Contactless E-Voting System

Shipra Varshney[1], Ashish Goel[2], Kunal Gupta[3], Shivam Adlakha[4], Shubham Gupta[5]
Dr. Akhilesh Das Gupta Institute of Technology and Management

Abstract: - In the past, people had to go to the polls to vote via the Electronic Voting System (EVM) by pressing the button of the party they wanted. But now that the recent epidemic has hit the world it is difficult for everyone to get to the polls and participate in voting. To solve this kind of situation, we have created a system where we can vote with zero humanity in social interaction. By using technologies such as machine learning and web development, people vote and vote counting can be done more efficiently and effectively, making processes easier and longer the lines in tents uncontrolled. We create a voting system with the help of hand gestures, QR code and face matching. Our system tries to keep the voting identity large and also tries to use someone who can be contacted.

Keywords:- Electronic Voting System, Zero Human to Human Contact, Epidemic.

I. INTRODUCTION

In a democracy, elections are an important step in the running of the country and they are held often. Voting prices go up over time. To save a large amount of resources and time, modern information technology can be used in elections.

Nowadays the problem of adding information technology to voting is learned in two ways. The first is electronic voting (E-voting) and the second is online voting (voting). As the years go by, experts begin to use modern information technology to meet precision, contrast, accounting, completeness, validation and privacy. In our research, we developed and implemented a program that involved QR code scanning and face recognition. With information technology, we can simplify the process and save resources and time. In line with this we use the system with accessibility, and provide demos to reduce learning difficulties in using the new system. Demos are provided in all regional languages and the voter care help line.

II. LITERATURE REVIEW

David Chaum [2] talked about the concepts of unsolicited electronic emails and digital allonyms, which we can use in the voting system. In this section, we aim to review the voting- related documents by E. At present, the voting machines used can be divided into five types [10]:

(1) Direct electronic voting: (DRE) is connected to a keyboard, touch screen, or buttons that a voter presses to vote. Counting of votes can be done very quickly. Another DRE is in doubt as to its accuracy as it does not keep voting records.

(2) Lever voting machine: Lever machine is a tool in which each oar is assigned to a specific person. The voter needs to pull the trigger to select the person they like. In this case the automatic counting of votes takes place. Its interface is not friendly enough so the voter needs training.

(3) Active voting machine: Each voter is asked to mark a circle according to his or her preference on an empty ticket, and the bells choose a black circle over each voting ticket and finally count the number of votes. This type of equipment counts tickets quickly. However, if the voter marks more than the circle, it leads to an error in the light scan

(4) Punch Card: Voter uses punching metal objects to make a hole in an empty ballot. Auto-calculation can be done, but if the voter hole is incorrect, the result may be incorrectly determined.

➢ Voting system in different countries
In recent years, E-vote was adopted in most countries. In this section, four examples are listed as follows:

(1). Japan: E-ballot was used in Japan to hold elections, such as the mayoral and mayoral elections in Okayama prefecture on June 23, 2002; election for mayor of Hiroshima city in 2003; and the 2004 Kyoto mayoral election. The survey was conducted at the end of the election. There were 81% of voters who agreed that the E-vote was credible, 56% suggested that the results of the E-vote and the ballot paper were the same but we could rely on the E-vote. The reason voters do not trust the E-voting system is: they are lonely with the abuse of the voting system and are not satisfied whether the voting is properly recorded or not.

(2) America: The US government conducts elections through a variety of practices. Each state is allowed to choose the most satisfactory way to conduct elections independently. There have been some voting issues, such as other votes not counted, or the process used to vote was disrupted during election day. [1]. It was suggested that voting should first include voting checks (VVPAT) to reduce electoral disputes during the process.

(3) Brazil: Brazil ran E-voting in 1998. After arriving at the dock, you need to show his or her ID to confirm. If he or she is found to be eligible to vote, he or she may be eligible to vote. Brazil's E-voting system delivers votes to the center quickly, leading to a faster notification of the counting of votes while voting ends.

(4) Belgium: State Parliament held elections in 2003. To help people know the E voting system, temporary training is provided. The efficiency of the counting of votes in the E voting system was better than in normal voting.

➢ Comparing different E voting systems

In addition to many developers making electronic voting machines, there are a variety of open source E-voting systems. We provide examples as follows [4,8]:

(1) AccuVote-TS: This method contains a touch screen, card reader, keyboard, earphone, and paper printer. The voter marks a loved one using him or her using a touch screen, and a printed paper tap is made to vote. The balance of policy, electoral process and technology can be seen. There are significant risks of attack as data storage occurs in the MS Access database without setting passwords.

(2) Votronic: Multilingual memory and flash are features of this system. Personal Electronic Ballot is a disk-like device to start voting machines. At the end of the election, employees use PEB to access voting records, provide PEB at the polling station or send data from the network. PEB password contains only 3 characters, so the risk of password breakage exists.

(3) Slate 3000: A voter is provided with an ID number from the staff, and arrives at the polling station to provide a PIN to the voting items. The wheelbarrow is rotated to select the candidate for baptism. Each signal is connected to a server. The counting of votes is sent to the server at each terminal via the network and saved. This program does not include data, so there is a security risk.

(4) SAVIOC: C language is used to write this program, and it is stored on disk. This application has no connection to any networks and many keys on the keyboard are disabled, preventing attackers from finding the attack method. The advantages are its simple design and low cost, but on the other hand, they require a GUI and easy use in SAVIOC.

(5) AVC Edge: Touch screen and flash memory are used in this program. There have been some issues with these machines being used in elections. For example, the vote count was incorrect, the system was interrupted when the user chose a language; he had nothing because of corruption.

➢ *E-Voting Security Issues*

External experience [9] revealed that they often encountered security problems while the electronic voting system was in operation. The source of the security issues that occurred was not only external (such as voters and invaders) but also internal (such as system developers and administrators), or simply because the legacy of certain items within the code is not valid. These errors caused the voting system to crash. Proposed solutions have been described to control these attacks [5]. For example, to avoid getting into the online voting system, we may set up our offline data transfer system. Another example is limiting the voter to enter certain details, preventing the command injection from working.

III.   SYSTEM ARCHITECTURE

We use touch screen so users can use this app with touch. The E voting system is divided into three parts: a QR scanner, a face scanner, and a voting machine. The scanned QR is first printed on a slip issued to people before the election. The QR scanner scans certain voting details from the QR, so that each QR is verified.

If the QR is compared to a QR scanner, the machine will confirm whether the QR was previously used for voting or not. In contrast, QR cannot be scanned again. Therefore, the machine will reject QR. In other cases, the voting machine will reject the unqualified QR as the voter may use his or her own QR. After this face matching it is possible to check whether the right voter is voting or someone else is voting.

After the face-to-face match is completed the voter is allowed to vote using a touch screen and a touch screen technology to cast his or her vote

➢ *Procedure*
(1) First, the voter sees the login page where he or she enters the dock id and password given to him or her.
(2) After logging in, the system displays a clear screen where the user checks the existing QR code on the slip. Details are verified in the background and if the confirmation is correct the message "success" is displayed on the screen. If verification fails the voter will contact the voter assistance service.
(3) After receiving the message of "success" the next step is to recognize the face. If the face corresponds to that stored in the database, then the voter moves on to the next step in another way, you need to contact support services.
(4) After a face-to-face identification the voter votes for the person he or she loves the most by using hand gestures and the voting process ends with a Thanksgiving message at the end.
(5) When difficulties are encountered at any stage of the voting process, a voter assistance service is located inside the voting booth to assist the voter in resolving the problem.

➢ *Vote Counting*
At the end of the election, the votes are counted using the database. After this calculation is combined to obtain the final result. Prior to the counting of votes, we verify that the counting is correct and accurate.

IV. CONCLUSION

This paper states that our implementation provides features like the voter's identity accuracy is maintained within the system. Next, details of voters are not used to break privacy of the voter. They are kept confidential. The system validates the voter's authorization to make sure that only legal voter cast the vote. In the future, to eliminate poor processes and human destruction, setting up of a E-voting system which is secure is important. It will rapidly increase the electoral procedures, make counting more efficient and use resources effectively.

REFERENCES

[1]. T. M. Carbaugh, "Secretary of State Kevin Shelley Announces Directives to Ensure Voter Confidence in Electronic Systems," California Secretary of State,2003.

[2]. D.L.Chaum,"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,*"Communications of the ACM"*, Vol.24, No.2, 1981,pp.84-88.

[3]. C. T. Chiou, "A Study of Election Reform in Taiwan: An Observation from e-Voting Experiences in Developed Countries, *"Journal of Research, Development and Evaluation Commission"*, Vol.28,No.4,2004, pp.25- 35 (in Chinese).

[4]. Compuware Corporation, "Direct Recording Electronic(DRE)Technical Security Assessment Report, "*Ohio Secretary of State*,2003".

[5]. C. A. Gaston, "A Better Way to Vote, *"Proceedings of the 38th Annual Hawaii International Conference on System Sciences"*, 2005, p.117c.

[6]. C. A. Gaston, *SAVIOC Voting Systems*, [Online], Available: http://www.savioc.com/,2007.

[7]. Internet Policy Institute, "Report of the National Workshop on Internet Voting: Issues and Research Agenda".

[8]. *Proceedings of the 2000 Annual National Conference on Digital Government Research*, 2000, pp.1-59.

[9]. A.M. Keller, A. Dechert, K. Auerbach ,D. Mertz, A. Pearl, and J.L. Hall ,"APC-based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot, *"Proceedings of the USENIX Annual Technical Conference*, U.S.A.", 2005,p.52.

[10]. T. Kohno, A. Stubblefield, A. D. Ribin, and D. S. Wallach, "Analysis of an Electronic Voting System," *IEEE Computer Society*, 2004,pp.27-40.

[11]. R. Mercuri, "A Better Ballot Box? "*IEEE Spectrum"*, Vol.39, No.10, 2002,pp.46-50.

[12]. C. H. Yang, *"Network Security: Theory and Practice"*, Key Hold Information Inc., Taipei, Taiwan, 2006 (in Chinese)