Smart Election : Blockchain based Machine Learning Solution for e-voting Electoral System

De Silva M.W.M.R
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
it20024536@my.sliit.lk

Withanage P.A.
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
it20392444@my.sliit.lk

Silva H. K. M. D.
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
it19005690@my.sliit.lk

Hettiarachchi R.T
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka it1
it20242022@my.sliit.lk

Uthpala Samarakoon
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
uthpala.s@sliit.lk

Pasangi Rathnayaka
Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
pasangi.r@sliit.lk

Abstract *- **Election is a central component of a country's political life cycle. Privacy, authentication and integrity of citizens' votes and their data are essential to any e-voting program. In order to resolve these concerns, we propose a stable e-voting system based on the principles of blockchain and machine learning. But there are some problems with this digital electoral system. By using a website or mobile app while filling the ballot paper, it can be hacked. By leaking that data, the election could fail completely. Voting should be confidential. But by digitizing this, a valid user's vote should be converted into an anonymous vote. We use blockchain to ensure the integrity and security of votes, machine learning model to detect attack in voting data centers and e-voting stations. In the proposed model, we use the concepts of personal and public blockchain. The personal blockchain is used for the purposes of voter registration and voting. The public blockchain is used to maintain the integrity of the personal data of the voters by storing the root hash derived from the Merkle hash tree and revealing the results of the voting stations as soon as the voting process is completed. The proposed blockchain-based e-voting system offers transparency, treasury, confidence and prevents attacks into the information exchange network. For the security of this place and the system, the security members are separated under certain administrators Through this research we introduce the system called "V-Mobile" and through the v-mobile, invalid votes can be canceled automatically, and the ability of anyone in any region to easily go to polling station to go to their current station and will make a preference and increased efficiency.***

Keywords— *Blockchain, Merkle Tree, Voting, Anonymous, Digitizing, Polling station.*

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 have witnessed, with its ups and downs, the entry of information and communication technology into the electoral process, which has led to the replacement of electronic voting (E-voting) with the traditional voting technique (paper vote) [6, 7]. However, the inclusion of these technical components has not been simple or unanimous in the election, particularly considering the issues they raise, their ability to meet the criteria that make paper voting effective, and several new issues relating to basic concepts like the secrecy of votes and the accuracy of the procedure. However, despite some countries having used electronic voting systems for many years, many still forbid their use.

As a result, electronic voting systems are still not commonly used in large elections, and we are witnessing countries regressing in their implementation of electronic

voting for national elections. Considering all these points, we will introduce the system called "V-mobile" through this project, eliminating the existing weaknesses. This "V-mobile" can be introduced as proposed device to avoid the unfavorable conditions caused by the manual election system, to stop unnecessary human labor, to make election work easier and to collect and apply various technologies to get the correct and optimal result. We conducted this project through four main components through this "V-mobile" method.

a). Voter Registration & Authentication Management
b). Votes Management and Analyzing System
c). Live Data Ingestion & Attacks Detection System
d). Staff Members and Security Members Allocation

The voting members will always have faith in the application while looking for a totally trustworthy E-voting that doesn't delete, insert, edit, miss, or report votes [8,9]. Consider the potential outcomes of a coordinated attack on the e-voting system, which include the incorrect tabulation of ballots, the absence of a citizen's vote, the raising of doubts about the validity of the election result, the delay in promulgation, and the destruction of the secrecy of the vote, to better understand the significance of trust in e-voting. The idea behind this work is the conviction that trust is a key factor in e-voting's adoption and recognition as a cutting-edge, socially effective technical framework. Understanding voter attitudes about e-voting and how to properly develop and implement such systems will depend on understanding what gives voters confidence in using the e-voting system.

Therefore, the purpose of this analysis is not to harm the confidence of the voters to increase reliability by introducing an e-voting system and solving its problems Blockchain will be primarily used.

The information and communication technologies research community's attitude on security and privacy when utilizing blockchain has changed as a result of the rise in adoption of blockchain technology in recent years. Blockchain uses peer-to-peer networking, digital signatures, and cryptographic proofs to create a distributed, unchangeable ledger of transactions [10]–[15]. Researchers are drawn to blockchain because of these characteristics to create distributed applications.

Recently published research [16]– [22] has previously reported on the usage of blockchain for electronic voting systems. The authors of [18] developed an E-voting system using blind signature technology in conjunction with the blockchain. This approach uses a Bitcoin transaction with an extra 80 bytes of data for voting. A blockchain-based electronic voting system was suggested by authors in [19] to boost the system's security and dependability.

There are some restrictions, though, as it has been presumed that voters use extremely secure devices and networks to cast their ballots. A hacker could compromise the system and vote through a user device or a significant network vulnerability by installing a malicious application.

Because of its decentralized design, immutability, and fault tolerance, as well as its immutability and fault tolerance, blockchain has the potential to develop highly secure and transparency-based solutions to solve these difficulties [7], [8]. Additionally, it has been implemented in several industries, including healthcare, education, and transportation [9, 10]. Blockchain technology will be the best substitute for conventional electronic voting systems since it has distribution, non-repudiation, and security protection characteristics [11]. Additionally, biometrics technology may be used for authentication during the voting time, maintaining the validity of the electoral process. Blockchain technology may be used with such sophisticated technology to (i) collect, (ii) process, (iii) store, and (iv) use biometric data for electoral reasons. The electoral process will become open, reliable, and impervious to corruption from all angles if face recognition and fingerprinting are taken into consideration for identifying and verifying a person's identification in the first place. The following are the paper's main contributions:

We research the state of voting technologies today. Use biometric and blockchain technologies together in electronic voting applications.

- We suggest a basis for face and fingerprint identification. A New Architectural Framework for an Application for Electronic Voting.

- To identify and protect the system against external vulnerabilities, we suggest a novel solution built on an intrusion detective.

The rest of this article is organized as follows: Section II describes the methodology adopted in this research. Section III, descriptive the results of the research are presented in the discussion section. Finally, Section V provides a brief conclusion and an outlook for further work.

II. METHODOLOGY

The system model for our proposed e-voting scheme is shown in Fig. 1. One can see that the system has several E-voting stations connected to the open blockchain. Other than that, we have a database that keeps track of every citizen's record for the entire city to determine who is qualified to vote at a certain polling place. We have servers (which may access data from the core database if necessary), voters, and voting equipment in each E-voting station. As seen in Fig. 1, where the notion of both public and private blockchains is used in our system, electronic voting machines employ private blockchains to register voters and tally votes for a particular cause or candidate. A private blockchain is preferred because it is more affordable and somewhat quicker than a public one. Additionally, it holds the record of our desired transactions in a separate and filtered form, which can be

very helpful when auditing the voting system, and it does not contaminate the public blockchain with raw data because it was designed to be used only for a digital currency, not for data storage.

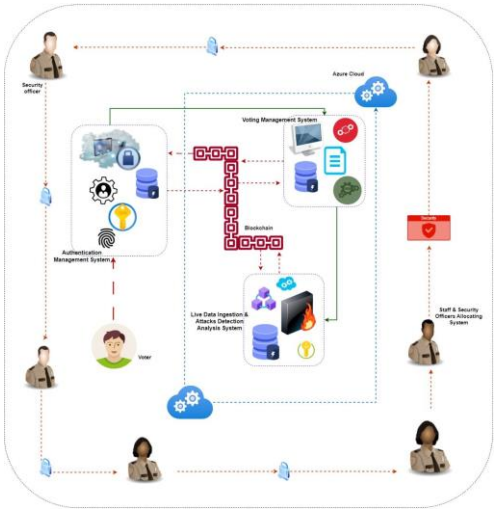


Fig. 1. High Level System Architecture

On the other side, the public blockchain is used to distribute the results of each polling location so that they are openly accessible to everyone and share the root hash provided by the Merkle tree in order to maintain the integrity of the data. In our system, there are a few steps involved in casting a ballot. First, an elector logs in and sends a request for registration through a web browser from the government's provided link to his or her corresponding E-voting station by providing some personal information, such as name, CNIC, father's name, place of birth, and date of birth, etc., a month before the election day. The primary data center is asked to provide communication to the desired user when the registration server hashes the data after receiving it. The voter must register and be eligible to cast a ballot on election day if hashes find a match. Prior to delving extensively into the suggested process, we must determine the E-voting design requirements.

A temper-evident, shared, and trusted ledger can be created using blockchain technology, which is a digitally distributed, decentralized, and ledger technology. It enables the sequential appending of cryptographically secure data transactions. Once data is added to the ledger, no transaction can be changed, and only relevant parties will be allowed access to the data through the blockchain. To prevent tampering with the recorded data and provide another degree of network security, blockchain also stores a timestamp. It offers end-to-end verification benefits and a decentralized node. Furthermore, smart contracts, also known as chain codes, can function logically in blockchain networks by mandating the implementation of consensus across ledgers when specific security requirements are satisfied [12], [13]. By creating electronic voting systems, blockchain can significantly improve the voting process [14].

It is possible to construct a blockchain using a variety of different methods, including (i) Public, (ii) Private, and (iii) Consortium Blockchain [6]. Two well-known frameworks are Ethereum and Hyperledger Fabric, with Ethereum being a public network best known for its in-built cryptocurrency while Hyperledger being a fully permissioned network that also offers a consortium network created for operations involving sensitive and confidential data [15].

A. Voter Registration & Authentication Management

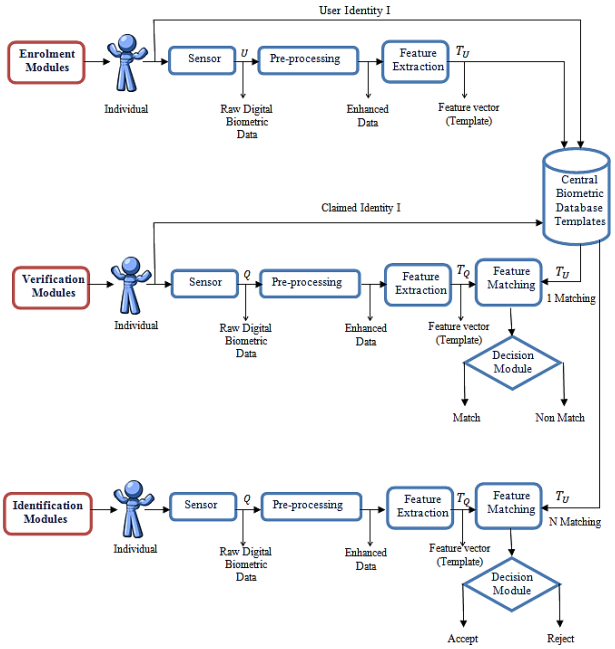


Fig. 2. Matching Modules of a General Biometrics

The use of technology that can automatically assess distinguishing bodily characteristics in order to identify a person or confirm the claimed identification based on some feature of their biological characteristics is known as biometric technology [19]. Both face recognition and fingerprint recognition are commonly used biometric identifiers, with facial recognition being somewhat more recent and allowing for the identification of persons [20]. The advancement and modernization of voting procedures and voter experience are promised by biometrics technology.

Utilizing biometrics, such as face and fingerprint recognition, to automate identification verification would improve security and privacy, increase operational effectiveness, and simplify the voting process. Every biometrics system has multiple stages in the process, such as enrollment and recognition, and each of these stages is broken down into two subcategories, verification and identification, as shown in figure 4. Following feature creation and data storage in the database, all necessary pre-processing, such as the gathering of digital biometric data and its augmentation, normalization, segmentation, and noise reduction, is carried out.

In contrast, the authentication mode for identifying a person just supplies the biometric trait to the system by entering any of the biometric templates that will be examined across the main biometric database in search of matching with potential resemblance or an unknown individual. In contrast, the authentication mode for identifying a person just supplies the biometric trait to the system by entering any of the biometric templates that will be examined across the main biometric database in search of matching with potential resemblance or an unknown individual. Facial recognition was created using a combination of artificial intelligence technologies that offers more precise, adaptable, and quick identity recognition. It is widely used in attendance access control, security, finance, smartphones, education, government management, network information security, and many other fields where it offers significant benefits in terms of security by enabling the early detection of suspicious situations and the tracking of suspects [23].

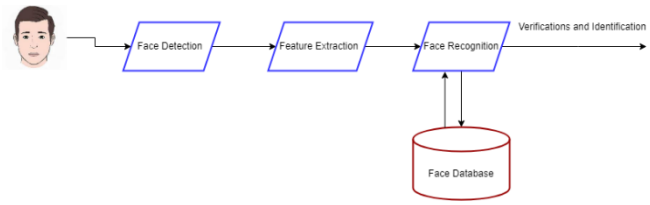


Fig. 3. Face Recognition Basic Structure

Figure 3 depicts the structure of the face recognition system, [24] and many methodologies, including local, holistic, and hybrid approaches are being used for the framework. Many nations are utilizing biometric voter registration, and the adoption of biometric identification has the most promising in general and remote voter identification in particular [25]. The adoption of facial recognition technology for voting will make the entire process safer and more reliable.

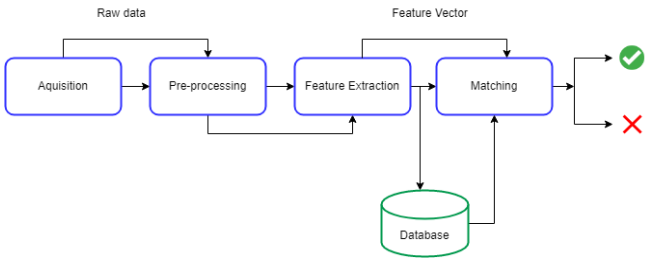


Fig. 4. Fundamental steps of fingerprint recognition

The adoption of facial recognition technology for voting will make the entire process safer and more reliable. Contrarily, fingerprints are pictorial patterns of ridges and valleys on the surface of the fingertips, and each person has a distinct fingerprint characteristic [26]. Voting uses fingerprint recognition, a well-known method of identifying voters. The use of voter identification or authentication for the voting system that uses fingerprints will be beneficial for a transparent and secure voting process.

B. Votes Management and Analyzing System

We developed a voting application using a blockchain that is based on Hyperledger Fabric due to the characteristics of blockchain networks. Votes cast using Hyperledger Fabric and its smart contracts allow for the configuration and usage of private blockchain, and every vote is guaranteed to be recorded in an unchangeable manner, ensuring voter privacy and confidence in the electoral process. Election authorities would also profit from the optimal assimilation of such a system, where the administration may design nodes in line with laws or the constitution [21]. In terms of system nodes, it offers a decentralized ledger platform with a special feature that permits pluggable implementations of various functionality.

We provide a unique architectural framework where we use the 4+1 view model to construct the Bie Vote system [33]. The framework consists of a few different parts, such as biometrics-enabled voter and candidate registration, a ballot box with a RESTful API, a smart registration and authentication component, a central server to be connected to a blockchain network, votes counting server to inherit the central server, and election commission oversight. The election commission will finally release the results.

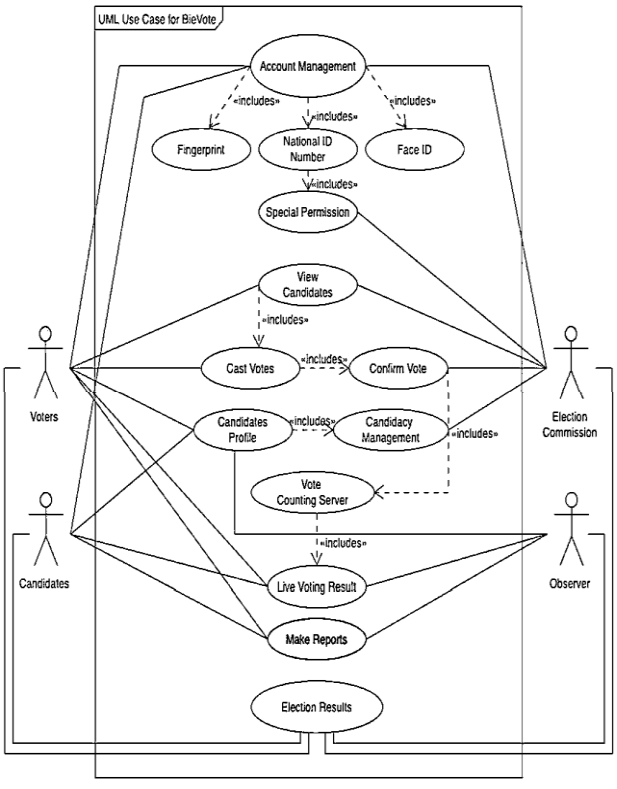


Fig. 5. Use Case Diagram for Bie Vote

A UML use case diagram for the suggested Bie Vote framework is shown in Figure 5. In the proposed application, we identified four main groups of stakeholders: (i) voters; (ii) candidates; (iii) observers; and (iv) the Election Commission. The lists of candidates and

their biographies, which will be handled by the election commission, are available to voters. After verifying that the voters have been verified by one of the biometric IDs, the voters must also cast votes, and each of the activities may then be accessed.

The process view in the 4+1 view model is concerned with the dynamic parts of the system that describe its processes and manner of communication. It focuses on the system's run-time behavior. For the suggested Bie Votes shown in Figure 6, we create a process view. Each element engaged in the entire process is connected in the process view model. The procedure starts with the registration of voters and candidates using biometrics, such as Face ID and fingerprints, which will be used during the sign-in process.

By illustrating the process diagram, we show how each component handles and processes data, as well as how data is transmitted, retrieved, and stored by a central server and smart registration & authentication, respectively. The main part of the suggested architecture that will be connected to the blockchain database is the central server. Finally, all the collected data is stored in OLTP Mongo DB.

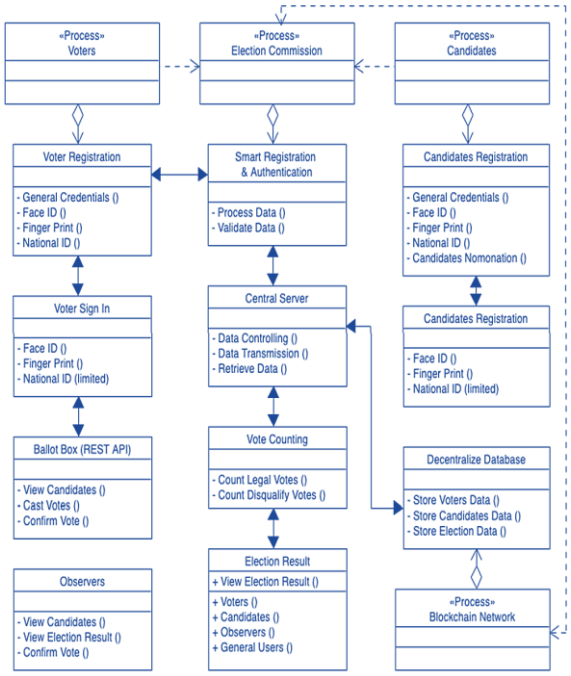


Fig. 6. Process View Model of BieVote System

The Bie Vote system is divided into four main stages, which are login or registration, cast vote, count vote, and publish the result, as illustrated in Figure 6. The proposed web application focuses on fingerprint and face recognition as the biometric registration and login methods. Although voters may use their user ID, a national ID card (NID), it will be restricted and subject to admin approval. To access the Bie Vote system, voters must first log in or register using their face ID or fingerprint.

C. Live Data Ingestion & Attacks Detection System

We use ETL tools to extract the votes from OLTP Mongo DB of Voting Management System. ETL stands for Extract, Transform, and Load, which are the three key processes involved in moving data from various sources into a data warehouse system. ETL tools are software applications that facilitate these processes by automating the extraction, transformation, and loading of data from different sources into the data warehouse. In the context of an e-voting system, ETL tools can be used to collect and process data related to the voting process. It shows in figure 7 as a high-level system architecture.

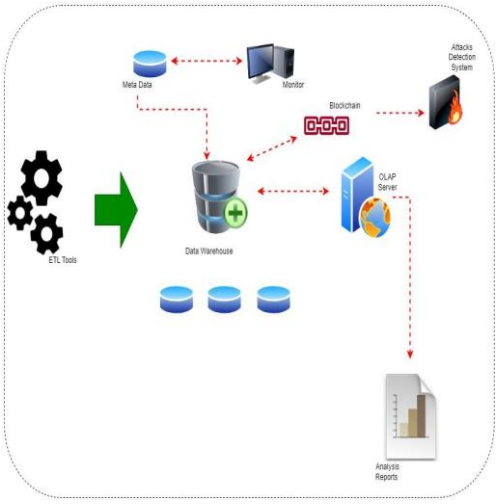


Fig 7. High Level System Architecture

For example, an ETL tool can extract data from various sources such as voter registration databases, voting machines, and online voting portals. The tool can then transform this data into a format that is suitable for analysis and loading into the data warehouse. During the transformation phase, the ETL tool may perform various data cleansing operations such as removing duplicates, correcting errors, and standardizing data formats. It may also perform data integration operations such as joining data from different sources and consolidating it into a single view. Once the data has been transformed, the ETL tool can then load it into the data warehouse where it can be used for analysis and reporting. For example, the data may be used to generate reports on voter turnout, voting patterns, and other key metrics related to the e-voting system. Overall, using ETL tools in a data warehouse system can help to streamline the process of collecting, processing, and analyzing data related to an e-voting system. This can provide valuable insights into the performance of the system and help to identify areas for improvement.

In order to defend the voting system from external threats by adding the IP attackers to the blacklist, we need to identify different assaults, in particular the DOS attack on the data center, where the citizen record is held, as well as other attacks within the network of the E-voting station.

These assaults have the potential to undermine democracy's foundation by undermining the electoral process. The detection of such assaults is demonstrated using the idea of machine learning. The Machine Learning Classifier uses network traffic analysis to anticipate assaults. To train our machine learning model, we used the USNWNB15 [29] data collection. Both examples of normal traffic and traffic assaults are abundant in the data set. Identifying zero-day attacks is made easier by regular traffic. We have trained support vector machine (SVM) classifier models with various kernel settings using this data set to identify intrusions using training data. We pre-process the data and choose the necessary features before feeding the pre-processed data to the model for training. The machine learning model used here consists of the steps shown in Fig. 8.

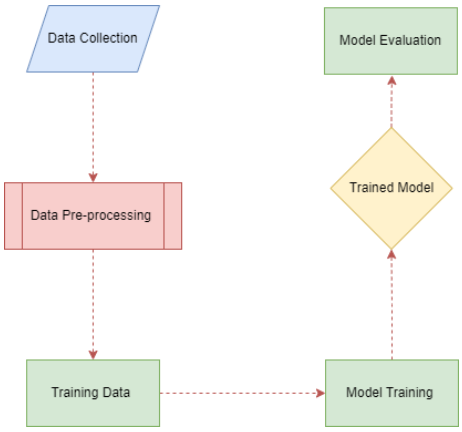


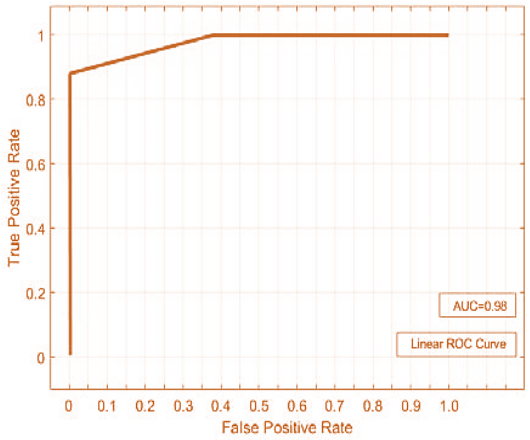
Fig. 8. Machine Learning Model

The accuracy and predicted speed of the classifiers are displayed in Table I. Both models are trained using a five-fold cross-validation in MATLAB 2020a. For both models, the accuracy and the area under the curve are computed in order to assess and contrast the models. Table I displays the results for both models, and SVM linear required more time to train but outperformed SVM Coarse Gaussian in terms of model correctness.

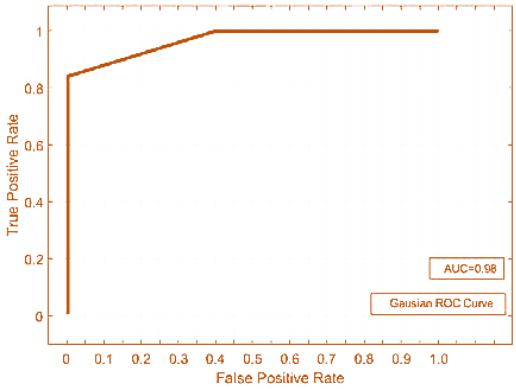
Table 1. ML Model Evaluation

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

Even though we employed two distinct models, the procedures for training the model are the same as those presented in Fig 9. 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. Fig. 10 displays the number of Transactions in relation to the total number of Voters. Both models are effective and capable of quickly and precisely detecting assaults, according to the data.



(a). SVM Linear



(b). SVM Gaussian

Fig. 9. ROC curves

To defend the E-voting network, the placement of the Intrusion Detection System (IDS) is very crucial. For the IDS to make precise predictions, the proper site must be discovered. It is important to talk about the maximum number of intrusions attempts for both the Data center (from which each E-voting station may obtain the data) and the E-voting station itself.

We installed the IDS at the perimeter of our data center to more accurately identify distributed denial of service (DDoS) assaults, and at the heart of the polling station network for the electronic voting machine so that it could monitor more traffic and defend the system more effectively.

In order to identify Dos assaults at the citizen data center, where the E-voting centers seek data for registration purposes, the data set we employed includes the attack instances of Dos.

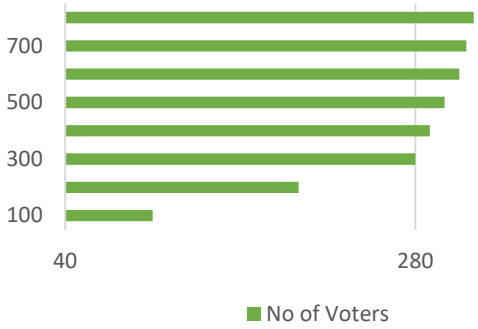


Fig. 10. No of Transactions Vs. No of Voters

Similar models may be used to find intrusions in the network of electronic voting machines. Once the breach has been discovered, we may consider the countermeasures we want to take in the future.

D. Staff Members & Security Members Allocation

This report presents a data-driven approach to allocate staff and security members for the implementation of the Smart Electronic Voting System. By analyzing historical records from the Commission and utilizing the commission security database, we aim to optimize the allocation process and enhance security measures. Additionally, this report provides a creative representation of how the allocation process can be automated by leveraging data and information obtained from previous research reports. To ensure a smooth and secure implementation of the Smart Electronic Voting System, it is crucial to allocate staff and security members strategically.

The following information is required for each personnel, Provide the name of the individual assigned to the position, Mention the age of the staff or security member for demographic analysis, Specify the residential location of everyone, Calculate the distance separately for male and female officers, indicating the proximity of their residences to the nearest polling station, To calculate the allocation of security personnel for polling stations, we can consider several factors, including historical records, risk assessment, and proximity to areas with previous incidents of violence.

While there is no specific equation, a data-driven approach can be adopted to determine the appropriate number of security personnel for each polling station and to enhance security measures, it is essential to consider historical records of the Commission and leverage the information stored in the commission security database. These records can provide valuable insights into areas where violence occurred during previous elections and areas with a higher risk potential. By analyzing this data, appropriate measures can be taken to allocate security personnel effectively. Utilizing the data collected from previous research reports, the staff and security member allocation process can be automated. By inputting the relevant data into a software system, the allocation algorithm can calculate the optimal distribution of personnel based on historical records, demographic analysis, and proximity to polling stations. This automated approach reduces human bias, maximizes efficiency, and ensures a fair distribution of resources. Figure 13 shows how to connect the election commission to our proposed system. We can create a simplified formula to demonstrate the data-driven approach for calculating the allocation of security personnel for polling stations.

$$\sum = (WHR \times HR) + (WRA \times RA) + (WPV \times P)$$

In this equation:

Allocation represents the number or level of security personnel allocated to a specific polling station. WHR (Weight_Historical Record), WRA (Weight_Risk Assessment), and WPV are weight factors assigned to each component, representing their relative importance in the allocation process. Historical Records represents the historical records component, which can be a score or a categorical value indicating the presence of previous incidents of violence. Risk Assessment represents the risk assessment component, which can be a score or a level indicating the assessed risk level for a particular polling station. Proximity (P) represents the proximity component, which can be a numerical value representing the distance between the security personnel's residence and the polling station.

The weight factors (Weight_HR, Weight_RA, and Weight_PV) can be determined based on the specific requirements and priorities of the election authority. They reflect the relative importance given to each component in the overall allocation process. The weights can be adjusted based on the context and the available data.

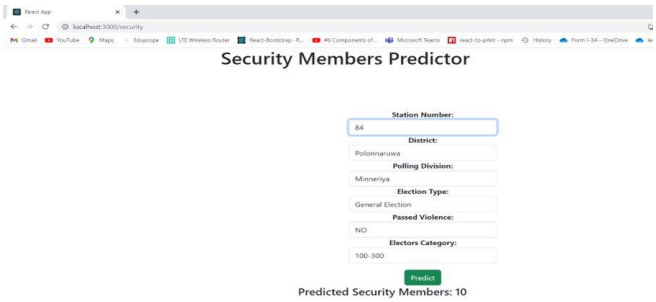


Fig. 11. UI of security members allocation

We can predict the total count of security members and staff members, using a model according to district, polling division, violence, electors for each polling station etc. First, we collect the relevant data for staff member prediction: current position, experience, age, gender, current salary, etc.

Ensure data quality and integrity. Collect data for security member prediction: district, polling division, historical violence records, number of electors for each polling station, etc. Ensure accurate and comprehensive

data collection. And preprocess the collected data to handle missing values, outliers, and ensure consistency. Normalize numerical features to bring them to a similar scale. Figure 11 shows the UI of security members allocation and from figure 12 shows the UI of staff members allocation. Encode categorical features using techniques like one-hot encoding or label encoding. After that we developed the model. For staff member prediction, develop a machine learning model using Python. Utilize features such as current position, experience, age, gender, and current salary to train the model.

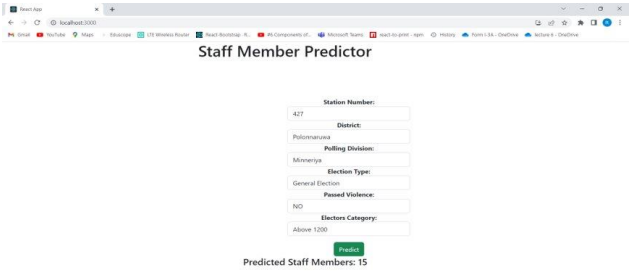


Fig. 12. UI of Staff Members Allocation

For security member prediction, develop another machine learning model using Python. Utilize features such as district, polling division, historical violence records, and number of electors for each polling station to train the model. And split the data into training and testing datasets.

Train the staff member prediction model using the training dataset. Evaluate the model's performance using appropriate evaluation metrics (e.g., accuracy, precision, recall). Train the security member prediction model using the training dataset. Evaluate its performance as well. Build a Flask server using Python to host the trained models and handle API requests.

Develop a React front-end interface to allow users to input the required information, such as current position, experience, age, gender, district, polling division, etc. Connect the front-end interface with the Flask server to send requests and receive predictions. Upon receiving input from the user through the React interface, send the input data as a request to the Flask server. Utilize the trained staff member prediction model to predict the position of the staff member based on the provided features. Utilize the trained security member prediction model to predict the total count of security members required based on the provided features. Return the predictions to the user through the React interface. Test the system extensively, ensuring it handles various scenarios and inputs accurately.

Continuously evaluate and refine the models and system based on feedback and performance analysis. Fine-tune the models, if necessary, by retraining them with updated data or adjusting hyperparameters. The above methodology provides a general framework for developing the described system.

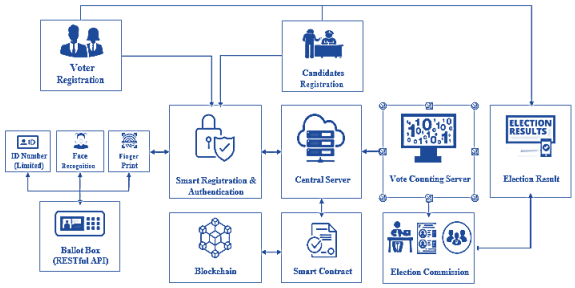


Fig. 13. Connection of the election commission

The actual implementation details may vary depending on the specific requirements, available data, and technical considerations.

III. RESULT AND DISCUSSION

There is a chance that the suggested architectural framework will be used in practical situations. We consider a number of factors while designing a system, including scalability, which implies that the system architecture must enable programmers to efficiently build the application. The architecture will offer cutting-edge voting solutions so that procedures may be carried out with precision, transparency, and dependability. Additionally, the Bie Vote architecture allows voters, candidates, and observers to keep an eye on the whole voting process.

By integrating biometric technologies, Bie Vote will boost security and transparency while making online voting more time and money efficient. After development procedures are finished, the suggested system will count and the blockchain network's vote records will all be made public. The framework considers and solves the drawbacks of both paper-based voting and the traditional electronic voting system, where the current Internet voting method is potentially highly risky and regularly fails.

As it relates to the credibility of all parties involved, the suggested approach seeks to find a balance between openness, privacy, and security in voting. A Hyperledger-fabric made of the hash function, which encrypts all secret information and greatly enhances the security of the system so that only authorized parties may access the information, is recommended to improve data integrity.

In order to protect the information system from external risks, blockchain deployment is done by identifying the risks and intrusions coming from outside and acting against them and preventing them from damaging the system. We have built a system for deploying security personnel to provide security to the polling station, automatic whitewashing under the conditions of introduction of newcomers.

IV. CONCLUSION

In this paper, the principles of blockchain and machine learning to provide protection and integrity to the voting. system is proposed to create a stable and efficient E-voting system architecture. As a network of electronic

voting stations, the proposed system deals with the security of voter data and the integrity of votes. Two machine learning models, each with a unique set of parameters, were mostly employed. The Gaussian Vector Support Machine and the linear Vector Support Machine are the two types. These two classifiers are compared by assessing their accuracy and AUC (area under the curve). Voter registration and vote receipt both employ the concept of a smart contract. while using the Merkle root algorithm utilized to obtain the root hash in order to guarantee the accuracy of the data kept at the citizen's data center.

We think that this voting architecture may be expanded to include I (internet voting), where users can cast their votes via secure web servers or applications. We didn't concentrate on the servers that provide user addresses for the blockchain that we use to register and process transactions, which might be part of our future initiatives to create an effective smart voting system combining blockchain and machine learning. Additionally, once we have identified an assault, we will be able to look at its countermeasures in the future.

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/S026736491930384X

[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/S0167923618301994

[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, agile Government and Adaptive Governance in the Public Sector. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0740624X17301478

[9] S. S. More and P. P. Gaikwad, "Trust-based voting method for efficient malware detection," Procedia Computer Science, vol. 79, pp. 657 – 667, 2016, proceedings of International Conference on Communication, Computing and Virtualization (ICCCV) 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916002155

[10] A. B. Masood, M. Lestas, H. K. Qureshi, N. Christofides, N. Ashraf, and F. Mehmood, "Closing the loop in cyber-physical systems using blockchain: Microgrid frequency control example," in 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM). IEEE, 2019, pp. 1–6.

[11] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K. R. Choo, "Neural-blockchain-based ultrareliable caching for edge-enabled uav networks," IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5723–5736, 2019.

[12] J. Gao, T. Wu, and X. Li, "Secure, fair and instant data trading scheme based on bitcoin," Journal of Information Security and Applications, vol. 53, p. 102511, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212619309688

[13] P. Lafourcade and M. Lombard-Platet, "About blockchain interoperability," Information Processing Letters, vol. 161, p. 105976, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020019020300636

[14] S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain oracles," Computers and Electrical Engineering, vol. 83, p. 106582, 2020. [Online].

Available: http://www.sciencedirect.com/science/article/pii/S0045790619316179
[15] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy in blockchain technology: A futuristic approach," Journal of Parallel and Distributed Computing, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731520303105

[16] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," Future Gen eration Computer Systems, vol. 105, pp. 13–26, 2020.

[17] "Simulation of transaction malleability attack for blockchain based e-voting," Computers and Electrical Engineering, vol. 83, 2020.

[18] J. P. Cruz and Y. Kaji, "E-voting system based on the bitcoin protocol and blind signatures," IPSJ Transactions on Mathematical Modeling and Its Applications, vol. 10, no. 1, pp. 14–22, 2017.

[19] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol. 9, no. 3, pp. 01–09, 2017.

[20] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for board room voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.

[21] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE, 2018, pp. 22– 27.

[22] Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, and M. Guizani, "A blockchain based self-tallying voting scheme in decentralized iot," arXiv preprint arXiv:1902.03710, 2019.

[23] A. S. A. Aziz, A. T. Azar, A. E. Hassanien, and S. E.-O. Hanafy, "Negative selection approach application in network intrusion detection systems," arXiv preprint arXiv:1403.2716, 2014.

[24] A. Osareh and B. Shadgar, "Intrusion detection in computer networks based on machine learning algorithms," International Journal of Com puter Science and Network Security, vol. 8, no. 11, pp. 15–23, 2008.

[25] S. Osken, E. N. Yildirim, G. Karatas, and L. Cuhaci, "Intrusion detection systems with deep learning: A systematic mapping study," in Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT). IEEE, 2019, pp. 1–4.

[26] H. F. Eid, A. T. Azar, and A. E. Hassanien, "Improved real-time discretize network intrusion detection system," in Proceedings of Sev enth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA 2012) Advances in Intelligent Systems and Computing Volume 201. Springer, 2013, pp. 99–109.

[27] A. S. A. Aziz, A. T. Azar, A. E. Hassanien, and S. E.-O. Hanafi, "Continuous features discretizaion for anomaly intrusion detectors gen eration," in The 17th Online World Conference on Soft Computing in Industrial Applications (WSC17), 2012.

[28] W.-M. Lee, "Testing smart contracts using ganache," in Beginning Ethereum Smart Contracts Programming. Springer, 2019, pp. 147– 167.

[29] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in Military communications and information systems conference (MilCIS). IEEE, 2015, pp. 1–6. 18

[30] M. Pawlak, A. Poniszewska-Maránda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Procedia Comput. Sci., 2018, doi: 10.1016/j.procs.2018.10.177.

[31] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-Based E-Voting System," IEEE Int. Conf. Cloud Comput. CLOUD, 2018, doi: 10.1109/CLOUD.2018.00151.

[32] Y. G. Gupta, A. Kushwaha, A. S. Rajeevan, and B. Dhakulkar, "EVoting using Block Chain Technology," Int. J. Comput. Sci. Eng., vol. 7, no. 5, pp. 925–931, 2019, doi: 10.26438/ijcse/v7i5.925931.

[33] P. P. B. P. Kruchten and B. Kruchten, "Architectural Blueprints — The ' 4 + 1 ' View Model of Software Architecture," IEEE Softw., vol. 12, no. November, pp. 42–50, 1995.

[34] P. Wolf, R. Nackerdien, and D. Tuccinardi, "Introducing Electronic Voting: Essential Considerations," Int. Inst. Democr. Elect. Assist., no. December, p. 39, 2011.

[35] H. Timeline, D. Recording, E. Voting, T. Australian, A. S. Ballot, and H. Hollerith, "Historical Timeline Electronic Voting Machines and Related Voting Technology," Chief Eng., pp. 1–7, 2011.

[36] B. Simons and D. W. Jones, "Internet voting in the U.S.," Commun. ACM, vol. 55, no. 10, pp. 68–77, 2012, doi: 10.1145/2347736.2347754.

[37] P. A. Colinvaux, "The past and future of Internet Voting," Sci. Am., no. 260, pp. 101–108, 1989.

[38] M. Górny, "I-voting – opportunities and threats. Conditions for the effective implementation of Internet voting on the example of Switzerland and Estonia,"

Przegląd Politol., no. 1, pp. 133–146, 2021, doi: 10.14746/pp.2021.26.1.9.
[39] T. Differences, “Difference Between Client-Server and Peer-to-Peer Network,” Website, 2017, [Online]. Available: https://techdifferences.com/difference-between-client-server-andpeer-to-peer-network.html.

[40] R. Shivers, M. A. Rahman, M. J. H. Faruk, H. Shahriar, A. Cuzzocrea, and V. Clincy, “Ride-Hailing for Autonomous Vehicles: Hyperledger Fabric-Based Secure and Decentralize Blockchain Platform,” Proc. - 2021 IEEE Int. Conf. Big Data, Big Data 2021, pp. 5450–5459, 2021, doi: 10.1109/BigData52589.2021.9671379.

[41] M. J. Hossain Faruk, H. Shahriar, M. Valero, S. Sneha, S. Ahamed, and M. Rahman, “Towards Blockchain-Based Secure Data Management for Remote Patient Monitoring,” IEEE nternational Cnference Degital Heal., pp. 299–308, 2021, doi: 10.1109/ICDH52753.2021.00054.

[42] M. J. Hossain Faruk, S. Hossain, and M. Valero, “EHR Data Management: Hyperledger Fabric-based Health Data Storing and Sharing,” Fall 2021 Symp. Student Sch., 2021, doi: 10.13140/RG.2.2.20299.05928.

[43] M. J. Hossain Faruk, S. Hossain, and M. Valero, “Students Certification Management (SCM): Hyperledger Fabric-Based Digital Repository,” CCSE Comput. Showc. Day, 2021, doi: 10.13140/RG.2.2.13642.08642.

[11] R. Bulut, A. Kantarci, S. Keskin, and S. Bahtiyar, “Blockchain-Based Electronic Voting System for Elections in Turkey,” UBMK 2019 - Proceedings, 4th Int. Conf. Comput. Sci. Eng., pp. 183–188, 2019, doi: 10.1109/UBMK.2019.8907102.

[12] D. R. Joseph, “Hyperledger Architecture, Volume II - Smart Contracts,” Gene, vol. 17, no. 3, pp. 341–344, 1982, [Online]. Available: creativecommons.org/licenses/by/4.0.

[13] K. Yamashita, Y. Nomura, E. Zhou, B. Pi, and S. Jun, “Potential Risks of Hyperledger Fabric Smart Contracts,” IWBOSE 2019 - 2019 IEEE 2nd Int. Work. Blockchain Oriented Softw. Eng., pp. 1–10, 2019, doi: 10.1109/IWBOSE.2019.8666486.

[14] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, “E-Voting System Based on Blockchain Technology: A Survey,” 2021 Int. Conf. Inf. Technol. ICIT 2021 - Proc., pp. 200–205, 2021, doi: