International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 611-614, November-2023

https://doi.org/10.47001/IRJIET/2023.711081

Smart Election: Blockchain Based Machine Learning Solution for e-Voting Electoral System

[1]Silva H. K. M. D, [2]De Silva M.W.M.R, [3]Withanage P.A, [4]Hettiarachchi R.T

[1,2,3,4]Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka

***Abstract* - An essential part of a nation's political life cycle is election. Any e-voting program must guarantee the privacy, authenticity, and integrity of citizens' votes and personal information. We suggest a reliable electronic voting system built on machine learning and blockchain concepts to allay these worries. However, there are a few issues with this electronic voting technology. It can be compromised by using a mobile application or website to complete the voting paper. The suggested blockchain-based electronic voting method provides confidence, transparency, and treasury while guarding against network intrusions.**

Keywords: Anonymous, Integrity, authenticity, blockchain, intrusions.

I. INTRODUCTION

Every person has the democratic right to vote, which permits them to select the leaders of tomorrow. Voting not only allows individuals to vote for political parties, but it also helps them grasp the importance of citizenship [20]. Many individuals do not vote because they believe that one vote does not matter, yet it does. Elections are used to develop the nation's democratic structures [18, 19]. Voting is an important process that keeps a country's political structure running. The e-voting smart election system is a modern approach to conducting elections that leverages technology to streamline the voting process, improve transparency, and increase participation. There have been changes over time, as seen using paper votes, the passage of new legislation to simplify elections, and the use of electronic tools to expedite the procedure [5].

There voters vote on the ballot paper and then put the paper in the sealed boxes provided by the poll. Department. When the election is over, the secret ballots are opened and counted by hand to announce the results. The traditional paper-based voting system served to increase people's confidence in majority voting. It helped to democratize it. The process and electoral system are valuable for selecting more democratic constituencies and governments. 167 nations with democracy in 2018, out of roughly 200, they are completely defective or hybrid [5,6]. Secret ballot has been the format. Since the beginning of the electoral system, it has been used to increase confidence in democratic systems. It is essential to confirm that certificate in the vote not less. A recent study revealed that the traditional voting process is not entirely healthy, which raises several questions. Including justice, equality and the will of the people, have not been adequately quantified [7] and understood in the form of government [2,8]. We research the state of voting technologies today. Used biometric and blockchain technologies together in electronic voting applications.

1.1 Face and Fingerprint Identification

Biometric technology uses bodily traits to automatically identify individuals, ensuring accurate identification based on biological features. Common methods include face and fingerprint recognition, with facial recognition offering more recent and precise person identification. Biometrics technology promises to modernize and enhance the voting experience, bolstering security, privacy, and operational efficiency. The process involves enrollment, recognition, verification, and identification stages, each with subcategories. Pre-processing steps, like data gathering, augmentation, normalization, segmentation, and noise reduction, are crucial for effective implementation after feature creation and data storage in the database. This technology holds the potential to revolutionize security and privacy measures in various applications.

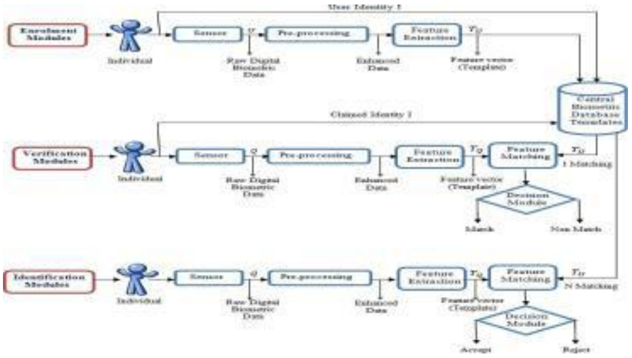


Figure 1: Matching Modules of a General Biometrics

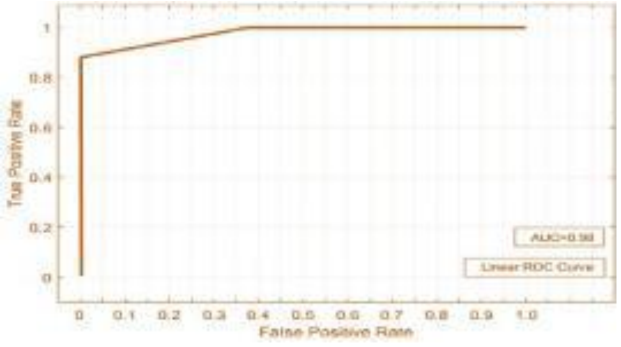
1.2 Intrusion Detective System

To safeguard the voting system, we employ machine learning to detect and prevent potential threats. This includes blacklisting IP addresses associated with attackers. Specifically, we focus on identifying DOS attacks targeting the data center housing citizen records, as well as other network-based assaults on E-voting stations. These attacks pose a significant risk to the democratic process. The Machine Learning Classifier uses network traffic analysis, trained on the USNWNB15 dataset containing both normal and attack traffic samples. Support vector machine (SVM) classifier models with various kernel settings are utilized for intrusion detection, following thorough data pre-processing and feature selection. This approach aids in recognizing even zero-day attacks for enhanced security. The accuracy and predicted speed of the classifiers are displayed in Table I. Both models undergo five-fold cross-validation in MATLAB. Accuracy and area under the curve metrics are calculated for assessment. Table I displays the results for both models.

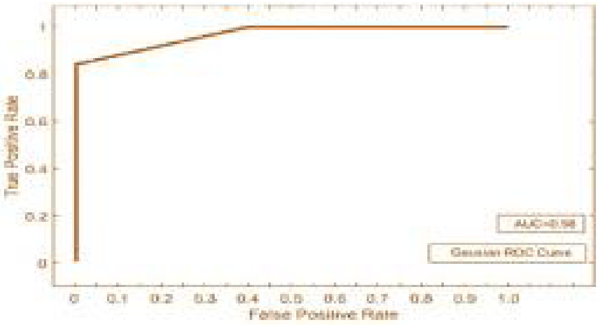
Table 1: ML Model Evaluation

Evaluation Metrics	Gaussian SVM	Linear SVM
Accuracy	0.949	0.952
Classifier Model	SVM	SVM
Area Under the Curve	0.98	0.98
Prediction Speed	1800 obs/sec	2900 obs/sec
PCA	Not applied	Not applied

Two models, same training procedure as shown in Figure 2. The ROC curve, sometimes referred to as the false positive rate and true positive rate curve, is produced for both classifiers. It provides a great statistic for evaluating the effectiveness of the classifier. The area under the curve, or AUC, demonstrates how well a classifier performs predictions. By utilizing two alternative kernels, it can be shown that there is a very tiny variation between the ROC curves, exactly like the difference in accuracy, as given in Table I.



SVM Linear



SVM Gaussian

Figure 2: ROC curves

Correct IDS placement vital for E-voting network defense. Precise site selection crucial. Discuss maximum intrusion attempts for Data Center and stations. IDS placed at data center perimeter for DDoS detection. Installed in polling station network to monitor traffic and enhance system defense. Dataset includes Dos attack instances for citizen data center identification.

II. METHODOLOGY

The system model for our proposed e-voting scheme is shown in Figure 3. The system includes E-voting stations connected to an open blockchain. A database tracks citizen records for voting eligibility. Each station has servers, voters, and voting equipment. The voting machines utilize private blockchains for voter registration and vote counting, chosen for cost-effectiveness and speed. This private blockchain maintains transaction records separately, aiding in auditing without cluttering the public blockchain. It's originally designed for digital currency, not data storage. The public blockchain shares polling results and maintains data integrity with Merkle tree root hash. The E-voting process involves registration, hash verification, and secure data appending through blockchain technology, ensuring tamper-proof records. Blockchain offers end-to-end verification, decentralized nodes, and smart contracts for secure consensus. Ethereum and Hyperledger Fabric are notable frameworks for public and permissioned networks, respectively.

2.1 Votes Management and Analyzing System

The voting application, built on Hyperledger Fabric blockchain, ensures unchangeable, private vote recording, bolstering voter confidence. Election authorities benefit from flexible node design. The system provides a decentralized ledger platform with customizable functionality. The Bie Vote system employs a 4+1 view model for its architectural framework. It includes biometric registration, RESTful API ballot box, smart authentication, blockchain-connected central server, vote counting server, and election commission oversight for result release.

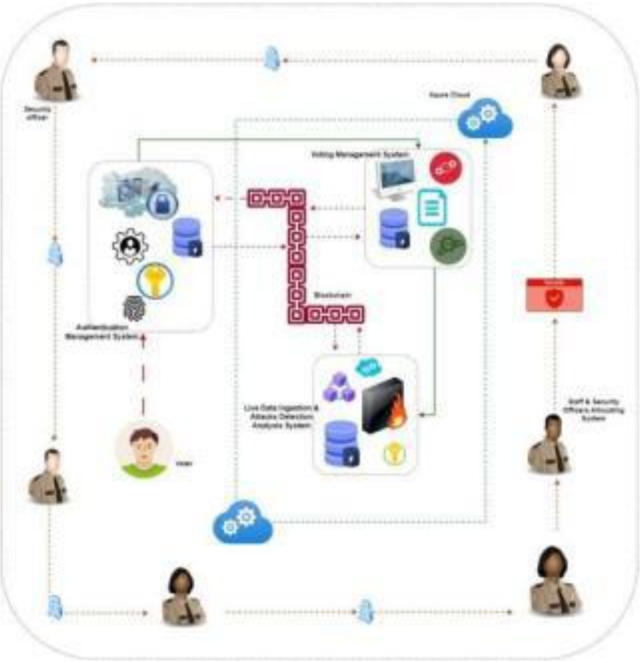
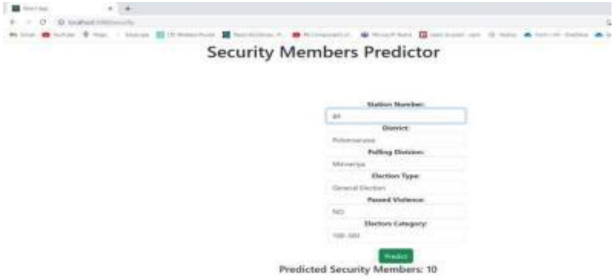

Security officer
Azure Cloud
Voting Management System
Blockchain
Authentication Management System
Live Data Ingestion & Attacks Detection Analysis System
Voter
Staff & Security Officers Allocating System

Figure 3: High Level System Architecture

2.2 Staff Members & Security Members Allocation

The report advocates a data-driven strategy for staff and security allocation in the Smart Electronic Voting System. optimal implementation and enhanced security measures. It emphasizes leveraging historical data and automation for. Strategic allocation is deemed crucial for system effectiveness.



Security Members Predictor

Station Number:
89

District:
Polonnaruwa

Polling Division:
Minneriya

Election Type:
General Election

Passed Violence:
NO

Electors Category:
100-300

Predicted Security Members: 10

Figure 4: UI of Security Member Allocation

For each personnel, essential information includes name, age for demographics, residential location, and distance calculation from the nearest polling station. Security allocation factors encompass historical records, risk assessment, and proximity to past incident sites. A data-driven approach, considering historical records and security database insights, aids in determining optimal security personnel for polling stations. Automation based on demographic analysis and proximity reduces bias, enhances efficiency, and ensures resource fairness. Formula simplifies data-driven security personnel allocation for polling stations.

$$\Sigma = (\text{WHR} \times \text{HR}) + (\text{WRA} \times \text{RA}) + (\text{WPV} \times \text{P})$$

The equation defines security personnel allocation with weighted factors for historical records, risk assessment, and proximity. The model predicts counts based on district, division, violence, and electors. Develop React front-end, connect to Flask server, test, refine based on feedback and analysis.

III. RESULTS AND DISCUSSIONS

The suggested architectural framework for the Bie Vote system offers advanced, secure, and transparent online voting. By integrating biometric technology and utilizing Hyperledger Fabric, it enhances security and data integrity. The system addresses the limitations of paper-based and traditional electronic voting. It also deploys security measures to safeguard against external risks. The architecture promotes openness, privacy, and credibility in the voting process, providing a comprehensive solution for modern elections.

IV. CONCLUSION

This paper proposes a stable E-voting system architecture, combining blockchain and machine learning for security and integrity. It employs two machine learning models, Gaussian Vector Support Machine and linear Vector Support Machine, evaluated for accuracy and AUC. Smart contracts ensure secure voter registration and voting. The architecture has potential for Internet voting expansion. Future endeavors may incorporate user address servers for enhanced blockchain transactions. Countermeasures for identified assaults will be explored.

ACKNOWLEDGEMENT

First, we would like to express our gratitude to our supervisor and co-supervisor for their invaluable advice on our study. Special thanks go out to Sri Lanka Institute of Information Technology for providing us with the chance to do a research project that allowed us to review all the theories and methods we had acquired while earning our degree. We are grateful for all the help we have gotten.

REFERENCES

[1] M. P. Wattenberg, Is voting for young people? Routledge, 2020.
[2] D. P. Redlawsk and M. W. Habegger, A Citizen's Guide to the Political Psychology of Voting. Routledge, 2020.
[3] C. Marsden, T. Meyer, and I. Brown, "Platform values and democratic elections: How can the law regulate digital disinformation?" Computer Law and Security Review, vol. 36, p. 105373, 2020. [Online]. Available:

http://www.sciencedirect.com/science/article/pii/S026736 491930384X.

[4] T. Dimitriou, “Efficient, coercion-free and universally verifiable blockchain-based voting,” Computer Networks, vol. 174, p. 107234, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619317414.

[5] Y. Xiao, H. Deng, X. Lu, and J. Wu, “Optimal ballot-length in approval balloting-based multi-winner elections,” Decision Support Systems, vol. 118, pp. 1 – 9, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167923618 301994.

[6] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, “Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing,” Journal of Parallel and Distributed Computing, vol. 130, pp. 91 – 97, 2019. [Online]. Available: http://www.sciencedirect.com/ science/article/pii/S074373151930262X.

[7] K. M. AboSamra, A. A. AbdelHafez, G. M. Assassa, and M. F. Mursi, “A practical, secure, and auditable e- voting system,” Journal of Information Security and Applications, vol. 36, pp. 69 – 89, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/

[8] M. Warkentin, S. Sharma, D. Gefen, G. M. Rose, and P. Pavlou, “Social identity and trust in internet-based voting adoption,” Government Information Quarterly, vol. 35, no. 2, pp. 195 – 209, 2018.

Citation of this Article:

Silva H. K. M. D, De Silva M.W.M.R, Withanage P.A, Hettiarachchi R.T, “Smart Election: Blockchain Based Machine Learning Solution for e-Voting Electoral System” Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET,* Volume 7, Issue 11, pp 611-614, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711081

****