Implementation of Authenticated and Secure Electronic Voting system

Hesham A. El Zouka
Computer Eng. Dept, College of Engineering and Technology
Arab Academy for Science, Technology, and Maritime Transport,
Alexandria, Egypt
helzouka@aast.edu, helzouka@gmail.com

Mustafa M. Hosni
Electrical Engineering Dept., Faculty of Engineering,
Managing Director of OMIKRON Technologies,
Alexandria, Egypt
mustafa.hosni@omikrontechnologies.com

Abstract — There are several issues should be addressed and taken into consideration prior to initiating the e-voting system. The proposed system in this paper will ensure the integrity and the transparency of the electoral process. The paper will also focus on what's really needed to design a robust, secure and scalable electronic voting system that ensures accuracy, neutrality, transparency, simplicity, flexibility, Sustainability, and security of the information. With respect to accuracy, the system must be safe and secure in the face of numerous threats. In order to safeguard the neutrality of voter registration process, the system should not favour a particular party or group. Looking at the risks and benefit associated with transparency, the process must be clear in terms of counting the electronic votes, taking the political and legal setting into account. For simplicity, the process must be easy to understand for citizens and elected politicians. The simplicity allows for extreme flexibility in adapting to disabled and illiterate voters as well. All the above mentioned points will be addressed in the proposed contribution**.**

Keywords- e-voting, validation, verification, privacy, authentication, threat, risk management.

I. Introduction

The objective of e-voting system is to permit voters to practice their right to express their decisions in regards to particular issues to pick their government and political party representatives. To permit the activity of this right, all voting frameworks around the world incorporate to achieve voter identification proof, recording of votes cast, vote tallying, and determination of election results. Voter distinguishing proof is required during the electing process.

Therefore, it is quite agreeable to have computerized voting system to reduce voting time, to make sure that the voting is a occurred correctly, to reduce flaws and errors in filling out ballots and finally to simplify the process for people with special needs [1]. As e-voting is gradually replacing the traditional voting systems, it becomes quite obvious and undeniable how electronic principles are depending upon electoral process's credibility [2].

Consequently, securing e-voting system would not be an easy task, as essential security properties will need to be ensured. But as yet, some e-voting security requirement sound contradicting and confusing like ensuring voter authenticity and vote anonymity [3].

In this paper, A windows communication foundation based distributed network and A NOSQL Cassandra distributed database management system are used to implement the proposed e-voting system [4]. The software implementation can be classified into two phases: the local phase and the global phase. The Local phase is organized by Windows Presentation Foundation program, and the global phase creates the "Silverlight ASP.NET website, and in both phases the source code is written in C #.Net language [5]. In addition, the mobile Agents technology is applied to achieve tasks and remotely controlling objects in the network [6]. Mobile agent is concerned with the actual implementation of deploying new objects as they do not need to be installed or deployed before their use. Mobile agents are simply created, and are self deploying. This makes it easier to deploy newer objects as they do not have to be pre deployed and installed before their use. Simply, NET Remoting runs over channel objects and forms the mode of transport for mobile agents between mobile agent platforms, providing larger bandwidth and security to the e-voting machines. Therefore, the data can be processed at various locations in the network and the code portion of mobile agents can be cached, reducing the bandwidth to just the data segments.

In the following sections the proposed architecture will be described in details. In Section II, the security requirements and concerns of e-voting systems are introduced and the importance of improving election transparency and ensuring the respect of democratic principles is discussed. Challenges in implementing e-voting systems are briefly introduced in section III. The architecture of the proposed e-voting scheme is presented in Section IV, while the implementation details are described in Section V. In Section VI, the design diversity of the embedded codes is discussed. Finally, a brief conclusion is given in Section VII.

II. Security requirements

A set of laws is set in each country in order to guide the voting system, to establish its organization and to ensure its impartiality, integrity, and democratic principles. In general, e-voting election processes should follow this set of laws and fulfill the following requirements [7], [8],[9].

a) Accuracy – The system must provide accurate results according to the rules of the electoral process. The process must be clear in terms of counting the electronic votes, taking the political and legal setting into account. In addition, vote counting shouldn't be observed by the poll watchers as it is basically done computationally. Vote receipts are needed, then, to allow voters check if their votes were correctly counted and prevent voter coercion or vote trading. No access is allowed to material evidence certifying to others the quality of others votes and voters should vote only once in the same election.

b) **Security –** The system must be safe and secure in the face of numerous threats, such as fraud, identity theft, stolen passwords and human errors, as well as ensuring the secrecy of the ballot during voting and counting stages. An audit trail of the whole voting process should be provided in order to detect fraud, software or hardware malfunction, or human operation errors.

c) **Confidentiality and Authenticity:** Votes should be kept confidential from its verification until the counting phase and partial counting should not be allowed. The verification of voter authenticity takes place in two phases at voter registration and just before the voting procedure as the system should prevent voter impersonation. The authorized user may host a service or vote, and the provided service will be handling as a super column family that indexed by his ID key, and returns multiple columns of services with different roles of factors such as statuses and timestamps.

d) **Integrity and Availability:** Final vote counting should present the exact number of votes and their intent. The voting service should be available and respect should be paid to the security requirements during the election process. Moreover, the system must be flexible to adapt to the disabled and illiterate voters.

e) Anonymity: Votes should remain anonymous during the process and any association on connection of the vote to its voter, or vice-versa should be strictly prohibited. The system also should not favor a particular party or group, and to ensure that competitions have equal opportunities at the level of participation.

f) Usability: The process must be easy to understand for citizens and elected politicians. Therefore, the e-voting system should be user-friendly; to offer visual, touch and audio resources to allows/help the voter to vote quickly and without any assist.

g) **Scalability:** In order to maintain scalability, performance, durability, transaction and queued calls of the proposed model, instance management will be used as a part of WCF web socket service to bind and specify query parameters, such as instance handles, data states, and client requests.

In this paper WCF will be used to support classical Request-Replay model as well as "One-way call" and "Call-back" service [10]. Both calls will establish a connection without creating dependency issue, whether by asynchronous call or callback operations. However callback operation has benefit over asynchronous calls since it can perform any operation at any time with guaranteed success. Thus, remotely controlling the consumer is the key role of the client side In addition; the endpoint address of the service will be kept on changing. By using WS Discovery protocol, the client can change the endpoint address and identify the service dynamically as shown in Figure 1 [11].

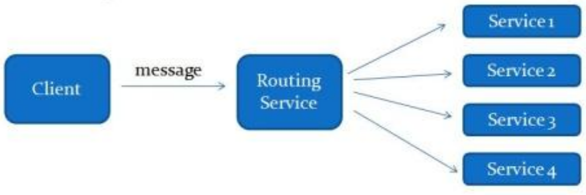

Figure 1. WCF Routing Service

Binding will describes how client will communicate with service, as it provides secure communication for peer-to-peer environment and network applications. It uses TCP protocol for and provides full support of SOAP security, transaction, and reliability. In our proposed model, WS Http Binding will be used to send large messages in announcement and discovery operations, regardless of what may be specified elsewhere in the coding file of the voting system. In our model all columns are added dynamically within the <runtime> section. The following code fragment implements the specified <Binding> code:

```
CF: Locks, K: ID, C: ID, Until
SCF: Services, K: ID, SC: Service, C: ID, SID, Role, Time
SCF Mobiles, K: ID, SC, Mobile, C: ID, Number, validity
CF: Votes, K: ID, C: ID, Time, CID, SID, Candidate
```

Assuming that partitioning and snitching are initially started up; RackAware and DatacenterShard apply the replication strategy on a volume level. So when voting system getting a file ID, it can specify the replication strategy. For example, the code may be provided via one or more of the following statements:

```
Replicate once on the same rack
Replicate once on a different rack, but same data center
Replicate once on a different data center
Replicate twice on two different data center
Replicate once on a different rack, and different data center
```

This proposal fulfills such properties and provides vote–materialization; it is able to materially reproduce the quality of each vote in order to allow manual vote recounting, when needed.

III. CHALLENGES IN IMPLEMENTING E-VOTING SYSTEMS

In 1960s, e-voting systems for electronics were first used after punched card systems had debuted. They first boomed in the USA when seven counties decided to apply this method in the 1964 presidential election. As for the more recent optical scan voting systems; they make computers count voters' marks on a ballot. DRE voting machines, on the other hand, are mainly used for colleting and tabulating votes in a single machine in all elections in Brazil, India, Venezuela and the United States. They have been also used in Netherlands but soon decommissioned for some public concerns. Later on, internet voting systems were used on a wider scale in government elections and referendums in the United Kingdom, Estonia, and Switzerland, as well as in municipal elections in Canada and France [12], [13], [14]. In general, the different types of e-voting include:

a) Paper- based e-voting system:

Paper based or document ballot voting systems was first used as a system where votes are counted by hand using paper ballots. Then, electronic tabulation showed up and paper cards or sheets were marked by hand, but counted electronically. These systems included punched card voting, mark sense and digital pen voting system at the very end. The "Decherd design" was first demonstrated by open voting consortion in 2004. It is a general-public license, open-source paper ballot printing system with open-source barcodes on each ballot.

b) Direct – Recording Electronic (DRE) voting system:

It records votes with the help of a ballot display provided with mechanical or electro-optical components (like buttons or a touch screen) that can be achieved by the voter and possesses date with computer software, and hence records voting data and ballot images in memory components. It can produce a tabulation of the voting data stored in a removable memory component and as a printed copy after the elections and it may provide a means for transmitting individual ballots or vote details to a central location, as well in order to consolidate and report result from the precincts at the central location.

A precinct count method is used by these systems in order to tabulate as they are cost and print the result after the close of polling at the polling place.

The Brazilian electoral justice launched their "voting machine" after conducting tests on more than so municipalities in 1996. Since 2000, all Brazilian voters have been able to use the electronic ballot boxes to choose their candidates.

In 2002, the help America vote Act, in USA, has permitted one handicapped accessible voting system for each polling place as most jurisdictions have been chosen to satisfy with the use of DRE voting machines.

India had e-voting machines (EVM) in 2010 for its elections to the parliament. 880 million voters had cast their ballots using more than a million voting machines. The machines were designed and developed by two identical government-owned, Defense-equipment-manufacturing units, Bhanat electronics limited (BEL) and Electronics Corporation of India Limited (ECIL). Both systems were developed specially for the election commission of India.

c) Public network DRE voting systems:

It is an election system that uses electronic ballots and transfers the voting data from the polling place to another location over a public network. Voting data could be transferred individually, periodically or as one batch at the close of voting: (internet voting or telephone voting). As for internet voting, it uses remote locations or traditional polling locations with voting booths possessing internet connected voting systems [15].

In Switzerland, whose DRE is on established part of local referendums, voters can get their passwords to access the ballot via posted service.

In Estonia, most voters can cast their vote in local and parliamentary elections via the internet, as most of those on the electoral call have access to an e-voting system which is the largest one run by an European Union country.

What made the task much easier for the Estonians is that they carry national identity cards equipped with a computer readable microchip to get access to the online ballot. Consequently, voters only need a computer, an electronic card reader, their id card and its pin to vote from anywhere in the world. E-votes in Estonia are only cast during the days of advance voting, but on the Election Day itself, people go to polling stations and fill-in a paper ballot.

d) Online voting:

Arizona, for example, has mark transitional moves towards online voting as each registered democrat received personal identification number in the mail. The voters could cast ballots at a designated location or over the internet [16], [17]. Those who preferred to vote the internet were asked to insert their pin and answer two personal questions. After verifying the information, they can have the voting options in return. In Estonia, again, internet voting has been popularized, as each voter had a national id card that is used to identify each citizen and ensure read reliability in votes. Security ethical said that they didn't detect any usual activity or tampering of the votes [18].

IV. THE ARCHITECTURE

This fully computerized proposed architecture uses a three–ballot scheme. The data scheme would use three equal ballots for each vote and each one would have a unique numeric identifier. The voter would then, check his candidates in two ballots, whereas for the rest of the candidates, one check only would be needed. Therefore, the candidates will have two marks in the three ballots set, and all of the other candidates will have one mark each. During this process, the ballot chosen by the voter randomly will be copied as a vote receipt. Then, the three ballots will be stored and the electoral authority will publish all copied ballots after the election in order o let the voter check if their votes were counted or not. The proposed algorithm is based upon the following: a registration agent, a voting console, a voting manger, an electronic ballot box, an electronic bulletin board. First of all, the vote will present themselves to the registration agent to be allowed to vote, then, the agent will interact with the voting manager to get the corresponding ballot IDs and have then used to possess credentials that would be returned to the voters. Next, the voters will use the voting console to vote and the voting manager will then, store the votes in the electronic ballot box and the voting console will give a voting receipt to each voter. Ultimately, the electoral authority and the election representations will count the votes and publish the receipts in the electronic bulletin board.

The order of voters getting in access to the registration agent is unpredictable in order to prevent voter anonymity violations. After indentifying themselves to the registration agent, the agent will verify whether the vote can vote or not. Then, three ballot IDs will be taken out of the ballot randomly, signs them and returns them to the voter. The repository of voters will be updated in order to check that the voter would be qualified to vote or not and to check his uniqueness. The registration agent chooses three new IDs and the voting console's public key will be used by the registration agent to cipher every single new ID separately.

A biometric device will help in obtaining a template of the voter's fingerprints that would be ciphered by the voting console's public key and get attached in. Such procedure will guarantee the voter's authenticity and prevent impersonation during voting. The ID's will be unknown to the registration agent after being ciphered and the agent will hence, perform a blind signature on the IDs to build the voter's credentials. Any interactions within the public key infrastructure will include signature authenticity verification procedures, as all the transactions between entities will be digitally signed [19].

During voting, all the messages from the voting from the voting console to the voting manager are due to the interactions between them. If biometric authentication is used during registration, the voting console will get a biometric template which will be decrypted and its authenticity will be verified by the registration agent's digital signature. The voting console will also ask for the voter's fingerprints with the help of a biometric derive. This kind of verification will depend on comparing the template gained from the device with the template coming from the registration agent. Any information related to the voter's biometric identification will not be sent to the voting manger to ensure voter's impersonation in the first phase. The voting console makes the registration agent signature valid using public key infrastructure and deciphers the three IDs sent by the voting manager through the agent. Then it takes the first ID from the credential and names it receipt ballot ID, which will then, be sent the voting manager to verify the voting console's signature to check if the ID is valid or not in order to prevent a reply attack. If the ID is valid, the voting manager will restore the ballot signed by the electoral authority and will replicate it to start a set with three equal ballots. Then, the manger will log the ID to trace the voter's activity in the voting phase.

The voting manager adds an initial mark in a ballot that is chosen randomly in the three ballot set for each candidate and sends the marked ballots to the voting console. Such step simplifies the voting phase in order to improve the usability of the three ballot scheme. As he voting manager has already marked the ballots, once each in the three ballot set, the voting console will also facilitate the vote verification phase and ask the voter to choose a ballot to keep as a voting receipt. Afterword, the chosen ballot will be assigned with the ID and the other two ballots will also be assigned with the two remaining IDs received from he registration agent with the voter's credentials. A backup copy of the three ballots will be masked by the voting console and each of the three ballots will be encrypted randomly with the help of the public key. Then, the voting manager will receive he encrypted ballots, sign them, and send them to a different repository. Each electronic ballot box will validate the voting manager's signature, and store it randomly after ciphering it, then reply with an acknowledge message. Then, the manager will update the information to ensure that the three ballots have finished the voting phase.

Also, the public authority public key will encrypt the unbound encrypted ballots and send them with the receipt ballot in clear text to the repository. Double encryption guarantees the voters cannot make their votes. The electoral authority will decrypt the votes using voter's respective private keys and print a summary of them and put it in a physical ballot box [20], [21].

In the storage phase, the voting electronic ballot boxes will be responsible for storing the ballots sent by the voting manager and computing the vote counting. When the elections are finished, the counting unit starts counting votes, because the election representative will provide his private key in return and the ballots will be encrypted by the election representative's public key in the first phase. This procedure takes place if the representatives' private keys are only valid for the current election and are recorded in the counting unit in order to avoid partial counting. Afterwards, the counting unit will require all ballots stored in the three repositories so that each one will fulfill the counting unit requirements.

As for partial bulletins, they will be automatically sent tot the election bulletin board database and will be published in a web page. In order to check that the election bulletin board has received and stored the election bulletins and vote-receipt list correctly, it replies with an acknowledge message to the coning unit. The counting unit will need some information, that are mainly given by the IDs provided by voting manager, to identify votes that could be published on the bulletin board. Afterwards, votes will check the votes against their receipts to make sure that their votes are correctly counted.

V. Implementation

A proof-of-concept prototype has been utilized with the help of web services and email services. As for the former, they provide standard services and security, while the latter provide standard XML schemes to define voting data structure. XML is the most powerful data storage and transfer medium on the web. In addition, manipulating XML data in SQL server could be facilitated to test database voting systems. The two most rational database manage systems used nowadays are SQL Service from Microsoft and MySQL from Apache for SQL pattern applications which are normally used in Emails. Email schemes are always organized in terms of three phases: pre-election, election a past-election.

The proposed prototype utilizes several email schemes in the pre-election phase. Its modules have been developed with the help of Apache Tomcat to run Java server pages and Apache Axis to provide SoAp (simple object access protocol) support to communicate among system entities. Any action that is relevant to any of these entities is recorded by a logging systems and any relevant information in the voting system is stored in a database. In addition, Apache Cassandra is used to store object metadata and transaction state. Cassandra is an apache open source totally free project with horizontal and vertical scalability. Horizontal scalability is the ability to add new hardware to a system without any interruption or downtime. An ideal horizontally scalable system does not require reconfiguration and supports incremental addition of hardware. Vertical scalability is the ability to add new resources in the cluster and automatically be detected and efficiently used. Cassandra allows gracefully adding commodity hardware and incrementally scaling on demand.

Therefore, with Cassandra we can add new nodes to the cluster and new resources to nodes without the need to reconfigure the e-voting system. Cassandra can be configured and optimized to manage response time versus data accuracy [22]. In addition, Cassandra offers caching on each of its nodes, making an efficient use of the data stored in the cache memory. In the proposed model, Cassandra is used along with the voting database as an ideal solution for dynamic web development and database management system that requires maximum flexibility and performance with high reliability. The proposed column family Cassandra consists of seven columns: Locks, Credentials, Votes, Services, Consumers, Mobiles, and Candidates. All column families are indexed by the national identification number in order to satisfy the row based search criteria, which is more efficient than column based rational database management alternative

On the other hand, the apache Rampart module for Axis, for example, provides support to WS security. All relevant action of each entity are recorded by the logging system using the TomCat logging facility during the voting phase and relevant information in the voting system including registration, voting and counting phases is stored in a database . An Oracle database, for example, is used for each repository and XML Xpath/XQuery is used for database operations. [23]

As for the Apache rampart, it is used to send XML-encrypted and signed massages to verify signatures. The authentication controller of registration agent, the fingerprint template checker all communicate with voters to obtain and verity their IDs that are stored according to EML 420 and 430 schemes [24].

The fingerprint pattern can be easily selected and stored in a database that the scanner queries each time it is utilized. There are two essential Boolean conditions the scanner then experiences when a individual’s print is examined. First and foremost, the print is typically searched for in a database of fingerprints, once it is found it then looks at the print to see what access features are associated with the print and compares them in attempt to ensure and accurate comparison and keep the two matched up. Regardless, a log of the event is typically stored for security purposes the size of these scanners and associated devices is another reason they become so popular recently. Today, fingerprint scanners can be found on door Knobs for room access, building access systems, build into laptop computer keyboards and on credit card sized devices. Finger printing recognition, the electronic strategies for recording and perceiving an individual biometric fingerprint, progressed generously during the most recent decade of the 2th century. Today, ID can be achieved in a few seconds with more than 95% accuracy. Thus, the utilization of computerized fingerprint ID frameworks (CFIF) that record, store, match and distinguish fingerprints is quickly expanding. CFIF can be integrated with a microcontroller based system and other peripherals to structure an installed system which is an extensive e-voting machine with fingerprint recognition system to assist practitioners in building the e-voting framework.

Therefore, Microcontroller is used to built up and control this e-voting machine. commands will be given through switches , Each switch can correspond to the vote of only one candidate, Buzzer and led will indicate that the vote has been recorded by the system, Digital display will show which out settings is active and which candidate has got vote, Finally display will show the result of the vote. Figure 5 shows a microcontroller schematic with relevant circuit diagram, including switches, keypad, LCD, and parallel port interface. The interface used to connect the Microcontroller to the hosting program on a PC, exchanging data can be done through this terminal as illustrated in figure 2.

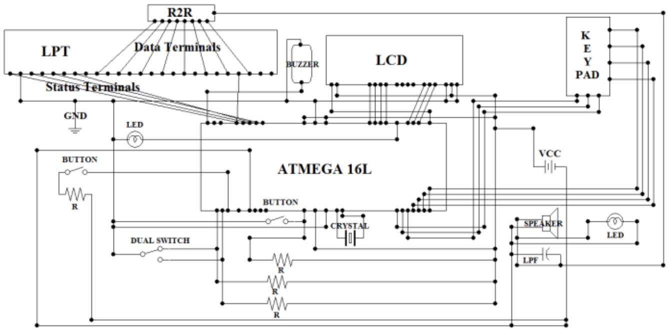

Figure 2 Circuit Diagram

The finger print technology and embedded systems are used in order to accomplish this task. This data collector is a device that collects data from the Finger print module and codes the data into a format that can be understood by the controlling unit. This system also collects information from the master device and executes their commands. The objective of the process is to develop a microcontroller based security that consists of a finger print reader, microcontroller, the interfacing unit in a manner that allows the communication between different units such as microcontroller and Finger print module while preventing any alterations or unauthorized access to the database. Therefore, the microcontroller device is designed to operate with the proposed finger print system. The device initially continuously fading the screen until the voter pushes the start button, the screen flashes, welcomes the voter, informing the microcontroller. Microcontroller then checks the PC host program connectivity, informs the host that a new voter is ready and applies new voting process that asks the voter to enter his national identification number. The finger print authenticating process will take place by sending both numbers achieved from the last stage to the finger print system using UART interface, and waiting for confirmation. After receiving authentication response information, the voter will announce his preferred choose. Just after voting, the identification, serial and voting number will be casted, encoded, and sent to the host. Then, the whole process will roll back to its initial state and waiting for a new voter registration certificate.

The user has to show his/her voter ID card in order to retrieve the biometric feature whenever he goes to the polling booth to poll his vote .This operation consumes time as the user has to check the voter ID card with the list he has and confirm it as an authorized person. To avoid this kind of problems, a finger print based voting machine was designed where user doesn’t need to carry his ID which contains his entire details. When enrolling user needs to enter his finger through optical sensor, a template is generated and stored. This data will pass to the microcontroller, the other template is received from the database and comparison takes places between the two templates. Table 1 gives the specifications of the applied finger print module.

The block diagram and circuit diagram for this implementation is shown in figure 4 where the timer programming, serial communication LPC 2148 microcontroller are all illustrated. The proposed machine contains a microcontroller (LPC 2148) with PC interface and 5v DC Power supply, fingerprint identification module, Electrically Erasable Programmable Read Only memory (EEPROM), LCD display 2x16 character matrix, and keypad. Each of these components is described in more detail below.

Table 1. Specifications of finger print module

Power	DC 3.6V-6.0V	**Interface**	UART(TTL logical level)/ USB 1.1
Working current	Typical: 100mA Peak: 150mA	**Matching Mode**	1:1 and 1:N
Baud rate	(9600*N)bps, N=1～12 (default N=6)	**Character file size**	256 bytes
Image acquiring time	<0.5s	**Template size**	512 bytes
Storage capacity	120/ 375/ 880	**Security level**	5 (1, 2, 3, 4, 5(highest))
FAR	<0.001%	**FRR**	<0.1%
Average searching time	< 0.8s (1:880)	**Window dimension**	18mm*22mm
Working environment	Temp: -10℃- +40℃	**Storage environment**	Temp: -40℃- +85℃
	RH: 40%-85%		RH: <85%
Outline Dimention	Split type	Module: 42*38*7mm Sensor:56*20*21.5mm	
	Integral type	54.5*20.6*23.8mm	

The LPC 2148 ARM processor is used for controlling the system. It controls the LCD display settings as well as the finger print module. It also receives input commands from switches and has a control unit to receive the data, performs comparison, gives command to LCD to display messages, and also displays the results. The development and implementation of design can be divided in two main parts: Hardware development and software development. Hardware implementation deals in drawing the schematic on the plane paper according to the application, testing the schematic design over the breadboard using the various IC's to find if the design meets the objective, carrying out the PCB layout of the schematic tested on breadboard, and finally preparing the board and testing the designed hardware. However, the software part deals in programming the microcontroller so that it can control the operation of the IC's used in the implementation. In the present work, Proteus design software for PCB circuit was used with the help of the MATLAB software development tool to write and compile the source code The Finger print module is an input device used for security authentication. When a finger print is entered, the system will generate a template of the finger and compare it with templates of the fingers stored in library.

The software embedded in the LPC2148 is programmed to communicate with finger print module and operates according to the commands received from user via the connected LCD display and switches. Therefore, after each successful validation, the switches add the fingerprint to the database, and the LCD displays the commands, options, and responses. The system wiring diagram is shown in Figure 3.

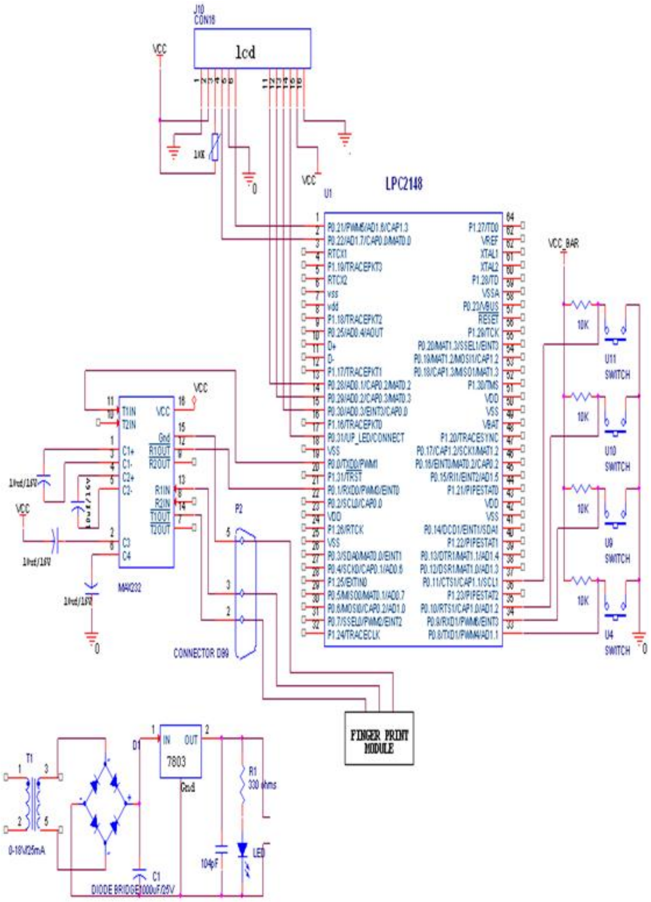

Figure 3 LPC2148 Wiring diagram

The validity of the candidate still has to be verified by the embedded security system and before the casting process take place. With this method, only the candidate who has the same finger print stored in the database will have the right to vote.

So, if the fingerprint matches with the stored template fingerprint, the corresponding message "PLEASE VOTE" will be displayed on the LCD panel. Once the voter presses the button and selects his most preferred candidate, a digital code is generated and sent to the control unit. Once the casting is complete, a message is displayed to whom they voted for, and securely sent to the website.

The LCD (16x2) panel is used to display the messages during the voting action. The response from the voters will be also displayed on the LCS screen along with any returned error messages. 16-character x 2-line Dot matrix LCD module has been widely utilized in many industrial applications, especially in the field of terminal display or embedded systems [25]. The module comprise of sufficiently good contrast, a large viewing angle, and gray level capability. All display functions are integrated into the base microcontroller unit and handled by a 2 line by 16 character alpha-numeric module. The ID manager and the credential controller provide voting credentials, as the voter registration manager implements the core of the registration agent.

The scheme defined in EML 410 is also used by the ID manager to generate IDs. The ballot manager makes the initial candidate marks in each three-ballot set in order to let the voting manager controller and the voting console interaction manager build the core of the voting manager. As for the voting console implementation, it is a web page running a JSP voting application for the voter.

Vote counting bulletins are sent for publication in the electronic election board is provided by the note repository manager and the counting unit. On one hand, EML 510 defines the counting format and on the other hand, EML 520 defines the publication formats. Secure web pages provide electronic election bulletin board public access.

It is highly recommended to place the voting console in a kiosk under external vigilance if voter coercion and vote trading were possible during the election process same as conventional elections where the voter uses the voting console safely.

VI. Design diversity

E-voting system should be applied using standard interfaces and design diversity to define the requirements of the e-voting system. Standards are quite essential for designing and implementing software components that are convenient to system application [26]. Approved software can be selected to dynamically build the e-voting system using a homologation process to determine which software is compatible with the adopted standards without using a single vendor or specific technology.

C# and ASP.NET frameworks are used to build the web applications, with the capability to serialize the data as XML, transport the data using HTTP, and de-serialize the XML back to meaningful data.

It’s a framework that makes building Web Services easy, allowing developers to focus on the application logic not the plumbing.

Whenever the client connects to a web proxy server and makes a request to the application server, the application server calls a corresponding service method in the proxy class. This method takes the name of the web service method that is being called and its arguments, and then formats them so that they can be sent as a request in a SOAP message. The web service receives this request and processes it, sending the request as a SOAP message. When the client application receives the SOAP response from the Web server, the proxy class decodes it and returns the results to the client application to access them. The proxy contains methods that can invoke either synchronous or asynchronous calls to the .NET web services. The .NET framework uses an open-source library to make asynchronous calls more appropriately

Each entity module can be made from one component that is chosen randomly from a set of previously homologated components and this strategy can also be applied to the whole system to provide better resistance against software fault. Some efforts have been made to define computer election standards, such as IEEE P-1583 voting equipment standard which defines formats and protocols for election data exchange.

This proposal should be applied in real environment to check and assess its behavior on a large scale, as it will be possible to evaluate its usability, flexibility and scalability. It can also be used in elections in large geographical areas with small deployment costs because the distributed components of which are interacting through web services. With small deployment costs as it is structured as distributed components interacting through web services. This proposal can still be used to support internet-based election even if vote trading and voter coercion are not likely to take place or even when reliable mechanisms that can deal with them are available.

VII. Conclusions and Future work

Electronic voting systems do have advantages and disadvantages that may show up in any step, like distributing, voting, collecting and counting of ballots. Moreover, potential disadvantages may include flaws or weakness in any electronic component. No matter how complex voting systems are, still different methods of election fraud are possible. In this paper we first gave a detailed description of e-voting systems and their security requirements. We then examined the robustness of the methodology employed in conducting the case studies and analyzing the results of various e-voting systems. The topics of verification and validation have increasingly been discussed in the field of computational biometrics, and many other authentication schemes. After that, we proposed an e-voting system that uses rule based techniques in order to allow the voter to interact through a web-based environment. LPC2148 microcontroller based system was used to implement the controlling e-voting system and to store fingerprints data in its flash program memory. The software embedded in the LPC2148 was programmed to communicate with finger print module and operates according to the commands received from user via the connected LCD display and biometric switches which add the fingerprint to database and return a byte of newly added ID. Apache

Cassandra code was developed to store object metadata and transaction state. These process generated has the ability to add new hardware to a system without any interruption or downtime. Full details of the proposed approach to the voting system are set out in order to ensure it impartiality, integrity, and democratic principles. In our future work, we plan to deploy and evaluate the proposed e-voting system in a real-world environment. In such environment, it might be possible to evaluate its usability, flexibility, and support elections in a large geographical area with small deployment costs as it is structured as distributed components interacting through web services.

VIII. References

[1] R. Rivest and W. Smith, "Three Voting Protocols: ThreeBallot, VAV, and Twin," Usenix/Accurate Electronic Voting Technology Workshop, 16th Usenix Security Symp., 2007

[2] M. Byrne, K. Greene, and S. Everett, "Usability of Voting Systems: Baseline Data for Paper, Punch Cards, and Lever Machines,"CHI 2007 Proc., Politics &Activism, ACM Press, vol. 1, pp. 171–180., 1997.

[3] I.Lin , M. Hwang, and C. Chang, Security enhancement for anonymous secure e-voting over a network. Computer Standards & Interfaces, 25(2):pp. 131–139., 2003

[4] Arin Sarkissian WTF is a SuperColumn? An Intro to the Cassandra Data Model. [Online].Available: http://arin.me/blog/wtf-is-a-supercolumn-cassandra-data-model, accessed on September,2014.

[5] "Programming Embedded Systems in C and C++" by Michael Barr. Publisher: O'Reilly & Associates, Inc. ISBN 1-56592-354-5. Copyright 2013.

[6] Matt Neely (2006, February). Write Mobile Agents In .NET To Roam and Interact on Your Network. [Online].Available: http://msdn.microsoft.com/en- us/magazine/cc163649.aspx, accessed on December,2014.

[7] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large-Scale Elections," Advances in Cryptology (Auscrypt 92), LNCS, vol. 718, pp. 244–251., 2007

[8] L. Norden, "The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost," Brennan Report, The Brennan Center for Justice, 2006.

[9] D.Gritzalis, Principles and requirements for a secure e-voting system. Computers & Security, 21(6):pp. 539–556, 2002.

[10] Tobias Manthey. Integrating WCF Services into UDDI based enterprise SOA. [Online].Available:

http://www.codeproject.com/Articles/32476/Integrating-WCF-Services-into-UDDI-based-enterpris, , accessed on Junary,2015.

[11] Saravanakumar and Manthey,. WCF tutorial. [Online].Available: http://wcftutorial.net/, accessed on Novamber,2014

[12] D. Jefferson et al., "Analyzing Internet Voting Security," Comm. ACM, vol. 47, no. 10, pp. 59–64, 2004

[13] M. Buchsbaum , E-voting: International Developments and Lessons Learnt. Proceedings of Workshop on Electronic Voting in Europe – Technology, Law, Politics and Society, 2004.

[14] N.Goodman, H. Pammett, J. DeBardeleben and J. Freeland, A Comparative Assessment of Electronic Voting, Carleton University Canada-Europe Transatlantic Dialogue, UK,2010.

[15] A. Rubin, Security considerations for remote electronic voting. Communications of the ACM, vol. 45 issue no. 12:pp. 39–44, December 2002.

[16] L. H. Nestas, Building Trust in Remote Internet Voting. M. Sc Thesis, Department of Informatics,University of Bergen,2010.

[17] Y. Chen, Jan, K. Jinn, Chen,L.Chin, The design of a secure anonymous internet voting system. Computers & Security,vol. 23, issue no. 54, pp. 330–337, 2004.

[18] A. Rubin, Security considerations for remote electronic voting over the Internet. The Magazine of USENIX and SAGE, vol. 1, issue no. 26, pp. 20–28, 2001.

[19] B. Bederson, , B. Lee, and R. M. Sherman, Electronic voting system usability issues. In Human Factors in Computing Systems: Proceedings of CHI, pp. 145–152., 2003

[20] J. Benaloh and D. Tuinstra, "Receipt-Free Secret-Ballot Elections," Proc. 26th Ann. ACM Symp. Theory of Computing, ACM Press, pp. 544–553, 2011

[21] B. Schneier, Applied Cryptography, 2nd ed., John Wiley &Sons, pp. 125–133, 1996

[22] Chaker Nakhli (2010, May). Cassandra's data model cheat sheet. [Online].Available: http://www.javageneration.com/?p=70, accessed on Dec.,2014.

[23] D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology (Crypto 82), Plenum, pp. 199–204, 1982.

[24] Oasis, "The Case for Using Election Markup Language (EML)," white paper, Oasis Election and Voter Services TC, 2007.

[25] W. VoteHere Inc., Network Voting Systems Standards, Public Draft 2, USA, April 2002.

[26] "Embedded Microprocessor Systems: Real World Design" by Stuart R. Ball. Publisher: ButterworthHeinemann. ISBN 0-7506-9791-1. Copyright 1996. Third edition ISBN 0-7506-7534-9. Copyright 2002.

/