ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Review on Biometric-Secure E-Voting System for Election Process in India

[1]Gokul Ranjan V, [2]Mohammad Rashid Ansari
[1] [2]Department Of Electronics and Communication Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1] gokulranjan@Galgotiasuniversity.edu.in

Abstract: This paper proposes a multifaceted online e-voting system. The proposed system is capable of handling multiple-scale electronic ballots at the same time, e.g. presidential, regional, and parliamentary, among others. The system ensures the fairness of the election process in terms of functional and non-functional criteria. The practical criteria included in the design of the proposed system warrant well-established identification and authentication processes for the elector through the use of integrated simple biometrics. The nature of the system guarantees that no votes in favor of the candidate are lost due to the incorrect counting of the ballots, with the correct implementation of the FLAG system. Transparency of voting comes through at all points of the electoral process in order to convince the voter that his / her vote was in favor of his / her candidate of choice. In addition to its key functional properties, the proposed system is designed to satisfy a range of important non-functional requirements. Requirements for accuracy, robustness, coherence, continuity and protection are of the utmost importance. Intensive computer simulations have been performed in a number of voting conditions to check the robustness and reliability of the proposed system. Voter's number, inter-arrival voting times, malicious acts launched, etc. The results of the simulations show that the reliability and efficiency of the device is based on expectations. Such findings provide the correct criteria that would direct the decision-maker in customizing the proposed system to suit his particular voting needs.

Keywords: E-Voting, Biometric Secure System, Electronic Ballots, Election Process, Identification and Authentication Processes

INTRODUCTION

In a manual, paper-based election, voters cast their votes in order to select their candidates, simply depositing their chosen ballots in sealed boxes scattered across the electoral circuits of a given country. By the end of the election cycle, all of these boxes will be officially opened and the ballots will be counted manually in the presence of accredited representatives of all parties until the numbers are collected. This method ensures accuracy both at the time of casting and at the time of counting.Often, however, error counting occurs and, i n some cases, voters find ways to vote more than onc e, creating irregularities in the results of the final cou nt, which could, in rare cases, require a repeat of the electoral process altogether!However, in some countries, deliberately implemented manipulations of electoral votes are taking place in order to skew the outcome of the elections in favor of certain candidates. There, all such mishaps can be avoided by a carefully scrutinized election process; but when electoral votes are too high, errors can still occur. International oversight bodies are often expected to track elections in certain countries. This naturally calls for a fully automated, computerized online election process. In addition to overcoming commonly encountered electoral pitfalls, counts are made in real time that, by the end of the Election Day, the results are automatically eliminated.The election process can be easily enhanced with various features based on the demand and requirements of different countries [1]around the world. As a result of global developments in computer and telecommunications technology and the underlying infrastructure, online voting or e-voting is no longer an Indian or Western phenomenon. This high-tech way of casting a ballot has spread and spread

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

throughout the world. Through the developed countries of Europe to the developing countries[2] of Asia and India with more states and a growing population, EVoting, along with its advantages and mishaps, can now be found. The implementation[3] of electronic voting has been the biggest change to the Irish electoral system since the establishment of the state more than 80 years ago. E-Voting could soon become a global reality or a global nightmare.In addition to reliable e-Voting systems[4], there is a significant need for international standards regulating technology, software reliability and accuracy, processes and algorithms used within the system, and the testing of all hardware, software and protocols involved. Such principles would ultimately make it possible for elections to be held in any part of the world without the need for oversight bodies.

AUTHENTICITY OF THE VOTING PROCESS AND PRIVACY OF THE VOTER RIGHTS

Some factors play a major role in the voting process in any particular country. Culture itself and the underlying social factors / values largely determine the rules and regulations regulating the voting process. For countries where election results are decided by voting counts, which are counted by the direct deposit of specially designed voting cards in the voting boxes, there is a tendency for electoral votes to be misappropriated in many ways; some electors may tend to try to vote more than the number of times permitted by law for a given candidate; other electors may try to vote in li.Counterfeit/Malice is yet another issue that can jeopardize the integrity of an election process. Automation of the election process, while relying on state-of - the-art computer and ICT technology, will greatly reduce many of the factors that would hinder healthy progress in the election[5][5] process. Nevertheless, depending solely on the information technology available can only explain authentication / validation of the identity of the elector, but would still not have the capacity to prevent any effort to manipulate the voting system[6], i.e. certain electors who actually try to vote on behalf of others (fraud).Current applications, including banking apps, the safety of high-security institutions, the surveillance of passengers through border posts, among many others, are seeing an increase in the level of use of biometric technologies and tools. Biometrics is best defined as observable physiological and/or biological characteristics that can be used to verify an individual's identity. These include fingerprints, retinal and iris scanning, hand mechanics, speech patterns, facial recognition, gait recognition, DNA and other techniques. They are of interest in any field in which it is necessary to verify the true identity of the person.Originally, these methods were mainly used in limited high-security applications; however, they have now seen their uses and potential uses in a much wider range of public situations. Essentially, the biometric device has two characteristics: recognition and authentication. The former includes the identification of an individual from all biometric measurements collected in the database. The question this method aims to address is: "Who is this? “Therefore, it requires a one-to-many match. Verification requires authenticating the claimed identity of a person from his / her previously enrolled template.It requires a one-to - one contest. Verifying the identity of a person against a biometric test requires five steps that the system needs to go through. The input data is read from the person at the beginning through the reading sensors. Collected data is then sent over a network to some of the main repositories that host the biometric program. The system will then perform identity matching with standardized and/or custom matching techniques.The integration of biometric technologies can be as easy as using a single biometric system. Nevertheless, a single biometric test is always subject to security breaches if it is not adequately attended and implemented. It obviously involves security codes, fingerprints, and signatures, all of which can be spoofed when used in an unattended environment. This is significantly reduced and device security improved by the proper implementation of integrated simple biometric steps.The implementation of integrated poor biometrics leads to systems that are less complex and more reliable in terms of the level of protection obtained. There are strong single biometric measures including retinal and iris scans that are difficult, if not impossible, to break down, which usually lead to more complex systems that, in effect, slow down the underlying mechanism of biometric matching due to the amount of data processing involved. For these purposes, among others, the type of biometrics discussed in this work is of the former type, which includes the combined biometrics of the weak types.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

THE PROPOSED E-VOTING SYSTEM

This paper proposes the web-enabled e-Voting software architecture of the client / server. The architecture is shown in Figure 1, seen right around. In addition to the main functional properties of the voting system, as stated in the previous section, the e-voting system must cover a range of important non-functional requirements. Requirements for accuracy, robustness, coherence, continuity and protection are of the utmost importance. On the server side, a national database for all registered voters and candidates is maintained. The server also runs in real-time and provides backend data for the entire election cycle.On the client side, two additional specifications are required. To order to reduce the traffic rate on the network connections, a local client-side database is necessary to host the data relating to the local voting center. This DB is a rather dynamic one, in the sense that the data stored in its tables that differ over the election period. The scale of the local DB at any voting center is only a small fraction of the regional DB on the server side. The use of the local DB improves the performance of the voting process. Nonetheless, this method introduces a synchronization issue that will be discussed later in this segment. The second requirement is consistency in the voting process.The elector has no input into how his / her vote is interpreted and/or counted. In a paper-based election, the elector fills the ballot and drops the candidate himself into a sealed box. Votes shall be counted in the presence of candidates or their members. The elector is certain that his / her vote with his / her vote is in the right box. Of course, confusion in the shape of the ballot (as was the case in the US presidential election in 2000) can make clarity somewhat misleading. In an electronic version, the voter trusts the computer hardware, software and network infrastructure that manages his / her vote.Hence, the e-Voting [7]system in its broadest form may render the process a non-transparent one.

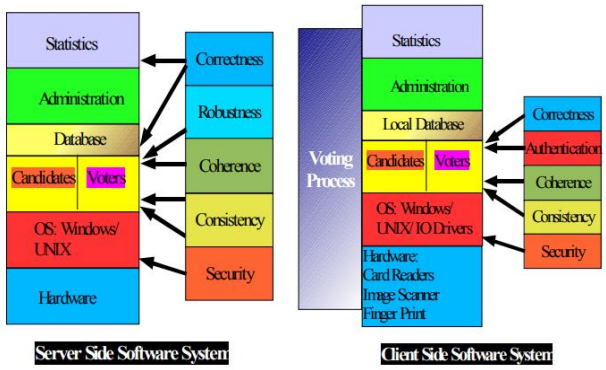

Figure 1: Server and Client Side Software System

It has suggested a two-sided approach to the transparency problem. On the one hand, the machine prints a hard copy of the vote cast by the elector. The elector shall check the authenticity of his or her vote and keep a copy of his or her records. On the other hand, the system generates another copy of the vote with a new unique key identifier; the name and identity of the elector are secret. This copy is kept in a protected box and can be used later to verify the validity of the votes as stored in the final destination of the DB. This copy side can be printed as a bar code that can be quickly scanned and read automatically.Only a randomly selected set of these copies must be tested. This two-sided method provides consistency by providing evidence of the accuracy of how the cast vote is entered into the system and how it is eventually processed in the DB tables. One of the challenges facing the e-Voting system is to ensure that no voter can impersonate another voter and that no voter can vote more than once. The identification accompanied by an authentication process was used in the proposed system.The electoral record provides a biometric profile of the elector. The system of fingerprint authentication was used in this analysis[8]. The elector will be disqualified if his / her fingerprints do not match those held. To order to reduce false refusals, a number of copies of his / her fingerprints taken at different time intervals can be stored for each voter. Fingerprints are processed as encoded text in order to reduce the amount of storage the images consume. This dual method will ensure that no one can wrongly impersonate the elector.To avoid two or more votes per elector, use the "voting status flag" in the register of electors. This flag is set to the FALSE flag. The voting status flag is set to TRUE in the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

central DB whenever the identity of the elector is checked (before authentication). If the authentication fails, the flag will be reset to FALSE. If the elector leaves the station without having completed a ballot, the flag is also reset to FALSE; thereby giving the elector another chance to try again to cast his / her vote. If the voting process is completed by the candidate, the flag remains set to TRUE.Note that even if the result of the vote is not committed to the central DB in due time, the flag in the central register of the elector is set to TRUE, thus eliminating the possibility of another attempt to vote by the same elector or by someone holding a counterfeit ID card. This requires that, whenever an elector's record is accessed for identification, even when the record is found at the local DB, the flag on the central record must be checked.If TRUE has already been set, the voter will be denied access and his / her attempt will fail. If two people carrying the same ID card (one is real while the other is counterfeit) try to vote at the same time, the first to access the record will set the flag to TRUE, load the record and prevent the other from accessing the record. Of course, if a person with a counterfeit card obtains a record, the vote cast will fail at the next authentication point. It is likely that the record will be loaded into two different voting canters due to a block switch from the central DB to the local DB.When an elector tries to access the record at any of the stations, the client checks the main record flag. If set to TRUE, access is denied; otherwise, the flag is set to TRUE and access is granted. Note that simultaneous requests for the same record will be synchronized with the DB query serialization process (only one query can access any table at any given time). However, this mandatory flag check in the central DB will add extra overhead to the network. This overhead will be further measured in the simulator, but will not be recorded in this study due to time and space constraints.Another synchronization resolution is required when a vote is to be registered in the record of a candidate. If a candidate is chosen by a number of voters at the same time, a certain assignment plan must be drawn up so that all votes are registered (no misses) and added to the candidate's record. Again, use the "count" flag / mutex to record the candidate. The count flag is initially set to false [9]. Once the record is chosen by the voter, the flag is set to TRUE before the record count is updated, and the flag is reset to FALSE. Both votes for the same candidate will be kept until the flag is reset to FALSE. A copy of the vote will be printed only when the vote is successful and the candidate's record is updated.This criterion, initially made for transparency purposes, offers a final test for the consistency and validity of the procedure, in particular in the case of thread hung-ups. The precision and consistency of the device using the two flag attributes is demonstrated (physically present) in the current simulation test. When the flags were switched off, there were several breaches and problems with accuracy. They were remedied when the flag attributes were switched on. The voting process, as discussed above, is shown in the flow diagram in Figure 2a and 2b.Voting canters are scattered across the country. One or more polling stations may share a local database. That voting station in the voting center is fitted with a card reader, a fingerprint scanner, a touch screen and a multimedia subsystem. The multimedia subsystem is used for people with special needs (physically challenged) such as the blind and those with difficulties reading or hearing pictures, texts or sounds. The proposed system is capable of handling multiple-scale electronic ballots at the same time, e.g. presidential, local, parliamentary and other. Nevertheless, the simulation setting in this study is limited to a single voting area.

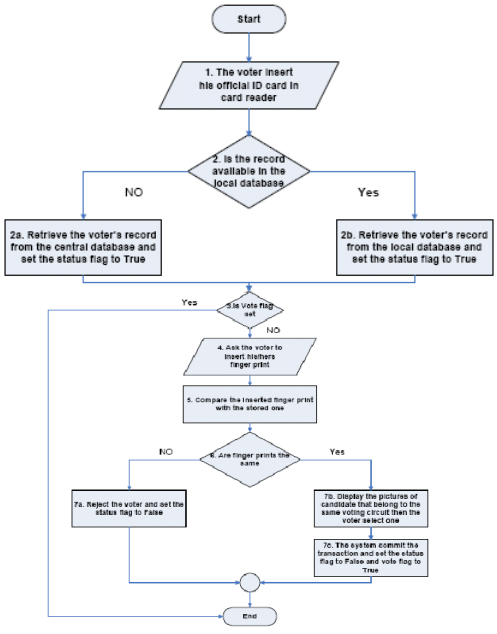

Figure 2: Voting Process Flow Chart

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

SIMULATION RESULTS

A simulation model has been created to study and analyse the actions of the new electronic voting system. Simulation is also useful for providing proper instructions on the design of the e-Voting system in terms of server specifications, network bandwidth, voting stations, and the like. The simulation environment contains an Oracle database system for electors and candidates. In addition to personal identification information, the documents contain authentication information and the location of the elector and/or the candidate. The simulator also contains modules that simulate the presence of voters in the canters and the voting process itself. The simulator allows an elector to cast a vote at any polling station, regardless of its actual polling district (locality). This is one of the main advantages of the e-Voting system. Voters arrive at a polling station according to the Poisson arrival method, and the time interval separating the different arrivals is modelled as an exponential random variable. The estimated maximum number of electors arriving at the polling station is determined by the program admin a priori; this is explained by the fact that the number of electors in the polling district is calculated beforehand. Every voter would swipe his / her official identification card through a magnetic card reader, at which point he / she would be prompted to print his / her finger at the end of which a candidate's screen would appear showing photos of candidates in the electoral circuit of the elector. If the voter's record indicates other necessary types of display / presentation (as contained in the details on the voter's ID card), such as sound, then these forms will be used instead of the candidate image / s. The elector would choose his / her candidate of choice by touching the image of his / her candidate of choice. The system also allows the vote to be cast by audio means for those voters with special needs. At this point, the voting process for the chosen candidate is complete and the number of electors is counted in favor of the chosen candidate. In the simulator, the speed of the voting process is controlled by a variety of limiting factors: first, the change in the length of the queue had a detrimental effect on the rate at which the electors were able to cast their votes. Second, the system's response time, right from the moment the elector enters the voting center until the cast vote is counted in favor of one candidate or another, is adversely affected by the server end of the database answer. Second, the network response time, i.e. the available network bandwidth, is very high when calculating the transaction time per elector. In our simulations and for the specific purpose of this paper, it has been presumed that the bandwidth of the network is infinite.Nonetheless, using the client / server model with built-in local DB infrastructure, it anticipates a minimal impact of the network constraints on the overall process. Although a fairly large number of simulations of the proposed voting system have been carried out, taking the number of electors over the sample range from 5000 to 20,000 per polling center and ending at 20,000 per polling center, and due to the limited space of this paper, our evaluation of the model is limited to 5,000 voters per polling center as our case study. The total number of voters in a given center is fairly constant, as it depends mostly on people living in the vicinity of a polling station. So it decided to set the number of voters at the polling station in the simulator. In practice, this number may differ by a small percentage due to the fact that people will be allowed to vote at any other center they choose for convenience of voting, in particular those who live in townships outside their voting districts, or those who cast their votes through embassies outside their home country. The other parameters that affect the outcome of the simulation are the number of voters (voter density) arriving simultaneously at the station and the average time between the two consecutive arrivals. Inter-arrival time is modelled as an Exponential random process with an average inter-arrival time (μ). Remember that the method will be more challenging for large λ and small μ. The length of the queue will grow indefinitely, and the voters must wait in-line forever. Note that this result is obtained from voters casting their votes at one polling station. One way to solve this problem is by adding one or more stations, where the voters are divided equally between the stations. Essentially, each station would receive voters at a rate of 5 to 5 instead of 10. Keeping the same inter-arrival rate, it observe that the system becomes stable and the queue length and waiting Time are fairly finite (Figure 3). Note that the time of human response, e.g. walking, typing, and finding out what to do, and so on, was not included in the simulations. Therefore, the total waiting time in the figures represents a system-restricted waiting time due to queuing activities. The findings, as shown, are averaged over three program runs to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

minimize any bias in the simulation performance. It is well known that on Elections Day, turnout varies over time. In the early hours, the turnout is usually low, then picks up about noon, then slows down. Occasionally, a large number of voter outbursts occur towards the end of the voting period. Figure 3 indicates the machine actions of low voter turnout with λ=2 and μ=2. The situation where the number of electors arrives in small numbers, but the movement of electors is rather rapid (λ=2 and μ=10). The average queue length is 15, while the maximum waiting time is 3.2 seconds. Remember that it is possible to control the length of the queue and the average waiting time in the queue. When the voters burst volume, i.e. the voter density is that, adding one or more polling stations will ease the problem. When the burst rate is high, i.e. if voters arrive at a faster rate, the line-up of voters outside the voting center will ease the pressure on the electronic voting system. Remember that voters may continue to experience long waiting times; however, machine response time may continue to be reasonable and indefinite postponement or starvation may be avoided.

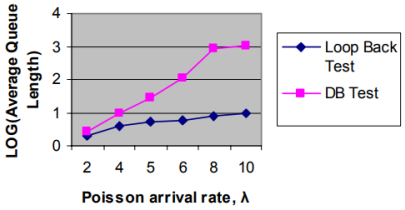

Figure 3: Log Average Queue Length vs. Arrival Rate Parameter (Λ)

Finally, it analysed the various simulations it obtained in order to verify the robustness / susceptibility of our proposed evolutionary system. From the figure it is noted that the DB response, provided that it was running a live DB in our simulations, plays a rather important role in determining the growth of the queue length; where the queue length stayed at acceptable levels when it emulated the situation of the ZERO DB response time (Loop Back test), including the live DB access (DB Test) test, showed that the queue length began to increase exponentially.

SYSTEM SUSCEPTIBILITY AND ISSUES IN CYBER SECURITY

Information security is of great importance to our program. There is an intrinsic need to protect all contact between clients and their local DB servers. Communications between the local DB(s) and the central DB server must also be secured. The machine may use the Internet or any other public network to connect to local servers or clients. Thus, the system is vulnerable to many attacks.

- Interruption, delay, refusal of receipt or denial of service; in such cases, assets and information are made unavailable.
- Interception or snooping; in this case, an unauthorized party will be able to access private sensitive information by browsing through files, eavesdropping or reading communications.
- Modification or alteration; in this case, the information in transit shall be changed or stored for later access by an unauthorized party.
- Manufacturing, masquerading, or spoofing; in this case, an attacker can inject false information into the system and make it look like it came from a legitimate entity.
- Repudiation of origin; this is a false denial that a person has done (send / create) something.
- There are also other potential threats, such as: replay attacks, denial of service and session hi-jack. To achieve security assurance, it is necessary to ensure that all of the following objectives are met: • Confidentiality: keeping data and resources secret or hidden.
- Integrity: Ensuring approved modifications; requires accuracy and reliability. May also refer to: quality of data and integrity of origin.
- High Availability: Provide permitted access to data and services where necessary.
- Accountability: Ensure that the action of the entity can be traced solely to that entity.
- Non-repudiation: Preventing false denial of an act.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

In order to achieve the desired level of safety in our system, it proposes the use of Kerberos. Kerberos is a computer network protocol that provides a high level of security for parties who communicate over non-secure networks and enables them to communicate in a secure manner. Kerberos was originally proposed to researchers at the Massachusetts Institute of Technology (MIT). It has been used by many systems around the world and has proved to be secure and reliable. Kerberos will require mutual authentication for clients and servers over unsafe connections. It also provides protection against eavesdropping and replaying attacks.It believe that it will provide the best option to immune our system against all the aforementioned attacks.

Kerberos allows clients and servers to be closely synchronized in time. The method shown in Figure 3 suggests the use of a double Kerberos protocol. The first will be between clients and their local DB server. The second is between the local DB servers and the main DB. The reason why it proposes the use of double Kerberos is to achieve a higher level of security and to completely separate the central server from its clients. With Kerberos, each local server will be separated into an authentication server (AS) and a service server (SS); in our case, a local DB server.Typically, the shared code or key is extracted from the user name and password of the user logging in to the client computer. After the AS has verified the identity of the client, it will provide the client with a ticket. This ticket will be used by the client to request additional tickets from the AS to the SS (our local DB servers). These tickets can be used to get SS services. If the local servers need to contact the central server, the second Kerberos protocol must be used.In this case, the local servers act as clients on the central server and the same process is repeated. However, one point of concern remains when Kerberos is used. Because Authentication is made to rely solely on the Authentication Server, the AS is a single point of failure. Once the authentication server is down, contact between the client and the SS is stopped. It results in the failure of the current voting process and, as a result, an inevitable rise in the queue length of the electorate in the affected sectors. To mitigate this effect, a redundant AS can be set up in stand-by mode, which can take over the main AS in the event of an outage.

CONCLUSIONS

In this paper, an online e-voting system was proposed that could address all previous issues encountered in the conventional (manual) voting system. The new system keeps voting statistics in real time, while maintaining the integrity of the voting process from the moment the elector continues to cast his / her vote until the cast vote is recorded in favor of the chosen candidate in the globally allocated DB repository. By maintaining full transparency in voting, both at the level of the voter and at the level of the system, the proposed system is capable of denying access to any illegitimate voter / s, preventing multiple votes by the same voter, and blocking any types of malice that have been implemented that would adversely affect them.In addition, the new voting system caters to the needs of physically challenged voters by offering unique digital services that would make voting simpler for the convenience of the voter. Thus carefully monitoring the security needs of the system, at all stages of the voting process, the design of the system often meets a number of important functional and non-functional specifications that are adequately addressed in every aspect of the system design, including hardware, software, and the underlying encryption and network infrastructure. The simulation results of the program, when running a live DB backend server, show a number of important factors that should be carefully evaluated by the party implementing a system like this for any sort of election operation prior to its final implementation.

Such considerations include the number of polling stations required at any polling station, as illustrated in the voting needs of the polling district, the need for the network bandwidth of the polling station, the size of the local DB to meet the needs of the polling district, among others.The method, by means of these simulations, ha s shown robustness and sustained efficiency in the pr evention of multiple votes by the same voter and in th e maintenance of internal system audits that would w arrant no missing votes, per candidate, in the voting p rocess.With the use of the e-voting system, as suggested in this paper, many of the problems that have threatened conventional voting systems in the past are likely to be addressed by ensuring peace of mind for both voters and election candidates. It is expected that with a well-managed / designed e-voting system, countries that have long been

monitored by foreign monitoring bodies, though performing their own electoral processes, will soon be able to operate on their own and still gain the democratic independence they have longed for.

REFERENCES

[1] D. E. W. Sanjay Kumar, "ANALYSIS OF ELECTRONIC VOTING SYSTEM IN VARIOUS COUNTRIES," *Int. J. Comput. Sci. Eng.*, 2011.

[2] I. N. D. Inuwa Ibrahim, I. Inuwa, and N. D. Oye, "The impact of E-Voting in developing countries: Focus in Nigeria," *Int. J. Pure Appl. Sci. Technol.*, 2015.

[3] A. Hartami and P. W. Handayani, "The critical success factors of e-voting implementation in indonesian local elections: The case of jembrana regency election," in *Proceedings of the European Conference on e-Government, ECEG*, 2012.

[4] S. Wolchok *et al.*, "Security analysis of India's electronic voting machines," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2010.

[5] G. S. Matharu, A. Mishra, and P. Chhikara, "CIEVS: A cloud-based framework to modernize the Indian election voting system," in *2014 IEEE International Conference on Computational Intelligence and Computing Research, IEEE ICCIC 2014*, 2015.

[6] R. Bhuvanapriya, S. Rozil Banu, P. Sivapriya, and V. K. G. Kalaiselvi, "Smart voting," in *Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies, ICCCT 2017*, 2017.

[7] W. Han, D. Zheng, and K. F. Chen, "Filling the gap between voters and cryptography in e-voting," *J. Shanghai Jiaotong Univ.*, 2009.

[8] S. Kumar *et al.*, "Analysis of Electronic Voting," *Int. J. Comput. Sci. Eng. - IJCSE*, 2011.

[9] M. T. I. Ziad, A. Al-Anwar, Y. Alkabani, M. W. El-Kharashi, and H. Bedour, "E-voting attacks and countermeasures," in *Proceedings - 2014 IEEE 28th International Conference on Advanced Information Networking and Applications Workshops, IEEE WAINA 2014*, 2014.

[10] Vishal Jain, Mahesh Kumar Madan, "Information Retrieval through Multi-Agent System with Data Mining in Cloud Computing", International Journal of Computer Technology and Applications (IJCTA) Volume 3 Issue 1, January-February 2012, page no. 62-66, having ISSN 2229-6093 .

[11] Vishal Jain, Mahesh Kumar Madan, "Multi Agent Driven Data Mining for Knowledge Discovery in Cloud Computing", International Journal of Computer Science & Information Technology Research Excellence Vol. 2, Issue 1, Jan-Feb 2012, page no. 65-69, having ISSN 2250-2734.

[12] Kavita Arora, Dr. Kavita, Dr. Vishal Jain. (2020). A Study On Attacks In Mobile Ad-Hoc Networks. International Journal of Advanced Science and Technology, 29(8s), 279 - 289. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/10502

[13] J Ganeshkumar, N Rajesh, J Elavarasan, M Sarmila, S Balamurugan, "A Survey on Decentralized Access Control Strategies for Data Stored in Clouds", International Journal of Innovative Research in Computer and Communication Engineering, 2015

[14] J Ganeshkumar, N Rajesh, J Elavarasan, M Sarmila, S Balamurugan, "Investigations on Decentralized Access Control Strategies for Anonymous Authentication of Data Stored In Clouds", International Journal of Innovative Research in Computer and Communication Engineering, 2015

[15] VM Prabhakaran, S Balamurugan, S Charanyaa, "Sequence Flow Modelling for Efficient Protection of Personal Health Records (PHRs) in Cloud", International Journal of Innovative Research in Computer and Communication Engineering, 2015