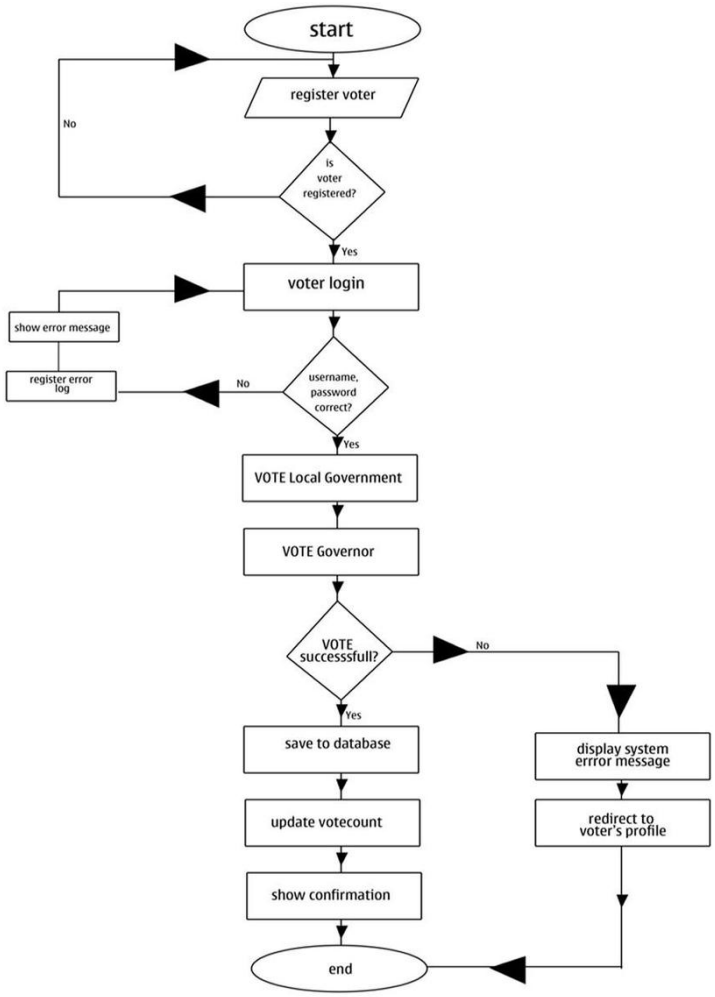

Figure 2: Illustration of the Flowchart of the System

Specifications of the System

With the following specifications in mind, the system was constructed;

Interactive and control-based Graphical User Interface: An interface with graphical controls like buttons and sliders enables users to interact more efficiently with software applications.

Object Oriented Development: Object-oriented development emphasizes reusable code and constructing software systems using objects with properties and methods.

Java 2 Programming Platform: J2SE provides programmers tools and APIs for building Java applications, including the Java Virtual Machine for platform-independent code and libraries for GUIs, networking, and databases.

Native application: A native application, designed for a specific platform, offers high performance and a seamless user experience due to direct access to hardware and operating system resources.

Multi Operating System compatible program: A multi-operating system compatible program is designed to run on various platforms using platform-independent programming languages and frameworks.

MySQL Database Engine 5 on the Server: MySQL Database Engine 5 is a free, scalable, and reliable RDBMS that manages data, serving multiple applications either as a standalone server or integrated with other software.

PHP 7 language processor: PHP 7, an open-source scripting language, is used for dynamic web applications and offers new features and improvements over PHP 5.

System requirements

The following requirements were needed for the system to function;

Hardware Requirements
- Pentium IV with 1GHZ speed and above
- 512 MB Memory
- 20GB Hard Disk
- Digital Persona Fingerprint Scanner

Software Requirements
- Operating systems: Windows /Linux/Unix/etc
- Java Virtual machine, running either JRE or JDK
- Digital Persona Software Development Kit (SDK)
- MySQL server on the Server System, Running MySQL 5 or Apache WAMP OR LAMP OR XXAMP 5
- Database Management software Like PHPMyADMIN on the Server.
- PHP 7 Engine

System setup

The researcher established a MySQL database and PHP 7 engine on the server to manage system data and create its online component. Apache WAMP server was set up on the server system, enabling database development, modification, and management using PHPMyAdmin. Importing the database from the development server to the implementation server was necessary for system launch. The usability of the fingerprint scanner was crucial for the project's success, serving as a fundamental component of its operation. Ensuring the accurate installation of the fingerprint scanner was essential before implementing the project. To enable proper functionality, key steps included installing the Java virtual machine, the Fingerprint SDK, and the device driver along with other utility programs provided.

For our JDK-based project, we installed the JDK runtime on the designated server. We utilized the "Free_Fingerprint_Verification_SDK" for fingerprint functionality, which included the required driver for the Digital Persona Fingerprint Scanner. No specific installation was required for this implementation, as the Java-based project was built as an executable program compatible with any operating system. Deployment involved executing the build command in Netbeans and copying the "dist" folder from the project directory to host the Java application. To run the "ElectronicVoting.jar" executable program, it needed to

be accessed within the "dist" folder. After deploying the project and conducting system testing on Windows 10, we waited for the appropriate moment to launch the programme. To initiate the MySQL database, we activated the Apache server on the server system, facilitating data retrieval. Subsequently, we launched the "ElectronicVoting" (Online Multi-factored Authentication voting System) from the "dist" folder after the database server program was started, with the programme opening with the admin login page.

Results and Discussion

Login Page

Prior to granting access, the system initially presents an admin login screen requesting the user's username and password. After a successful login, the user receives a welcoming message, and access to the system is granted through the display of the Menu page. If the login is unsuccessful, access is denied, and the only alternative is to exit the system.

Below are pictures of the user login system;

Figure 3: User Login page

The user is granted access after their provided username and password are verified and approved as shown below. Conversely, if the user enters incorrect login credentials, access will be denied.

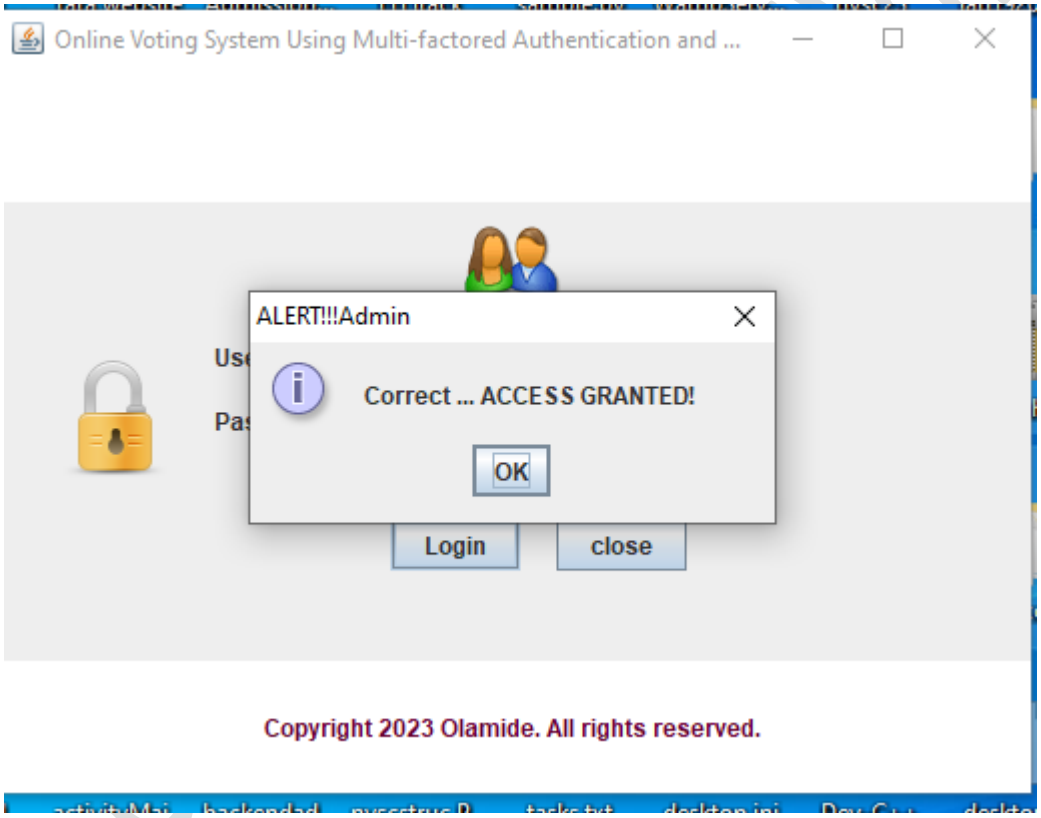

Figure 4: User Access page

Voter Registration

To register a new voter, the "register new Voter" menu option needed to be chosen from the menu page, granting access to the registration page. On this page, the voter's fundamental details were completed, and their fingerprint was captured for registration purposes.

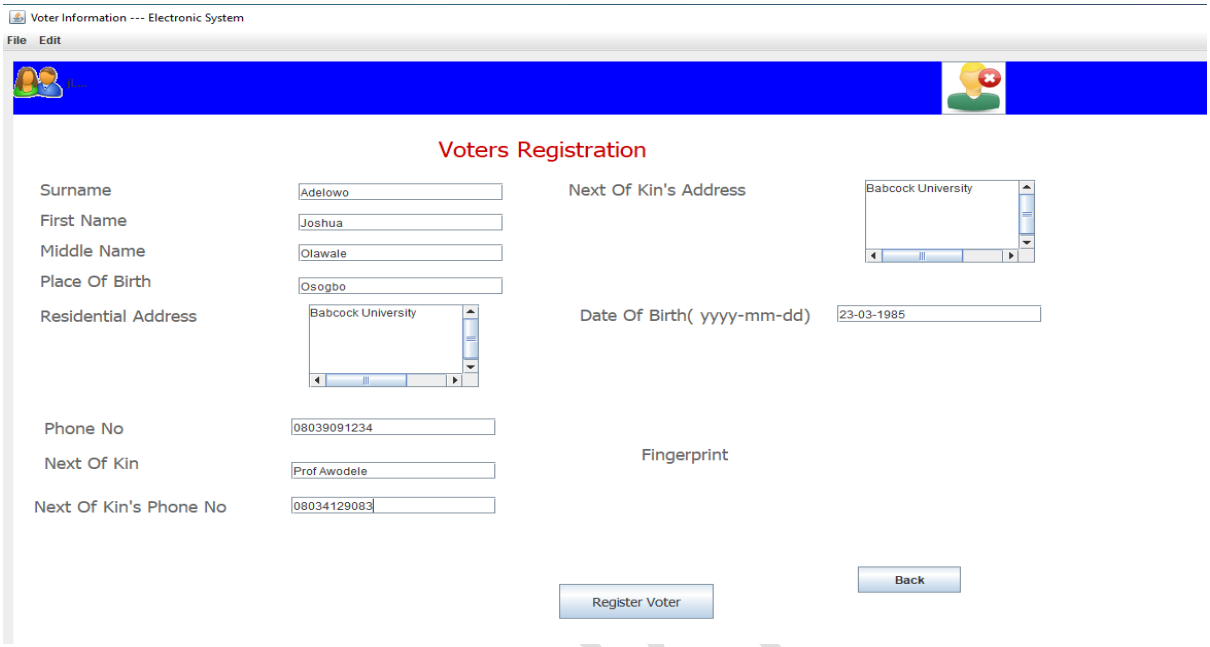

Figure 5: Voter Registration

During this process, the administrator registered every political party taking part in the election and identified the candidates for each party. To access the registration page for a new Party/Candidate, one had to choose the "register new party and candidate" menu option from the menu page. On this page, essential information about the party or candidate was input, and the party logo was uploaded.

Figure 6: Illustration showing Party and Candidates Registration

Voting Process

By selecting "Open Voters Start page" from the menu, the administrator commenced the voting process. Intending voters then followed a sequence of steps, which included:

1. Voters authenticated with registered Surname and Phone number previously registered.
2. Authenticated users underwent biometric verification. If successful, the fingerprint image displayed was displayed. Mismatched or unregistered users were not able to proceed.
3. A visual captcha ensured human voting by displaying text in an image that only a human would be able to comprehend.
4. After captcha, voters accessed the ballot, selectedtheir preferred candidates and parties before submission, which completed the voting process.

Figure 7: Multi-factor authentication for the online voting system

Verified voters

In this stage, accredited voters are verified and then proceed to the next step where their information will be captured, allowing them to cast their votes.

Figure 8: Illustration showing a verified voter

Security of the System

To ensure proper security, the system requires a validation code known as a captcha, generated by the system. If the user correctly inputs the validation code, access is granted.

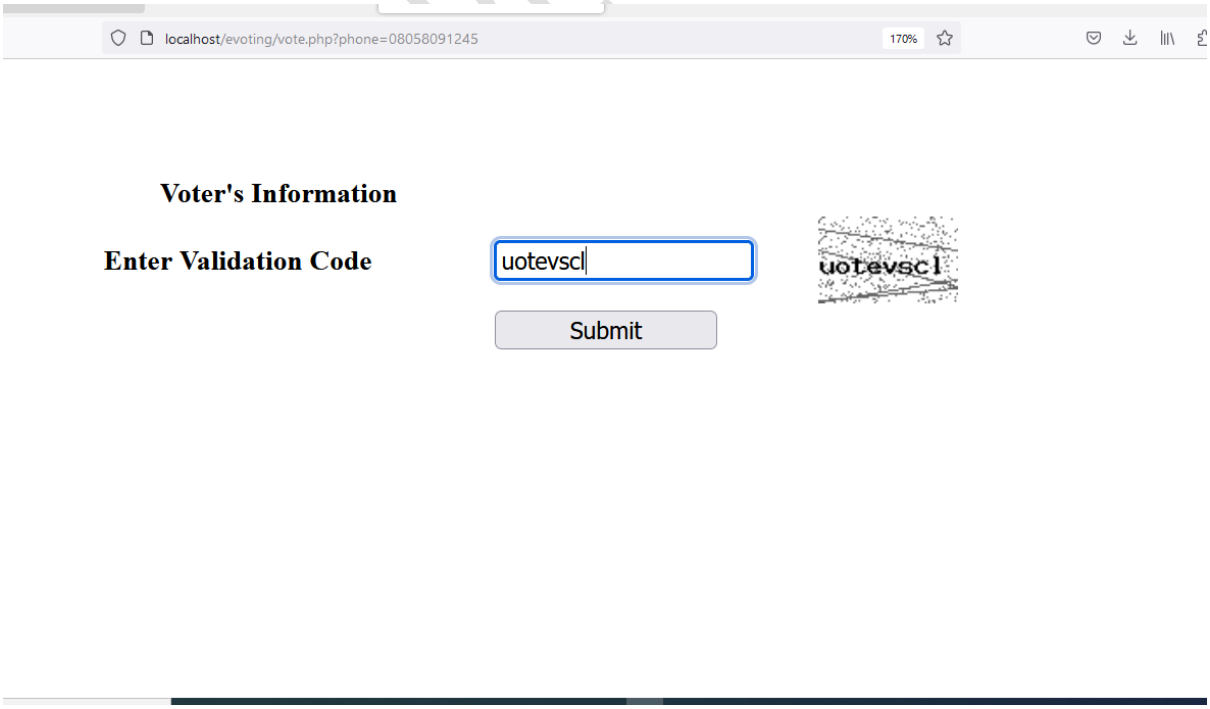

Figure 9: System Security

Select Candidate

In this scenario, as depicted in the image below, accredited voters possess the right to vote for any party of their preference.

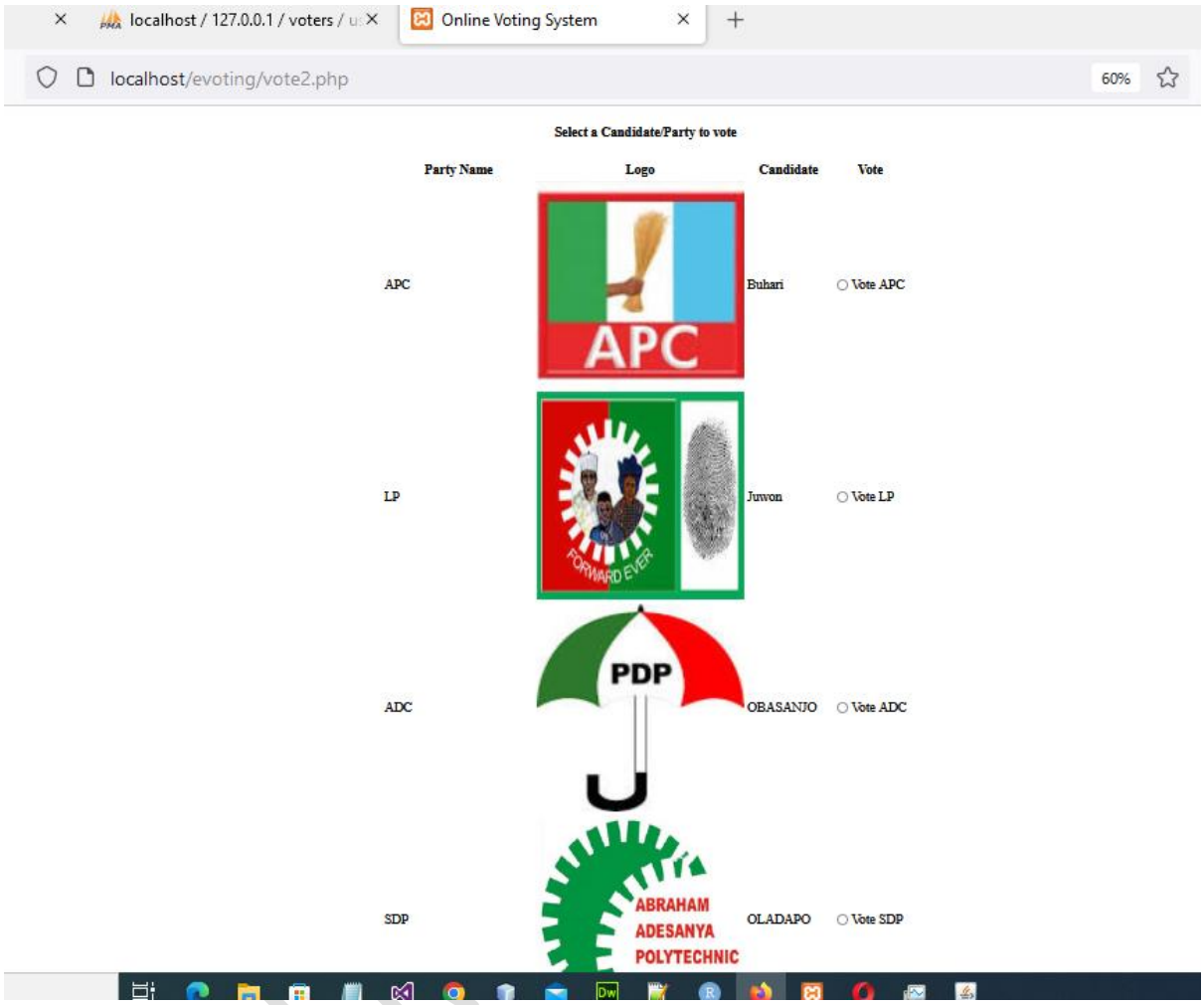

Figure 10: illustration showing the "select candidate" window

Success Page

Upon selecting their preferred candidate and clicking the vote button, the page exhibits the success page.

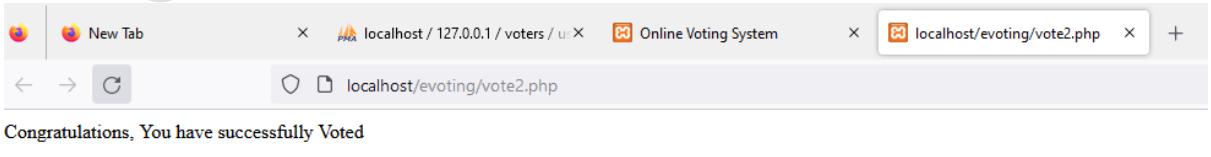

Figure 11.Exhibition of success page

Vote Counting

On the Vote counting page, the administrator will have the capability to generate a report of the voting conducted thus far, presenting the total number of times a user attended class and providing the corresponding percentage of attendance for that user.

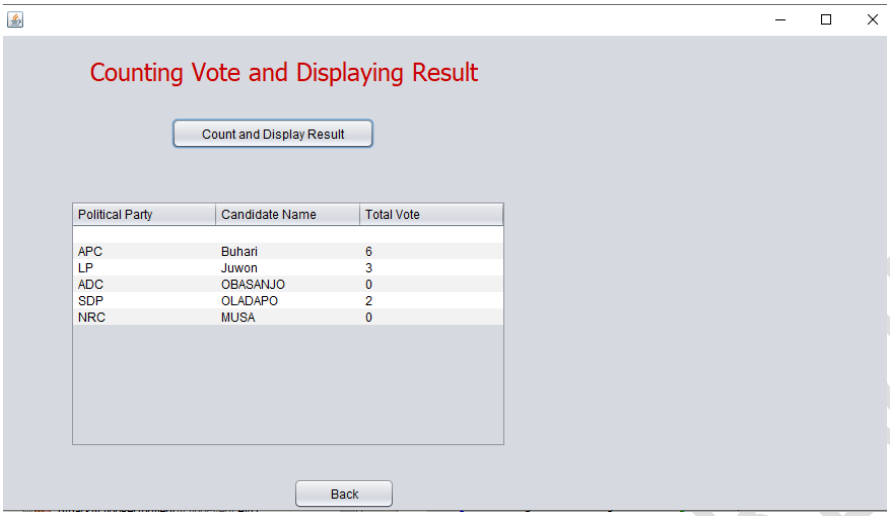

Figure 12: Illustration showing the "Vote Counting System Evaluation"

Performance

The researcher's online voting system application underwent performance testing three times. In the third test, a noticeable reduction in timings occurred, as illustrated in the figure below:

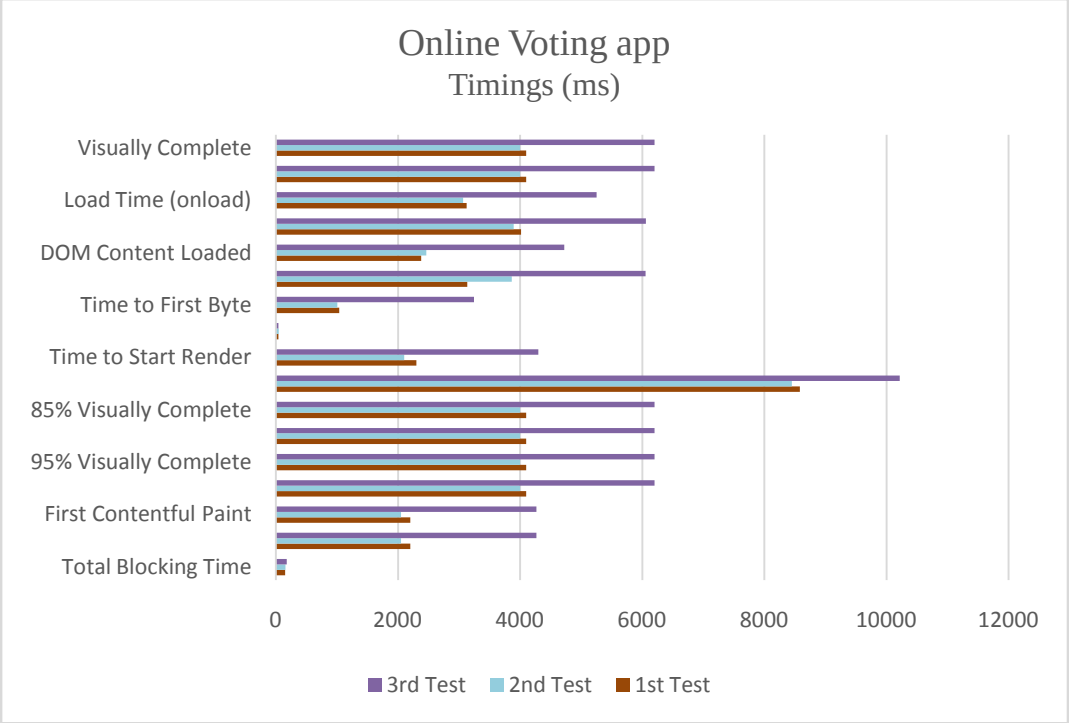

Figure 13: Graph showing "performance of online voting system"

4.4.4 Performance of Online voting app against other voting platforms(Eligo. social and Voxvote)

The researcher compared the voting applications already in existence with the one constructed by the researcher. This test was replicated three times, as depicted in the graph below. The results from the test clearly indicated that the researcher's system outperformed the others.

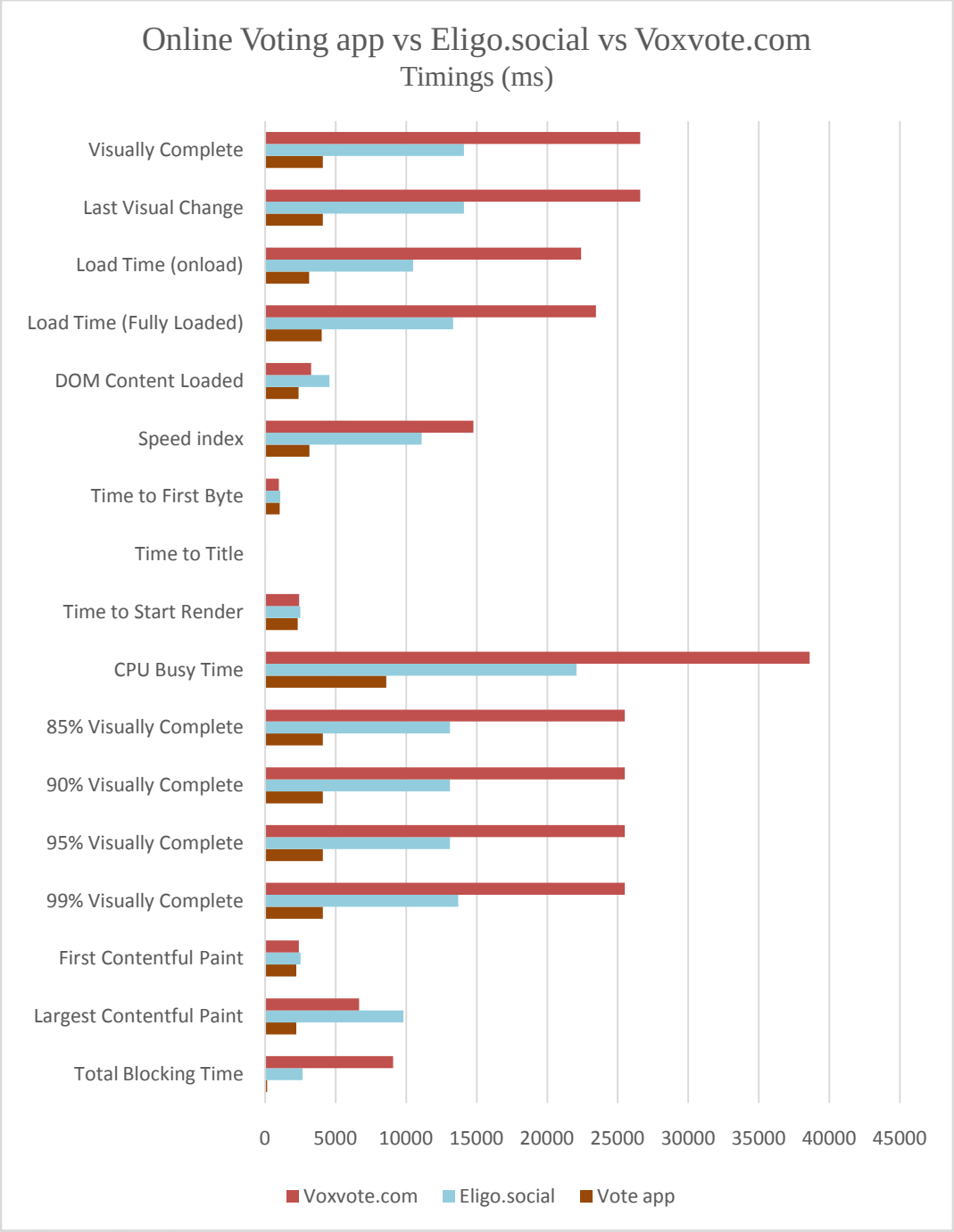

Figure 14Graph showing "Comparison of online voting system vs Eligo vs Voxvote"

Comparing Performance Metric Values for Online Voting, Eligo.social, and Voxvote.com.

After being compared to other voting platforms, the researcher's online voting app displayed a total time of 56865ms, Eligo Social exhibited a total time of 208921ms, and

Voxvoterecorded a total time of 5776ms. When assessed using Google Lighthouse, the performance of the researcher's online voting app reached 92%, Eligo Social scored 15%, and Voxvote scored 33%.

Table 1: Comparison of Performance Metric Values for Online Voting, Eligo.social and Voxvote.com

Performance Metrics	Onling Voting app Time (ms)	Eligo.social Time (ms)	Voxvote.com Time (ms)
Visually Complete Time	150	2949	150
Last Visual Change Time	2303	14093	2203
Load Time (On Load)	2302	2311	2202
Load Time (Fully Loaded)	4300	14700	4100
Document Object Model	4300	14100	4100
(DOM) Content Loaded	4300	14100	4100
Speed Index (SI)	4300	14100	4100
Time to First Byte (TTFB)	8680	33190	9580
Time to Start Render (TSR)	2300	2300	2300
Central Processing Unit (CPU) Busy Time	42	12	42
85% Visually Complete	1138	1155	2038
90% Visually Complete	4134	12022	3134
95% Visually Complete	2578	4111	2878
99% Visually Complete	4116	24305	4016
First Contentful Paint (FCP)	3322	11673	4122
Largest Contentful Paint (LCP)	4300	21900	4600
Total Blocking Time (TBT)	4300	21900	4100
Total Time	**56865**	**208921**	**57765**

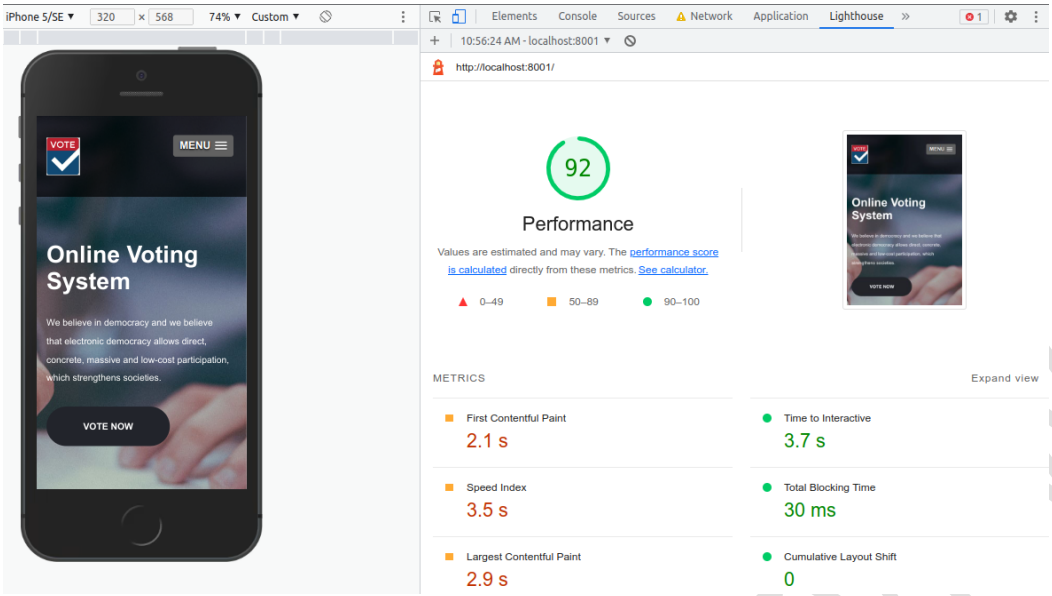

Figure 15: Screenshot showing "Online Voting Performance at 92%"

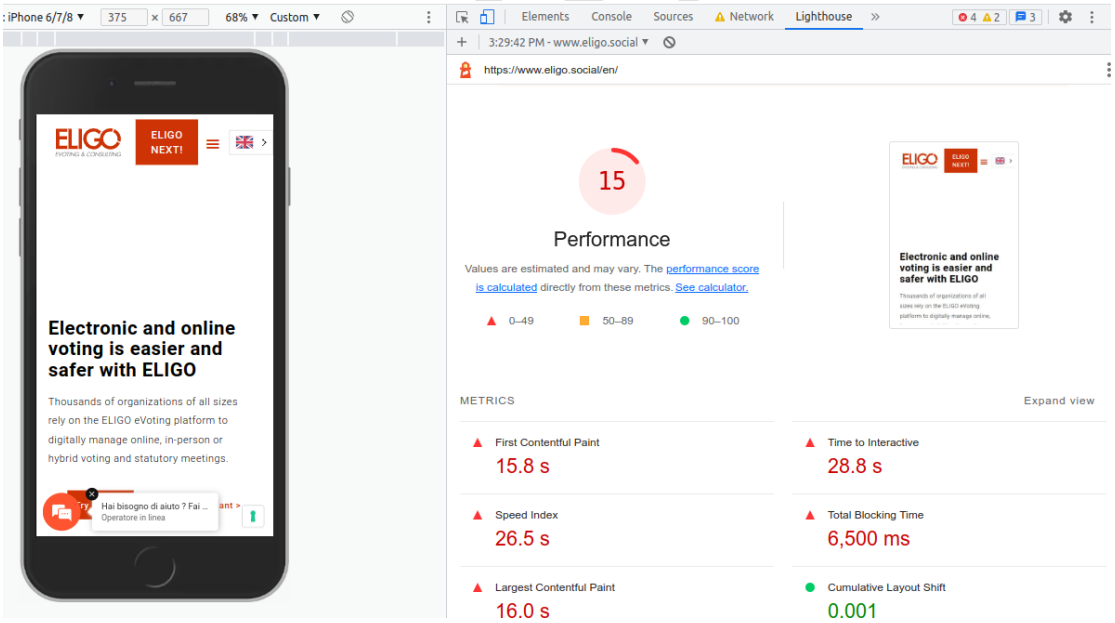

Figure 16:Screenshots showing "Eligo.social performance level at 15%"

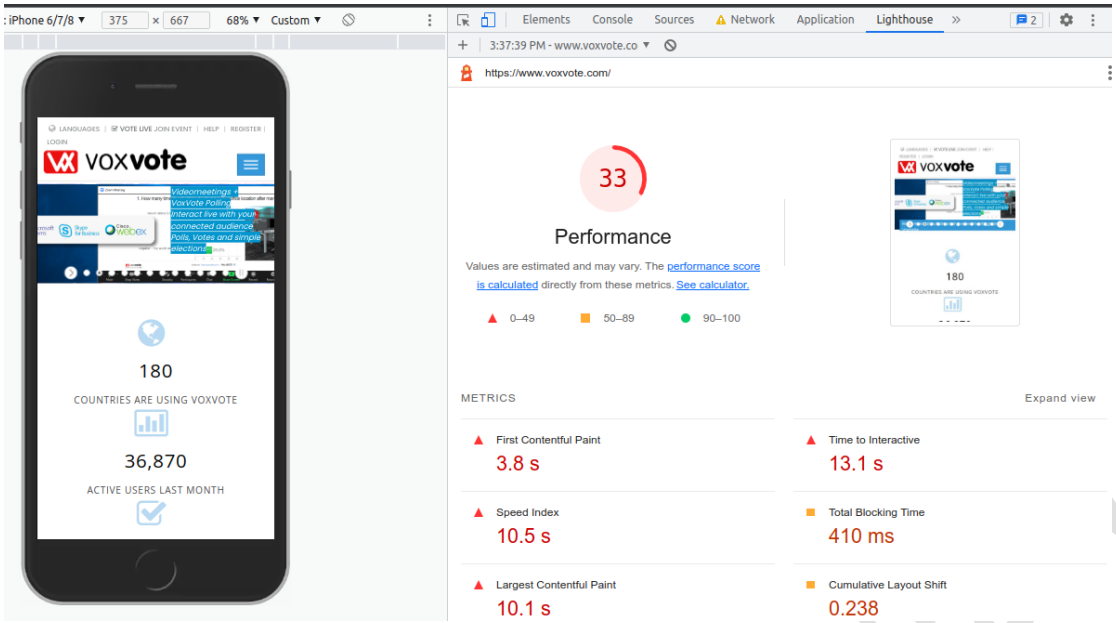

Figure 17: Screenshots showing "Voxvote.com performance level at 33%"

Accessibility

When assessed using Google Lighthouse, the researcher's online voting system achieved a 93% accessibility score, Eligo Social scored 88%, and Voxvote scored 80%. This indicates that the researcher's system exhibits higher accessibility compared to the others. These are all demonstrated in the images below;

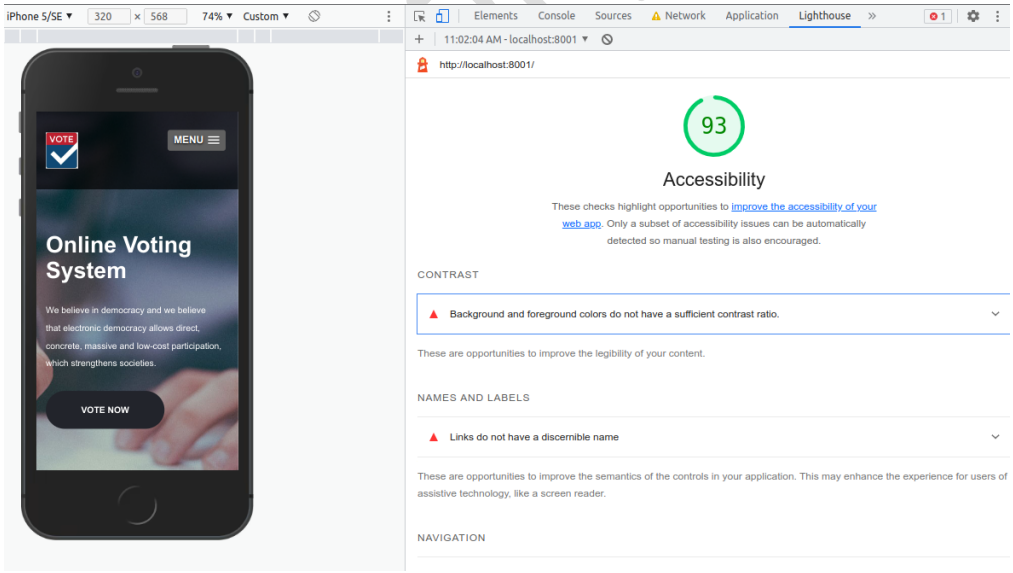

Figure 18: Screenshot showing "Voxvote.com performance level at 93%"

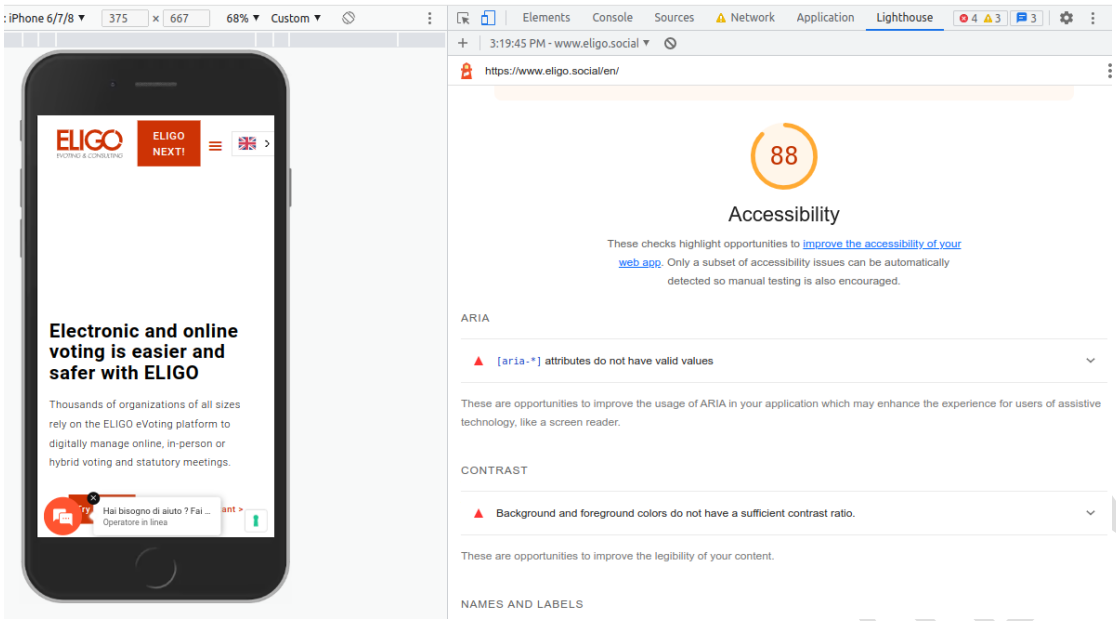

Figure 19: Screenshot showing "Eligo.social accessibility level at 88%"

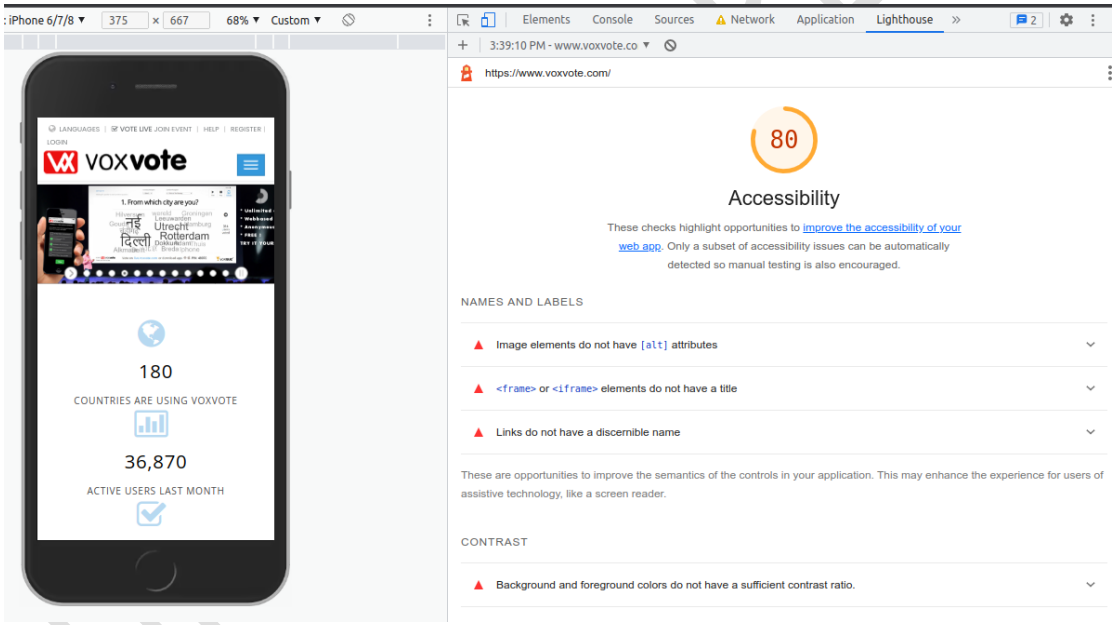

Figure 20: Screenshot showing "Voxvote.com performance level at 80%"

Reflection of Discussion and Findings

The study aimed to enhance voting system security by implementing a robust security mechanism using visual cryptography and multi-factor authentication. It identified vulnerabilities in existing systems and designed a new framework to address these issues, resulting in improved security, accuracy, and accessibility. The study recommends that organizations and bodies should adopt this online voting mechanism to bolster the security of their voting system. In conclusion, the study successfully created a more secure voting system which is apositive implication voting systems in general.

Conclusion

The study concludes that incorporating multi-factor authentication and visual cryptography into the voting system significantly enhances security and reduces clone phishing risks. Visual cryptography limits access to decryption keys, maintaining voting process integrity, while multi-factor authentication adds an extra layer of defense against unauthorized access. The researcher's online voting system outperforms competitors in performance metrics, with a faster overall time and higher scores in Google Lighthouse evaluations for both performance and accessibility. The study emphasizes that combining visual cryptography and multi-factor authentication is essential for boosting voting system security and reliability.

Recommendations

To enhance the electoral process and outcomes, the electoral commission of Nigeria and other relevant electoral bodies are advised to consider the system. For this purpose, raising awareness among voters and stakeholders regarding the significance of multi-factor authentication and visual cryptography in the voting process is crucial. This knowledge will contribute to boosting voters' confidence in the voting procedure. Moreover, the involvement of pertinent parties in the electoral process, including the electoral commission, political parties, and civil society organizations, plays a vital role in implementing visual cryptography and multi-factor authentication.

Limitation of Study

1. In certain countries, the implementation of visual cryptography and multi-factor authentication could pose challenges due to the required infrastructure, resources, and technical expertise, which might not always be readily accessible.
2. The introduction of novel technologies such as multi-factor authentication and visual cryptography might present difficulties for election stakeholders in terms of adoption.
3. Integrating visual cryptography and multi-factor authentication into the voting system could lead to increased complexity, thereby requiring additional training for both voters and electoral officials.

Suggestions for Future Works

Despite the significant advancements made in voting system security through the current study, there are otheropenings for further research. Usability studies assessing the effectiveness of these security measures in real voting scenarios and the scalability of these methods, especially in countries with large voter populations, remain areas of interest. Standardization protocols are needed to ensure the seamless integration of visual cryptography and multi-factor authentication, maintaining compatibility, security, and usability. Ongoing monitoring is essential to prevent security breaches or attacks, particularly those involving clone phishing. Future studies could alsoinvestigate the integration of additional technologies such as blockchain, artificial intelligence, and machine learning. The establishment of a legal framework would be necessary to implement these security measures in accordance with election regulations and data protection laws.

References

Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2022, October). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *Journal of King Saud University - Computer and Information Sciences*, *34*(9), 6855–6871. https://doi.org/10.1016/j.jksuci.2022.06.014

Finkenzeller, M., Sander, A., Volkamer, M., & Krimmer, R. (2016). Election fraud detection: A review of statistical and technological approaches. IEEE Security & Privacy, 14(6), 28-37.

Kulyk, O., Ferrari, E., &Volkamer, M. (2018). Verifiability of internet voting: A comprehensive literature review. Government Information Quarterly, 35(4), 677-692.

Makki, S. S., Al-Jumeily, D., & Hussain, A. (2018). Securing electronic voting system against phishing attacks using visual cryptography and steganography. International Journal of Distributed Systems and Technologies, 9(4), 35-52.

Microsoft. (2019). Security Research & Intelligence. https://www.microsoft.com/security/blog/2019/08/20/new-study-identifies-the-most-effective-security-controls-to-prevent-cyber-attacks/

Möller, B., &Poddebniak, D. (2016). Visual cryptography for authenticating web pages. Journal of Computer Security, 24(4), 471-501.

Pereira, B. M. B., Torres, J. M., Sobral, P. M., Moreira, R. S., Soares, C. P. D. A., & Pereira, I. (2023, May 15). Blockchain-Based Electronic Voting: A Secure and Transparent Solution. *Cryptography*, *7*(2), 27. https://doi.org/10.3390/cryptography7020027

Sulaiman, M., & Abdullah, R. (2019). Improved clone phishing detection using enhanced decision tree algorithm. International Journal of Advanced Computer Science and Applications, 10(7), 465-472.

Verizon. (2020). 2020 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf