iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4397

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Real-Time Voting System using Biometrics

Nitin chavhan[1], Ajit Deshmukh[2], Simran Bhat[3], Shilpa Kukade[4], Prof. Majushree Mahajan[5]
[1, 2, 3, 4] *Students, Department of Computer Engineering, GHRCEM, Wagholi, Pune, India.*
[5]*Assistant Professor, Department of Computer Engineering, GHRCEM, Wagholi, Pune, India.*

Abstract: "Realtime Electronic Voting System" is based on the online services like where a voter can cast his/her voting right online without any difficulties. In this system people who have citizenship of India and whose age is above 18 years of age can cast vote online without going to any polling booth. The election commission of India has maintained a database server in which all the names of the voter with complete information is stored. The voter has to fill a registration form to register himself with the help of a USER ID and DYNAMIC PASSWORD. This information is checked by the database server which has already all the information about the voter. If conditions are wrong then that entry will be discarded and he would not be able to vote. This system will be helpful for voters who live far away from their home city and want to cast their vote from anywhere in India. The main advantage of In this machine voting is that the percentage of voting will increase. It decreases the cost and time and also increase the voting process and hence it will be more secure.
Keywords: Online E-voting, Distance voting, Finger Scanner Module, Database server, Verification.

I. INTRODUCTION

Real-time Electronic Voting System Machine is a machine that is used to store the votes in place of ballot papers and boxes were used in traditional voting system.

Voting's are of two types: Distance voting and Presence voting. In distance voting voter cast his or her vote from a place other than a polling booth i.e. via mail or internet voting. In present voting a voter can cast his vote at a polling booth. To increase the efficiency and security of voting proccess, computerized voting systems were developed.

Protecting the voted data is the main challenge of electronic voting system, hence designing a secure e-voting system is very important. Therefore security is the main aim of computerized e-voting system where election data collection is recorded, stored and processed as digital information.

There are different levels of e-voting security. Online voting process verification can be done with fingerprint sensing at the time of voting at voting booth.

To make the system more secure we are making use of the Adhar Card Number which is unique for each person. This entire system can be implemented using login which requires the Name of the candidate, Adhar Card Number and the fingerprint scan. Valid voters will have their name, fingerprint and other details in the government database server for each state district wise. This will therefore ensure with the help of unique Aadhar card number and fingerprint scanner only legitimate users can cast their vote. Online voting system contains:

1) Voters' information in database.
2) Voters name with Id.
3) Voters fingerprint scan.
4) Voters vote in the database.

A. E-Voting Process

1) *How Does a Fingerprint Optical Scanner Work?:* A fingerprint scanner has two basic applications -- it needs to take an image of your finger perfectly, and it needs to determine whether the pattern of ridges and valleys in this image matches to that of pre-scanned images. Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No fingerprint image are ever saved, It can available series of numbers (binary code), which is used to verify. No one can duplicate your fingerprints because the algorithm cannot be reconverted to an image.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

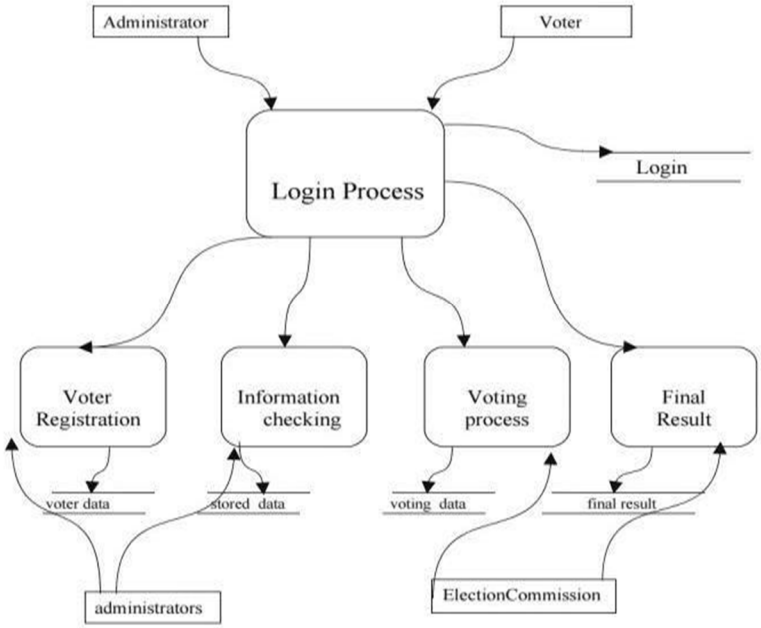


Fig.1: Login Process

B. Advantages of Fingerprint Authentication

There are several ways an electronic time clock system can verify that somebody is who they say they are. Most systems are looking for one or more of the following:

1) What you have ?
2) What you know ?
3) Who you are ?

You need some sort of "token," such as an identity card with a magnetic strip to get past a "what you have" system, A "what you know" system requires you to enter a password.

A "who you are" the system can be required for physical evidences that you are who you say you are a specific fingerprint pattern on the available system.

C. "Who you are" have a number of advantages, They are follows:

1) Fingerprints cannot be easily faked than identity cards.
2) Guessing a fingerprint pattern is impossible like you can think and guess a password of any system.
3) You cannot misplace your finger, like you can misplace an id cards any ware.
4) You can't forget your fingerprints like you can forget or change password of any system.

II. LITERATURE SURVEY

All computer scientists who have done work in or are interested in electronic vot- ing seem to agree that online voting does not meet the requirements for public elec- tions and that the current widely-developed voting systems need improvement. In IndiafirstelectionusingelectronicvotingwasheldfromApril20toMay, 2004.The recent EVM have also implemented real time clock and date-time fa-cility which authorize them to record the real time and date whenever a key is pushed. In recent years, a considerable number of countries has adopted E-voting for their ocial elec- tions. These countries include America, Belgium, Japan, and Brazil.

The work stated that owing to the need to increase public confidence, various states are increasingly considering electronic voting systems that provide voter ver- ified paper records. In the work, an analysis and evaluation of New Jerseys criteria againstseveraldifferente-votingmachinetypesrevealedpotentialthreatsandpossi- ble solutions on privacy, security, and performance issues. The authors in propose a secure electronic voting protocol that is suitable for large scale voting over the Inter- net. In their

work, the protocol allows a voter to cast his or her ballot anonymously, by exchanging untraceable yet authentic messages. The protocol ensures that only eligible voters are able to cast votes, a voter is able to cast only one vote, a voter is able to verify that his or her vote is counted in the final tally, nobody, other than the voter, is able to link a cast vote with a voter, and if a voter decides not to cast a vote, nobody is able to cast a fraudulent vote in place of the voter. The following assumptions were made in the context of this protocol viz.

III.RELATED WORK

Many scientists who have done work in e-electronic voting seem to agree that online e-voting system does not fulfill the demands for public elections and that the current widely-deployed voting systems need improvement. In India first election using electronic voting was held from April 20 to May 10, 2004. Throughout history, election fraud has occurred in many electoral processes from which experience shows that the manual voting process is major source of such vices and violence in many democratic countries. In recent years, a considerable number of countries has adopted E-voting for their official elections. These countries include: America, Japan and Brazil, etc.

IV.MTHODOLOGY

The knowledge based (password) and token based (key or card) security systems are prone to compromise because passwords can be forgotten or guessed and cards can be lost or stolen. Biometrics which refers to automatic identification of a person based on his or her distinguishing characteristics, is inherently more secure than knowledge based or token based identification.

Our fingerprint-based biometric e-voting system is essentially a pattern recognition system a person may be authenticate of his/her fingerprint. The enrolment module is responsible for registering and verify individuals in the biometric system database (system DB). During the enrolment checking phase, the available fingerprint of an individual person is acquired by a fingerprint scanner to produce raw digital representation.

The steps involved in fingerprint recognition are explained as follows:

A. Step 1: Fingerprint Acquisition

On the basis of collection procedure, fingerprint images can be classified into three types, namely, rolled, plain and latent. Generating plain fingerprints images are acquired by pressing the fingertip on to a available flat surface. Latent fingerprints are usually storing from crime scenes, in which the print is lifted and object must be surfaces that were by mistake touched or handled.

A fingerprint image is classified based on the mode of acquisition as:

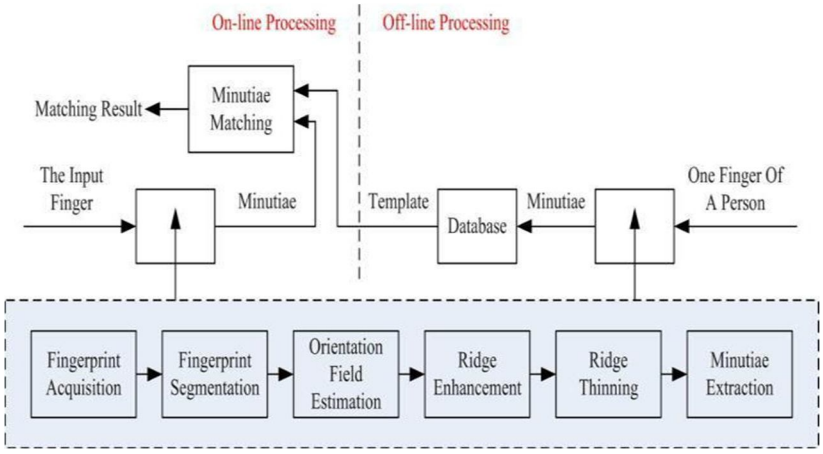


Fig. 2: Fingerprint Acquisition

1) *Offline image*: A fingerprint image assumption was performed by using **"**ink-technique**"**: the finger can spread with black ink and pressed on paper card; the paper card was scanned by using a common paper card-scanner, producing the final digital image as per need.
2) *Live scan image:* A digital image is directly obtained by placing the finger on the surface of a fingerprint reader. No ink is required in this method. The unique significant characteristics of fingerprint the readers can capturing the area their resolution.

B. Step 2: Fingerprint Segmentation

An automatic fingerprint recognition system is the important step in segmentation of fingerprint images. A captured fingerprint image are two types, which are called the foreground and the background. The foreground is the component that originated from the contact of a fingertip with the sensor. The noisy area at the borders of the image is called the background. The task of the fingerprint segmentation algorithm is to decide which part of the image belongs to the foreground and which part to the background. A fingerprint segmentation goal was discard the background, reduce the minimum number of false features, and thus improve maximum matching accuracy of system.

C. Step 3: Orientation Field Estimation

By considering a fingerprint as a texture pattern can be utilize the both fingerprint orientation and frequency information to segment latent. Most of the approaches proposed in the literature for singularity detection operate on the fingerprint orientation image. The orientation of the image represents the property of the available fingerprint images and also defines the invariant coordinates for available ridges. By viewing a fingerprint image as an oriented texture, a number of methods have been proposed to estimate the orientation field of fingerprint images.

D. Step 4: Ridge Enhancement

Uniqueness of the fingerprint is exclusively depended on the local ridge and relationships. The two most prominent ridge characteristics called minutiae are

Fig 3: Ridge Enhancement

1) *Ridge ending:* A ridge ending is defined as the point where a ridge ends abruptly.
2) *Ridge bifurcation:* A ridge bifurcation is defined as the point where a ridge forks diverges into branch ridges.

E. Step 5: Ridge Thinning:

The final image can be enhancement step typically involving to performing prior to extraction is thinning. Morphological operation of thinning that erodes successively the foreground pixels until and one pixel is wide. A standard thinning algorithm is employed, which performs the thinning operation using two sub-iterations. The examining of an pixel each pixel sub-iteration begins by examining the neighbourhood of each and every pixel in the binary image, and based on set of the pixels-deletion criteria, it checks whether the pixel can be deleted or not. These sub-iterations continue until no more pixels can be deleted. This skeleton image is then after used in the generating extraction of minutiae.

F. Step 6: Minutiae Extraction

Almost maximum number of fingerprint features, minutia point features. The minutiae features can be representation of reducing the problem of complex fingerprint recognition and point to the pattern matching problem. Finally, a simple image scan allows the detection of pixels that correspond to minutiae through the pixel-wise Computation of crossing number. There are maximum number of minutiae extraction methods available . We can classify these methods broadly into two types .Those that work on binarized fingerprint images. Those that work directly on gray -scale fingerprint images.

G. Step 7: Minutiae Matching

Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. The alignment can be find between template and input minutiae sets of that results in the available minutiae pairings. This is the most popular and widely used in commercial applications, because of its good performance and low computation time, especially for good quality images.

V. PROPOSED WORK

A. Design Considerations

The proposed system is focused on improving the existing system by making voting available to all registered voter who cannot be present in home city during election period. First voter need to register and give valid reason for his/her absence in city during election time. The authorized officials will then have to create a new record in database for that voter. Voter must give all required personal details to register for this system. Special record to be entered in database will be voters fingerprint. Id passwords are not required as voter will only need his/her Unique ID/Voter ID and fingerprint later to login. This system will bring increase in overall percentage of voting which will help to choose best leader. Following diagram show process of voting:

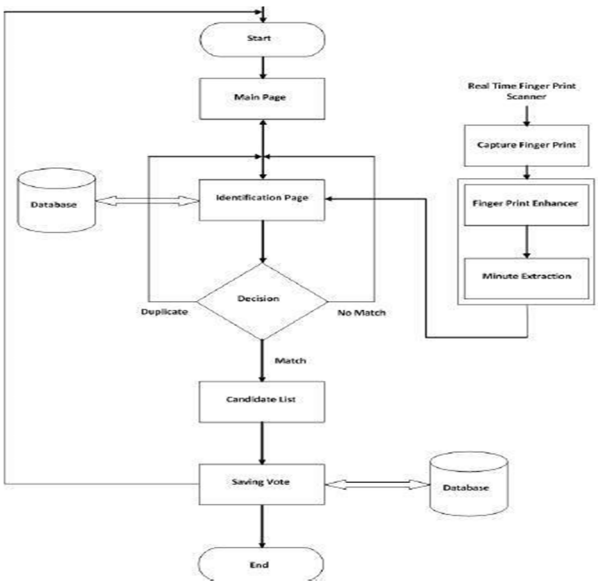


Fig. 4: Voting Process

B. Hardware Used

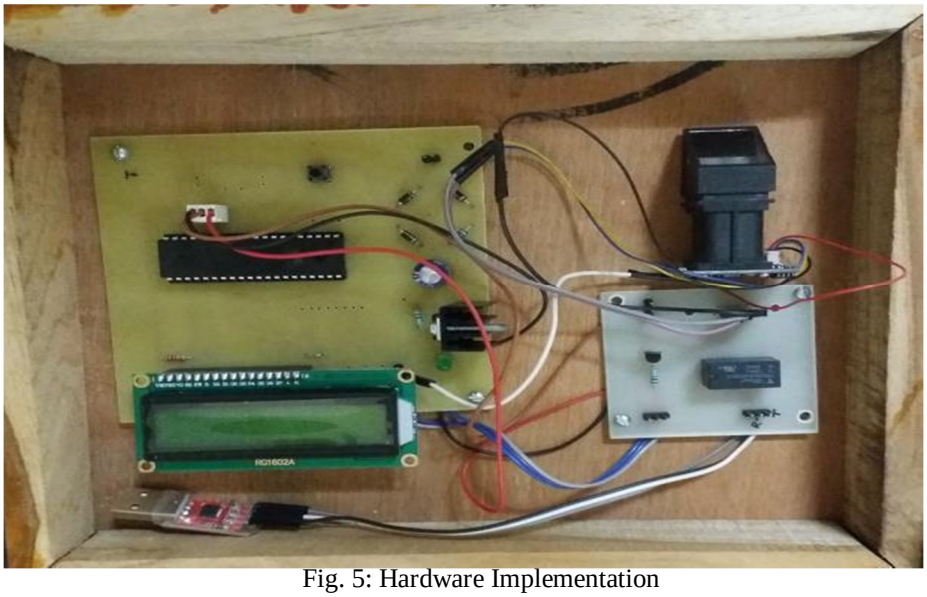


Fig. 5: Hardware Implementation

C. Software Implementation

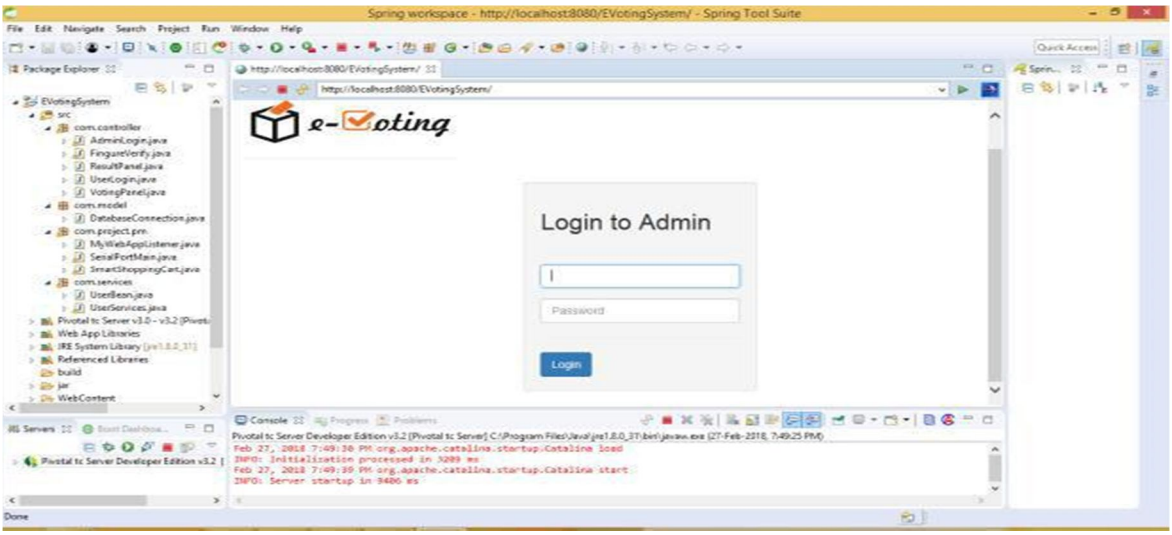


Fig. 6: Software Implementation

VI. CONCLUSIONS

Paper voting based Election are never perfect, even in the world of paper ballots put into the boxes and lever machines read the outputs of dials. Today, volunteers are faced with electronic voting machines manufactured and maintained by private firms that have software that hasn't been rigorously tested and source code that is not available to experts of all political persuasions.

In this e-voting system will manage the Voter's information like voters Aadhaar card and voting card details, by which voter can login and use his voting rights. The system will incorporate with all features of voting system. The machine will have faster tabulation of results, improved accessibility, greater efficiency, lesser cost rate, more accuracy, and lower risk of human and mechanical errors. Voter's detail will be stored in database after registration. By voting system percentage of voting increases. It decreases the cost and time of voting process.

Future enhancements focused to provide online e-voting with some authentication parameters like facial recognition. In case of usage offline e-voting authentication processes like, Finger Vein and iris matching and detection can be done.

REFERENCES

[1] Jean Bacon,Fellow, DavidEyers, Thomas F. J.-M. Pasquier, Jatinder Singh, Ioannis Papagiannis and Peter Pietzuch, "Biometrics using Electronic Voting System with Embedded Security", IEEE Transactions on Networkand Service Management, VOL. 11, NO. 1, MARCH 2014.

[2] Reem Abdelkader and Moustafa Youssef, "UVote: A Ubiquitous E-Voting System", 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing.

[3] Claudia Garcya-Zamora, Francisco RodriguezHenriquez, Daniel Ortiz-Arroyo, "SELES: An e-Voting System for Medium Scale Online Elections," enc, pp.50-57, Sixth Mexican International Conference on Computer Science (ENC'05), 2005.

[4] Hsing-Chung Chen and Rini Deviani, "A Secure E- Voting System Based on RSA Time-Lock PuzzleMechanism", 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications.

[5] Balkrushna Bhagwatrao Kharmate, Shahebaz Shaikh, Prashant Ravindra Kangane, Tushar Anant Lad, Prof. Ashvini Y. Bhamare, "A Survey on Smart E-Voting System Based On Fingerprint Recognition", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 9, September 2015.

[6] Alaguvel.R, Gnanavel.G2, Jagadhambal.K , "Biometrics using Electronic Voting System with Embedded Security", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.

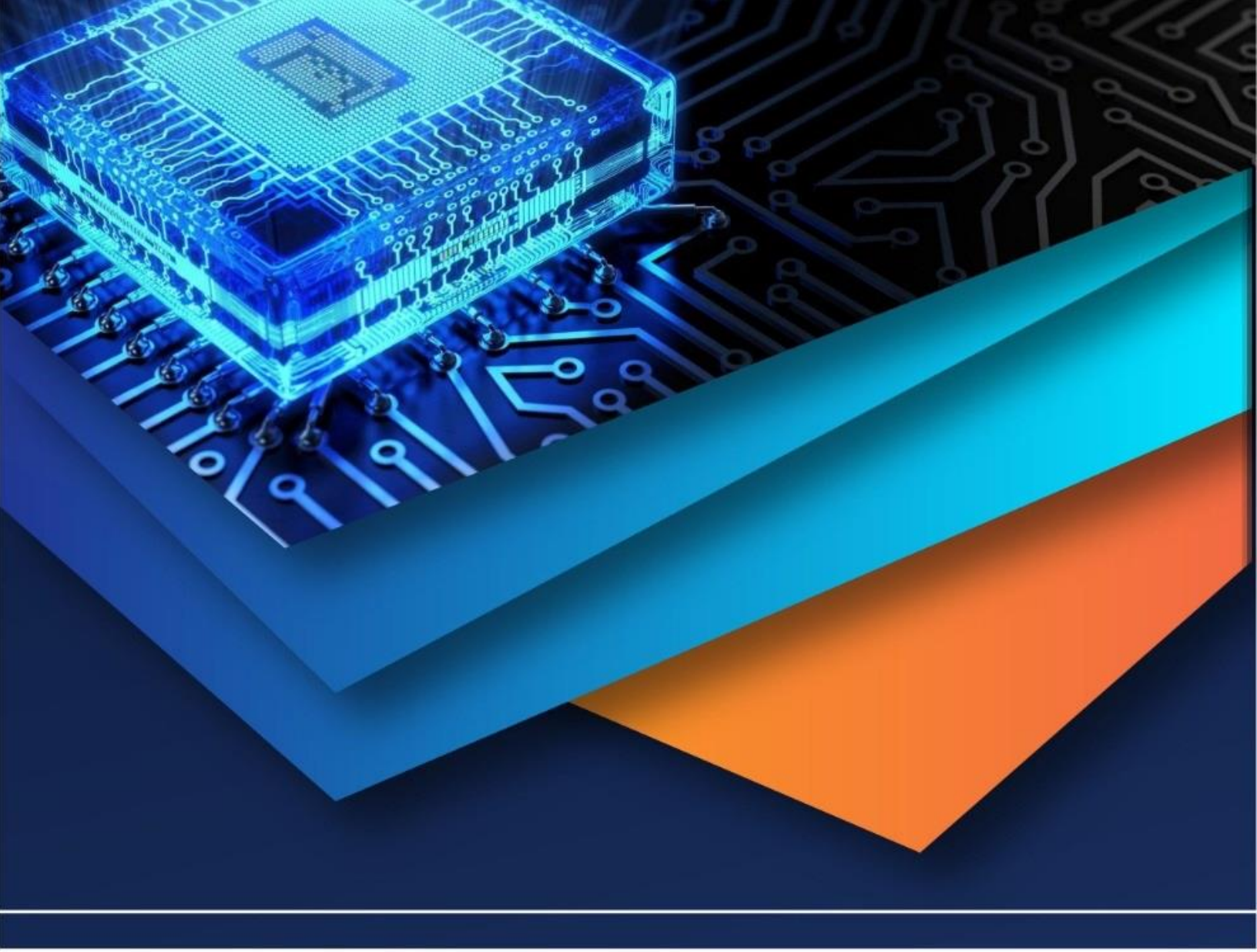
[7] M.O Yinyeh, K.A. Gbolagade, "Overview of Biometric Electronic Voting System in Ghana", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[8] Firas Hazzaa, Seifedine Kadry, New System of E- voting Using Fingerprint, International Journal of Emerging Technology and Advanced Engineering", Vol 2, pp 355-363, 2012.

[9] Muhammad Imran Razzak, Rubiyah Yusof and Marzuki Khalid, "Multimodal face and finger veins biometric authentication", Scientific Research and Essays Vol. 5(17), pp. 2529-2534, 4 September, 2010.

[10] Mrs. S.M.Shinde, Mrs. Priti Subramanium, "BIOMETRIC GSM VOTING SYSTEM", International Journal of Technical Research and Applications, Volume 1, Issue 4 (sept-oct 2013), PP.103-107.

[11] Shanu Agrawal, Pradeep Majhi, Vipin Yadav, "Fingerprint Recognition Based Electronic Voting Machine", International Journal of Engineering and Technical Research ISSN: 2321-0869, Special Issue .



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY