ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India

Distributed Voting System Using IOT

Channakeshava RN

Assistant Professor, Department of Computer Science, Government Science College, Chitradurga, India

ABSTRACT: online voting system provides a model for using latest technologies in the traditional voting system in general elections in a country like India. The model designed to match the present manual/electronic voting machine voting system presently used. Since electronic voting machines first introduced in 1998, technology has changed a lot. The latest technology such as IoT better fits for implementing in voting systems. The model proposed enables the voter to poll his vote any of the polling station in his state (for assembly elections) or anywhere in the country (for parliament elections). The voting terminals may be interconnected using IoT technology may be called as IoT voting terminals.

KEYWORDS: Terminal, IoT, Biometric, Polling, Voter, Candidate, Elections, Adhaar. Pooling station. Security, Authentication.

I. INTRODUCTION

Indian government has to spend crores together money for General Elections in India. Similarly it also costs something for voters if they have to travel all the way to their native for casting their right. As a considerable percentage of population migrate to distant places for their living, a considerable number of people travels back to their natives for casting their votes. Some of them cannot turnout to cast their right due their schedules. A new initiative to provide voters without visiting to their native voting booth/station will also help to increase voting percentage.

It is almost 2 decades that we have introduced electronic voting machines. During this time, lots of technologies are evolved for choosing for implementation. Also there are so many major projects going on such t as ADHAAR which has kept biometric details of almost citizens. The voter lists are digitized and a voter may get his booth details his part number serial number just by inputting voter ID number. Even new initiatives are also taken for counting using totalizers to count votes polled panchayat-wise instead of booth-wise. Even with the introduction of smartphones and lesser data costs most of the population is well versed with the technological world. Hence educating the voters or officials is simplified.

Allowing a voter to vote in any of the booth may be a policy matter. But a collection of data is available, technology is available and the lifestyle of people is also changing. Then why not new technology can be adopted and elections system is made easy with technologies.

II. RELATED WORK

[1] A new applied e-voting system by Feras a. Haziemeh, Mutaz kh. Khazaaleh, Khairall m. Al-talafha has developed a prototype which uses web services to connect to a database of voting system. And stresses importance on data security by means of cryptography. [2] Highly Secured Online Voting System over Network - K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan. Emphasizes on recognizing faces through updated face images that are taken every 6 months for avoiding recognition problems. [3] The Design of Web Based Secure Internet Voting System for Corporate Election- Jagdish B. Chakole, P. R. Pardhi. The system is for registering vote casted in a corporate elections where user has to login via username and password. [4] Survey on Secure Online Voting System, Smita Khairnar, Reena Kharat have proposed a model which is very nearby to the present voting system of general elections. Which includes admin panel, candidate panel and user panel? [5]OnVote – Secured online voting - Priyanka Chordia,Pooja Chavan, Bhagyashri Patil, Rutuja Patil, Mrs. Priyanka More have proposed a model for secured online voting through recognition of person through fingerprints and pin + security key which encrypts the casted vote so that modifying the data unauthorized is impossible.

Almost all the voting systems online are concentrating on proposing a model so that a voter can cast his vote by sitting in his home through his desktop. Different security measures are taken for protecting the secrecy.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India

III. DISTRIBUTED VOTING SYSTEM

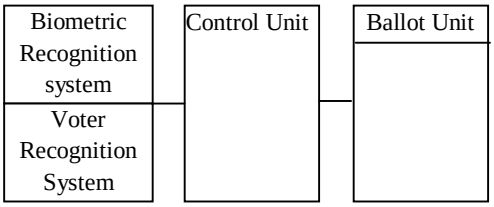
There are a lot of restrictions for the technology to be introduced in voting system otherwise even it might be possible that a person by sitting in his home in front of desktop or a android mobile phone might cast his vote by just inputting his voter ID and providing his biometrics for verification.

But adopting this system may raise many concerns about truthfulness of polling once the result of the election voting can be declared in the next day morning. Losers will try to show that all the polled data is false.

The distributed voting system is an attempt to fit technology in the existing system for voting procedure. This model replaces the traditional EVMs with IoT enabled Voting Terminals, where these voting terminals does two things

1. Identifies a person based on his biometrics and allows him to cast his Vote.
2. If the person appearing for voting is registered with some other pooling station, contacts with the Main server/Remote IOT Voting terminal. After successful verification of his identity he is allowed to cast his vote and registered vote is sent to the original voting station of his registered booth.

For accomplishing this IoT Voting terminal with two parts is allowed along with present control unit/ or the present control unit may also be replaced with improved version for taking controls from IoT Terminal. IoT voting Terminal has two parts.



Block diagram of IoT voting terminal

1. **Biometric Recognition System:** consist of Database of the voters registered in that Booth. The database may also be accompanied with it biometric details of that voter (Probably we may integrate Biometric information from Adhaar database). The biometric recognition system works as an authenticating module for casting the vote.

The biometrics that may be used for authentication for allowing voting may be finger print, Iris reader, or face recognition. As recognizing person using Iris has some oppositions and recognizing using face may be done by using simple manual verification with the identity proofs use of fingerprints for authentications may be a good deal and force security effectively.

2. **Voter recognition system** consists the voters list who has casted their vote. This database may include 1. Voters of this booth casted vote in this booth. 2. Voters of this booth who has casted votes from any other booth. 3. Voters of other pooling station who has casted their votes in this booth.

This module Intakes identification numbers of voter/ his serial number for casting his vote. Based on this if the voter is belonging to the same pooling station it will take authentication from biometric recognition system, and allows the control unit to take the vote through the ballot unit. If the voter is belonging to any other pooling station then the voter recognition system requests the IoT Voting terminal of the corresponding pooling station. The remote IoT provides authentication for the voter to cast the vote remotely. On receiving permission for casting vote the local Voter recognition system asks control unit to take the voting from the voter. The casted vote is passed to the remote IoT terminal and a copy of this is also stored in local IoT Terminal, until it receives confirmation of update from Remote IoT Terminal.

If the candidates to be elected are different than the ones in which the voter is casting his vote; this raises another technical issue; this can be simply ignored and the voter may be asked to cast his vote against the serial number of the candidate in his constituency. Or newer technology may also adopt in the form of dynamic touch screen ballot unit; which can load candidates list according to the requirements.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

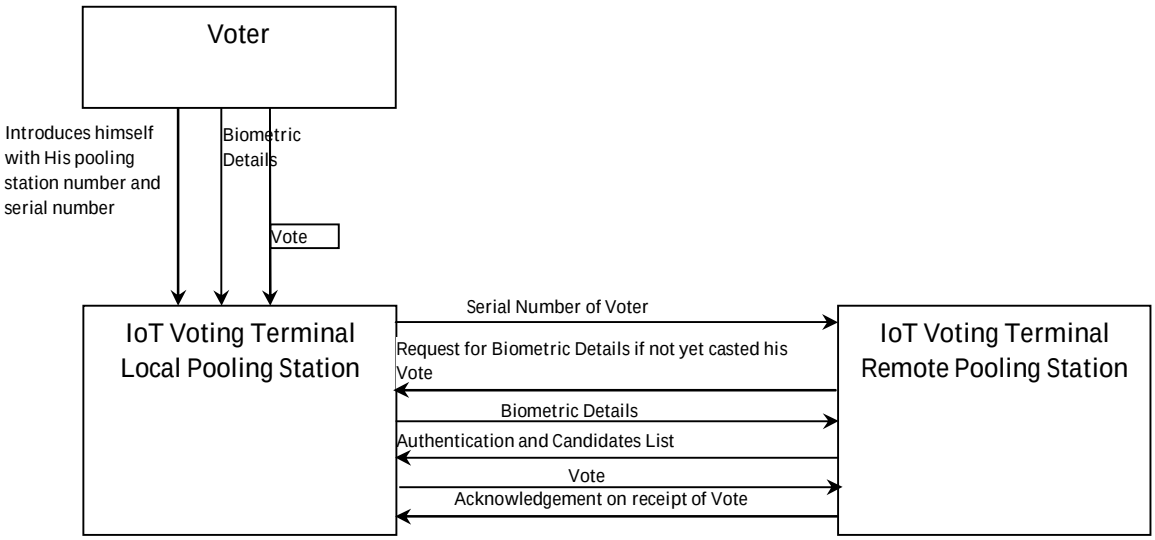
International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India



This model also emphasizes on inputting the voters part numbers and serial numbers in the voters list manually, As it reduces overhead of processing his biometric details for matching with biometric details of persons in the database.

This model does not emphasize on a centralized server model rather it proposes data transfer between the IoT Voting Terminals. Imagine more than 70 crore authentication requests in a single day that too within 10 hours of voting period, suppose a server crashes the whole system collapses. By diverting the authentication requests to the concerned IoT Voting Terminal the processing is divided among several IoTs and any technical issues arise will not harm the whole system.

After all, the people always ask that the voted system has to be in their eye sights, as they believe physical things rather than technology. It is also necessary to note down the statistics of the casted votes after the voting. This model provides room for all these.

This model fits into the system presently in use along with the touch of technology and importantly two goals are achieved. 1. Recognizing a person with his biometrics avoids tendered and fake voting. 2. A voter is given freedom for casting his vote from any distant location than his native so that he needs not to travel to his native for exercising his right.

IoT TECHNOLOGY: IoT is a technology to interconnect devices with unique addressing say an IP. This technology can be used to interconnect any devices. Here in this model we are using the technology to interconnect voting terminals. The ability of Internet of Things technology to scale is the most important thing that it can scale up to trillions of devices using IPV6.

The major advantage is that the IoT technology can be built over nay of the communication technology such as WiFi, Bluetooth, Wired LAN. Cellular data, copper wire connections or etc. so we have the flexibility that we can construct our own network or can also use the existing establishments. However as we have to choose protocols which has long coverage such as cellular data or copper wires.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

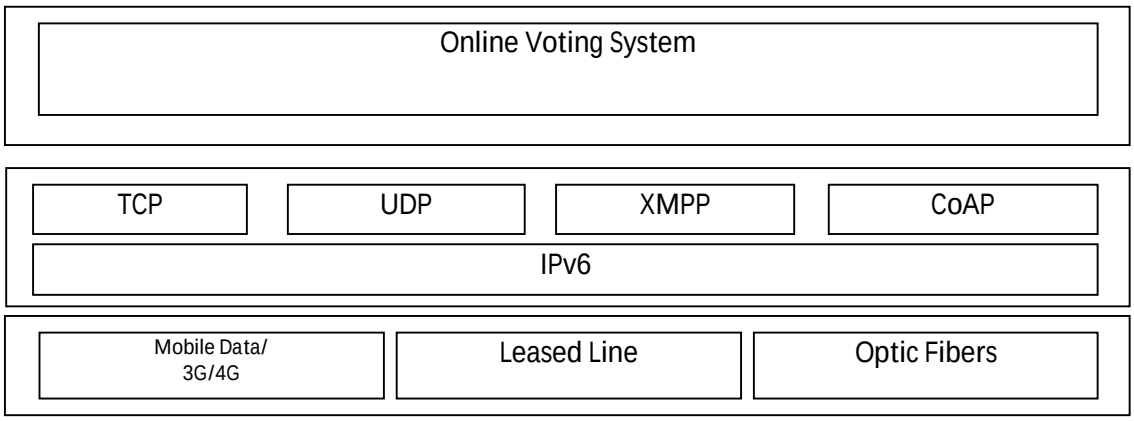
International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India



The IoT enables connecting things to the internet. The devices able to connect directly to internet must use an IP in order to exchange data in between by the use of IP suite. Otherwise if non-IP protocol is to be used the device has to use internet gateway. As the terminals are to be identified by their IP addresses we have to identify them using IP Suite only.

IP suite is the set of protocols for identifying the device over the internet; it is the global standard for computer to computer communication. For the devices such as terminals for voting system we may have to use a embedded IP suite.

The number of IoT voting terminals required will be estimated to be over a million. For accompanying addresses for all these terminals we must require addressing technique such as IPv6. IPv6 is an addressing based on Internet protocol which uses 128 bits for addressing, which enables IPv6 to be able to address 3.4 X 10^{38} devices. Also IPv6 supports a 1280 byte packet size without fragmentation, which increases communication of biometric details for authenticating. It requires use of IPSec protocol suite and is a secure IP communication also. IPSec uses Cryptography for providing security for the communications between terminals.

IPv6 uses Multicast Listener Discovery (MLD) messages to manage membership in local subnet groups. ICMPv6 Router Solicitation and Router Advertisement messages are used to determine the IP address of the best default gateway. To resolve IP addresses to link-layer addresses it Multicast Neighbor Solicitation messages.

Security in Communication: The votes cast possess even more importance than monetary transactions done on any bank, as the whole voting procedures conducted may leave behind many loopholes so that the communication between two IoTs is hacked and fake votes may be updated into the databases which will destroy the structure of democracy. So this enforces the importance of security measures during communication.

There must be a mechanism for identifying each of the IoT voting terminals uniquely and the communication done through that IoT is identified by all other IoTs statically or through an Identified Server. It

A monitoring system is also required for the studying the un-authorized attempts for hacking the system. The communication between two IoT Terminals should also requires encryption, The use of IPv6 in the communication model makes it mandate for the use of IPSec for securing the transmission. IPSec provides security in two modes:

a. Tunnel mode: encapsulates the whole IP Packet to be communicated.
b. Transport mode: This only encapsulates the IP payload for secure channel of communication.

IPSec use an Authentication Header (AH) or an Encapsulating Security Payload (ESP): used for authenticating the sender and the latter includes encapsulation.

There are a number of protocols available for implementing with IoT; HTTP, HTTPS, WebSocket, XMPP, CoAP, MQTT, SMCP, STOMP, Mihini/M3DA, AMQP etc. we find XMPP and CoAP are the two of the protocols useful for discussion.

XMPP: extensible Messaging and Presence Protocol can be useful for instant messaging and presence Information. This protocol may be best useful for connecting terminals (Machines) to the server M2S. This protocol can be used with TCP protocol.

XMPP-IoT: the variant of XMPP protocol which enables to Machine to Machine communication and Machine to People Communication. This protocol is very useful for pushing messages to distant machines, but it is a slow protocol.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India

XMPP also have one more disadvantage. It lacks end- to end encryption. Which is necessary for our model, it may also be implemented in a higher level.

CoAP: Constrained Application Protocol was designed by IETF for low power and constrained networks. This protocol is best suited for communications between two machines (M2M). This protocol can be used with UDP protocol.

CoAP uses UDP protocol for sending and receiving messages. The messages can also be marked as confirmable or non-confirmable. SSL/TLS securities are not available for UDP so CoAP can use DTLS datagram Transport Layer Security. The default level of encryption being 3072 bit RSA Key. Only disadvantage of CoAP is being group broadcasts are not available. However it is not a drawback for our requirement.

CoAP is designed to use minimal resources, both on the device and on the network. Instead of a complex transport stack, it gets by with UDP on IP. A 4-byte fixed header and a compact encoding of options enables small messages that causes no or little fragmentation on the link layer. Many servers can operate in a completely stateless fashion.

MQTT: Message Queue Telemetry Transport (MQTT) Similar to CoAP, it was built with resource-constrained devices in mind. MQTT has a lightweight packet structure designed to conserve both memory usage and power. It can be used for broadcasting purposes which is a lack of CoAP, but it lacks encryption.

IV. WORKING OF DISTRIBUTED VOTING SYSTEM

Once voter visits Voting terminal he can introduce himself with his voting booth number and serial number. He can also introduce himself with Adhaar number or VoterID number. If booth number is known the IoT translates it into IP address of the booth where the voter is registered. And the IoT voting Terminal of the voters' native is contacted for further authentication information. The voters registered IoT returns back the biometric authentication information of the voter. The voting terminal authorizes the voter of the inputted biometrics matches, and requests a list of candidates for whom voter votes. The candidates list is displayed on the ballot unit of the voting terminal. Pooled vote is sent back to the native terminal for registering. If the voter has to be identified by the Adhaar number or VoterID then the voting terminal requests native terminals IP and biometric details from the Online Voting System. Rest of the communication is continued with the native terminal.

The system can also be implemented with a minor change that the voters list, biometric details, and the voting may be stored in a centralized online voting system. As it makes the traffic is centralized to the server and it may reduce the performance of the system. The traffic is diverted to the respective voting terminals of the stations.

The centralized online voting system server can be used as a monitoring the authenticating procedures and it is also possible to adopt monitoring patterns to identify unauthorized access attempts from particular locations.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

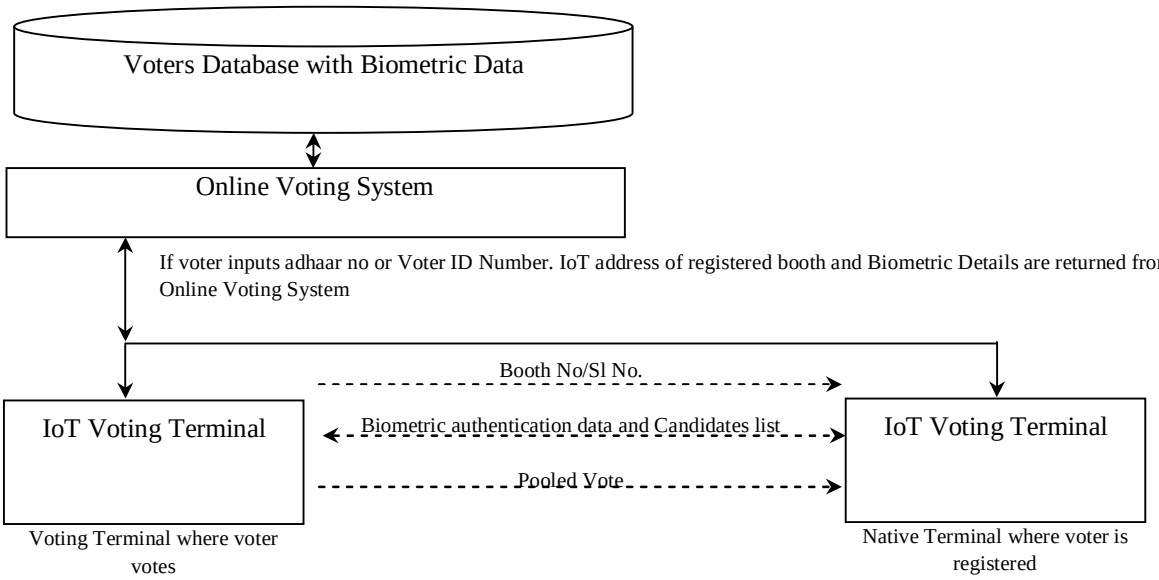
International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India



V. CONCLUSION AND FUTURE WORK

The online voting system requires investment in terminals, establishment of communication, integrating the databases, and a little education to the end users. But can achieve great advantages.

1. Increasing voting percentage.
2. Duplicate voting or tendering is reduced to nil.
3. Reduced man power.
4. It also reduces cost for the voter to reach his native polling station if he is staying away.

This model is proposed by considering the current practices of election procedures. So it can be very easy for migrating to this system. The biometric authentication systems might identify the voter even without providing his identity numbers, but searching through the databases for his details with available biometric information reduces the efficiency of the system hence the voter is asked to introduce himself with his voterID/ Adhaar number/ Voter list number. Inclusion of Algorithms to detect security breaches should also be incorporated along with this model.

Limitations of the model are that this requires the one stage election procedure. Or at least both the pooling stations should have the voting on the same day.

In this module we only discussed the polling of votes only the next procedures of counting votes and results is not discussed.

REFERENCES

[1] New applied e-voting system- 1feras a. Haziemeh, 2mutaz kh. Khazaaleh, 3 khairall m. Al-talafha.
[2] Highly Secured Online Voting System over Network- K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan.
[3] The Design of Web Based Secure Internet Voting System for Corporate Election- Jagdish B. Chakole, P. R. Pardhi.
[4] Survey on Secure Online Voting System, Smita Khairnar, Reena Kharat
[5] OnVote – Secured online voting - Priyanka Chordia,Pooja Chavan, Bhagyashri Patil, Rutuja Patil, Mrs. Priyanka More
[6] http://www.protocols.com/pbook/tcpip2/
[7] http://searchenterprisewan.techtarget.com/definition/IPv6
[8] https://en.wikipedia.org/wiki/IPsec
[9] ceokarnataka.kar.nic.in
[10] http://www.infoworld.com/article/2972143/internet-of-things/real-time-protocols-for-iot-apps.html
[11] Study on Security of Online Voting System Using Biometrics and Steganography- Neha Gandhi M.Tech Scholar, Deptt. Of Computer Sc. & Appl, K.U., Kurukshetra
[12] Advanced Secure Voting System with IoT- Ms. Nithya.S, Mr.Ashwin.C, Mr.Karthikeyan. C, Mr.Ajith kumar.M