IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Preserving Voter Privacy and Security in Online Voting through Diffie-Hellman Encryption

Rosemarie C. Arcaya
College of Arts and Sciences, Surigao del Norte State University, Surigao City, Philippines

Abstract: *This research paper presents an advanced online voting system, incorporating the Diffie-Hellman encryption algorithm, to ensure voter privacy and address key challenges in digital elections. The system offers additional features such as anonymous authentication, verifiable decryption, and secure ballot transmission. Through a rigorous evaluation process, the proposed approach received an overall evaluation score of 3.55 out of 5, indicating its effectiveness in upholding voter privacy and system efficiency. Specific evaluation criteria revealed accuracy with a score of 3.57 out of 5, efficiency at 3.53 out of 5, reliability at 3.54 out of 5, timeliness at 3.50 out of 5, and a commendable security rating of 3.59 out of 5. These results highlight the system's potential in providing a secure and user-friendly online voting platform, encouraging voter participation and reinforcing the democratic principles of transparency and integrity.*

Keywords: Diffie-Hellman algorithm, encryption, evaluation, privacy, online voting

I. INTRODUCTION

In recent times, the advent of technology has revolutionized various aspects of our lives, including the way we conduct democratic processes such as voting. Online voting systems have emerged as a promising solution to increase voter accessibility, convenience, and participation in elections[1][2]. However, the implementation of online voting brings forth critical challenges, most notably concerns related to voter privacy and data security.

Ensuring voter privacy is an indispensable aspect of any voting system, be it traditional or digital. The sensitive nature of voter information demands a robust and reliable approach to protect it from unauthorized access, manipulation, or disclosure. To address these concerns, this paper proposes the utilization of the Diffie-Hellman encryption algorithm as a fundamental mechanism to ensure voter privacy in online voting.

The Diffie-Hellman algorithm, a widely recognized cryptographic key exchange protocol, offers a strong foundation for secure communication between two entities over an insecure channel[3][4][5]. In the context of online voting, this algorithm can be effectively employed to establish secure and confidential communication between voters and the central voting authority, ensuring that the voter's identity and ballot choices remain anonymous and protected.

This paper aims to explore the potential of the encryption algorithm in bolstering the privacy and confidentiality aspects of online voting systems. By providing an in-depth analysis of the algorithm's underlying principles and its integration into the online voting framework, we seek to highlight how this approach can mitigate security risks and enhance voter trust in the digital voting process.

It is a fervent belief that by employing the encryption algorithm, online voting systems can pave the way towards transparent, secure, and confidential electoral processes, upholding the democratic principles that lie at the heart of modern societies.

II. BACKGROUND STUDY OF THE ONLINE VOTING SYSTEM

With the ever-increasing integration of technology into various aspects of human life, traditional methods of voting have evolved to embrace the digital age[6][7]. Online voting systems have emerged as a promising solution to improve voter accessibility, increase participation, and streamline electoral processes. However, the transition to online voting raises critical concerns related to voter privacy and data security. Ensuring the confidentiality and anonymity of voters is paramount to maintain the integrity and credibility of any democratic process. This background study focuses on

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

addressing the challenges of voter privacy in online voting and explores the potential of the Diffie-Hellman encryption algorithm to enhance security and confidentiality in digital voting systems.

Challenges in Online Voting and Voter Privacy: Online voting introduces new complexities that must be addressed to instill trust in the electoral process. One of the most significant challenges is maintaining voter privacy and anonymity. In traditional voting, voters cast their ballots in private booths, ensuring their choices remain undisclosed[8][9][10]. In contrast, online voting faces the challenge of replicating this level of privacy in a digital environment.

Several concerns arise in online voting that directly impact voter privacy:

- Voter Identification: Online voting systems must accurately verify the identity of voters while preventing the disclosure of personal information that could be used to compromise voter anonymity[11][12].
- Ballot Secrecy: Ensuring that voters' ballot choices remain secret is critical to protect against coercion or influence that could compromise the integrity of the election.
- Data Breaches and Hacking*:* Online voting platforms are susceptible to data breaches and cyber-attacks, potentially exposing sensitive voter information and undermining trust in the system[13][14].
- Verifiability and Transparency: Voters need to be confident that their votes are accurately recorded and counted, while also being able to verify the election results without revealing their individual choices.

The Diffie-Hellman Encryption Algorithm:

The Diffie-Hellman encryption algorithm, developed by Whitfield Diffie and Martin Hellman in 1976, is a pioneering cryptographic protocol that allows two parties to establish a shared secret key over an insecure communication channel[15][16]. It is based on the concept of discrete logarithms and modular arithmetic, making it computationally infeasible for adversaries to determine the shared key even if they eavesdrop on the communication.

The Diffie-Hellman algorithm operates as follows:

- *Key Generation:* Each party generates a private key and a corresponding public key based on the modular exponentiation of a generator value.
- *Key Exchange:* The parties exchange their public keys over the open channel while keeping their private keyssecret.
- *Shared Secret Calculation:* Using the exchanged public keys and their own private keys, the parties calculate a shared secret key using modular exponentiation.
- *Encryption:* The shared secret key can be used for symmetric encryption to secure further communication.

Applying Diffie-Hellman Encryption in Online Voting:

The Diffie-Hellman algorithm holds significant promise in addressing the challenges of voter privacy in online voting. By using this algorithm, an online voting system can achieve the following:

- *Anonymous Authentication:* Voters can authenticate themselves to the system without revealing their true identities, preserving their privacy.
- *Ballot Encryption:* Each vote can be encrypted using the shared secret key, ensuring that only authorized entities can decrypt and count the ballots while keeping the choices hidden from unauthorized access.
- *Verifiable Decryption:* The encrypted votes can be decrypted using the shared secret key while maintaining the privacy of individual votes. Voters can also verify that their ballots were correctly decrypted and counted without revealing the contents of their ballots.

The transition to online voting presents both opportunities and challenges in preserving voter privacy and ensuring the integrity of the electoral process. The Diffie-Hellman encryption algorithm offers a robust solution to enhance security, anonymity, and confidentiality in online voting systems[17][18]. By incorporating this encryption protocol, online voting platforms can instill greater trust among voters and pave the way for a more transparent and secure democratic future. However, it is essential to continue exploring and refining cryptographic techniques to stay ahead of potential threats and maintain the sanctity of the electoral process.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

III. DESIGN OF ONLINE VOTING SYSTEM THROUGH DIFFIE-HELLMAN ENCRYPTION

The study aims to provide a secure and confidential online voting platform that ensures voter privacy while maintaining the integrity of the electoral process. This system software design outlines the architecture, components, and functionalities of the online voting system that utilizes the Diffie-Hellman encryption algorithm.

3.1 System Architecture

The system architecture consists of the following key components:

1. Front-end Interface: A user-friendly web-based interface that allows voters to access the online voting system. It provides the necessary functionalities for voter authentication, ballot submission, and verification.
2. Back-end Server: The back-end server manages the core functionalities of the online voting system. It handles user authentication, encryption, and decryption of votes, and ensures secure communication between voters and the voting authority.
3. Database: A secure database stores encrypted votes, voter information, and system logs. It is protected against unauthorized access and ensures data integrity.
4. Diffie-Hellman Module: A dedicated module implementing the Diffie-Hellman encryption algorithm, responsible for generating shared secret keys between voters and the voting authority.
5. Authentication Module: Handles voter authentication using techniques like biometrics, OTP, or other secure methods to verify the identity of voters while preserving anonymity.

3.2 System Workflow

The system workflow for "Online Voting through Diffie-Hellman Encryption" is as follows:

1. Voter Registration: Voters must register with the online voting system by providing essential personal information. The system generates a private-public key pair for each registered voter.
2. Authentication: When a voter attempts to access the system, the authentication module verifies their identity through the chosen authentication method.
3. Key Exchange: Upon successful authentication, the Diffie-Hellman module facilitates key exchange between the voter and the voting authority. The module generates shared secret keys to be used for encrypting and decrypting votes.
4. Ballot Submission: After key exchange, the voter can access the ballot and cast their vote. The ballot choices are encrypted using the shared secret key.
5. Vote Storage: The encrypted vote, along with any necessary metadata, is securely stored in the database.
6. Vote Counting: Once the voting period ends, authorized officials can access the encrypted votes, and using the shared secret keys, decrypt the votes while preserving voter anonymity.
7. Result Announcement: The final vote count is computed, and the election results are announced, ensuring transparency and integrity in the electoral process.

3.3 Security Measures

To ensure the system's security, the following measures are implemented:

1. HTTPS: All communication between the front-end and back-end is encrypted using HTTPS.
2. Authentication Mechanisms: Strong and multi-factor authentication methods are employed to validate voter identities.
3. Firewall and Intrusion Detection: Robust firewall and intrusion detection systems are implemented to protect against cyber threats.
4. Data Encryption: All sensitive data, including votes and shared secret keys, are encrypted to prevent unauthorized access.
5. Regular Audits: Regular security audits are conducted to identify and address potential vulnerabilities.

The system software design ensures a secure and private online voting platform. By leveraging the Diffie-Hellman encryption algorithm and implementing robust security measures, the system upholds voter privacy, trust, and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

confidence in the electoral process. This design serves as a foundation for the development and deployment of an efficient and reliable online voting system.

VI. METHODOLOGY

Voting is a vital part of the democratic process. As such, the efficiency, reliability, and security of the technologies involved are critical. In this part all the mechanics and ways needed in gathering information and data to be used in designing and developing the system is applied [19][20]. It also includes the flow on how the data were gathered and interpreted to meet the requirements of the system. The development of the voting system follows the systematic ADDIE design model approach shows in figure 1, that ensuring a well-planned and effective process.

Fig.1. ADDIE Model Approach

In the *Analysis phase*, key stakeholders are identified, and requirements are defined through needs analysis, considering features, security, accessibility, and privacy concerns. Existing voting systems are reviewed, and legal and regulatory compliance is assessed. Stakeholder feedback is gathered to inform the development process.

In the *Design phase*, the system architecture is planned, including the user interface, security measures, and data management. A user-friendly and intuitive interface is designed, and robust security measures such as encryption and multi-factor authentication are incorporated to safeguard the system. Accessibility design is considered to ensure the system is inclusive to all eligible voters.

During *Development*, the voting system is built based on the design specifications, including the implementation of the Diffie-Hellman encryption algorithm and database setup. Rigorous testing is conducted, and training is provided to election officials and administrators.

In the *Implementation phase*, the voting system undergoes pilot testing before gradual roll-out to a larger audience, with continuous support and assistance to address any challenges.

Lastly, the *Evaluation phase* involves data collection on system performance and user experiences, with analysis to identify strengths and weaknesses. The evaluation results inform continuous improvements, leading to a secure, user-friendly, and efficient online voting platform that upholds voter privacy and ensures the integrity of democratic elections.

4.1 Algorithm Used

The Diffie-Hellman encryption algorithm is based on modular exponentiation and uses the properties of prime numbers and primitive roots. It enables two parties to establish a shared secret key over an insecure channel without directly exchanging their private keys [21][22]. The algorithm is used in an online voting system to ensure voter privacy and secure communication between voters and the voting authority.

Mathematical Equation for Diffie-Hellman Encryption Algorithm in Online Voting System consists of the following:

Key Generation: Let's assume that each voter generates their private key (a) and the voting authority generates its private key (b). The voters and the voting authority also agree on a prime number (p) and a primitive root modulo (g).

4.2 Calculation of Public Keys:

Each voter calculates their public key (A) using the formula: $A = (g^a) \% p$

The voting authority calculates its public key (B) using the formula: $B = (g^b) \% p$

Key Exchange: The voters send their public keys (A) to the voting authority, and the voting authority sends its public key (B) to each voter over a secure channel.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Shared Secret Calculation: The voters and the voting authority calculate the shared secret key (s) using the received public keys and their own private keys:
For each voter: Shared secret key (s_voter) = (B^a) % p
For the voting authority: Shared secret key (s_authority) = (A^b) % p
The calculated shared secret key is the same for both the voters and the voting authority, ensuring secure communication between them.

4.3 Encryption and Decryption:
In the online voting system, symmetric encryption is used for secure ballot transmission. The shared secret key (s) is used to encrypt and decrypt the votes:
Encryption of Vote (v) by Voter: Encrypted Vote (E_voter) = (v ^ s_voter) % p
Decryption of Encrypted Vote (E_voter) by Voting Authority: Decrypted Vote (v) = (E_voter ^ s_authority) % p
By using the same shared secret key for encryption and decryption, the voting authority can verify the votes without knowing the individual choices of each voter, thus ensuring voter privacy.
The study follows a methodology that involves key generation, calculation of public keys, key exchange, shared secret calculation, and encryption/decryption of votes. By applying modular exponentiation and secure key exchange, the algorithm enables secure communication and protects the privacy of voter choices in the online voting process.

V. RESULT AND DISCUSSION

5.1 Design and Development
A.1 System Architecture

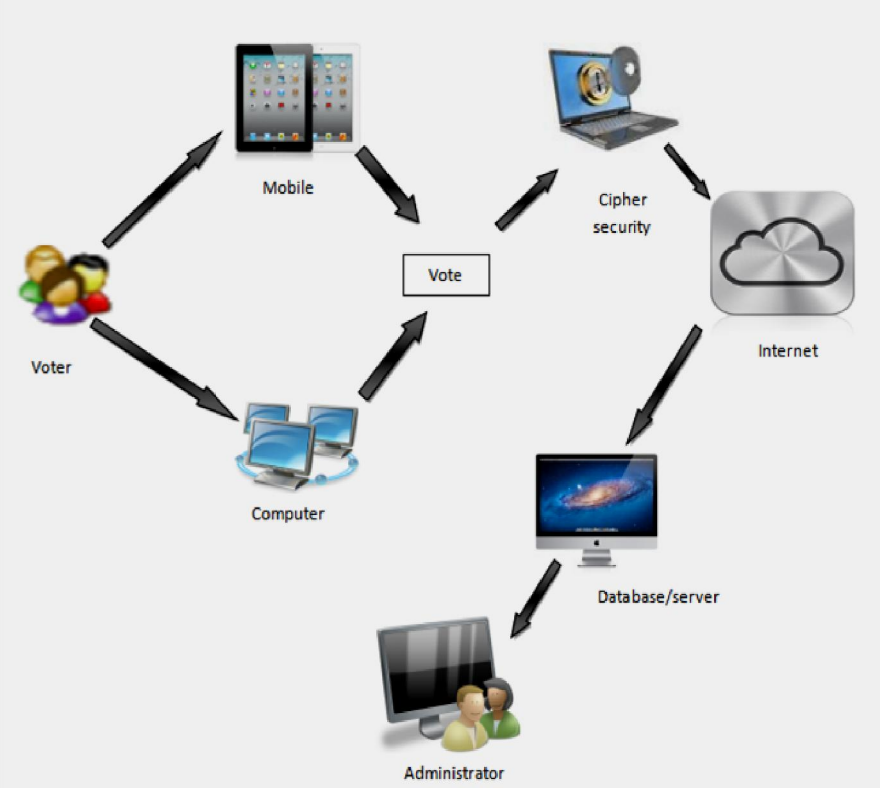

Fig. 2. System Architecture of the System

Show in figure 2 is the system architecture of Student Online Voting System using Diffie-Hellman Algorithm. It shows that the process should have the following: Voters vote via computer or mobile phone, the data is being ciphered for security before it will send to the database.The environment of this system should be HTML5, CSS,jquery and PHP. The outcome of this process is the automated Student Online Voting System.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

2. Class Diagram

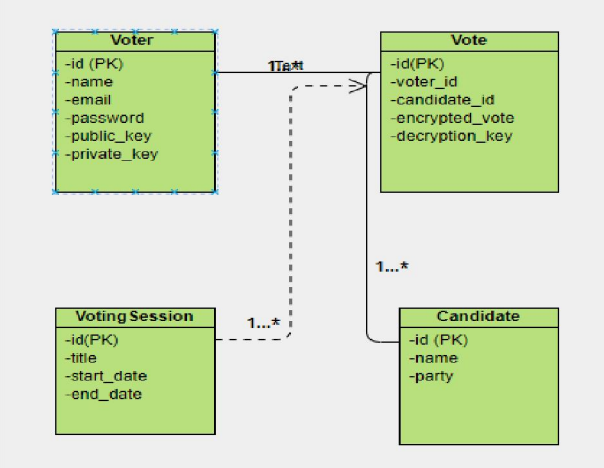

Fig. 3. Class diagram of the system

In this database class diagram:

The Voter entity represents the eligible voters in the system. It contains attributes such as id (primary key), username, password (hashed for security), public_key (used for encryption/decryption), and private_key (used for digital signatures).

The Candidate entity represents the candidates participating in the elections. It contains attributes such as id (primary key), name, party affiliation, and election_id (foreign key referencing the Election entity).

The Election entity represents the individual elections being conducted. It contains attributes such as id (primary key), name, start_date, end_date, and status (e.g., open or closed).

The Vote entity represents the individual votes cast by voters. It contains attributes such as id (primary key), voter_id (foreign key referencing the Voter entity), candidate_id (foreign key referencing the Candidate entity), encrypted vote (the vote encrypted using public key cryptography), and timestamp.

The Diffie-Hellman algorithm would typically be used during the key exchange phase to establish secure communication between the voter's device and the server.

5.2 Screenshot of the System

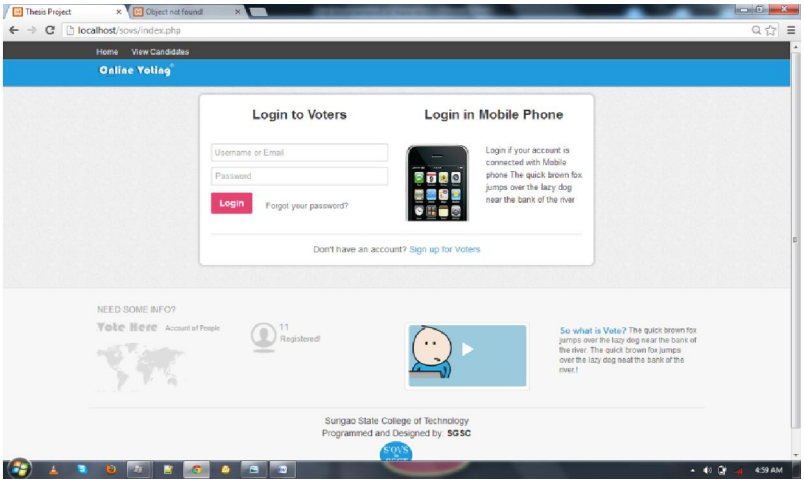

Fig.4. Voters Main Form

Figure 4 shows the voter's ballot form, this form is where the voters select their chosen candidates by clicking the radio button below the names of the candidates and submit it through clicking the submit button. Once the user finishes clicking the submit button a message will appear in the page and the system will automatically cast the vote automatically.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

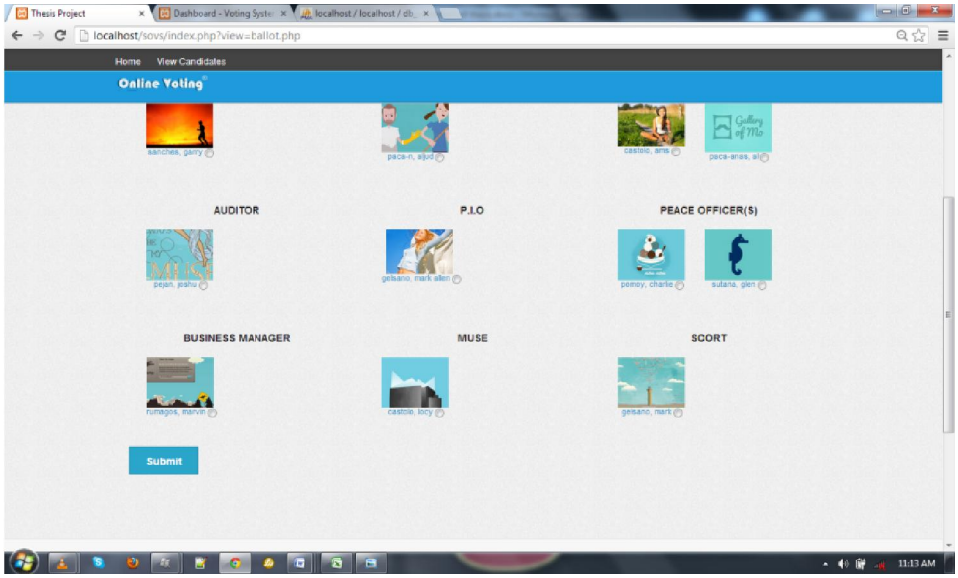

Fig.5. The voter's ballot form

The voter's ballot form shows in the figure 5. This form is where the voters select their chosen candidates by clicking the radio button below the names of the candidates and submit it through clicking the submit button. Once the user finishes clicking the submit button a message will appear in the page and the system will automatically cast the vote automatically.

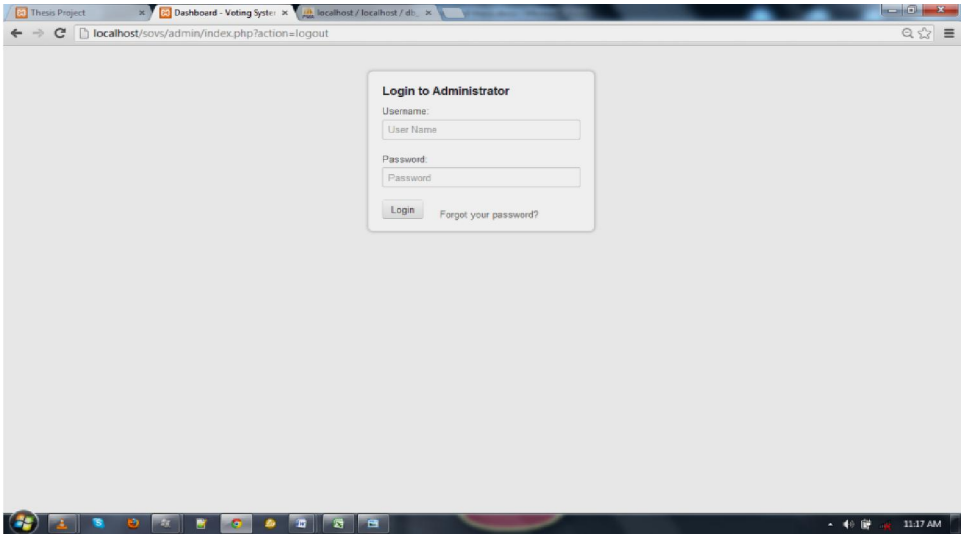

Fig.6. The administrator login form

The figure 6 shows the administrator login form, this is an exclusive form for the administrator control panel.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

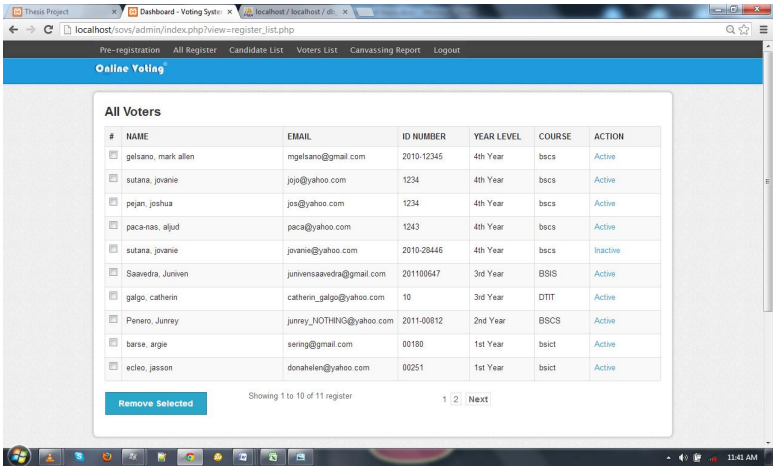

Fig. 7. The administrator control panel

The administrator control panel shows in figure 7, this an exclusive form where the only user that can access is the administrator. All the controls of the system is found in this form including the adding, updating and removing information of voters and candidates, canvassing reports and generating the election results. This form is design for a fine and clear interface design in order to enhance efficiency and reliability of the system..

5.3 Testing and System Evaluation

During this phase the system was tested and evaluated and the target respondents to test the system are the 120 students in Surigao Norte State University or 10% of the respondent's population. This phase shows the result of the implementation and evaluation.

Table 1: Accuracy of the system as Perceived by the User-Respondents

	MEAN	QD
1. The system has the ability to provide accurate results.	3.69	SA
2. The result of the system is easy to understand and provide useful information.	3.61	SA
3. The system can give precise information regarding the voting process.	3.49	SA
4. The system contributes better information about the candidates.	3.49	SA
5. All information given in the system is precise and correct.	3.58	SA
WEIGHTED MEAN	3.57	SA
Legend A - Strongly Agree (2.51–3.25) SA Strongly Agree (3.26 QD-4.00)		
Quantitative Description SD - Strongly Disagree (1.00–1.75) D–Disagree (1.76 2.50)		

Table 1 represents the accuracy of the system. It shows that the highest mean from among the items are 1 and 2". The system has the ability to provide accurate results" and "The results of the system are easy to understand and provide useful information" with a mean of 3.57 and a qualitative description of strongly agree.

This result explains that the features of the system satisfy the user requirements which provide the information accurately.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Table 2: Efficiency of the system as Perceived by the User-Respondents

	MEAN	QD
1. The system helps the students voting process becomes hassle free by just using a personal computer with internet connection.	3.61	SA
2. The system can cater thousands of students.	3.42	SA
3. The system helps to lessen the burden of the students upon looking all the candidates' information.	3.55	SA
4. The progression of the system meets the satisfaction of the respondents.	3.52	SA
5. It is easy and fast in terms of handling the system.	3.59	SA
WEIGHTED MEAN	3.53	SA
Legend SA-Strongly Agree (3.26 QD- 4.00) SD - Strongly Disagree (1.00 – 1.75) QD-Quantitative Description SA–Strongly Agree (2.51–3.25)D–Disagree (1.76 2.50)		

Table 2 shows on the efficiency of the system. It can be found that from among the items under this variable shows that the highest mean from among the items are 1 and 5. "The system helps the students voting process becomes hassle free by just using a personal computer with internet connection" and "It is easy and fast in terms of handling the system "got the highest means of 3.61 and 3.59 respectively with a qualitative description of strongly agree.

This result explains the features of the system and other item confirms the characteristics of how efficiency works effectively by the respondents.

Table 3: Reliability of the system as Perceived by the User-Respondents

	MEAN	QD
1. The system is reliable as it is control by the admin.	3.55	SA
2. The system provides facts and knowledge which assures the security of both the admin and the students.	3.51	SA
3. The system is functional.	3.51	SA
4. The system is reliable.	3.59	SA
5. The system given a satisfying performance.	3.55	SA
WEIGHTED MEAN	3.54	SA
Legend SA-Strongly Agree (3.26 QD- 4.00) SD - Strongly Disagree (1.00 – 1.75) QD-Quantitative Description SA–Strongly Agree (2.51–3.25)D–Disagree (1.76 2.50)		

Table 3 illustrated the reliability of the system. It is directly noticed among the items under this category that the highest mean among the items are 4, 1, and 5. Both 1 and 5 have similar results which give the weighted mean of 3.54 and qualitatively described strongly agree. Based on the results the researchers can conclude that the system is reliable to use according to its functionalities.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Table 4: Timeliness of the system as Perceived by the User-Respondents

	MEAN	QD
1. The system can count the votes on limited time allocation.	3.48	SA
2. The system has the capability to set its time schedule for registration process of voters.	3.45	SA
3. The system provides a timely and fast accessibility in all the process transaction.	3.54	SA
4. The system can give arrangement of process through time.	3.53	SA
5. The system provides exact and limitation time for voter.	3.48	SA
WEIGHTED MEAN	3.50	SA
Legend SA-Strongly Agree (3.26 QD- 4.00) SD - Strongly Disagree (1.00 – 1.75) QD-Quantitative Description SA–Strongly Agree (2.51–3.25)D–Disagree (1.76 2.50)		

Table 4 emphasized the timeliness of the system. As revealed from the total weighted mean 3.50 among the 5 items "The system can count the votes on limited time allocation"," The system has the capability to set its time schedule for registration process of voters", "The system provides a timely and fast accessibility in all the process transaction." , "The system can provides exact and limitation for voters" the results confirmed that the system is timeliness to use according to its function and . As a whole, the system is consistently has a characteristic of timeliness.

Table 5: Security of the system as Perceived by the User-Respondents

	MEAN	QD
1. The system controls by the administrator for security reason.	3.53	SA
2. The system is secured all the time.	3.53	SA
3. The system can provide permanent security to access to the users.	3.59	SA
4. The system is accessible for all users if there is an account to access.	3.58	SA
5. The system has a time to give security all the users.	3.75	SA
WEIGHTED MEAN	3.59	SA
Legend SA-Strongly Agree (3.26 QD- 4.00) SD - Strongly Disagree (1.00 – 1.75) QD-Quantitative Description SA–Strongly Agree (2.51–3.25)D–Disagree (1.76 2.50)		

Table 5 showed how security is being applied in the system. As we have seen from the table, they almost have the same results to come up with a weighted mean of 3.59. The proponent confidentially assures this feature plays a great role in the system.

The evaluation results, based on user feedback and system analysis, demonstrate promising performance of the proposed approach. The system received an overall evaluation score of 3.55 out of 5, indicating its effectiveness in upholding voter privacy. Specific evaluation criteria revealed accuracy with a score of 3.57 out of 5, efficiency at 3.53 out of 5, reliability at 3.54 out of 5, timeliness of 3.50 out of 5, and a commendable security rating of 3.59 out of 5.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

These findings highlight the potential of the Diffie-Hellman encryption algorithm in building a secure and trustworthy online voting platform, reinforcing the democratic principles of transparency and integrity.

VI. CONCLUSION

In conclusion, voter privacy is of utmost importance in the successful implementation of online voting systems, with the increasing reliance on digital technologies raising concerns about confidentiality and anonymity. This paper explored the challenges associated with voter privacy and highlighted the potential of the Diffie-Hellman encryption algorithm as a robust solution. Leveraging this algorithm allows online voting systems to achieve anonymous authentication, ballot encryption, and end-to-end verifiability, empowering voters to participate confidently while safeguarding their identities and choices. However, ensuring voter privacy is a multifaceted challenge that requires a comprehensive approach, encompassing system architecture, secure authentication, and data protection measures. Continued research and adaptation of cryptographic techniques are vital to counter emerging threats, and public awareness will foster trust in online voting systems. The Diffie-Hellman encryption algorithm offers a valuable contribution to the realm of online voting by enhancing security, preserving voter privacy, and upholding democratic principles. By incorporating this encryption protocol and adopting best practices, online voting platforms can inspire greater public confidence, encourage participation, and contribute to a secure and democratic future.

REFERENCES

[1]. Waller, L. G. (2020). The Possibilities of Internet Voting in Jamaica: Moving from Convenience to Fixing the Problem of Voter Apathy among the Youth. *Electronic Journal of e-Government*, *18*(1), pp17-29.

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

[3]. Kara, M., Laouid, A., AlShaikh, M., Bounceur, A., & Hammoudeh, M. (2021). Secure key exchange against man-in-the-middle attack: Modified diffie-hellman protocol. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, *7*(3), 380-387.

[4]. Huang, H., & Cao, Z. (2009, March). An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security* (pp. 333-342).

[5]. Jharbade, N. K., & Shrivastava, R. (2012). Network based Security model using Symmetric Key Cryptography (AES 256–Rijndael Algorithm) with Public Key Exchange Protocol (Diffie-Hellman Key Exchange Protocol). *IJCSNS International Journal of Computer Science and Network Security*, *12*(8), 69-74.

[6]. Pappas, I. O., Mikalef, P., Giannakos, M. N., Krogstie, J., & Lekakos, G. (2018). Big data and business analytics ecosystems: paving the way towards digital transformation and sustainable societies. *Information Systems and e-Business Management*, *16*, 479-491.

[7]. Jones, B., & Flannigan, S. L. (2006). Connecting the digital dots: Literacy of the 21st century. *Educause Quarterly*, *29*(2), 8-10.

[8]. Selvarani, X. I., Shruthi, M., Geethanjali, R., Syamala, R., & Pavithra, S. (2017, February). Secure voting system through sms and using smart phone application. In *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)* (pp. 1-3). IEEE.

[9]. Gibson, R. (2001). Elections online: Assessing Internet voting in light of the Arizona democratic primary. *Political Science Quarterly*, *116*(4), 561-583.

[10]. Adida, B., De Marneffe, O., Pereira, O., & Quisquater, J. J. (2009). Electing a university president using open-audit voting: Analysis of real-world use of Helios. *EVT/WOTE*, *9*(10).

[11]. Halderman, J. A., & Teague, V. (2015). The New South Wales iVote system: Security failures and verification flaws in a live online election. In *E-Voting and Identity: 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings 5* (pp. 35-53). Springer International Publishing.

[12]. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014, November). Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 703-715).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

[13]. Nwankwo, W., Chinedu, P. U., Masajuwa, F. U., Njoku, C. C., & Imoisi, S. E. (2023). Adoption of i-voting infrastructure: addressing network-level cybersecurity breaches. *Electronic Government, an International Journal*, *19*(3), 273-303.

[14]. Khodzhanovna, S. K. (2023). Cybertech Activities Affecting The Fate Of PoliticaL Elections. *Best Journal of Innovation in Science, Research and Development*, *2*(7), 126-129..

[15]. Rashed, M. G., Ullah, S., & Yasmin, R. (2013, January). Secured message data transactions with a Digital Envelope (DE)-A higher level cryptographic technique. In *International Conference on Engineering Research, Innovation and Education 2013*.

[16]. Gupta, M., & Saini, H. (2015). Workload Characterization of Elliptic Curve Cryptography and Other Network Security Algorithms for Constrained Environments.

[17]. Kajal, B., Vala, B., & Patel, W. (2021, May). A Review of Online Voting System Security based on Cryptography. In *Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021)*.

[18]. Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, *47*, 100530.

[19]. Mohedas, I., Daly, S. R., & Sienko, K. H. (2015). Requirements development: Approaches and behaviors of novice designers. *Journal of Mechanical Design*, *137*(7), 071407.

[20]. Slavin, S., & Schoech, R. (2017). *Human services technology: Understanding, designing, and implementing computer and Internet applications in the social services*. CRC Press.

[21]. Van der Berg, J. S. (2007). *Generalizations of the Diffie-Hellman protocol: exposition and implementation* (Doctoral dissertation, University of Pretoria).

[22]. Arancibia, J. D., Smith, V. F., & Fenner, J. L. (2019, November). On-The-Fly Diffie-Hellman for IoT. In *2019 38th International Conference of the Chilean Computer Science Society (SCCC)* (pp. 1-5). IEEE.