ESP IJAST
ESP International Journal of Advancements in Science & Technology
ISSN: 2583-9233 / Volume 1 Issue 1 May 2023 / Page No: 22–24
Paper Id: IJAST-V1I1P104 / Doi: 10.56472/25839233/IJAST-V1I1P104

Original Article

Analysis of Current Online Election Systems

Raghu M[1], Tej Sri. R[2], Dharananth.V[3], Ramya.R[4]

[1,2,3,4]*UG Students, Department of Computer Science, Alfa College of Engineering & Technology, Kurnool, Andhra Pradesh*

Received Date: 23 April 2022 Revised Date: 10 May 2022 Accepted Date: 15 May 2022

Abstract: *Traditional voting devices need the chores to be completed at a certain location and use a lot of time and energy. The fundamental concept behind these systems is to provide an online voting system that will assist in decreasing the use of the manual voting method while enhancing security by allowing voting from a distance. The suggested system comprises various levels of verification, such as face verification, OTP verification, biometrics verification, etc. with validation data, to verify the device's dependability. Each voter can only access the system after being identified and verified in order to continue with the next step.*

Keywords: *Image Processing, Python, Voting System, Face Recognition, MySQL, OTP, RFID, GSM.*

I. INTRODUCTION

Elections are the pillars of a democracy and its spirit lies in people choosing their own government. The current E-voting machine system has a lot of inaccuracies like the possibility of duplicate votes; presence of the voter at the allocated booth for the casting of votes which affects migrated and physically challenged people. With our country running towards digitization it is necessary to make a transition from the traditional ballots.

The current pandemic issue demonstrates the system's peril. Due to the requirement that the voter be there in person to cast their ballot, this could result in a failure of social distance throughout the voting process. The voting process strives to make it possible to participate in India's democratic system. It is flexible enough to permit voting from any far-off location. By implementing the necessary security procedures, the election is conducted in complete secrecy, allowing the voter to cast their ballot for any candidate who is running. The focus of internet voting is on issues of security, privacy, and secrecy as well as difficulties for stakeholder participation and process observation. a novel strategy for the voting process that stores the voter's identification using facial recognition.

The system captures the image and finds a match with the existing faces in the stored database. After confirmation of the Val id image, the OTP is generated and send to the voters. Voter is validated for the further process of voting. This ensures safe and secure voting and reduces the burden of the conducting authority.

II. LITERATURE SURVEY

The suggested system [1] includes a pre-recorded database of voters' biometric and personal information. The RFID card acts as the individual's security access. The RFID card is verified using an RFID reader module as part of the verification procedure. The reader detects the card and shows the information on it. After that, fingerprint verification and face recognition are performed. If the fingerprint and database match, the sensor module permits the user to proceed to the next stage of verification. For face identification, object detection with Haar feature-based cascade classifiers was employed. This is a practical technique to reduce the need for personnel and other illegal operations. Additionally, it removes human error from the verification process and provides a quick view of the polling results. The study [2] discusses the Iris and NA- based biometric voting method. In [2], biometric verification improves voting security and safety. The voter database is kept on the server, which also houses all of the storage. IOT is used to update the details, and fingerprint verification follows. After the biometric system has been successfully verified, the database will be checked. Following the voting, the server will be upgraded, and the GSM module will be enabled. It can reduce the number of manual errors that occur when counting. However, there is a disadvantage to compiling a voter database.

The Biometrics Secured Voting System with Fingerprint, Face, and Iris Verification is discussed in great length in Paper [3]. The voting process is more secure when [3] is used. It sends prints to the FM220 Starttek Scanner, a fingerprint scanner, which scans them by employing a minute matching process. The next step is to identify Iris from a face-photo using the Viola-Jones method. Adaptive thresholding and PCA (Principal Component Analysis) are used for iris matching and feature extraction. The programme used to compare and verify the input data with the training data is called Mat Lab. There

is no longer a need to keep track of any user names or passwords.

The fingerprint voting system built on Arduino is the main topic of the study [4]. The ATmega328 is utilised in Arduino. It is necessary to build a voter database. The databases are managed by a central database. This is an offline implementation of the Arduino electronic voting system using fingerprints. The fingerprint is tested first. The button is situated on the voting machine for security purposes. The device is only accessible by the administrator, who may also view the output. This technology keeps the voting process honest, makes it simple to use, and restricts access to unregistered voters.

[5] demonstrates the application of blockchain in voting systems. Small elections, such those held in boardrooms or corporate structures, can be held using [5]. This implementation makes use of the Ethereum smart contract. The purpose of [5] is to develop trustworthy third-party safe distributed voting apps using blockchain technology, homomorphic encryption, and secret sharing techniques. It offers an open and transparent voting procedure that safeguards voter confidentiality, data transfer privacy, and voting verification during the invoicing phase.Based on the Ethereum blockchain is [5]. The client-side UIis created to use Ethereum account for voting. The Truffle Framework is used to test smart contracts in this implementation and deploy them to the blockchain. Truffle Framework makes it easy to develop, test, and deploy the application.

[5] Contains the controller-serving third-party authentication server. The Cloud Sim device is used to simulate a cloud environment. It is an open source device made up primarily of Java libraries developed for various tasks that simulate a real cloud environment established in virtual mode. The encryption of the price price tag on the controller, the decryption of the price price tag on the cloud, the encryption of the ACK on the cloud, and the decryption of the ACK on the Controller are major duties in [6]. Blowfish, AES, and RSA are three examples of cryptographic algorithms that are used to provide secure communication between the components. The most crucial overall performance metrics are speed and security.

III. COMPARISON OF THE EXISTINGSYSTEM

Title of the Paper	Author	Features	Advantages	Disadvantages
Smart Voting System Using Rfid	B. SurendraRaoo(1), E. Prasanthh(2), R.SivaSai Tejah(3), Y. Sandip(4)	RFID reader used to confirm RFID card usage Face recognition and finger print verification using the HAAR cascade classifier	Minimal involvement of people. Simplified Progress	Expensive costs No provisions forremotevoting Requireme nt of required equipments
Biometric Voting Machine Based on Fingerprint Scanner and Arduino	Atharva Jamkar(1); Omkar Kulkarni(2); Aarti Salunke(3); Anton Pljonkin(4)	fingerprint verification Updation using IOT Use of Arduino module	Avoid manual mistakes when counting. improved security	establishment of a database for all voters isnecessary Cost of implementatio n Restricted access to voteremotely
Biometrics secured voting system withfingerprint ,face and Iris verification	Kavithaa. S. N, Shaahila. K,Dr. Prasana Kumar .S. C[3]	Use of FM220 Fingerprint scanner Use of minutiae matching fingerprint algorithm Use of Viola- Jones Iris detection algorithm	No need of remembering ID's and passwords Advanced security Minimum human involvement	Implementatio ncost Limited remotevoting access Equipment requirements

Finger print voting sytem using ARDUINO	A. Pirathipan, S. Sasikaran, P. Thanush kanth, S. Tharsikha, M. Nathiya, C. Siva karan, N. Thiruch chelvan, K. Thiruthanigesann [4]	Use of ATMEGA328. Offline version of voting. Use of fingerprint verification	Prevent success to illegal voters. Ease of use Transparent	No remote voting accessNeed for equipmen ts Security risks
Decentralized E- voting portal using Block chain	Patidar, Kriti, andSwapnil Jain[5]	Ethereum implementation Combines blockchain and homomorphic encryption. Truffle framework	Data privacy Transparent	Security risks Prior knowledge of the application required
Using a cloud-based, secure implementationof an online voting system	Ramya Govindaraj; P Kumaresan; K. Sree harshitha	Use of Cloud Sim tool Blowfish cryptographic algorithm	Use of secured cryptographic algorithm Less payload on thecloud. Faster than AES secured system	Software and internet issues Security risks

IV. CONCLUSION

With the rapid advancement of digitization, it is necessary to adapt to a newer, simpler, and more advantageous voting method. The various existing systems are investigated and contrasted while taking security and other technology into consideration. The ability to vote remotely and the associated security considerations are seen as performance criteria.

V. REFERENCES

[1] Surendra Rao, B., et al. "RFID Based Smart Voting System." International Research Journal of Engineering and Technology (IRJET) 6.4 (2019): 1577-1580.

[2] Jamkar, Atharva, et al. "Biometric voting machine based on fingerprint scanner and arduino." 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT). IEEE, 2019.

[3] Kavitha. S. N, Shahila. K, Dr. Prasanna Kumar .S. C, “Biometrics Secured Voting System with Finger Print, Face and IrisVerification”.

[4] A. Piratheepan, S. Sasikaran, P. Thanushkanth,S. Tharsika, M. Nathiya, C. Sivakaran, N. Thiruchchelvan, K. Thiruthanigesan, “Fingerprint Voting System Using Arduino” Middle-East Journal of Scientific Research 25 (8): 1793-1802, 2017.

[5] Patidar, Kriti, and Swapnil Jain. "Decentralized e-voting portal using blockchain." 2019 10th InternationalConference on Computing,Communication and Networking Technologies (ICCCNT). IEEE, 2019.

[6] KS, Gururaj &Thippeswamy K. (2019). Cloud based secured framework for implementation of online voting system. Indonesian Journal of Electrical Engineering and Computer Science. 15.328-335.