



Enhancing the Robustness of a Three-Layer Security Electronic Voting System Using Kerberos Authentication

Emeka Reginald NWOGU¹, Wilson Chukwuemeka AHIARA², Peter Mathew AONDOHEMBA³

¹Directorate of ICT, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria
nwogu.emeka@mouau.edu.ng

²Department of Computer Engineering, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria
ahiara.wilson@mouau.edu.ng

³Department of Computer Science, National Open University of Nigeria, Umudike Study Center, Abia State, Nigeria
mpeter2008@yahoo.com

Corresponding Author: ahiara.wilson@mouau.edu.ng , +2348039207982

Date Submitted: 06/08/2023

Date Accepted: 06/10/2023

Date Published: 14/10/2023

Abstract: The rapid advancements in technology have spurred interest in electronic voting systems as a means to modernize and enhance the democratic electoral process. However, ensuring the security and integrity of electronic voting systems remains a critical challenge. In this study, we present a highly secure and efficient model for an electronic voting system, featuring a robust three-layer security architecture that includes the device authentication, user authentication and network security. The proposed system incorporates Kerberos authentication and Advanced Encryption Standard (AES) to fortify device and user authentication. The segmentation of the system network into zones that includes the Virtual Private Network, the Public Network and the Demilitarized Zone also helps to mitigate potential cyber-attacks and fraudulent activities. Leveraging biometric security (fingerprint) and user tokens (voter's cards), the system ensures the accurate identification and authentication of voters, thereby enhancing the overall integrity of the voting process. Through a series of tests involving 500 enrolled users, the proposed electronic voting system demonstrated remarkable efficacy, achieving a 100 percent accuracy rate in ballot tallying. Having addressed key concerns related to security and transparency, the proposed voting system has the potential to instill trust and confidence in electoral processes.

Keywords: Electronic Voting System, Kerberos Authentication, Biometric Security, Demilitarized Zone, Advanced Encryption Standard (AES)

1. INTRODUCTION

Conducting elections, especially for large populations, has traditionally been an expensive, time-consuming, and fraud-prone process, but it is essential for democratic systems [1]. To streamline and improve the electoral process, researchers have explored various technological approaches, and one such innovation is Electronic Voting. This method involves voters using electronic ballots, which are securely transmitted over a computer system to the election tallying office. Embracing Electronic Voting has garnered interest from technology experts and policymakers alike. Nevertheless, to make it effective and reliable, the system's security must be a top priority [2, 3].

Despite the evolution of electronic voting designs, from punched cards to modern Direct Recording Electronic (DRE) Voting Systems, these systems still face challenges related to incomplete security and lack of standardization. This obviously has sustained research to address major security problems in electronic voting [4]. A secure Electronic Voting System holds the promise of reducing electoral violence and instilling confidence in the fairness of elections among politicians, supporters, and the general public [5]. A similar stance has been taken by Balzarotti *et al* [6] underscoring one of the importance and features of electronic voting to include the capability of hiding voters' identity or render them anonymous when casting votes to boost security. With the advancement in technology, the focus has shifted towards designing highly secure systems that can gain users' trust and prevent fraud [7]. Researchers and technology pundits are not unaware of the need for such system design and implementation to emerge in a form factor that is affordable, maintainable and scalable. Likewise, Hacker and Van Dijk [8, 9] posited that the technical solution and implementation details of such highly secure electronic voting system should be readily accessible to everyone.

Though the adoption of Electronic Voting has been slow due to the challenge of designing a highly secure system that can withstand fraudsters' attempts to exploits weaknesses in the security architecture [10, 11, 12]. Nonetheless, interest remains, and efforts are now focused on developing a trustworthy and secure system that can gain the confidence of users. To this end, numerous authors have proposed various means of enhancing security in Electronic Voting systems

For instance, Kumar *et al.* [5] proposed an electronic voting system based on Blockchain technology which stores voter details and votes in two separate blockchain networks and uses a unique Personal Identification Number (PIN) for voter access. However, relying solely on a PIN for voter identification may leave the system vulnerable to impersonation. Similarly, Prasetyadi *et al.* [13] conducted a research study on blockchain-based Electronic Voting System with special ballot and block structures using Secure Hash Algorithm (SHA)3-256 hash algorithm, and a voting protocol that conform to the extant voting and electoral laws in Indonesia.

Nwogu and Onwuachu [7] developed a Supervised Public Network Direct Recording Electronic Voting (PNDRE) system that incorporated good security measures but overlooked the problem of impersonation during login.

Gandhi & Scholar [14] proposed a voting system that makes use of Personal Identification Number (PIN) and fingerprint biometric to log into the system, they also added secret key cryptography as encryption system to secure the communication between the voting client and the voting server, However, these keys are unreliable as they are prone to potential discovery and need to be changed often and kept secure during distribution and in service.

Najam *et al* [15] developed an identification based system that employs two voter verification techniques: fingerprint and facial recognition for voter authentication and validation. However, their work did not consider the problem of man-in-the-middle attack, where a fraudster could hijack an ongoing session, and cast votes or perpetuate other fraud related actions on the system.

The work in [19, 20] relates authentication to Kerberos; authentication has been described as a method of identifying an identity to the needed level of confidence, and Kerberos deals with verification functions that have been designed to facilitate application level authentication. Similarly, some other researchers have explored cryptography-based approaches using algorithms like Rivest–Shamir–Adleman (RSA), Secure Hash Algorithm (SHA), and others to secure Electronic Voting systems [5, 16, 17, 18]. However, the reliability of cryptographic keys and their potential for discovery and misuse require careful consideration.

In view of these security breaches associated with Electronic Voting and the desire to create a tamper proof transmission system for authorization [19], this paper integrates a robust three-layer security architecture using Kerberos authentication. This work hopes to quell the issue of Distributed Denial of Service (DDoS) as reported in [21] along with other anomalies such as ballot stuffing, ballot changing, over voting, Man-in-the-middle attacks and impersonation by exploring a novel approach to safeguarding the integrity of the electoral system

2. MATERIALS AND METHOD

2.1 System Development Tools

A couple of programming languages and utilities were used to implement the proposed system. These include:

- i. Python Language: The primary language used for the system implementation. Python is a high-level interpreted language with very robust library.
- ii. JavaScript: This was used for scripting in the system. Like Python, JavaScript is a high-level programming language that supports multiple programming paradigms and commonly used for web development.
- iii. Django: Utilized for implementing the backend of the system. This open-source Python-based utility simplifies the complexity of building database-driven websites, enabling rapid development, code reusability, and low coupling
- iv. SQLite: Chosen as the relational database management system for the system implementation. SQLite, based on the C library, provided a reliable foundation for managing the system's database.
- v. GraphQL: Incorporated as the Application Programming Interface (API) for executing data queries and manipulations within the system.
- vi. Semantic UI: Employed to style the front end of the system, providing a visually appealing and user-friendly interface.
- vii. Requests: Used to implement Kerberos authentication in the system. Requests is a Python library used for implementing Kerberos authentication in the Python-based system.

2.2 Methodology

To achieve the design presented in this work, an algorithm for the system operation was developed. This algorithm was then translated into codes written in Python and JavaScript, enabling the software-based implementation of the system. The functionality of the system was tested using a mock election scenario.

2.3 Analysis of the Proposed System

The proposed system employs a three-layer security approach, encompassing user authentication, server-client (device) authentication, and network security. For user authentication, we propose the use of a token (Electronic voters' card) along with biometric security (fingerprint authentication). Additionally, we implement Kerberos for server-client authentication, and the Advanced Encryption Standard (AES) will complement Kerberos authentication for secure network data communication.

With user authentication, our aim is to ensure that only legitimate voters can log in and access the voting facility from the voting terminal (client). By combining a token and fingerprint authentication, we can prevent impostors from using harvested credentials to gain unauthorized access to another voter's account and cast votes on their behalf. Likewise, by implementing Kerberos for server-client authentication, we address the concern of man-in-the-middle attacks. This security

measure safeguards ongoing voting sessions against potential hijacking by hackers after a valid voter has logged in, thereby reducing the risk of fraudulent activities.

Furthermore, the use of the Advanced Encryption Standard for network data communication adds an extra layer of security to the communication between voting clients and servers. This encryption ensures that all data exchanged between the voting servers and terminals remains protected from unauthorized access during transmission. The system's design, as presented here, will achieve the following objectives:

- i. Prevent all forms of impersonation by employing two-level security (token and fingerprint biometric) during voter authentication.
- ii. Thwart impersonation attempts by making it challenging for an impostor to misuse stolen or cloned tokens, thanks to the two-level security setup at the voter authentication stage.
- iii. Ensure session security by employing Kerberos for server-client and server-server authentication, reducing the risk of session hijacking during ongoing voting processes.
- iv. Strengthen security by authenticating and authorizing terminals and servers through Kerberos, which acts as a trusted third-party authentication body.
- v. Enhance communication security between servers and voting terminals (clients) with the use of the Advanced Encryption Standard, providing an additional layer of protection.

2.4 The Proposed System Design

The proposed system follows a structured approach which includes: Voter enrolment stage, pre-election and election, and result processing and announcement stage. They are explained in the subsections below:

1) The voter enrolment stage design

This stage involves the capturing and recording of Voters' information (coded Electronic Voter's Card (Token) alongside fingerprint information) and subsequent storage in the Voter Information Database. The database allows for the authentication and authorization of voters during elections. To kickstart the process, the Voter Registration Machine undergoes authentication at the Key Distribution Centre of the Kerberos System, granting access to the Forwarding Server. This authentication is typically time-bound, during which the Machine Operator can register as many voters as possible. Once the Kerberos authentication is complete, the Operator proceeds with the voter enrolment process.

Also, the Voter Registration Machine does not have direct communication with the Voter Information Database, as the Voter Information Database sits in the Secure Private Network of the Electoral Commission. All communications with the Voter Information Database must be through the Forwarding Server which sits at the Demilitarized Zone (DMZ). According to Patel [22], the DMZ is a logical or physical subnetwork that exposes an organization's external services to an untrusted network. This means that the DMZ provides an extra layer between the internal or private network (LAN) and the external network preventing potential malicious attack occasioned by direct access to the trusted network. Figure 1 shows the visual representation of the Voter enrolment stage of the proposed system.

2) The Pre-election and Election Stage Design

This stage involves all activities ranging from device authentication, Voter authentication to ballot casting. Authentication in this light refers to a protocol that validates the identity of a user or host before granting access to secure network [23]. The Pre-election stage also involves the setting up and configuration of the election by the Electoral Officers and therefore forms a crucial segment of the proposed system to facilitate transparent and reliable electronic voting. The general election process architecture of the proposed system is depicted in Figure 2, while Table 1 outlines the election process algorithm.

3) Result Processing and Announcement Stage Design

The Result processing and announcement stage involves the collation of cast ballots in the Tallying Server. To collate a ballot X_n which is a single ballot paper in the form of an array containing names of candidates in a particular election, where n could take a value ranging from 1 to k , where k is the total number of votes/ballots/Voters and where $X_n = (X_{n1}, X_{n2}, \dots, X_{nm})$ and any of X_{n1}, X_{n2} or $X_{nm} \rightarrow \{1,0\}$ and represents a single candidate in an election, where m is the total number of candidates for an election and also represents the last candidate in the list of candidates for an election. The value of the ballot X_n is originally set to a default value of $X_n = (0, 0, \dots, 0)$. To successfully cast a vote for a candidate, the Voter only turns the value 0 representing the candidate's vote to the value 1. With the value 1 representing a valid vote for the candidate and the value 0 (default value) representing no vote for the candidate.

Thus, the result for the election denoted by an array X is given by $\sum_1^k X_n$
To announce the result, an Electoral Administrator will have to connect to the Tallying Server from the Local Area Network through the firewall and download the result of the election for announcement.

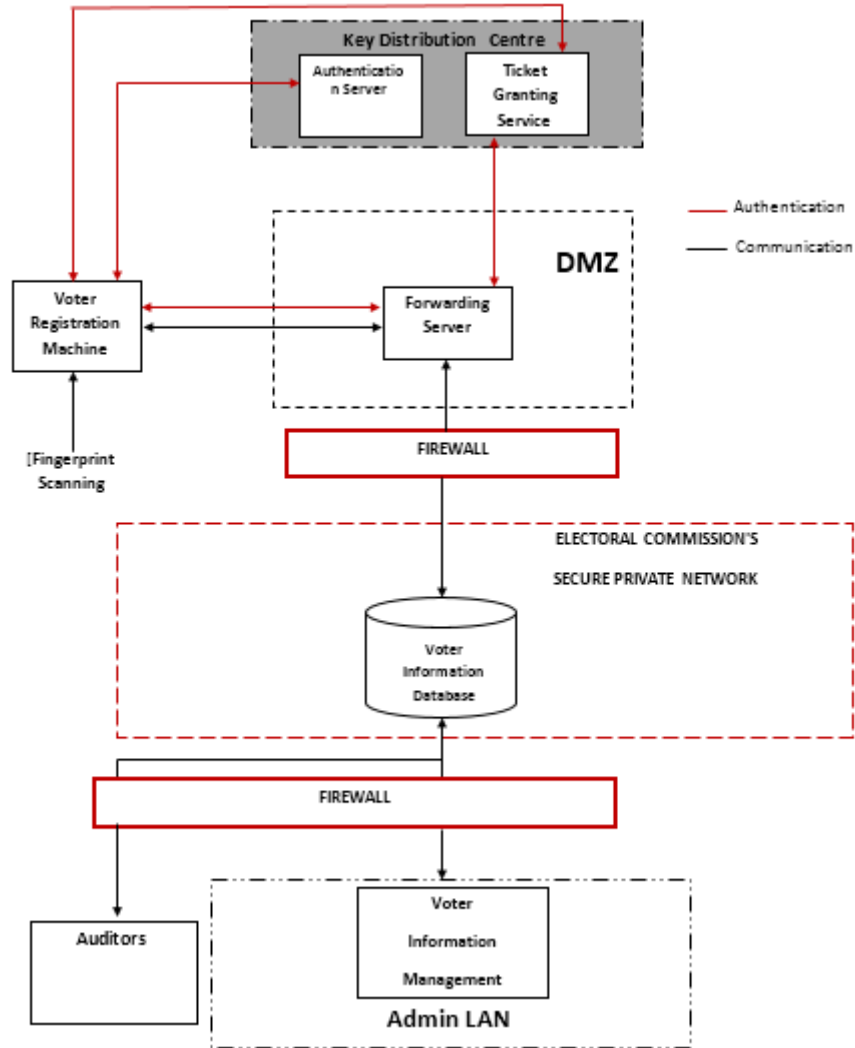


Figure 1: The architecture of the voter enrolment process

Table 1: The election process algorithm of the proposed system

The system algorithm	
Step 1 {User input settings}	Input: DevID, DevPSWD, TokenID, FingerPrtInf, FingerPrtInfTemp, AvElect, EBallotY {Process}
Step 2 (Voting Terminal Authorization)	2.1 The Voting Terminal sends the TGT and another message containing the Voting Terminal ID encrypted with the Ticket Granting Service/Voting Terminal Session Key to the TGS 2.2 The TGS decrypts the TGT using its Secret Key, and also decrypts the other message containing the Voting Terminal ID DevID 2.3 The TGS sends the Voting Terminal/Forwarding Server Ticket encrypted using the Secret key of the forwarding Server [Note at this point, the Voting Terminal has all credentials to request for connection with the Forwarding Server]
Step 3 (Forwarding Server connection request)	3.1 The Voting Terminal connects to the Forwarding Server and sends the following messages; the Voting Terminal/Forwarding Server Session Key VT/FS Key encrypted using the Secret key of the forwarding Server FSKey and Voting Terminal ID and timestamp encrypted using the Voting Terminal/Forwarding Server Session Key VT/FS Key 3.2 The Forwarding Server sends a confirmation message encrypted using the Voting Terminal/Forwarding Server Session Key VT/FS Key to the Voting Client

The system algorithm

3.3 The Voting Terminal uses the Voting Terminal/Forwarding Server Session Key VT/FS Key to decrypt the confirmation message from the Forwarding Server, and can now trust the Forwarding Server for communication between the two devices

Step 4 (Voter authentication)

- 4.1 The Voter inserts their token (electronic voters' card) on the token reader, which scans the TokenID on the card and forwards to the Forwarding Server
 - 4.2 The forwarding Server, on receiving the request queries the Voter Information Database for the Voter record
 - 4.3 Once the Voter Information Database confirms the availability of the Voter in its record, it requests for the fingerprint information FingerPrtInf of the Voter
 - 4.4 The Voter supplies their fingerprint information FingerPrtInf which is matched and confirmed with the sample template FingerPrtInfTemp for the Voter in the Voter Information Database,
 - 4.5 The Voter Information Database returns a valid Voter message to the Voter through the Forwarding Server
-

Step 5 (Voting)

- 5.1 To vote, the Forwarding Server queries the Election Database for available election AvElect for the Voter
 - 5.2 Once the available elections are displayed, the Voter casts their ballot for each election EBallotY to the Forwarding Server
 - 5.3 The Forwarding Server sends the ballot to the Tallying Server and also sends a ballot casting confirmation to the Election Database for it to deactivate the elections that have been completed for the Voter
 - 5.4 The Forwarding server disconnects the session with the Voting Terminal
 - 5.5 The Tallying Server Collates the result of each election for subsequent announcement by the Election Organizers
-

2.5 The Proposed System Security Module

The proposed system incorporates specific security modules to ensure a robust and secure electronic voting process. These modules are outlined as follows:

1) The server-client (device) authentication module design

This describes the method of authentication of the devices before communication. Only the Voting Terminal and Forwarding Server are authenticated. The Forwarding Server serves as a Proxy Server for all the Servers in the network. The Forwarding Server can access the Servers in the Secure Private Network .using an Access Control list implemented on a Firewall between the Demilitarized Network and the Secure Private Network, Similarly, all connections from the Administrators Local Area Network and the Auditors are made possible using an Access Control List implemented on the Firewall between the Secure Private Network and the Admin LAN.as depicted in the authentication setup process of Figure 3.

2) The Voter Authentication Module

The Voter authentication involves all activities required to grant voters access to successful voting during an election, as depicted in Figure 4. This system was designed to use a Token (Voter's Card) issued to registered voters during registration, along with their fingerprint template captured at that time. To access the voting system, a voter is required to allow the system scan their Token and send to the Forwarding Server, which queries the Voter Information Database to identify the voter. Once the Voter has been identified by confirming their record exists in the Voter Information Database, the system then requests for the fingerprint information in order to authenticate that the original Voter has presented the card. The fingerprint information is captured and sent to the Forwarding Server, which compares the fingerprint information with the template supplied by the Voter Information Database. Once the template in Voter Information Database matches with the captured sample, the system confirms the identity of the Voter and can now allow the Voter to proceed to the next stage of the process.

3) The Network Security Module

This module has three security domains, namely: The Demilitarized Zone (DMZ), Secure Private Network (SPN) and Local Area Network (LAN). The demilitarized zone security domain is a Wide Area Network that hosts the Voting Terminals at different locations and the Forwarding Server. Authentication was done using Kerberos authentication system to enable the Voting Terminals communicate with the Forwarding Server.

Similarly, the SPN hosts all important Servers of the Electronic Voting Network, which include the Voter Information Database, the Election Server and the Tallying Server. The SPN is implemented using a Virtual Private Network (VPN). Lastly, the Administrator's LAN is the last of the network security that enables administrators to manage the Electronic Voting System. All communications from the Administrators LAN to the Secure Private Network is done through a Firewall that allows only the authorized Administrator devices to access the Secure Private Network and perform such operations as voter information management, election update and result management. Similarly, apart from the Access Control implemented on the Firewalls, all other communications between the Forwarding Server and all Servers in the Secure Private Network and communications between the Servers in Secure Private Network and the Administrative Local Area Network also made use of the AES.

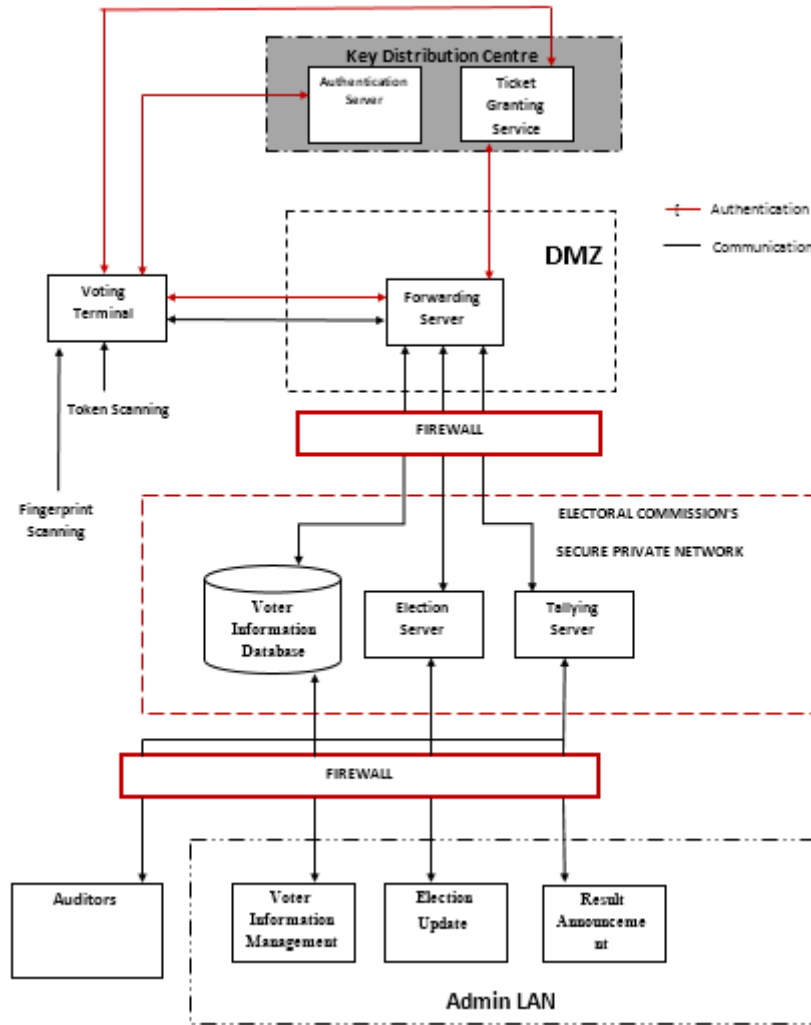


Figure 2: The General election process architecture of the proposed system

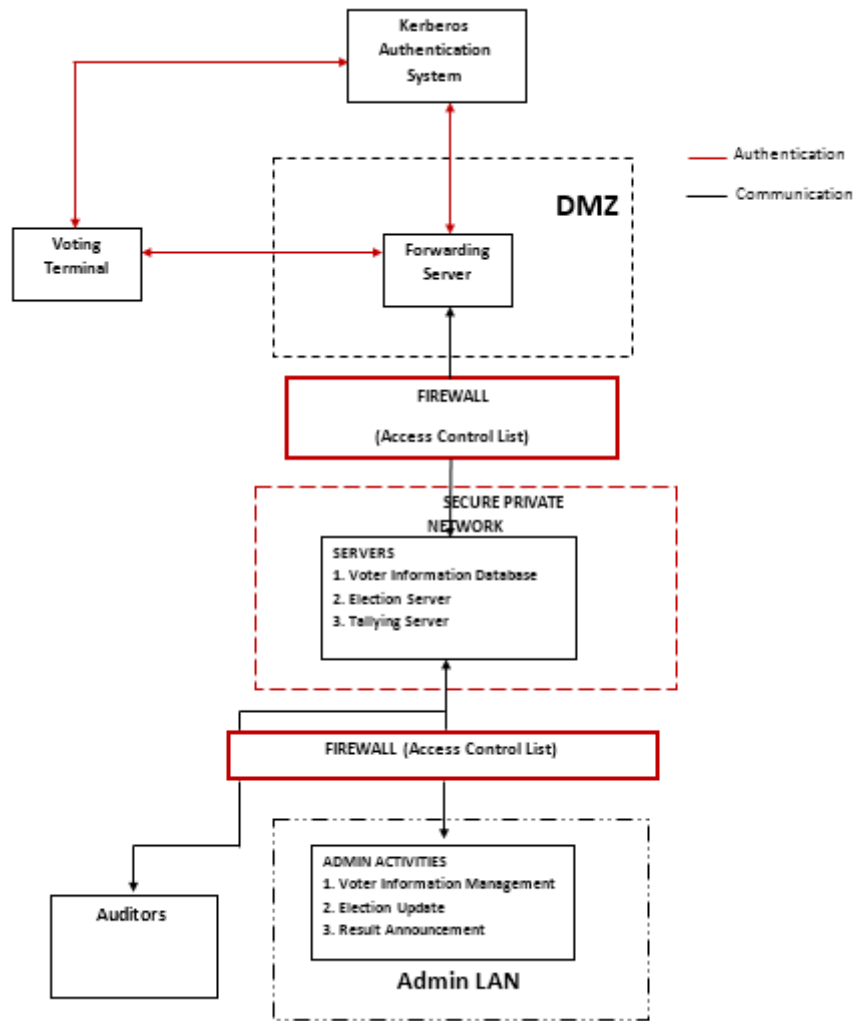


Figure 3: The device authentication process of the proposed system

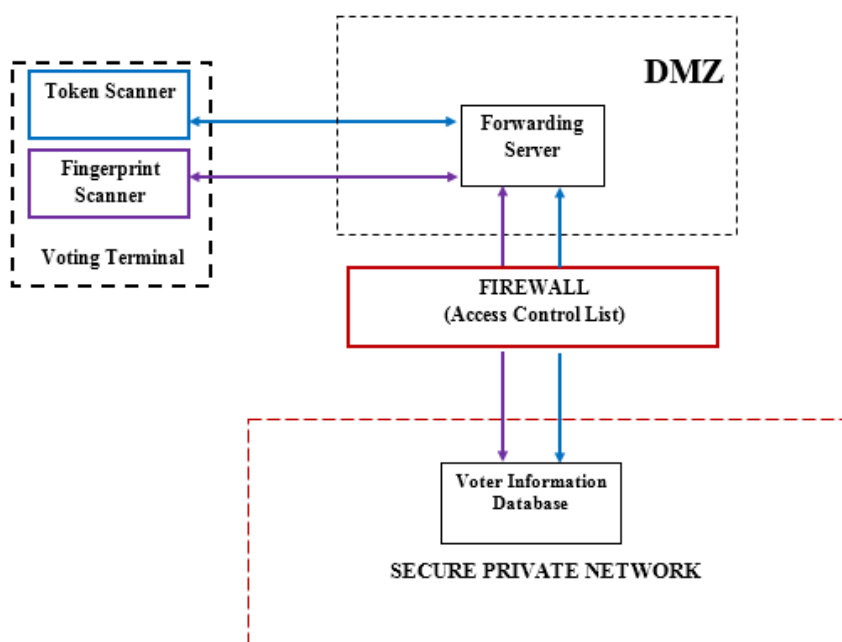


Figure 4: The voter authentication process of the proposed system

3. RESULTS AND DISCUSSIONS

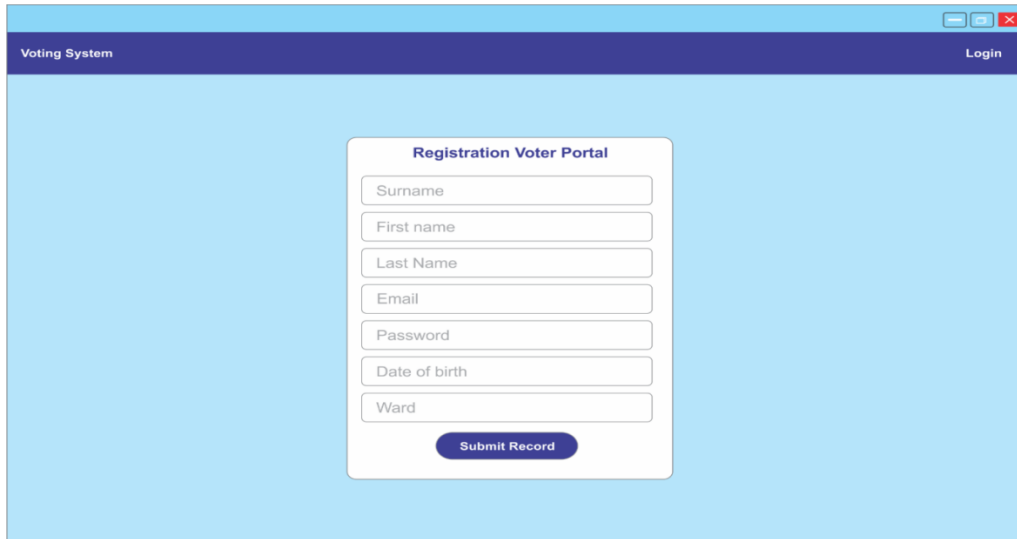
In order to assess the functionality and reliability of the system, 500 users were enrolled in the system as registered voters. These users supplied necessary information at the Voter registration terminal, and upon completion of registration, each registered voter was issued a unique software token (Voter's card). During the election, all registered voters utilized their token, password and fingerprint to log into the voting terminal in order to cast their vote. In all, there were 10 elections with a total of 25 candidates standing in the election.

To test the credibility of the system, all voters for each election were given precast ballot papers to complete on the online voting system. This was to enable us test the credibility and accuracy of the system. At the end of the result collation exercise, it was observed that the result published on the Electronic Voting System tallied with the result of the collated paper ballot, implying that the system returned an accuracy of 100 percent as shown in Table 2. Similarly, to test the security of the system, the Wireshark packet sniffer tool was used to sniff ballot-carrying packets during transmission to the forwarding server. It was observed that the ballot and all information was encrypted using the Advanced Encryption Standard, and as such, it was impossible for anyone to make any meaning from the captured packets.

Figure 5 shows the user-friendly Voter Registration portal where a new voter can be enrolled in the system to enable them vote in scheduled elections. Once registration is completed, the registered voter is issued a Token (Voter's card) linked to their identity and which they must provide together with a valid password and fingerprint to enable them gain access and participate in any election. Thus, creating a multi-layered authentication process.

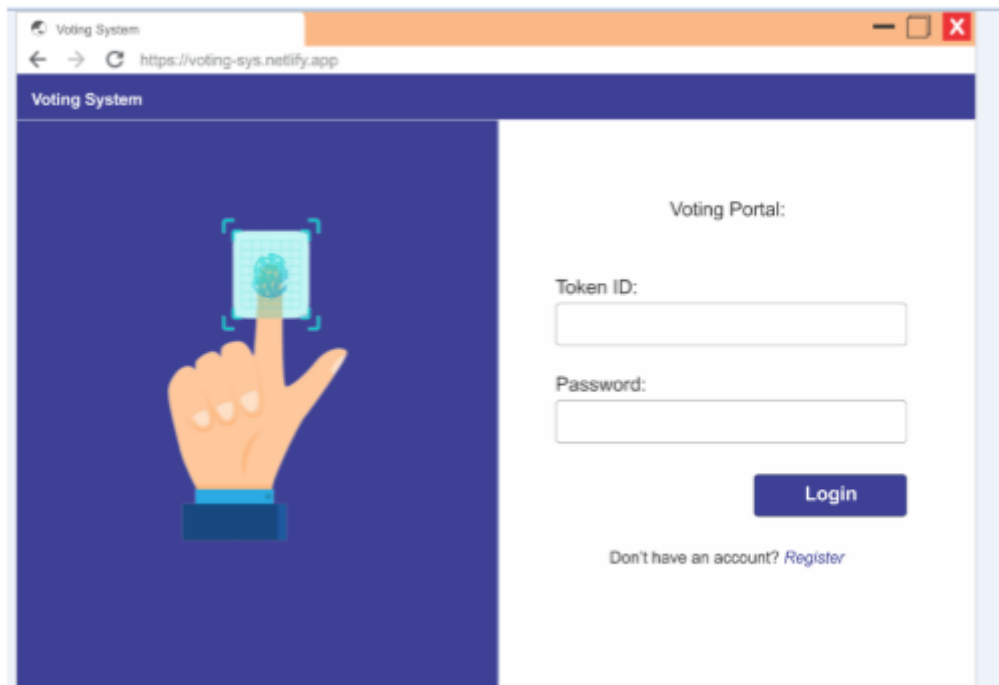
Table 2: The result of the electronic voting exercise

S/N	TITLE OF ELECTION	NUMBER OF CANDIDATE	NUMBER OF VOTERS	NUMBER OF VOTERS (CANDIDATE 1)	NUMBER OF VOTERS (CANDIDATE 2)	NUMBER OF VOTERS (CANDIDATE 3)	ACCURACY (%)
1	Presidential election 1	2	500	350	150		100
2	Presidential election 2	3	491	140	150	201	100
3	Presidential election 3	3	485	135	200	150	100
4	Gubernatorial election 1	5	500	270	230		100
5	Gubernatorial election 2	2	465	215	250		100
6	Gubernatorial election 3	3	470	170	210	90	100
7	Senatorial election 1	3	488	188	120	180	100
8	Senatorial election 2	2	495	255	240		100
9	Representative election 1	2	500	355	240		100
10	Representative election 2	3	480	160	180	140	100



The image shows a web browser window titled "Voting System" with a "Login" link in the top right corner. The main content area is light blue and features a white box titled "Registration Voter Portal". Inside this box, there are seven input fields: "Surname", "First name", "Last Name", "Email", "Password", "Date of birth", and "Ward". Below these fields is a dark blue button labeled "Submit Record".

Figure 5: The Voter Registration Portal



The image shows a web browser window titled "Voting System" with the URL "https://voting-sys.netlify.app" in the address bar. The page has a dark blue header with "Voting System" on the left and "Voting Portal:" on the right. On the left side, there is a large illustration of a hand with a finger pointing at a blue square with a fingerprint icon. On the right side, there are two input fields: "Token ID:" and "Password:". Below these fields is a dark blue button labeled "Login". At the bottom, there is a link that says "Don't have an account? Register".

Figure 6: The voting portal log on page

Figure 6 shows the voting terminal logon page where a valid (registered) voter can log in to see a list of scheduled elections. Figure 7 offers a user-friendly display of candidates contesting in a selected election. The voter only needs to click on the vote button against the name of their choice candidate. Once voting has been completed, the vote buttons become deactivated as shown in Figure 8, indicating that the election is no longer available for the Voter.

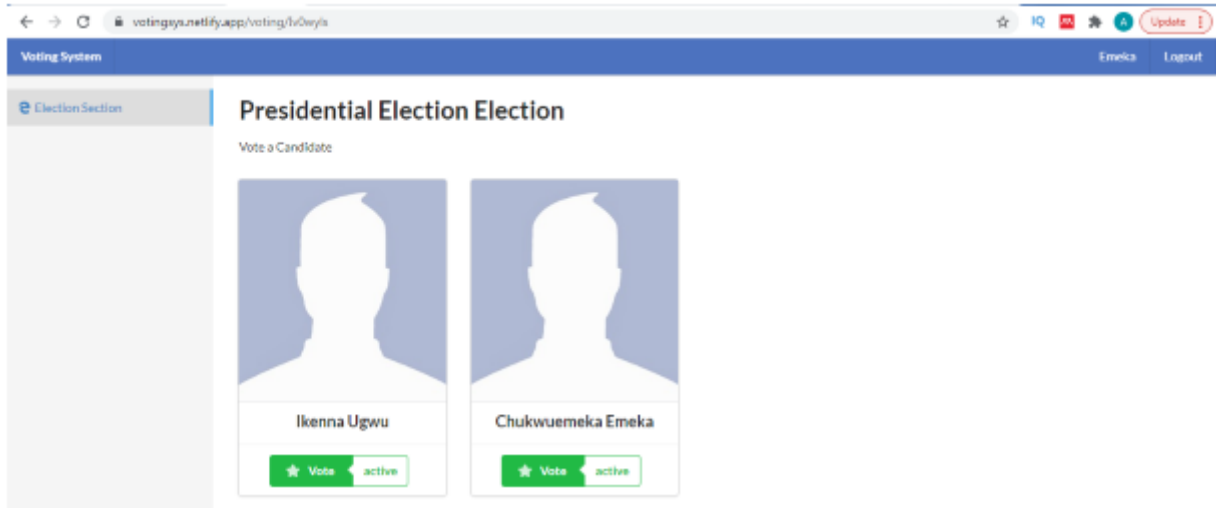


Figure 7: Listed candidates for the presidential election

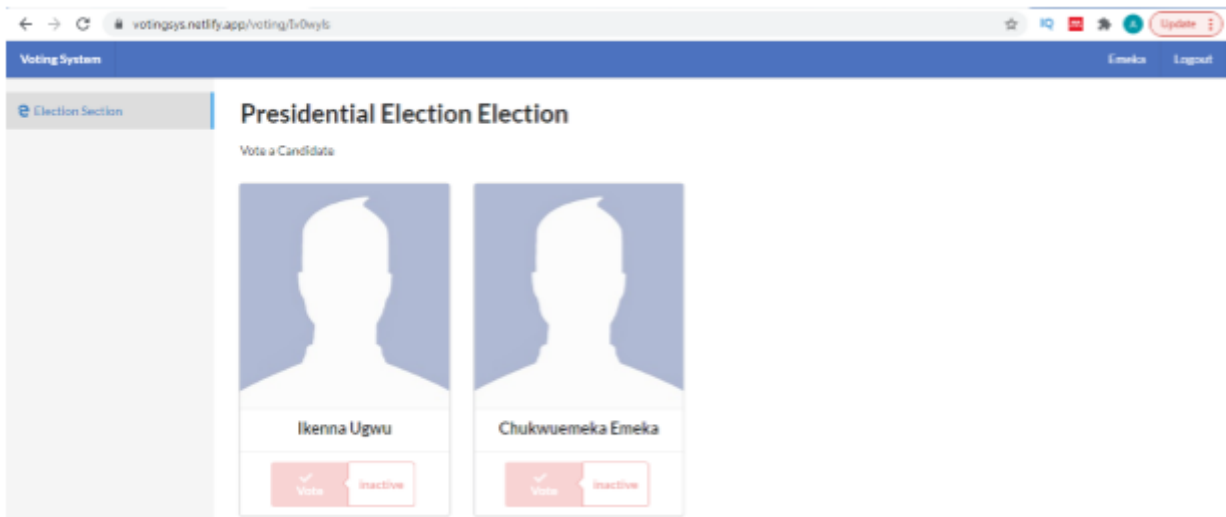


Figure 8: Deactivated election after successful voting

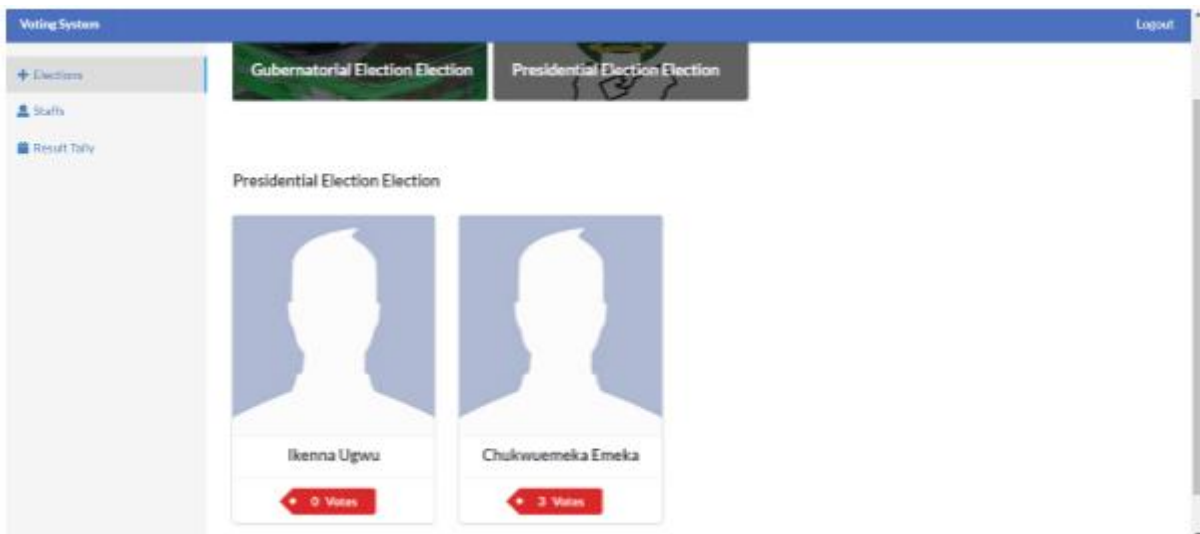


Figure 9: Published presidential election result

To collate and publish the result of a given election, the Electoral collation officer will need to log into the Vote tallying server and collate a selected election, and subsequently publish the result. Figure 9 shows the published presidential election result.

4. CONCLUSION

This work implemented a very secure model for implementing a workable electronic voting system using three-level security architecture. The incorporation of Kerberos authentication and Advanced Encryption Standard (AES) ensures a rigorous device authentication process, bolstering the overall integrity of the system, while biometric security (fingerprint) and user token (voter's card) was used for user and voter authentication respectively. The implications of this work are extensive and hold significant potential to foster increased voter participation and engagement, alleviate the general fear of compromise, as well as cyber-attacks associated with electronic voting system. By providing a secure and user-friendly voting experience, citizens are more likely to embrace electronic voting as a viable and trustworthy alternative to traditional methods.

While our study has made significant strides in the field of electronic voting security, we acknowledge that the journey towards widespread adoption and implementation may present challenges and complexities. As such, we recommend further research on comprehensive risk assessments and real-world testing to evaluate the system's performance under diverse scenarios and potential vulnerabilities so as to enhance the system's security and reliability.

REFERENCES

- [1] Angsuchotmetee, C. & Setthawong, P. (2020a). Blockvote : An architecture of ablockchain-based electronic voting system. *ECTI Transactions on Computer and Information Technology*, 14(2), 174–189. <https://doi.org/10.37936/ecti-cit.2020142.227455>
- [2] Oostveen, A.M. & Van Den Besselaar, P. (2009). Users' experiences with e-voting: A comparative case study. *International Journal of Electronic Governance*, 2(4), 357–377. <https://doi.org/10.1504/IJEG.2009.030527>
- [3] Nwogu, E.R. & Ihedigbo, C.E. (2016). A Structured and Layered Approach for a Modular Electronic Voting System: Defining the Security Service and the Network Access Layers. *IOSR Journal of Computer Engineering*, 18(04), 63–69. <https://doi.org/10.9790/0661-1804026369>
- [4] Ben Ayed, A. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications*, 9(3). <https://doi.org/10.5121/ijnsa.2017.9301>
- [5] Kumar, D.D., Chandini, D.V. & Reddy, D. (2020). Secure Electronic Voting System using Blockchain Technology. *International Journal of Smart Home*, 14(2), 31–38. <https://doi.org/10.21742/ijsh.2020.14.2.04>
- [6] Balzarotti, D., Banks, G., Cova, M., Felmetzger, V., Kemmerer, R., Robertson, W., Valeur, F. & Vigna, G. (2010). An experience in testing the security of real-world electronic voting systems. *IEEE Transactions on Software Engineering*, 36(4), 453–473. <https://doi.org/10.1109/TSE.2009.53>
- [7] Nwogu, E.R. & Onwuachu, U.C. (2016). Supervised Public Network Direct Recording Electronic Voting (PNDRE Voting) on Existing Global System for Mobile Communication Infrastructure; a Panacea for Cheap E-voting System Implementation in Nigeria. *International Journal of Research Studies in Computer Science and Engineering*, 3(2), 21–28. <https://doi.org/10.20431/2349-4859.0302004>
- [8] Hacker, K. & van Dijk, J. (2014). Digital Democracy: Issues of Theory and Practice. In *Digital Democracy: Issues of Theory and Practice*. <https://doi.org/10.4135/9781446218891>
- [9] Van, D. & Jan, A.G.M. (2012). Digital democracy: Vision and reality. *Innovation and the Public Sector*, 19(1), 49 - 62. <https://doi.org/10.3233/978-1-61499-137-3-49>
- [10] Khan, K.M., Arshad, J. & Khan, M.M. (2018). Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research*, 14(1), 53–62. <https://doi.org/10.4018/IJEGR.2018010103>
- [11] Kovic, M. (2017). Blockchain for the people: *Blockchain technology as the basis for a secure and reliable e-voting system*. June. <https://doi.org/10.31235/osf.io/9qdz3>
- [12] Essex, A. (2016). Internet Voting in Canada: A Cyber Security Perspective. *Brief Submitted to the House of Commons Special...* <https://www.ourcommons.ca/Content/Committee421/ERRE/Brief/BR8610535/br-external/EssexAleksander-e.pdf>
- [13] Prasetyadi, G.C., Mutiara, A.B. & Refianti, R. (2020). Blockchain-based electronic voting system with special ballot and block structures that complies with Indonesian principle of voting. *International Journal of Advanced Computer Science and Applications*, 11(1), 164–170. <https://doi.org/10.14569/ijacsa.2020.0110121>
- [14] Gandhi, N. & Scholar, M.T. (2014). Study on Security of Online Voting System Using Biometrics and Steganography. *International Journal of Computer Science & Communications* 5(1), 29–32.
- [15] Najam, S.S., Shaikh, A.Z. & Naqvi, S. (2018). A novel hybrid biometric electronic voting system: Integrating finger

- print and face recognition. In arXiv. <https://doi.org/10.22581/muet1982.1801.05>
- [16] Del Blanco, D. Y. M., Alonso, L. P., & Alonso, J. A. H. (2018). Review of Cryptographic Schemes applied to Remote Electronic Voting systems: Remaining challenges and the upcoming post-quantum paradigm. *Open Mathematics*, 16(1), 95–112. <https://doi.org/10.1515/math-2018-0013>
- [17] Oo, H.N. & Aung, A.M. (2013). Implementation and Analysis of Secure Electronic Voting System. Implementation and Analysis of Secure Electronic Voting System. *International Journal Of Scientific & Technology*. 2(3), 158–161.
- [18] Nwogu, E.R. (2015). Mobile, Secure E -Voting Architecture for the Nigerian Electoral System. *IOSR Journal of Computer Engineering Ver. II*, 17(2), 2278–2661. <https://doi.org/10.9790/0661-17222736>
- [19] Dayanand L., Nida K. G, Sahana D S, Brahmananda S H, Madhurya J A (2020).Kerberos: Security Analysis of Authentication Protocol. *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9(5), pp. 7569-7575 <https://doi.org/10.30534/ijatcse/2020/94952020>
- [20] Al-Janabi, S.T.F. & Rasheed, M.A. (2011). Public-Key Cryptography Enabled Kerberos Authentication Conference: Developments in E-systems Engineering (DeSE), pp209-214. Doi:10.1109/DeSE.2011.16
- [21] Wolchok, S., Wustrow, E., Isabel, D. & Halderman, J.A. (2012). Attackingthe Washington,D.C. internet voting system. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7397 LNCS. https://doi.org/10.1007/978-3-642-32946-3_10
- [22] Patel, Manan (2020). Demilitarized Zone: An Exceptional Layer of Network Security to Mitigate DDoS Attack. *Electronics Thesis and Dissertations*, 8306, Accessed online on January, 2023. Available at <https://scholar.Uwindsor.ca/etd/8306>
- [23] Nilesh, A.L., Salendra, P. & Mohammed, F. (2016). A Review of Authentication Methods. *International Journal of Scientific &Technology Research* 5(11), 346-249