Voting System using Retina with Secure Socket Tunneling Protocol

R. Jayachitra
UG Scholar,
V.R.S College of Engineering & Technology,
Arasur,

K. Kalaiyarasi
UG Scholar,
V.R.S College of Engineering & Technology,
Arasur,

R. Kavitha
UG Scholar,
V.R.S College of Engineering & Technology,
Arasur,

***Abstract*— the main aim of our project is to churn out the changes in Indian voting scheme as fully systematic software, which is reusable with advanced networking and biometric security. The proposed system involves the voting carried with high level authentication and unremitting manpower. So once privacy is given high value. The client server communication is the imperative value of this proposed system because the vote count is handover from client to server with the help of tunneling protocol wh ich establishes a private network that provides the systematic progression without the interruption of manpower throughout the process. When compared to the existing system, the proposed system consumes less time for voting. This voting system reduces the man power that is utilized to secure existing system, until it is sent to the public vote counting session. This system reduces booth capturing by the anti social element. Another main benefit of this system is mobility. This technique abolishes the counterfeit votes by the favor of the chosen candidate. Thus the proposed system is the highly structured by overcoming all the disadvantages in the existing technique. Hence we will have a crystal clear election with low expenditure in a faultless manner. Further, we will discuss the implementation and working of our envisioned system in a clear view.**

***Keywords*— Election, voting, voter, candidate.**

I. INTRODUCTION

EVM- now a day, a machine used for polling of vote, which is very costly and difficult to maintain. At this 20th century our world likes only the ready-mate things. And all are moving like busy ants. But, there is no time to wait for anything. The result for the election taking hardly a month to release. To change this bad situation, we are best planned to made the voting method are systematic which is highly secured, safe and at low cost too. In EVM the votes are stored in EEPROM. To overcome the security problem in that tunneling protocol is used to transfer the vote in a high secured network path and votes are stored in a centralized database. Let us see about this in detail by the following.

II. EXISTING SYSTEM

Electronic Voting Machines ("EVM") are being used in Indian General and State Elections to implement electronic voting. EVMs have been under a cloud of suspicion over their alleged tamp arability (crime) and security problems during elections. Indian voting machines use a two-piece system with a balloting unit presenting the voter with a button (momentary switch) for each choice connected by a cable to an electronic ballot box. Most of the countries were banned this type of voting machines because it is unsecured.

III. SECURITY PROBLEM

In April 2010, an independent security analysis was released by a research team led by Hari Prasad, Rop Gonggrijp, and J. Alex Halderman. The study included video demonstrations of two attacks that the researchers carried out on a *real EVM*, as well as descriptions of several other potential vulnerabilities.

A *BEFORE VOTING*

One demonstration attack was based on replacing the part inside the control unit that actually displays the candidates' vote totals. The study showed how a substitute, "dishonest" part could output fraudulent election results. This component can be programmed to steal a percentage of the votes in favor of a chosen candidate

B .AFTER VOTING

The second demonstration attack used a small clip-on device to manipulate the vote storage memory inside the machine. Votes stored in the EVM between the election and the

public counting session can be changed by using a specially made pocket-sized device. When you open the machine, you find micro-controllers, under which are electrically enabled programs, with 'read-only' memory. It is used only for storage. However, you can read and write memory from an external interface. The researchers developed

a small clip with a chip on the top to read votes inside the memory and manipulate the data by swapping the vote from one candidate to another.

But Election Commission of India points out the tampering of the EVMs, one needs physical access to EVMs, and pretty high tech skills are required. Given that EVMs are stored under strict security which can be monitored by candidates or their agents all the time, its impossible to gain physical access to the machines. Plus, to impact the results of an election, hundreds to thousands of machines will be needed to tamper with, which is almost impossible given the hi-tech and time consuming nature of the tampering process.

IV. PROPOSED SYSTEM

The proposed system was more secured than the EVM. Because the proposed system uses retina image for every individual person, the UID (Unique Identification) number which is provided by the Government of India and the confirmation of vote is also enhanced to the system.

The procedure followed by the proposed system is listed below:

- The system will get started after the candidates are announced legally by the election commission for all the parties.
- Initially the server system stores the parties‘ symbols and their name in the database.
- Then the server update the client system with the booth number, booth name, area, parties name, symbol and their candidate name.
- The client database updated separately with the voters list, UID number and the retina image.
- Before the voter register their vote, there are two authentications should be followed.
- The person will enter the UID number to display the voter details. If the number typed is correct, then the voter details will be displayed. If not the voter will not allow to poll their vote.
- The second authentication is to scan the voter‘s retina image by the retina scanner.
- After the authentication will get over, the voter is allowed to register their vote.
- The candidate name, parties name and their symbols are displayed on the screen with their serial number.
- The voter enters the serial number of the party which they want to vote. After entering the serial number the confirmation message will be displayed on the screen.

If they want to do any changes in their vote they can press the cancel button to reenter the serial number.

If not the voter can press the yes button to confirm their vote. After the voting is confirmed, then the thank you message will be displayed on the screen.

V. RETINA SCANNER

Retina-scan technology makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. Retinal Scan technology is based on the blood vessel pattern in the retina of the eye.

The principle behind the technology is that the blood vessels at the retina provide a unique pattern, which may be used as a tamper-proof personal identifier.

Among its advantages are its resistance to false matching or false positives and the fact that the pupil, like the fingerprint remains a stable physiological trait throughout ones life. The retina is located deep within one‘s eyes and is highly unlikely to be altered by any environmental or temporal condition.

VI. TUNNELLING PROTOCOL

The Secure Socket Tunneling Protocol (SSTP). SSTP is a mechanism to encapsulate Point-to-Point Protocol (PPP) traffic over an HTTPS protocol, as specified in and this protocol enables users to access a private network by using HTTPS. The use of HTTPS enables traversal of most firewalls and web proxies.

The SSL is a secure socket layer which was established by Netscape Communication Corporation for strengthen the security level by means of encryption.

The SSTP has three major functions. They are

1. Key negotiation
2. Encryption
3. Integrity traffic checking.

Relationship to Other Protocols: The following network stack diagram shows the relationshipwithe other protocols

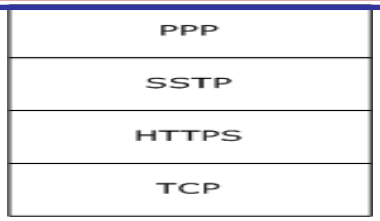


Fig 5.1: Encapsulated Protocol.

The following encapsulation operations occur on the client:

1. Application packets are encapsulated over any transport protocol (for example, TCP and UDP).

2. Transport layer packets are encapsulated over a network protocol (for example, IP).

3. Network layer packets are encapsulated over a PPP data- link layer.

4. PPP packets are encapsulated over SSTP.
   - SSTP Packets are encapsulated over SSL/TLS.
   - SSL/TLS records are encapsulated over TCP.
   - TCP packets are encapsulated over IP.

5. IP packets are sent over any data-link layer.

6. On the server side, operations to remove the encapsulation occur in the reverse order.

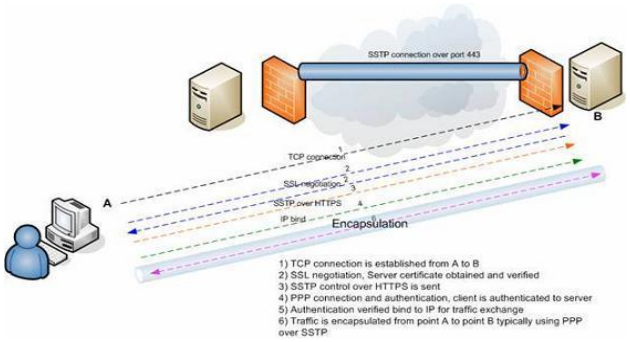
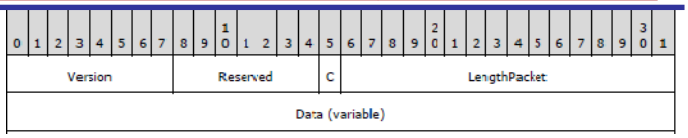


Fig 5.2: Structure of Tunnel

Message Syntax

SSTP Packet

The following diagram shows the format of the SSTP packet that is sent on the HTTPS connection. The fields of the header MUST be transmitted in byte order from left to right.



Version (1 byte): An 8-bit (1-byte) field that is used to communicate and negotiate the version of SSTP that is used. The upper 4 bits are the MAJOR version, which MUST be 0x1, and the lower 4 bits are the MINOR version, which MUST be set to 0x0. This means that the 8-bit value of the Version field MUST be 0x10 and corresponds to Version 1.0.

Reserved (7 bits): This 7-bit field is reserved for future use. MUST be set to zero when sent and MUST be ignored on receipt.

C (1 bit): A 1-bit field that is used to indicate whether the packet is an SSTP control packet or an SSTP data packet (the data packet is used for sending a higher-layer payload). The value is 1 if it is a control packet and zero if it is a data packet.

.

The sequence of steps that occurs is as follows:

1. The TCP connection is established by the SSTP Client to the SSTP server over TCP port 443.
2. SSL/TLS handshake is completed over this TCP connection. The SSTP server is authenticated by the SSTP client. However, the client authentication by the server is only optional.
3. The HTTPS request-response is completed. SSTP negotiation begins. The SSTP client sends Call Connect Request message to the SSTP server.
4. The SSTP server validates the request and sends Call Connect Acknowledge message that contains a nonce to be used by the SSTP client in the Call Connected message.
5. PPP negotiation is initiated, and PPP authentication is completed. For more information about PPP.
6. The SSTP client sends the Call Connected message, which contains the following items:

- The SSTP server validates the Call Connected message, and SSTP negotiation is completed.
- PPP negotiation (that is, a network control protocol such as IP Control Protocol (IPCP) is negotiated) is completed.

Higher-layer triggered events:

The SSTP layer interfaces with the PPP layer using the following events. These events are triggered by the PPP layer.

Send PPP control frame: This event is used by the PPP layer to send a PPP control payload to the SSTP

layer. The SSTP layer then sends the PPP control payload to the HTTPS layer after performing the necessary encapsulation.

Send PPP data frame: This event is used by the PPP layer to send a PPP data payload to the SSTP layer. The SSTP layer then sends the PPP data payload to the HTTPS layer after performing the necessary encapsulation.

PPP authentication completed: This event is used by the PPP layer to notify the SSTP layer that PPP authentication has been completed. The PPP layer uses this event to pass the higher layer authentication key (HLAK) to the SSTP layer. The SSTP layer on the client will use this attribute to generate and send the crypto binding attribute to the server. The SSTP layer on the server will use this attribute to validate the crypto binding attribute sent by the client.

Interface with Https

The SSTP layer on both client-side and server-side implementations interfaces with the local HTTPS layer using the following events.

Open HTTPS connection: This event is used by the SSTP client to initiate an HTTPS connection to the SSTP server. The SSTP layer specifies the hostname or IP address of the SSTP server when calling this event. If the HTTPS connection is established successfully, the HTTPS layer returns the server certificate hash .

Accept HTTPS connection: This event is used by the SSTP server to accept a new incoming HTTPS connection from the SSTP client.

Close HTTPS connection: This event is used by an SSTP peer to close the HTTPS connection.

Send HTTPS stream: This event is used by the SSTP client and the SSTP server to send an SSTP control packet or an SSTP data packet to the local HTTPS layer. The HTTPS layer encrypts the SSTP packet as a byte stream and sends it to the SSTP peer.

Receive HTTPS stream: This event is used by the HTTPS layer to indicate a stream of bytes to the local SSTP layer as received from the SSTP far end. The SSTP layer delineates the stream of bytes into SSTP control packets and SSTP data packets. If delineation fails, the connection is immediately aborted and a lower link down event is sent to the PPP layer. If delineation succeeds, the SSTP control packets are passed to the SSTP state machine for further processing. The SSTP data packets, including all PPP control frames and all PPP data frames, are passed to the PPP.

HTTPS connection disconnected: This interface is used by the HTTPS layer to indicate a disconnection of the HTTPS connection. This disconnection can happen due to events such as network interface failure, network failure, TCP failure, SSL/TLS failure, lower layer HTTPS session disconnected, and similar scenarios. In all such scenarios, the SSTP layer MUST immediately clean up the call-related information without any over-the-wire interaction. The SSTP layer MUST send a lower-link-down event to the higher layer (PPP).

VII. CLIENT-SERVER ARCHITECTURE

The votes are stored in the client database and the client system sends the votes to the server by the tunneling protocol after the voting gets finished. When we use normal IP protocols the data transfer from one point to another, the data is fragmented into packets and send to the another point. The packets get damaged or broken before it reaches the destination. So when we use tunneling protocol,

The client transfers the polled vote to the server by using this protocol. Because of this tunneled structure the packet cannot be broken and the hackers cannot hack the data.

The third person cannot interrupt in this way of voting system. So the voting is more efficient.

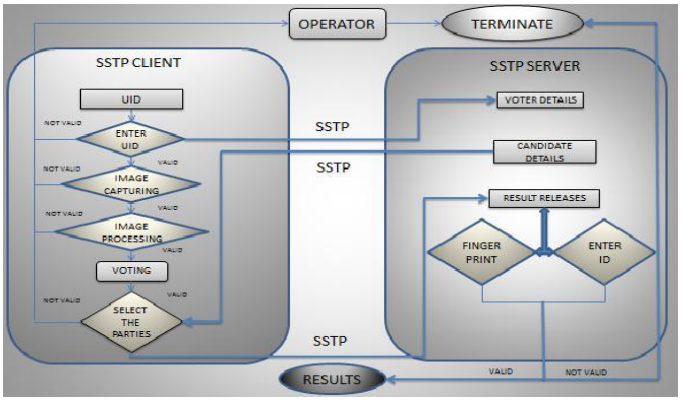


Fig 6.1: Client-server architecture

Before the result will announced, there are two authentication will be followed. First, the chief election commissioner enters their 10 digit serial number. If it is correct then the commissioner fingerprint will be scanned by the fingerprint scanner. Then the result will be published through the internet.

The above process are take place between client and server after establishing the SSTP tunnel .through the tunnel all data packet will get transferred .
The below figure will explain in a brief manner:

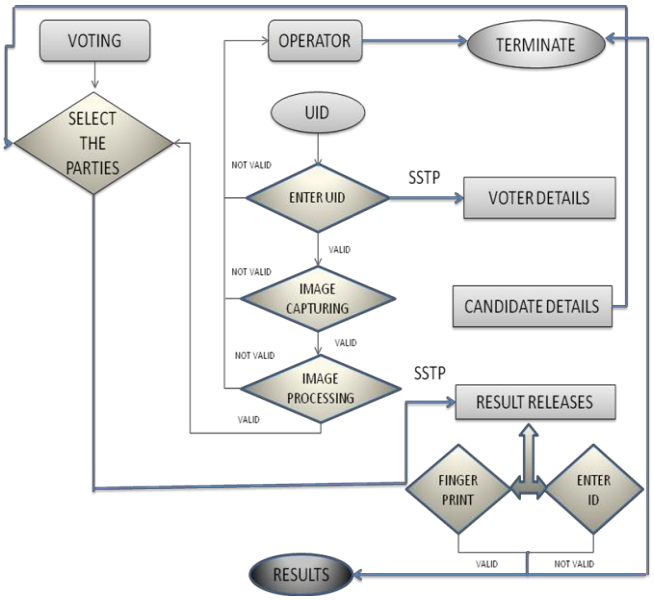


Fig 6.2: Process flows in proposed system

VIII. DATABASE MANAGEMENT

. The client database contains the voters list, voters UID number, voter retina image, booth number and the booth name. The server maintains database with the parties name, symbol and the candidate name. The server updates these details to the client database. After the polling gets over the client system will automatically shut down. It will send data to the server before the client gets turn off. The server maintains another table which contains the booth name, booth number, number of voting areas details. The server generates the 10 digit booth number automatically and sends to the client. The server saves the database automatically.

IX. ADVANTAGES

- The main advantage of using this system is to reduce the man power and increase the security system.
- The counting can be done without any interruption of man power.
- The result is announced immediately after the polling gets over.
- The cost of the system is very less and needs client and server system only.

X. CONCLUSION

Thus our project was highly secured and safe method for polling of votes at the minimum cost. When this method was implemented, really the Government of India will retain the $1/3^{rd}$ of the cost used for election in the present. The authentication such we are used in this method was highly prompting. Hence the malpractice was strictly avoided. Mainly the result will be announced immediately after closing the vote polling. So definitely in future we will have a very efficient election.

XI. REFERENCES

[1] www.technet.microsoft.com. chapter11-This reference includes the information source about the point to point protocols and its range of usage over the network regarding data transfer over PPP.

[2] www.sans.org –This reference includes the sources regarding the Biometrics Scanning Technology which have a features explanation over retina and finger print scan.

[3] Disadvantages of Electronic Voting", www.newagebd.com- This references have the information regarding how the present electronic voting system are vulnerable and discuss about its cons of e-voting.

[4] Indian Voting Machines www.en.wikipedia.org/wiki/Indian_voting_machines- This references have the documents regarding Indian voting machines and its features‘.

[5] Security Analysis of India's Electronic Voting Machines: Hari K. Prasad, J. Alex Halderman, Rop Gonggrijp, The Indian voting machine, known in India as EVMs, have been praised for their simple design, ease of use, and reliability, but recently they have also been criticized because of widespread reports of election irregularities.

[6] India‘s Electronic Voting Machines Have Security Problems, ED FELTEN. The independent Electoral Commission of India, which is generally well respected, has dealt poorly with previous questions about EVM security. The chair of the Electoral Commission has called the machines –infallible‖ and –perfect‖ and has rejected any suggestion that security improvements are even possible.

[7] UDAI, www.uidai.gov.in, Adhaarcard-UIDnumber, www.uidnumber.org –This reference intended to give the information about the adharcard and its features. And its also discuss about the pros and cons about the uid that are using now in India.

[8] Retinal recognition by Ravi Das. This article focuses on a unique biometric technology: retinal recognition. In view of the rich and unique blood vessel patterns in the retina, there is no doubt that retinal recognition is the _ultimate‘ biometric.

[9] E-voting project in Indian Institute of Technology, Madras. E-voting project which is done by IIT students and it is under research by Election Commission of India.

[10] www.functionx.com, client-server communication.-This references discuss regarding how the communication is take place between the client and server and its way of communicating with its high protocols layer .

[11] www.fbi.gov , this references deal with the finger-print authentication technology and its working procedure.

[12] www.web.mit.edu, this reference deals regarding about network and security information.

[13] [MS-SSTP] –Secure Socket Tunneling Protocol: Microsoft corporation. This document describes the Microsoft Secure Socket Tunneling Protocol, is a mechanism to encapsulate PPP traffic over an HTTPS protocol.