International Journal of Engineering & Technology, 7 (4.10) (2018) 295-297

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Hashing based Hybrid Online Voting Using Amazon Web Services

Murali S[1]*, Manimaran A[2], Selvakumar K[3], Dinesh Kumar S[4]

[1]*School of Computer Science and Engineering, VIT, Vellore, Tamilnadu*
[2,4] *School of Advanced Sciences, VIT, Vellore, Tamilnadu*
[3] *School of Computer Science and Engineering, VIT, Vellore, Tamilnadu*
**Corresponding author E-mail: murali.s@vit.ac.in*

Abstract

The secured web-based voting framework is the need of the present time. We propose another secure authentication for the online voting framework by utilizing face recognition and hashing algorithm. A simple verification process is accomplished during the initial registration process via email and phone. The voter is asked to give a unique identification number (UIN) provided by the election authority and face image at the time of main registration. This UIN is converted into a secret key using the SHA algorithm. The face image that is saved in the Amazon web service (AWS) acts as an authentication mechanism which enables people to cast their vote secretly. The voters, who cast numerous votes amid the way toward voting is guaranteed to be counteracted by encrypted UIN. The election organizers can see the election parallelly as the voting is saved in the real-time database. The privacy of the voter is maintained as the details are converted into the key. In this system, an individual can vote from outside of his/her allocated constituency.

Keywords: *Authentication, Hashing, Face recognition, One-time password, online voting framework.*

1. Introduction

These days, election process assumes an imperative part in the democratic country. The election is a process for selection of a candidate who will lead the country. In a majority rule government, individuals pick their pioneer by giving their vote. As of late in India, the electronic voting framework is utilized. In this framework, voter accessibility at in the city is necessary. This is a noteworthy downside of an electronic voting framework. A web-based voting framework is an answer for voter can vote from anyplace. The critical issue in an online voting framework is security. In this, we have suggested a solution for authenticity and confidentiality of voter's data and non-traceability of a casted vote. The encrypted UIN and pin are used during the authentication followed by face recognition. For the casted vote the voter is kept secret using a hash algorithm.

2. Literature Review

A voting system based on aadhar number proposed by Himanshu Agarwal [1]. In this model, aadhar number and auto-generated password are used for authentication. The password is kept away as it is in the database. So, secrecy of password isn't kept up. Then, a voter is permitted to vote. Voter's secret password and unique fingerprint impression are affirmed before the vote is acknowledged in the primary database of the election commission of India. In this way, it splits validation into two parts. The second part which contains biometric confirmation is connected straightforwardly to the casted vote. So, the secrecy of the casted vote is also not maintained. The author proposed an android platform for the online voting system [2]. A voter does not have to go surveying pooling booth. He / She can vote form mobile. Here, just the login credentials and a secret password is required for validation. Anybody having login and password can vote instead of the authorized voter. So, this form of authentication is not secure. For proper authentication, we need non-transferable measures like biometric. An online voting system based on unique id and face recognition proposed in [3]. The voter does not have to use traditional approach of visiting polling station physically. A voter can vote from the web portal. Here, just login credentials and an image of the face is required for authentication. The image and unique id are just stored in a database without privacy. Anyone having the unique id and face picture would be able to vote. This system cannot be used for authentication. We need credentials which cannot be manipulated like fingerprint scanning or face recognition with encryption.

The author presented a web-based online voting system using multiple encryptions [4]. This paper operates on encryption and digital signature. Initially, the votes are encrypted and then voter verifies the votes using a digital signature. The noteworthy issue with the system is that the vote is directly connected with the voter's signature. For the validation, only login and password is used which is transferable measures. Use of biometric credentials is required as it is non-transferable. A design for an online voting framework based on dependable web services proposed in [5]. At that point, he displayed this framework with RBD and Reward Petri Nets. At long last, he assessed these models quantitatively. Likewise, by taking a gander at the consequences of an assessment, he can choose to utilize or not to utilize this framework. We can see that his engineering expanded reliability in particular. Likewise, he considered primary necessities of voting like privacy, portability, integrity, uniqueness and so on. Focusing on security needs of voting, he utilized some ways to deal with making a pro-

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

tected framework. He demonstrated that this framework won't flop regardless of whether a few segments fall flat and both accessibility and security as the most critical particular of voting frameworks will be tended to. As voting by means of the web is simple and has no time and cash costs for voters. In this way, frameworks would anchorage be able to individuals to partake in the race.
Observation from the Existing method are given below,

- Two databases are connected so if one database is breached then the data from both the storage will be lost or manipulated.
- No non-transferable method is mentioned. It has only password and encryption mechanism to secure this system.
- Existing system does not have any solid mechanism to secure the vote or maintain the voter's privacy. In this author writes about face comparison but he does not mention any secure channel for this authentication.
- Existing system does not have the non-transferable procedure to secure the voting system. In this literature author mentioned about digital signature but this signature can be accessed through a password.
- Many algorithms are used but transferability is still present, with no biometric or face recognition.

3. Proposed Framework

In this proposed system, there are three modules.

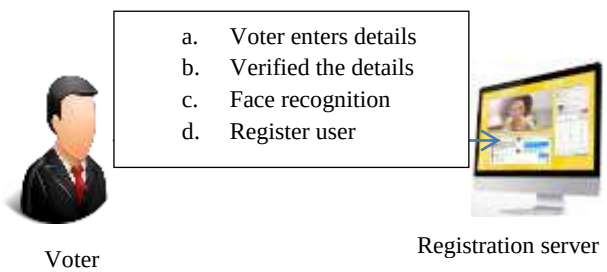
- Voter registration
- Authentication, vote casting and recording
- Counted Vote and final result

3.1. Voter Registration

In the registration process, the voter has to provide personal details and facial recognition. After the registration, a voter is allowed to vote at the time of an election. The steps involved in registration process are:

- The voter has to give their initial credentials like email id password and phone number.
- After the verification of above-mentioned credentials, the voter is asked to fill rest of the field like unique identification number, address, gender etc.
- The Face image is taken for further authentication.
- The voter gets a message for successful registration.
- The election organizer will enter the candidate information after getting authenticated

The proposed project work is a combination of hashing and facial recognition. Hashing includes secure hash algorithm (SHA) so, anything that is present in the database will be converted into a key. No details regarding voting will be kept public. The initial registration of a voter is verified via email id and mobile number. A verification link with the code will be sent to the voter's email Id with an OTP on phone number. The voter has to fill the received credentials after opening the link for further registration. The further registration will consist of personal details and facial information. The unique identification number when entered it gets converted into a share key of 512 bits and stored in the respective database.



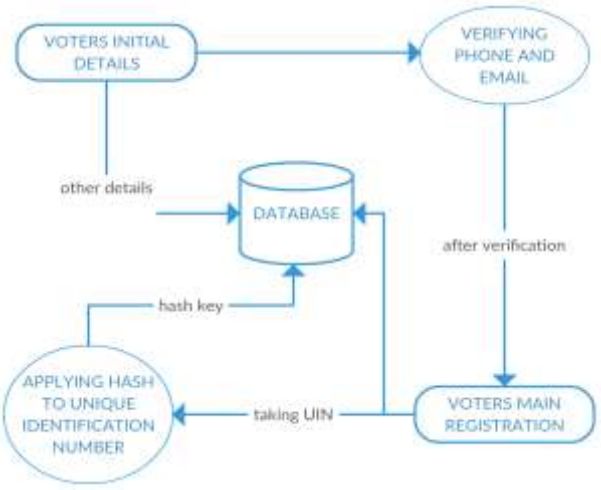


Fig. 1: Registration Process

After the registration of this part, now in the second part, the server has to take the face of the voter. The face image will be taken and it will be stored in AWS S3 bucket. Amazon Web Services Simple Storage Service bucket behaves as a repository for objects stored in Amazon. For example, if the object name is photo/flower.jpg and is stored in the tulipflower bucket, then it will be addressed using URL http://tulipflower.s3.amazonaws.com/photos/flowery.jpg.
The bucket can be used for several purposes like they arrange the Amazon S3 namespace at the most elevated amount; they distinguish the record in charge of capacity and information exchange charges, they play an integral role in access control, what's more, they fill in as the unit of collection for usage description. The bucket can be configured so that they can be created for a particular region. The user can likewise design the bucket with the goal that each time any new object is included; Amazon S3 produces a one of a kind ID and relegates it to the object.
Thus whenever voter clicks his/her image for the registration purpose, the image is then sent to the S3 bucket for the storage. The bucket assigns unique Id to the particular image. Now the election organizer has to enter the information of the candidate into the specified database. The organizer has to enter their credentials to get verified. After the verification, the organizer will be allowed to enter the candidate information.

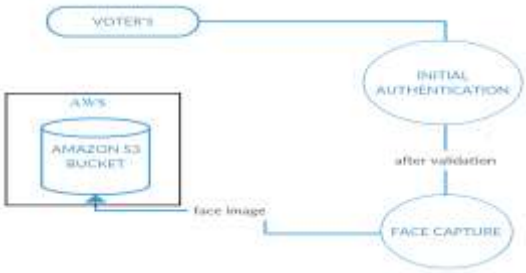


Fig. 2: Process of storing captures face

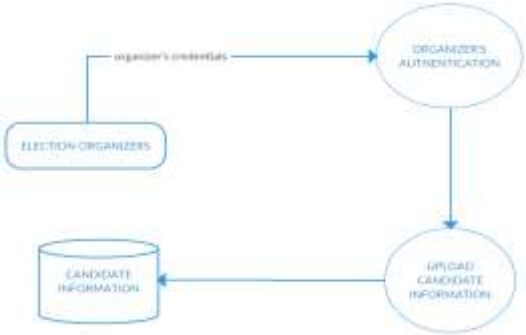


Fig. 3: Candidate Information

3.2. Authentication, Vote Casting and Recording

At the time of voting the voter needs to go through the validation process. If a voter is a legitimate user then he/she is allowed to vote.
The fig: 4 depict that when the time comes for voting the voter has to first login with their unique identification number and password. The system will verify the voter whether it is authentic or not. After the initial verification, the voter has to proceed with the face recognition. The face will be captured by the server and then it will be matched by the object made by the bucket in AWS during the registration process. The face will be verified by each object which is present in the bucket. The image should be in base64-encoded image byte or as a reference to an image in an Amazon S3 bucket. In this procedure the image to be uploaded should be in JPG or JPEG format. After the verification, a success message is returned with the matching percentage of the facial landmarks like coordinates of eyes and mouth etc.

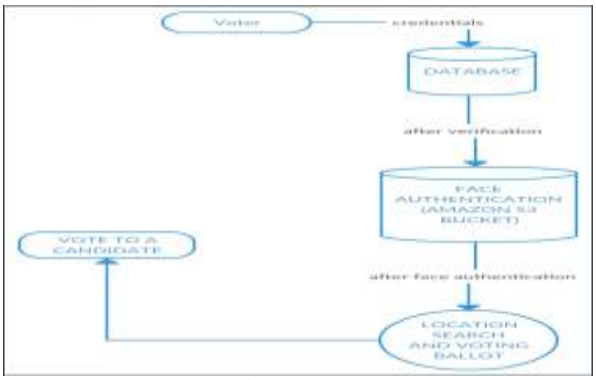


Fig. 4: Process of authentication during voting

After the process of authentication, the voter will be directed to location page where constituency of the voter will automatically be searched and then after pressing submit the voter will enter to voting ballot page. The ballot page will consist of candidate information like name, education, criminal cases, images etc. It would be easy for the voter to select the candidate by viewing the given information.



Fig. 5: Voting Ballot

After getting to the voting ballot, the voter has to select the candidate from the given list. After selecting the candidate the voter has to press the 'PRESS TO SUBMIT' button to register the vote.

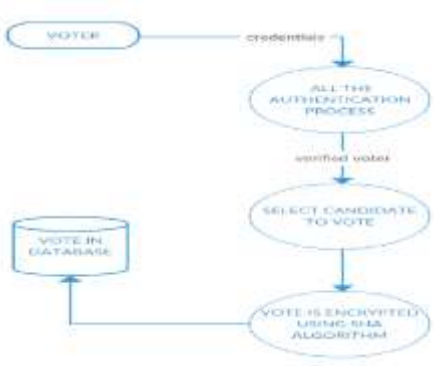


Fig. 6: Encryption of Vote

The name of the voted a party will be encrypted and will get saved in the specified database.
As soon as the voting begins and the vote count starts getting increased the counting of votes will start automatically. The different constituency will have a different database for their vote count. The election organizer will have authority to see the election live i.e. the voting process will be shown on the organizer's login. The privacy of the voter will be maintained as the details of the voters are encrypted.

3.3. Counted Vote and Final Result

After the compilation of election, the organizer has to enter into the database and take out the counted result. After getting the result, the organizer would be able to publish the result.



Fig. 7: Result of Election

The above figure shows how the final results are displayed in the organizer database. Hence after analysing, the results can be published.

4. Conclusion

The proposed secured online voting framework utilizes OTP, UIN, and face recognition for verification. Non-transferable accreditation, for example, the face is utilized which makes verification secure. Hash code is utilized to check if the unique identification number is altered or not. The algorithm used for face recognition makes security breach impossible.

References

[1] Himanshu Agarwal and G.N.Pandey, "Online Voting System for India Based on AADHAAR ID", *Eleventh International Conference on ICT and knowledge Engineering* 2013
[2] Vishal Kulkarni, Mangesh Devraj, AjitSingh Chauhan, Anujkumar Pandey and Prof. Smita Chavan, "E-Voting System using Android and Web-Based Platform" *International Journal of Advanced Research in Computer Science* Vol. 6, 2015.
[3] Tanmay Kadam, "Online voting system", *International Journal of Engineering Trends and Technology*.Vol.37 No.5, 2016.
[4] S. M, Jambhulkar, Jagdish B. Chakole, Prafl. R. Pardhi "A Secured Approach for Web Based Internet Voting System using Multiple Encryption", *2014 International Conference on Electronic Systems, Signal Processing, and Computing Technologies*, 2014.
[5] Amir Omidi, Saeed Moradi "Modeling and Quantitative Evaluation of an Internet Voting System Based on Dependable Web Services *International Conference on Computer and Communication Engineering (ICCCE 2012)*, 2012.