Secure online voting dashboard with general hash aproach

Candidate name: Kallepalli N V Nirisha Mtech CSE(cnis) (MVGR) Internal guide name:

Email: niru.1st@gmail.com

Maharaj vijayanagaram gajapathi raj college or engineering http://www.mvgrce.com

I.Abstract:

In Previous days, the Indian voting System is completely done by the people by physically. Problem is becoming serious with the non-availability of a way to let voters cast votes who are residing outside their election-areas. This Procedure for NRI's and Indian Army is also not showing significant improvement. For that, in this paper we proposed the online voting dashboard which is remotely working by anywhere. This article tries to solve this issue with the design and development of online voting which is not only very easy to use but is also robust, secure and trusted. In this Paper, we have focused on designing a secure and globally trusted voting system through online (mobile and computer) to enable Indian citizens to cast vote in their respective country's election via their GSM Mobile Phones from anywhere in the globe irrespective of their physical location. Apart from this, Here we use SHA-2 Algorithm for generate the key to cast the vote uniquely and Base-64 algorithm is used for encrypt the generated key for security. We evaluate its security in light of relevant election procedures. We conclude that, they are vulnerable to serious attacks that can alter election results and violate the secrecy of the ballot. We demonstrate two attacks, implemented using custom hardware, which could be carried out by dishonest election insiders or other criminals with only brief physical access. This case study carries important lessons for Indian elections and for Online voting security more generally. GHA(general hash approach) is the technique which is implemented to generate the key.

*(**Key Terms:** Remote voting, secure casting, Key generation, key Encryption, hash approach.)*

II. Introduction:

In Before days, the voting system is statically done by the people one by one. The procedure of casting votes at the ballet centers is very time consuming process. By this system the voting process is completed very lately and at the same time the people who were staying at other countries have to face the problem with this voting system by necessary to came to their native places to caste the votes. With the present voting system the people are unable to use their votes. Whereas coming to this online voting system, everyone who is having authorization can vote their Leaders. With this proposed online voting dashboard elections will be completed 100% successfully.

A major agreement supports Internet Online voting dashboard provides that Internet is an inherently secure platform. Indeed, various attacks including worms, viruses, spy ware, spoofing, denial of service and others, cannot be used to compromise the voting results, to secure the voter's secrecy, and cannot interrupt the elections.

In our society, the main aim of the voting system is to collect the people opinion and reflect their opinion. With this voting system everyone will accept one Leader to run our country successfully. Present days the voting system is running at boots. To cast their votes compulsory the voters has to present at boot.

The voters may not be able to present at the boots at elections time because of various reasons. And so many people may present at various places and they may not able to come to boots, so many of them not using their votes. Everyone votes are valuable in our society, especially the youth and maximum voter portions of today are moving away from voting. There are many reasons like the unable to adjust their timings and their busy schedule and etc., so to avoid this problem and run elections successfully this Online voting system is very useful.

III. Related work:

In Previous days, many electronic devices are used to collect the votes from the people. But these electronic devices are also faced many problems like service problem, power problem and etc. so this process was not sufficient. In this process also users have to be going to vote their election commission. After many years, based on this concept the people are proposed of their own techniques, these techniques also having many secure problems so according to the above existing projects here we had proposed a new advanced system that is online voting system.   By this system I have taken many identity proofs from related people and store them into database for security reasons.

In present voting system, all valid voters have to register themselves to Election Commission of any country and get their voter ID-Card. This ID-card is used as photo identification while casting vote. This protocol adds an extra field to the present Voter ID-Card namely: UID (The AADHAR UID) (Unique Identification Authority of India, Planning Commission).While registering to election commission, user will register his/her mobile number. Firstly, the user has to activate given mobile number to enable mobile voting.

The mobile voting activation procedure for voters would be as follow:
After proper verification, a secret number will be sent on the user's registered mobile number. After getting this number, user has to log-in to the Indian Election Commission's online mobile-voting activation gateway and provide following information:

1. The Secret key Number
2. The User ID as on voter's ID-card
3. The Voter ID as on voter's ID-card
4. Mobile number on which this information is sent

This will be a single time activity which has to be done. An automated verification will be done on back end side and on success; the number will be activated for mobile voting. Also a secret key will be passed to the mobile user (this will be used to decrypt the secured encrypted SMS from election commission). The user also needs to download and install a small cryptography application (used to decrypt and view secure SMS from election commission).The detailed description of this protocol is elaborated down onwards.

General Hash approach(GHA): which is used to generate the 19 digit security key for each and every login and this key will be persisted for each user's session.
   The format of the key is as follows:
9102742470724239404
GHA algorithm:
Input : string : random string S
Output : hash2
hash − 1315423911
T1 = hash << 5;
For each I in S
Loop start
T2 = S(i) + (hash >>2);
End;
Hash1 = T1 + T2;

1. Online Voting Process:

Online voting system is advanced approach to collect votes from people anywhere in the world. This system will provide feasible environment to the user. No need to go to the election centers for cast the votes and the people who were stayed in other countries no need to come for voting in their native places.

The Election commission must need to host into the internet with their profile and party details. And also the users have to be registered with this system then they get their own secrete key through the email. Using that key they can cast the votes to their favorite election commission. The generated key will be used at one time only. Next time it won't work. Hence one user can vote only one time. The duplicated users can't be registered more than one time. The advanced technique SHA-2 algorithm is used to generate key for every registered user. For the security reasons we proposed an algorithm of BASE-64 to encrypt and decrypt the generated key. The key will view by that particular user only.

When registration time the user should submit their identity proofs like ADHAR CARD, PAN CARD, address proof, mobile number, email.
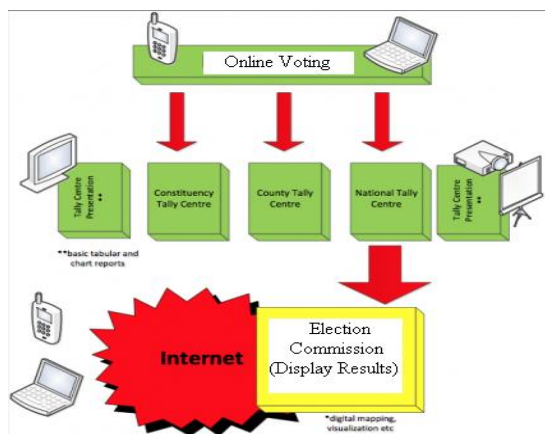

Figure.1: Overview

3.1 Features in remote voting:

1. Election Commission
2. User Profile creation
3. Key Generation
4. Key Encryption-Decryption
5. Voting Process

Description:

1. Election Commission:

The election commission can manage the election process remotely. He had his own account and he has to register with that for manipulating the user's accounts and casting results. He can view the population count and day by day registered users like how many people have got to create their accounts with election commission for voting. Here the Election Commission can view the each party voters list and count them individually for announce the results.

2. User Profile Creation:

To cast the votes, every user should create account with Election Commission by producing their proofs like Adhar Card, Pan Card, Mobile Number, Residence Proof these proofs are used for identify the user uniquely and make them secure.

3. Key Generation:

According to the user profile that were registered, the system automatically generate key. The key is identical to every user. The key would be generated using technique of GHA will be encrypted and send to the user through email. Using that key user has to vote for election. That key has to be change every

time in the voting time for every user for every election time.
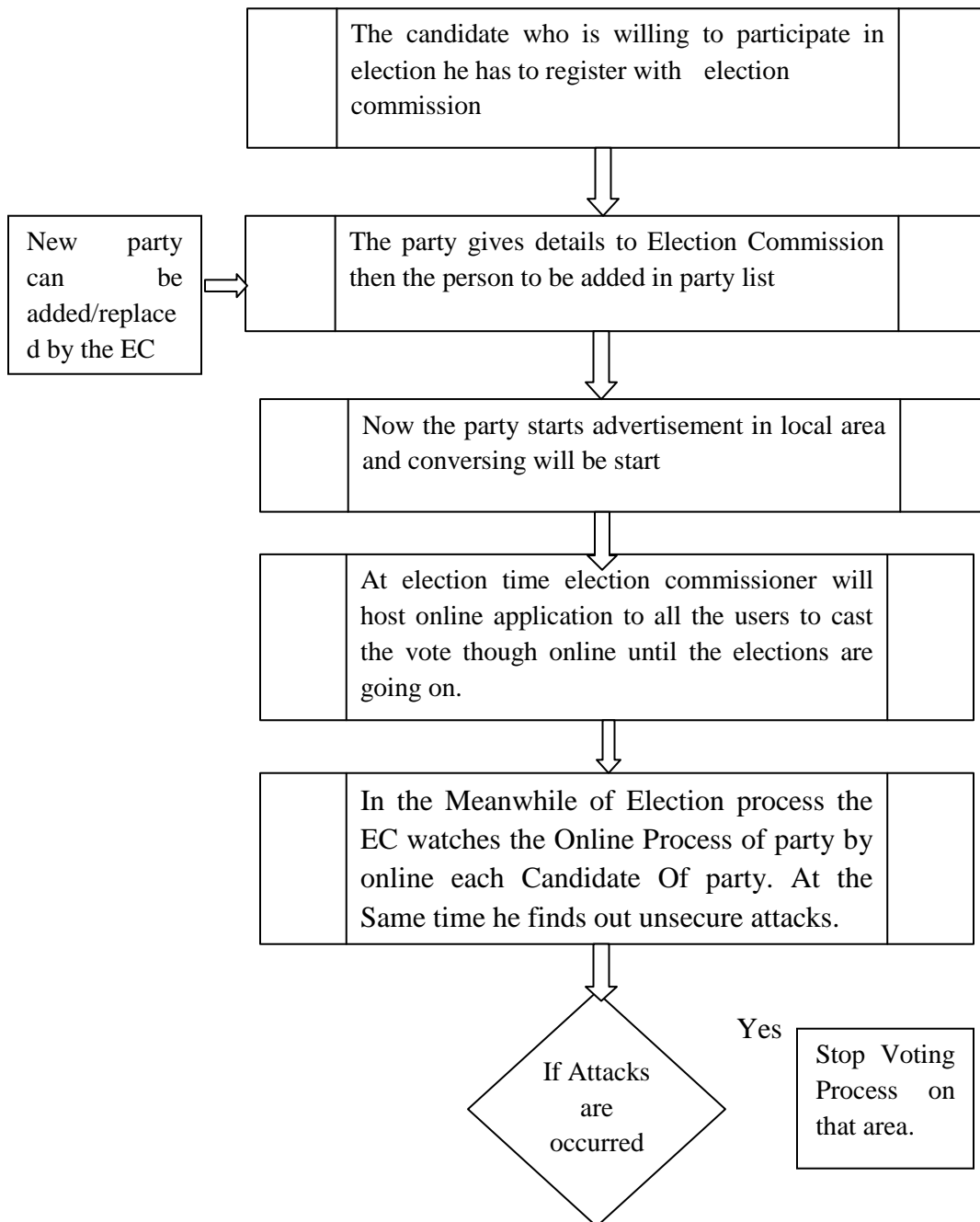
4. Key Encryption-Decryption:

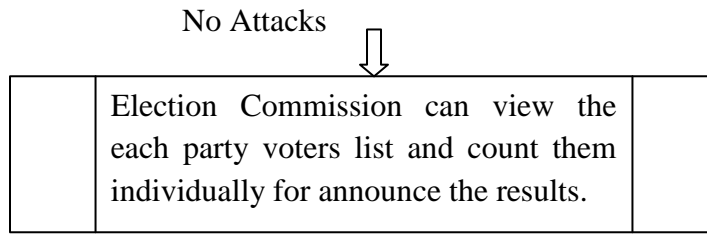The generated key encrypted and decrypted by the General hash aproach.

5. Voting Process:

In this process, the user uses his generated key which was got by the email for login to the voting. In this, the user gets many party candidates list. The user has to select his favorite one and vote them. The voting details will be forward to Election Commission automatically for every voter.
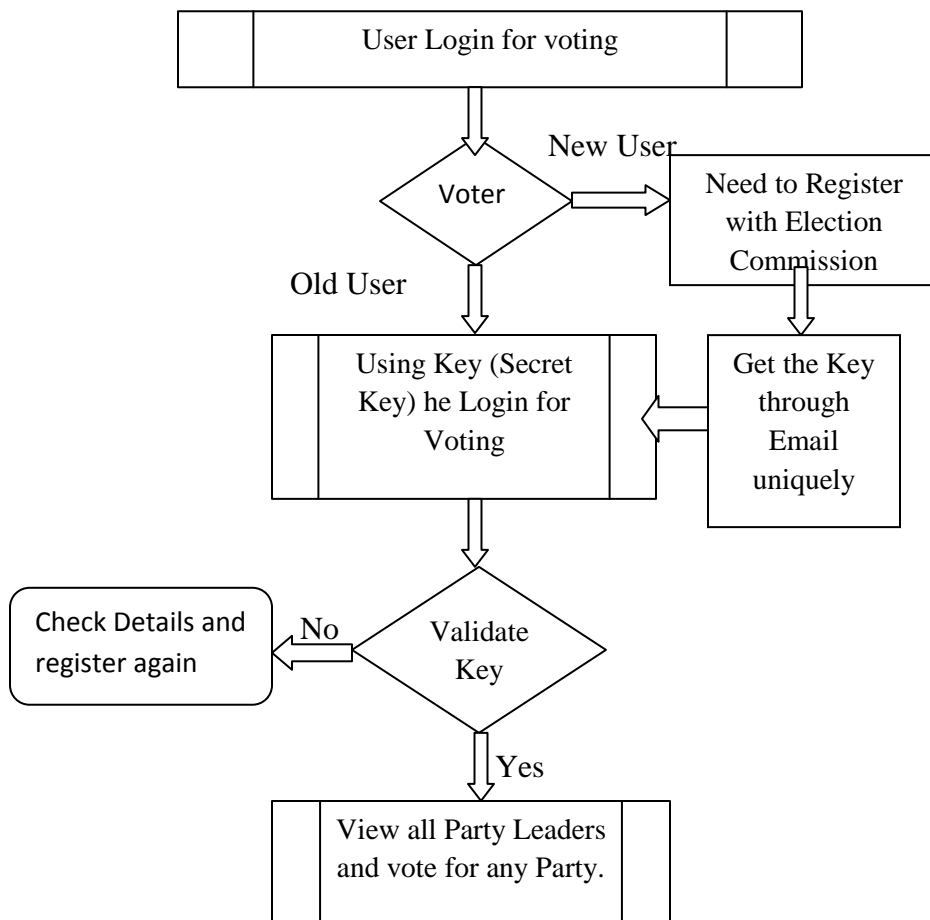
2. Working Architecture of Voting System

4.1 Flowchart Dimension for Election Commission:

No Attacks

	Election Commission can view the each party voters list and count them individually for announce the results.	

4.2 Flow Chart Dimensional for Voters:

	User Login for voting	

Voter

New User

Need to Register with Election Commission

Old User

Using Key (Secret Key) he Login for Voting

Get the Key through Email uniquely

Check Details and register again

No

Validate Key

Yes

View all Party Leaders and vote for any Party.

V. Performance and Conclusion: Compare to regular voting online voting is flexible for net users. It increases voting percentage with old and who is aware of world wide web. Our aproach hash aproach is simple and secure to generate the unique key even though the number

of voters increases. So hash aproach is one which is unique and highly shielded to preserve in synchronizing with voter. After doing the vigourous experiments of on the real dashboard the 78% stability is observed with end result.

Miss Kallepalli N V Nirisha pursuing Mtech CSE(cnis)

VI. References:

1.   Hari K. Prasad, J.Alex Halderman, Rop Gongriijp, Scott Wolchok, Eric Wustrow, Arun Kankipati, Sai Krishnan Sakhamuri, Vasavya Yagati (April 29,2010) , "Security Analysis of India's Electronic Voting Machines"

2.   Unique Identification Authority of India, Planning Commission, Government of India (July 7, 2010), "Aadhar Handbook for Registrars", Version 1-July 2010, pp 3-5

3.   Manish Kumar, T.V. Suresh Kumar , M. Hanumanthappa, D Evangelin Geetha, "Secure Mobile Based Voting System", pp 324-326

4.   India Elections Statistics, http://www.indian-elections.com/india-statistics.html, accessed 19 October, 2011.

5.   Wikipedia, Indian General Election 2009, http://en.wikipedia.org/wiki/indian_ general_election,_ 2009, accessed on 19 October , 2011.