iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3053

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 7 Issue III, Mar 2019- Available at www.ijraset.com

Gallup for Election Initiatives

Dr. M. Preetha[1], Eniyan Kumar. M. U[2], Deepakkesavan. B[3], Naveen Kumar. S[4]
[1] *Assistant Professor,* [2, 3, 4] *Department of Computer Science & Engineering, Student, Department of Computer Science & Engineering, S.A. Engineering College*

Abstract: ***Voting is the soul of representative government. Voting gives us opportunity to select a Leader to control problems and other issues. The main premise of this project is to create an Android application through which the polling can be performed. Before the user polls their vote, he/she should register in order to login into the application to cast their votes. This application delivers a new way of casting votes using mobile phones. The main purpose of developing this application for android devices is to deploy an easy and flexible way of casting votes anytime and from anywhere. The application is especially developed for organizations to vote for any new policy regulation or issues. The issues or queries are fed into the system by the admin or by the candidate. Employees can then cast their vote as yes or no. One voter can only post one vote for a posting. Each and every vote casted is stored in the database for the respective candidate. At the end of the voting process, the system counts the total votes and provides a brief report of it to the admin. Thus, the app helps the company to get proper feedback of the employees.***

I. INTRODUCTION

Election in India has been a major process in today's world so that the people can cast their votes and elect the person has a leader based on his /her queries. Nowadays people enroll their votes through the booths located nearby their locations which causes congestion among the people during the voting process and also tedious process so many of the people will not cast their votes .Due to this, some representatives may cast false votes using others identities. This may leads to variations in the outcome of the election process. Around 78% of people only cast their votes during election. But the remaining 22% of people doesn't cast their votes due to inconvenience .In order to overcome this issue various security measures should be implemented.

II. DOMAIN INTRODUCTION

Android is a Linux based operating system and it is an open source. This OS is used in smart phones, tablets and computers. Open Handset Alliance who developed android and it is led by Google. It is software and it can be used for game consoles, cameras and other electronic products. There are different versions in android. The first version is introduced by Google in the year of 2007 and it is named as Beta. Along with beta they added some more features and it is named as Android1.0. In our application we are using the version 8.0 which is coded as Oreo and its API level is 26-27.It is user friendly platform. It can be customized by anyone. In android, there is N number of mobile applications. It gives more advanced features like weather monitoring, gaming applications and other services.

III. RELATED WORKS

Individual sensors are the main component in large-scale networks for security reasons. Any compromised node can inject false sensing reports .These reports ,if left undetected, will be forwarded to other nodes which may cause not only false alarms but also leads to depletion of energy in battery powered network. In order to overcome this, Statistical en-route filtering(SEF) mechanism is used to detect the false reports and drop those during the forward process of reports. SEF utilizes the network scale in order to filter the false reports by decision-making process by detecting nodes and false detection by the nodes used for forwarding process. SEF's performance and feasibility is assessed through analysis, implementation and simulation. The outcome shows that SEF's can be implemented efficiently. It results in drop down of 70% of false reports by the compromised nodes within five hops and also decreases the energy consumption by 65% or more in most of the cases. [1] In wireless sensor network, any compromised node can feed false data during the process of data aggregation and data forwarding. The existing systems of false data detection techniques consider only the false data insertions during the process of data forwarding and do not allow any change in data .This paper represents the data aggregation and authentication protocol called DAA to get the false reports with data aggregation and confidentiality. In order to support data aggregation, every node will conduct data aggregation process and compute message authentication code in small-size for data verification. In order to support confidentiality, the sensor nodes between the aggregators, in each node, will encrypt the message rather than sending it in plain text. After the analysis, the performance by this process is resulted as the detected false data will not be forwarded to further next nodes which are in the transmission path. [2]

Wireless sensor networks are usually unguarded when it comes to false data insertion attacks. In the process of false data insertions, attackers will inject the false data by the use of compromised nodes which leads to the depletion of resource like battery draining in relaying nodes. This project uses the commutative cipher-based probabilistic filtering scheme. Here, a security boundary is built, in order to determine the no of nodes participating in transmission, controlled by fuzzy rule-based systems with several factors that shows the network status. The proposed system is more suitable and energy-saving than the existing systems in both legitimate and false traffic. This results in achieving extra energy saving process by using verification probability determining method[3]

Wireless Sensor Networks consists of adhoc devices that have the specifications of low power, limited memory and processing power. WSN are located in truculent environment, due to which the intruders can insert false data easily. Due to disperse nature of WSN, intruders from any positions can inject the false data into the network since the sensor nodes don't guarantee for data integrity and does not have high level of authentication mechanism. This paper evaluates and analyzes the performance of other existing false data filtering schemes and suggests a new scheme in order to recognize the false data inserted by the compromised node. In this paper, a scheme is proposed which makes use of cryptographic hashes evaluated on data, linking the consecutive blocks together in order to form a block chain. This iterative process checks the integrity of data in transit and protects data against various attacks. Proposed Schemes suggests better and efficient schemes rather than other existing schemes[4]

Smart Grids can implement the two-way transmission of data. While improving the process management level of the power system, the deep integration of data physics system may bring more risks to the system. Attack known as False Data Injection is mainly used for power system state estimation. The intruder bypasses the traditional detection scheme which may lead to change in state estimation results. This leads the Control Centre to take wrong decisions and also threatens the safe running operation of the power grids. In this paper, DBN-based attack detection method is used in proposed system. From the bottom of the restricted Boltzmann machine .Unsupervised Learning is performed in order to provide the initial weightage of the network. Back Propagation algorithm is used in order to propagate the error from top to bottom. Here, the proposed system tests different scenarios to verify the feasibility and performance of the detection scheme. The outcome achieves a better performance when compared to the SVM-based detection scheme[5]

Estimating the power system states exactly is a crucial task to the reliable operation of power grids. The threat of cyber=attacks such as false data injection attacks are faced by the traditional weighted least square (WLS) state estimation methods. The proposed system specifies a new detection scheme to detect the false data injected by sensing the dynamics of measurement variations .The Kullback-Leibler method is used to estimate the distant between the two probability distribution derived from measurements. When the intruder sends the false data, it will affect measurement variation from the historical data. The proposed system is checked and analyzed with different attack scenarios. Once it is analyzed with a sample test case, it accurately detects the false data injected. [6]

Estimating state is crucial to the operation and working of the power grids. Some of the cyber-attacks such as false data injection attacks can evade conventional detection methods and affects the normal operation of power grids. Such attacks on AC state estimation is more critical than DC state estimation due to the power utilities in AC are high. So, the proposed system is mainly used for AC state estimation to detect the false data injected. The proposed scheme can capture such inconsistency by analyzing consecutive estimated system states by using wavelet transform and deep neural network techniques. This scheme is tested for performance with case studies in 300 bus power systems. The outcome indicates that the scheme can attain satisfactory attack detection accuracy[7].

False Data Injection Attacks (FDIA) in smart grid is an object of broad investigation. Attack strategies and several detection mechanisms have been implemented by various researchers. The aim of the intruder is to bias the estimated state. This paper proposes to evaluate a figure of merit of the bias in the state variables introduced by the attacker, known as Aberration Index. The standard residues indicate the effect of the attacks implemented on the measurements. This paper derives the detection of attacks using Aberration Index and Normalized residues for different attack possibilities.[8]

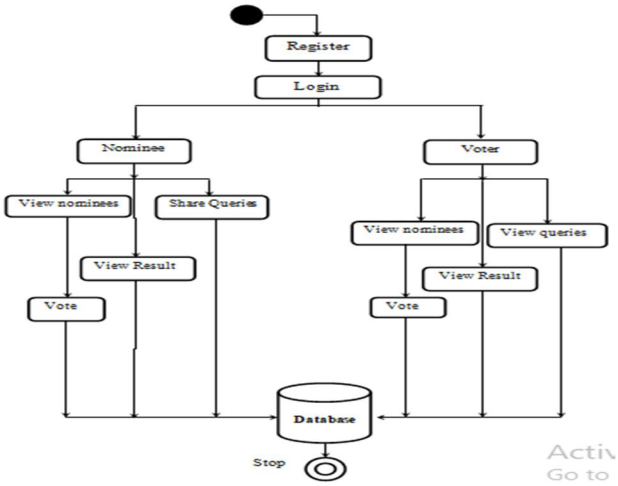
Cyber-attack is well-known as a visible risk in smart grids. In this paper, we disclose a potential link between the data attacks and consequences and also by undergoing analysis to know how the attacker launches the malicious data attack to trigger sequential outrages and causes damages to the grid. In this mechanism, the intruder builds an False Data Injection attack to trigger the branch outage that may affect other multiple branches and causes failure subsequently. This attack mechanism integrates constructing an optimal data attack and identifying critical lines, and imposes a substantial security impact with a high probability of occurrence. Simulations on the IEEE 118-bus system Sverify the introduced attack mechanism and highlight the risk of such attacks in today's smart grids.[9]

The main objective of the democracy is "vote" by which the people can elect the candidates for forming an efficient government to satisfy their needs and requests such that their standard living can be improved. To ensure 100% voting automation came into play.

The proposed system is to develop a compatible voting machine with high level of security. It has three different modules. First the details of the persons who are above 18years are gathered from aadhar card database. Automatically a new voter id with necessary details will be created and intimation will be given to the persons through their e-mail. During the voting process, the user can check their id and password. To ensure more security, Finger print process can be used as authentication. The system allows the voter to vote through his fingerprint. Finger print is mainly used to uniquely identify the user. Finger print is used as a authentication for the voters. As soon as they cast their vote, their voter id and other details will be erased automatically and the aadhar card details which they used will be tracked and will be locked to access. This is done to preserve the security. When people cast their vote the results will be updated automatically according to the voting process and on the same day of election, the results will also be published[10]

IV. PROPOSED SYSTEM

Our application, delivers a new technique of casting votes using mobile phones. It is an application developed for android devices to deploy an easy and flexible way of casting votes anytime and from anywhere. This application is especially developed for the organizations to vote for any new policy regulation or issues.Here the database holes the Voter's information anddetails and Voter's Id. It also Calculate the total votes carried by each person and Checks the information of the voter. It also Remove the wrong information. The advantage of Online Voting over the common queue method is that the voter shave the choice of voting at their own free time and there is reduced congestion it also minimizes on errors of vote counting. Registration is mainly done by the system administrator for security reasons.

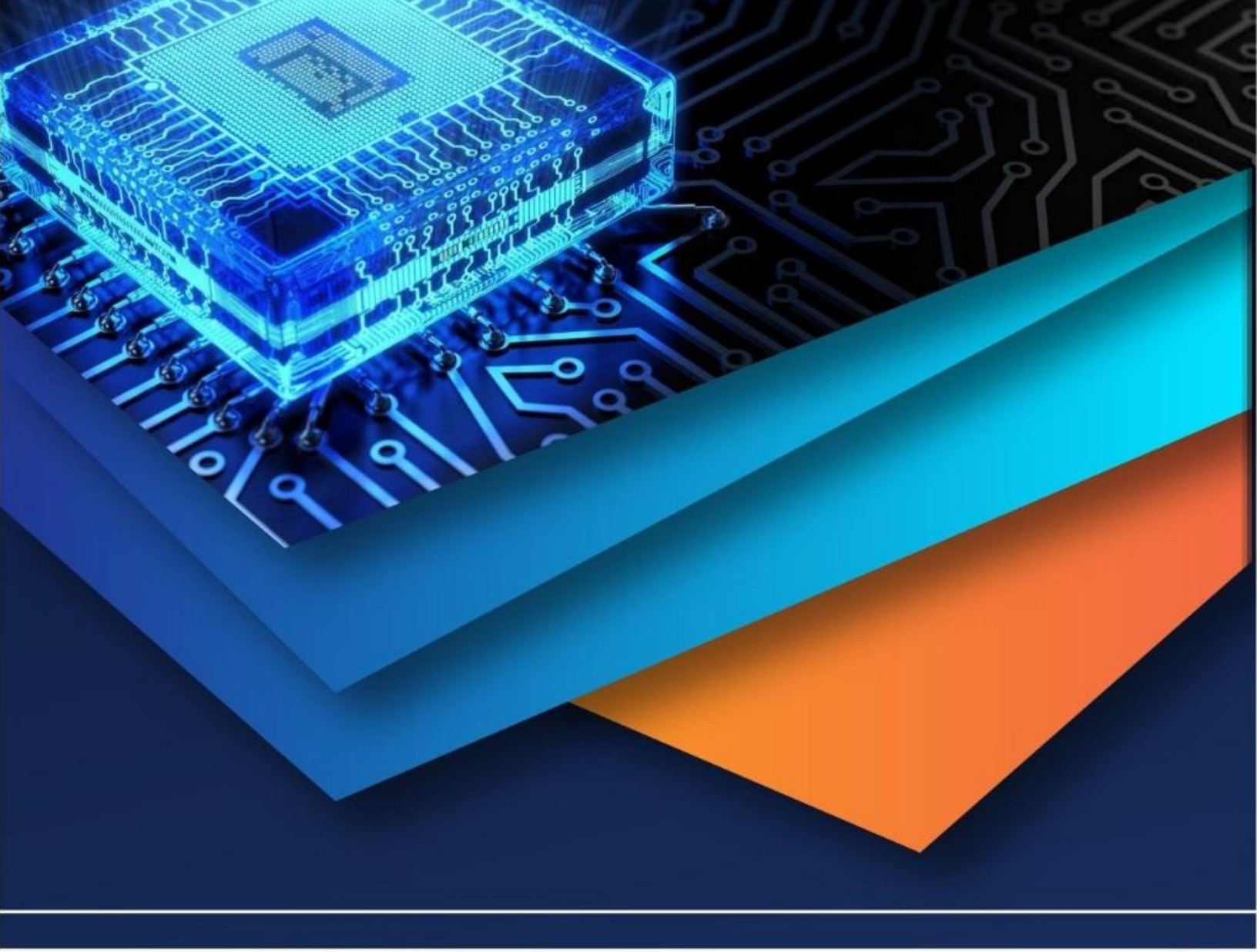


V. CONCLUSIONS

Thus, in this paper comparison and further more differences between the proposed system and the existing system has been explained and executed. We have tried to recover all the disadvantages of the existing system.The proposed system helps to select a Leader to control other issues and problems.The main advantage of Online Voting over the common queue method is that the voters have the choice of voting at their own free time and there is reduced congestion and also minimizes on errors of vote counting.

REFERENCES

[1] Statistical En-Route Filtering of Injected False Data in Sensor Networks(Fan Ye ; H.Luo ; Songwu Lu ; Lixia Zhang)- 04 April 2005
[2] Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks.(SuatOzdemir ; Hasan Cam)- 24 November 2009
[3] Adaptive False Data Filtering Method for Sensor Networks Based on Fuzzy Logic and Commutative Cipher(Hae Young Lee ; Soo Young Moon ; Tae Ho Cho)- 20-22 Dec. 2008
[4] Detection of False Data in Wireless Sensor Network using Hash Chain(Mahak Tariq ; Mashal Khan ; Sana Fatima)-5 Sept. 2018.
[5] False Data Injection Attacks Detection with Deep Belief Networks in Smart Grid(Lei Wei ; Donghuai Gao ; Cheng Luo)-30 Nov.-2 Dec. 2018
[6] Detecting False Data Injection Attacks in AC State Estimation(GuChaojun ; PanidaJirutitijaroen ; MehulMotani)-06 February 2015
[7] Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks(James J. Q. Yu ; YunheHou ; Victor O. K. Li)-10 April 2018
[8] False Data Injection Attacks and detection scenarios in the power system(SindhujaMangalwedekar ; Sunil K. Surve ; H.A. Mangalvedekar)-17-20 Dec. 2015
[9] False Data Injection Attacks Induced Sequential Outages in Power Systems(Liang Che ; Xuan Liu ; Zuyi Li ; Yunfeng Wen)-19 September 2018.
[10] Smart voting(Bhuvanapriya R. ; RozilBanu S. ; Sivapriya P.Kalaiselvi V.K.G.)-11 July 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY