ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Enhancement of secured Mobile voting based on IMEI number as Key

Venkatesh J[1], Viswaprasath KS[2]

Professor, Department of Information Technology, Velammal Engineering College, Chennai, India[1]

UG Scholar, Department of Information Technology, Velammal Engineering College, Chennai, India[2]

ABSTRACT: for the past few days the usage of mobile in the world wide level is keep on increasing. World have now changed totally into a digital with the help of mobile devices. To provide a good dynamic key encryption algorithm and to avoid usage of other mobiles for private voting, here we have proposed a system. In this paper we would like to bring our novel approach in using the mobile IMEI number as the encryption key used by the voter. This mobile IMEI number also helps us to check whether the mobile is used once or more than once. This proposed system is another enhancement in the current mobile voting environment. With this system we can be sure that every individual can vote from one only mobile for one time and also the messages which are encrypted cannot be hacked by hackers easily.

KEYWORDS: M-Voting, Mobile voting, Verified mobile voting, IMEI based Mobile voting, Secured voting.

I. INTRODUCTION

M-voting can be an efficient and effective way for conducting a voting procedure and for attracting specific group of people to participate. The term M-voting is used hereby to denote a voting process, which enables voters to cast a secure and secret vote using their mobile phone powered with internet.

This project deals with the development of mobile application for Election mobile based Voting System where each and every individual can vote using their mobile in highly secured manner. Here the project which has been proposed will make every single mobile user to use the mobile which is equipped with internet connection to vote. This project is very unique from previously available system.

Here the eligible person is made to enter a portal to get registered. During the time of registration as a normal process followed during the time of election all the details, along with the user mobile phone IMEI are obtained. This is very essential for this project. We get this IMEI so that the person can vote only from that mobile for that election else they can visit to normal both for voting; and also others can't vote from another mobile even if they know another person's voter id and password. The IMEI number is used as the key for the process of encryption in the registered user side and decryption in the server side.

The encryption algorithm which is going to be used here is entirely new which is highly secured. The algorithm which has been proposed here for encryption/decryption of messages can get 4 characters as input at a single time and they will return back 4 characters in encrypted form. This can accept any ASCII characters and give output as ASCII character which is then converted using Base64 algorithm for transmission in network

II. OBJECTIVE

The main objective of this project is that each and every eligible candidate should vote by any means. The normal traditional method is followed by almost 78.12 %(in 2011 voted) of the people in India. Remaining people who skipped were normally students and busy business peopling who are having most of their time in travel. The main intention is to make the remaining set of eligible candidate to cast their vote.

Another objective of this project is to make each and everyone with mobile phone and internet to give their vote using their mobile itself. So that eligible persons need not stand in long queue. The electronic method of voting is considered to be more secured than traditional method. In traditional method many may have to stand for long time and in some cases there are some problems from outsiders. This can be eliminated by this method.

And the cost spent on the election can be considerably reduced. Because the human resource required for this will be very low and normally there will be need mostly only the computer servers which will be located in remote place and only for that server we need to give both physical security and software based security.

III. METHODOLOGY

The basic process of election system applies here too. We would like to consider only the methods which will be necessary of mobile voting. The below categories are very essential for doing mobile voting. They are as follows

- Registration for mobile voting.
- Voting
- Decryption on Server Side
- Conformation

The above mentioned process can be started after the general voting registration is done by each and every individual user in their locality. Before starting any government election generally government will get details from each and every individual personally. This step cannot be altered anywhere and it is very essential for any voting system introduced. This is because there may be chances people will cheat government and can show additional persons in their houses and can give vote to any of the candidate which they like most.

A. Registration for mobile voting

The registration for the mobile voting can be done only from the mobile which they will be using for giving the vote. After entering to registration portal first he has to give his unique voter ID number and the password which he gets from the government. The moment he enter them it is checked with the database which is available with the government as whether the candidate has entered correct user ID and password and whether he is eligible to vote. Then he is displayed with the area details where his registration has happen i.e., his booth number. After he verifies it the main stage of registration starts. The mobile application will automatically get the IMEI number as a background process and user can submit. As the user clicks the submit button the details like unique number, password for login, IMEI number, and booth details are sent to database. This time the database which is used for storing is different from the previously used database. This new database will be having the details of the mobile voting registered candidates.

B. Voting

On the Election Day alone the candidate will be allowed to vote from his mobile phone.

- ***Validation Phase***

For that process a Login screen will be coming when the user open the application. During that time the user has to give the unique voter ID and the password. When he submits he is again checked with the database which will be having the details of the registered mobile voting candidates which will be having the details like voter ID, password and the IMEI number of the mobile phone. If either the password is wrong for that voter ID or if the mobile phone from which he tries to vote is different then he is not allowed to move to next step.

- ***Voting phase***

If the person is registered and the voter ID, password and IMEI are correct then he moved to next screen where the lists of candidates who are standing in that booth for that election are displayed. From that list of candidate the eligible voter is allowed to choose to whom he would like to vote. After he chooses the person from the list of candidates he is again verified with the vote he has given.

- ***Encryption Phase***

The details are encrypted using playfair algorithm encryption and details are as follows.

The encryption which is done here is two step process. In the first step consider the 4 character and find the cipher text for them which are told in detail below, during the separation of these 4 letters if any two letters found to be similar then introduce X between them. Then if any character are left free add X, Z and finally _ to make them as a pair of 4 characters. And then using Base 64 algorithm again convert them into cipher text which can be displayed in the text editor application.

Steps involved in the encryption process are as follows.

1. Consider the 4 characters of the plain text. Divide them as groups.

2. Then have to find the cipher text of the each four character using the below table. See that it is in circular fashion. i.e., first letter will be having 2nd as next letter and then 3rd and next to next and 4th letter as final letter. While for 2nd letter, 3rd as next, and 4th as next to next and 1st as the final letter. And it will be going

on for all the letters.

3. After getting the cipher letter hexadecimal values, have to find the binary value for each and every hexadecimal we have got.

4. Then with the help of Base 64 algorithm we will find cipher.. The final result of cipher will be any one of A-Z, a-z, 0-9 ,+ and /.

5. Then have to find the corresponding printable character and make it as the final cipher and save them to send it through network.

TABLE I. ENCRYPTION PROCESS OF EXTENDED PLAYFAIR

Plain Text of the poly char	**Plain Text of the poly character**				**Cipher Text of poly char**
	1st Letter	***2nd Letter***	***3rd Letter***	***4th Letter***	
1st Letter	Row	Column	Matrix Row	Matrix Column	1st Letter
2nd Letter	Matrix Column	Row	Column	Matrix Row	2nd Letter
3rd Letter	Matrix Row	Matrix Column	Row	Column	3rd Letter
4th Letter	Column	Matrix Row	Matrix Column	Row	4th Letter

- ***Submission***

After all the encryption process all the details like Voter's Identity number, the person whom he has voted are send to the database where everything got from the eligible candidates are stored.

C. Decryption on Server Side

Then before entering to the actual database all the details are inserted into temporary table where there will be encrypted message of all the details instead of actual details, after that all the messages are decrypted and then are inserted to another new table. This is done to enhance the security of all the votes made by the users. The decryption steps are as follows.

The Decryption involves almost the similar step of the encryption where it also have 2 steps. The exact reverse steps as in encryption. Both in the encryption and decryption we are using the same key. The key here is obtained earlier during the registration of the mobile voting itself. So we are very secured in each and every transmission of data. The detailed steps are as follows.

1. The first step is to receive the cipher text from the network which is made as readable in the notepad.

2. Then convert them into 6 bit binary values according to the Radix 64 table. Make them as 8 bit binary values. Convert them to the hexadecimal values so that the plain text is obtained.

3. Then as in encryption separate the characters into 4 and then make use of below table to get the original plain text.

4. Then after getting as the values it has to be compared with the ASCII table and make them to normal plain text as it had been before encryption.

5. Then if any unwanted additional X or Z or _ are fond in the middle of the message or at the end of the message, those have to remove then.

TABLE II. DECRYPTION PROCESS OF EXTENDED PLAYFAIR

Cipher Text of the poly char	**Cipher Text of the poly character**				**Plain Text of poly char**
	1st Letter	*2nd Letter*	*3rd Letter*	*4th Letter*	
1st Letter	Row	Matrix Column	Matrix Row	Column	1st Letter
2nd Letter	Column	Row	Matrix Column	Matrix Row	2nd Letter
3rd Letter	Matrix Row	Cube Column	Row	Column	3rd Letter
4th Letter	Matrix Column	Matrix Row	Column	Row	4th Letter

D. Confromation

Then finally the conformation message is sent to the user only as he his vote has been submitted. This is for user satisfaction and acknowledgement.

IV. ANALYSIS OF THE PROPOSED EXTENDED PLAY FAIR CIPHER

Here is the example with the key "HeisMult-Tand"
Plain text is: God is great
Poly Char: {God }, {is g}, {reat}
Hexadecimal values: {47 6F 64 20}, {69 73 20 67} , { 72 65 61 74}

A. Key matrix Generation

TABLE III. THE KEY MATRIX TABLE USED FOR ENCRYPTION AND DECRYPTION OF ANY ONE USER BASED ON HIS IMEI

	Column 1				**Column 2**				**Column 3**				**Column 4**			
Row 1	48	65	69	73	3C	3D	3E	3F	A0	A1	A2	A3	D0	D1	D2	D3
	4D	75	6C	74	40	5B	5C	5D	A4	A5	A6	A7	D4	D5	D6	D7
	2D	54	61	6E	5E	5F	60	7B	A8	A9	AA	AB	D8	D9	DA	DB
	64	41	42	43	7C	7D	7E	7F	AC	AD	AE	AF	DC	DD	DE	DF
Row 2	01	02	03	04	44	45	46	47	B0	B1	B2	B3	E0	E1	E2	E3
	5	6	7	8	49	4A	4B	4C	B4	B5	B6	B7	E4	E5	E6	E7
	9	A	B	C	4E	4F	50	51	B8	B9	BA	BB	E8	E9	EA	EB
	D	E	F	10	52	53	55	56	BC	BD	BE	BF	EC	ED	EE	EF

Row 3	11	12	13	14	80	81	82	83	57	58	59	5A	F0	F1	F2	F3
	15	16	17	18	84	85	86	87	62	63	66	67	F4	F5	F6	F7
	19	1A	1B	1C	88	89	8A	8B	68	6A	6B	6D	F8	F9	FA	FB
	1D	1E	1F	20	8C	8D	8E	8F	6F	70	71	72	FC	FD	FE	FF
Row 4	21	22	23	24	90	91	92	93	C0	C1	C2	C3	76	77	78	79
	25	26	27	28	94	95	96	97	C4	C5	C6	C7	7A	30	31	32
	29	2A	2B	2C	98	99	9A	9B	C8	C9	CA	CB	33	34	35	36
	2E	2F	3A	3B	9C	9D	9E	9F	CC	CD	CE	CF	37	38	39	00

B. *Encryption*

TABLE IV. ENCRYPTION OF 47 6F 64 20

Plain Text of the poly char	**Plain Text of the poly character**				**Cipher Text of poly char**
	47	*6F*	*64*	*20*	
47	Row	Column	Matrix Row	Matrix Column	48
6F	Matrix Column	Row	Column	Matrix Row	8C
64	Matrix Row	Matrix Column	Row	Column	BF
20	Column	Matrix Row	Matrix Column	Row	20

TABLE V. ENCRYPTION OF 69 73 20 67

Plain Text of the poly char	**Plain Text of the poly character**				**Cipher Text of poly char**
	69	*73*	*20*	*67*	
69	Row	Column	Matrix Row	Matrix Column	5A
73	Matrix Column	Row	Column	Matrix Row	14
20	Matrix Row	Matrix Column	Row	Column	43
67	Column	Matrix Row	Matrix Column	Row	6C

TABLE VI. ENCRYPTION OF 72 65 61 74

Plain Text of the poly char	**Plain Text of the poly character**				**Cipher Text of poly char**
	72	*65*	*61*	*74*	
72	Row	Column	Matrix Row	Matrix Column	41
65	Matrix Column	Row	Column	Matrix Row	A2
61	Matrix Row	Matrix Column	Row	Column	1C
74	Column	Matrix Row	Matrix Column	Row	74

The **resultant hexadecimal cipher** value is **48 8C BF 20 5A 14 43 6C 41 A2 1C 74**
Binary value for above in 8 bit is

010010001000110010111111001000000101101000010100010000110110110001000001101000100001110001110100

Encoding the binary value using Radix 64 Algorithms
MDEwMDEwMDAxMDAwMTEwMDEwMTExMTExMDAxMDAwMDAwMTAxMTAxMDAwMDEwMTAwMDEwMDAwMTEwMTEwMTEwMDAxMDAwMDAxMTAxMDAwMTAwMDAxMTEwMDAxMTEwMTAw is the cipher text which will be send in the network

C. Decryption

Cipher text:

MDEwMDEwMDAxMDAwMTEwMDEwMTExMTExMDAxMDAwMDAwMTAxMTAxMDAwMDEwMTAwMDEwMDAwMTEwMTEwMTEwMDAxMDAwMDAxMTAxMDAwMTAwMDAxMTEwMDAxMTEwMTAw

Decoding of cipher text using Radix 64 Converter
010010001000110010111111001000000101101000010100010000110110110001000001101000100001110001110100
The **resultant hexadecimal cipher** value is **48 8C BF 20 5A 14 43 6C 41 A2 1C 74**

TABLE VII. DECRYPTION OF 48 8C BF 20

Cipher Text of the poly char	**Cipher Text of the poly character**				**Plain Text of poly char**
	48	*8C*	*BF*	*20*	
48	Row	Matrix Column	Matrix Row	Column	47
8C	Column	Row	Matrix Column	Matrix Row	6F
BF	Matrix Row	Cube Column	Row	Column	64
20	Matrix Column	Matrix Row	Column	Row	20

TABLE VIII. DECRYPTION OF 5A 14 43 6C

Cipher Text of the poly char	Cipher Text of the poly character				Plain Text of poly char
	5A	14	43	6C	
5A	Row	Matrix Column	Matrix Row	Column	69
14	Column	Row	Matrix Column	Matrix Row	73
43	Matrix Row	Cube Column	Row	Column	20
6C	Matrix Column	Matrix Row	Column	Row	67

TABLE IX. DECRYPTION OF 41 A2 1C 74

Cipher Text of the poly char	Cipher Text of the poly character				Plain Text of poly char
	41	*A2*	*1C*	*74*	
41	Row	Matrix Column	Matrix Row	Column	72
A2	Column	Row	Matrix Column	Matrix Row	65
1C	Matrix Row	Cube Column	Row	Column	61
74	Matrix Column	Matrix Row	Column	Row	74

The final plain text hexadecimal value is **47 6F 64 20 69 73 20 67 72 65 61 74**

On comparing the above hexadecimal values with the ASCII values the result obtained as follows **"God is great"** which is our plain text.

V. CONCLUSION

The above system which has been proposed has lot of advantages over the previously available M-voting system. Here our main target is to make the eligible voters to vote and also to avoid fake vote, which are made by some people. The system which has been proposed here makes everyone comfortable to give their vote from home using their mobile phones and each mobile are mostly used only one time.

REFERENCES

[1] William Stallings, Cryptography and Network Security Principles and Practices, Fourth edition, Pearson Edition.

[2] Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh , Internatinal Journal of Computer Applications (0975 – 8887) Volume 51– No.2, August 2012 1048576

[3] Radix 64 Converter-http://www.oktay.de/decode/base64.htm

[4] . Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition, The McGraw- Hill companies, New Delhi, 2007.

[5] English Character frequency table- http://www.cryptograms.org/letter-frequencies.php

[6] Dhiren R.Patel, Information Security Theory and Practice. First Edition, Prentice-Hall of India Private Limited, 2008.

[7] Electronic voting systems: Requirements, design, and implementation by Ghassan Z. Qadah, Ran Taha