

ROLE OF INTERNET OF THINGS AND DESIGNING OF SOFTWARE MODEL FOR VALIDATING IDENTITY OF E-VOTER

DR. H. B. BHADKA

Dean, Faculty of Computer Science, C. U. Shah University
C. U. Shah College of Master of Computer Application, Wadhwan City. Gujarat.

harshad.bhadka@yahoo.com

ABSTRACT: *The developments of this country affect positively many countries of the world. So far, peoples of country need to be elect powerful administrators and right persons. Nowadays, the hand-held devices have become highly usual things as they have many advantages. They are widely adopted and used by the people of both urban and rural India. The internet increases the utilities of similar devices. In India, one of the big democratic countries in the world, casting vote for choosing members of Assembly and Parliament is crucial task of the people. The wide adoption and acceptance of Information Technology; the people whisper and demand casting their votes from geographically located anywhere. The purpose of this work is to utilize the identity concepts of the Internet of Things (IoT) and design a model for E-Voters. Identity mechanisms in the IoTs are different than those in the manual system. Electronic voting has a wide spread throughout U.S. The world needs to pay attention to reliability, security, or transparency. Today's e-voting systems use proprietary code and vendors have often asserted the confidentiality of this code when independent reviews of the certified systems were requested. There is a conflict between confidentiality and the transparency required for public elections. [1].*

1. INTRODUCTION:

This work focuses to address the important topic of identity management and validation in the IoT as specifically applied to the E-Voting applications. This work presents that the IoT is of a particular importance and has a great potential in E-Voting systems and environments due to the commonness of objects and devices including mobile devices. The software model has various stages including registration, E-Voting and focus on possible threats.

2. REGISTRATION:

The registration process of any person for E-Voting system has specific requirements which include collecting the information related to Eye Retina, Finger sign (single finger) of both hands, address with proofs, etc similar to those for the Unique Identification Number by UIDAI [2]. QR Code is generated on each 'Aadhar' card. Further, the information needs to be collected from the people will include Election Card Number, Mobile Number, PAN details / Driving License / Ration Card details / Passport Card details / Bank Account Number / LIC Policy number

3. E-VOTING:

Before announcement of elections, people who register as E-Voters must get verified the all details / information (as stated above) and get official identity to cast his / her votes as E-Voters. People who wish to cast their vote online, needs to fill all the details and scan the QR Code of "Aadhar" in the presence of competent officer authority identified by the government office. The persons get verification codes on their register mobile number and the other message be forwarded to these officers on their registered mobiles. After entering all the details and verification code from both; the voter will be considered as E-Voter. The model contains the following steps:

Step-1: Oath of Privacy and Promises – Once 'accepting', it will jump to the next step.

Step-2: Collect election card details from the user.

Step-3: Collect the Birth date(as mentioned on the Election Card).

Step-4: Collect information of PAN details / Driving License / Ration Card details / Passport details / Bank Account Number / LIC Policy number.

Step-5: Scan QR Code from "Aadhar" and match with the UIDAI repository.

Step-6: Scan and collect any left / right finger.

Step-7: Scan and collect the eye retina picture.

Step-8: Enter verification code received on the user's registered mobile.

Step-9: Enter the verification code received by the competent election officer's mobile.

Step-10: Display election details, list of candidate of respective constituency with single selection option, view the profile and cast the vote by selecting any one.

Step-11: Finish by submit the vote and send confirmation SMS / email to E-Voter.

All the steps are mandatory and then will open the next window in the software model after providing and verifying the person identity. False information cannot match with the stored information; the model immediately flashes the message on the screen. Give three chances to provide the details. If people cast their vote through the Computer, the different devices for scanning the QR Code, Finger and Eye Retina are required to be connected to the computer. Alternatively, person can use his / her mobile device (with high quality resolution camera and touch screen) to provide the details.

4. THREATS:

Network Security Experts are alert that online voting can be dangerous. There is no guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future. In the cyber security world today attackers are more powerful and can attack can result in the wrong election of undeserving.

This model has various steps to validate the identity of the E-Voters. Software model uses proven algorithm (e. g. Hamming Code) for encryption / decryption of data with 128 bit SSL encryption key and transfers to the server. The mobile operators have to be under observation / vigilance once the people cast their votes through this system.

5. CONCLUSION:

E-Voting can prove to be risky. This service can be availed with quality devices to capture photo, Finger print, QR Code Reader.

6. REFERENCES:

1. "Inside Risks", Matt Bishop and David Wagner, Communications of ACM, November 2007, Vol. 50, No. 11 Pg. 120.
2. Official website of Unique Identification Authority of India (UIDAI) uidai.gov.in