An Efficient Mobile Voting System Scheme Based on Elliptic Curve Cryptography

Monali Shetty, Priyali Patil, Akshita Gandotra, Shivam Mishra

Abstract— The wide-spread use of mobile devices has made it possible to develop mobile voting system as a complement to the existing electronic voting system. Mobile voting systems have the potential to improve traditional voting procedures by providing added convenience and flexibility to the voter. Voter's casted vote is protected using enhanced system security which is based on Elliptical curve cryptography scheme. Most of the Cryptographic Techniques used in many of the devices has certain limitations which make them less effective and secure. In this paper, we propose Elliptical Curve Cryptography (ECC) as the secure alternative for other less effective cryptographic techniques.

Index Terms— Elliptic Curve Cryptography, Mobile Voting.

1 Introduction

THe wide-spread use of mobile devices has made it possible to develop mobile voting system as a complement to the existing electronic voting system. However, due to limited onboard resource, it is challenging to achieve both efficiency and security strength for mobile voting system. The users' votes are secured by using the elliptic curve cryptography (ECC) algorithm.

The aim is to make use of Elliptic Curve Cryptography which is proved to be more secured over RSA for encryption. The paper presents design of proposed system for mobile voting system based on ECC scheme.

Lack of efficient protocols makes the security issue of mobile networks more challenging. The public key cryptography can provide the Authentication, Confidentiality, Integrity and non-repudiation. However, the appropriate encryption scheme for mobile communication must have small amount of data calculating and quick operation as of its inherent restrictions of small quantity and low calculating ability.

2 Existing System

2.1 Traditional Voting

Traditional voting technologies include hand-counted paper ballots. Each voter uses one ballot, and ballots are not shared. The voter casts his/her ballot in a box at a polling station. These systems can result in a number of problems, including: Unacceptable percentages of lost, stolen, or miscounted ballots, Votes lost through unclear or invalid ballot marks, Limited accommodations for people with disabilities.

2.2 Electronic Voting Machine

An EVM consists of two units: Control Unit and Balloting Unit. The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. This will enable the voter to cast his vote by pressing the blue button on the Balloting Unit against the candidate and symbol of his choice. The controller used in EVMs has its operating program etched permanently in silicon at the time of manufacturing by the manufacturer.

It has some limitations such as voter has to reach the allotted destination to cast his/her vote which may be inconvenient for disables or some other purpose. Also it requires extra manpower and money to carry out the process. EVMs are easy to tamper

2.3 Online Voting

Online voting is also one of the way that is used in elections of managerial boards of private offices, committees etc. But this is also not secure as the votes can be manipulated by intruder. Intruder can create many accounts through which he can make voting bias towards particular candidate. Internet voting sceptics point out that poor and minority voters have less access to computers and the Internet and so would be less likely to benefit from online voting.

3 Proposed System

Voter anonymity and voting correctness are important issues for mobile voting mechanisms. Compared mobile voting with traditional elections, a mobile voter is able to cast his/her ballot through the Internet in any place and at any time if he/she can access the network. Therefore, convenience and mobility make electronic voting become more popular. Mobile voting systems offer multiple advantages over traditional paper-based voting systems such as reduced costs, increased participation and voting options, Greater speed and accuracy placing and tallying votes, Greater accessibility for the disabled.

3.1 Architecture of Proposed Model

The proposed system consists of following components:

- *Mobile Equipment/Voting Device (ME):* In electronic voting schemes, voters need to use dedicated voting devices to cast their votes electronically, for instance, Internet connected smartphones.
- *Online Registration:* Users have to register themselves on a website to store their information in the online database server.
- *Validation Centre (VC):* VC is an entity within the network which validates the authentication parameters

i.e. username and password and authenticates the mobile equipment.

- *Encryption Algorithm:* The vote casted by user is encrypted using ECC algorithm and sent to the counting server.
- *Collecting and Counting Server (CS):* CS is the server that collects and decrypts the encrypted vote and counts them to give the final result. CS's action need to be audited by all candidate parties.

3.2 Working of Proposed Model

The process is as follows:

- *Voter online Registration*: - Initial process involves voter registration on the website to store their information. In this process voters get to choose their username and password which they will be using to login in mobile voting app.
- *Voters Validation Phase*: - If the voter is validated then only he will be allowed to participate in the next steps of voting. This phase is default phase and it works automatically once users try to use the e-voting.
- *Voting Phase*: In this phase, after the voter logs in to the app he/she gets to vote the candidate of his choice
- *Encryption phase*: When the voter casts his vote, that vote is encrypted using ECC algorithm and then it is sent to the counting server.
- *Counting Phase*: - At the time of counting CS decrypt the ballot with its private key and retrieves the vote and increments the count of the candidate who is given the vote.

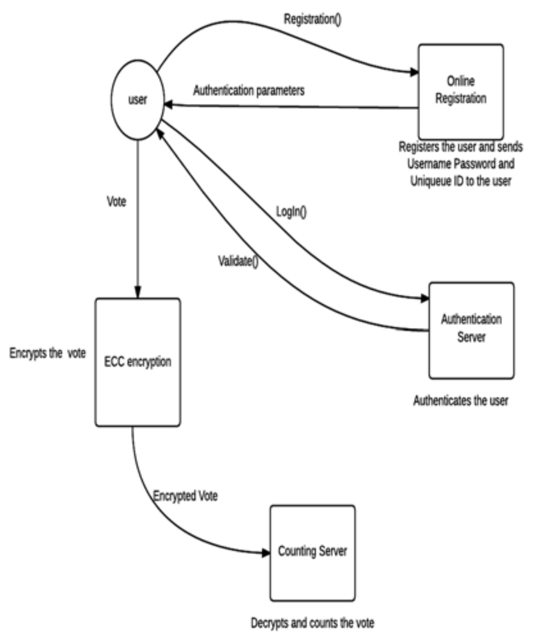
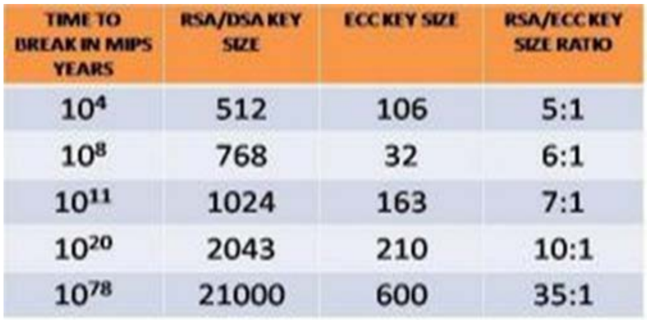


Fig. 1. Data flow Diagram.

3.3 Reasons for choosing ECC as Security Scheme

As ECC selects point which satisfies the elliptical curve equation and generate keys which are exchanged with intended receiver. If intruder wants to attack then he/she has no access to starting and ending point i.e. public and private key, he just gets the random values on this curve. To predict the curve it needs lot of computation using superfast processor which may take around 20 years with conventional computers. Also compared to RSA, ECC offers equivalent security with smaller key sizes, which results in faster computations, lower power consumptions as well as bandwidth savings.



TIME TO BREAK IN MIPS YEARS	RSA/DSA KEY SIZE	ECC KEY SIZE	RSA/ECC KEY SIZE RATIO
10^4	512	106	5:1
10^8	768	32	6:1
10^{11}	1024	163	7:1
10^{20}	2043	210	10:1
10^{78}	21000	600	35:1

Fig. 2. RSA vs ECC comparison.

3.4 Analysis of different methods of ECC

Over finite prime field:

It is suitable for s/w applications and for the processors having large multipliers for performing integer arithmetic. They do not need the extended bit-fiddling operations required by binary curves.

Prime field Fp, where p is a prime
Elliptic Curve equation:

$$y^2 \bmod p = x^3 + ax + b \bmod p \qquad (1)$$

where, $4a^3 + 27b^2 \bmod p \neq 0$.

Over binary field:

Suitable for implementation of embedded systems and for h/w implementation as simply XOR and AND gates are needed to implement the whole system. Less no of logic gates as compared to prime field implementation are required.

Binary field F2m, where m is a positive integer
Elliptic Curve equation:

$$y^2 + xy = x^3 + ax^2 + b \qquad (2)$$

where $b \neq 0$.

3.5 Elliptic Curve Cryptography Algorithm:

1. Both sender and receiver agrees to some publicly-known data items:

i. The elliptic curve equation containing parameter values of 'a' and 'b' and prime, p
ii. The elliptic group computed from the elliptic curve equation
iii. A base point, B, taken from the elliptic group

2. Each user generates their public/private key pair
- Private Key = x, an integer selected from the interval [1, p-1]

3. Public Key = Q, product of private key and base point (Q = x*B)
4. Suppose Alice wants to send to Bob an encrypted message.
   Both agree on a base point, B
   Alice and Bob create public/private keys.

   Alice:
   Private Key = a
   Public Key = $P_A = a * B$

   Bob:
   Private Key = b
   Public Key = $P_B = b * B$

5. Alice takes plaintext message, M, and encodes it onto a point, P_M, from the elliptic group.
6. Alice chooses another random integer, k from the interval [1, p-1]
   The cipher text is a pair of points

$$\mathbf{P_C = [(kB), (P_M + kP_B)]} \quad \mathbf{(3)}$$

7. To decrypt, Bob computes the product of the first point from P_C and his private key, b

   i.e. b * (kB)

   Bob then takes this product and subtracts it from the second point from P_C

$$\mathbf{(P_M + kP_B) - [b\ (kB)]}$$
$$\mathbf{= P_M + k(bB) - b\ (kB)}$$
$$\mathbf{= P_M} \quad \mathbf{(4)}$$

   Bob then decodes P_M to get the message, M.

3.6 ECC Diffie-Hellman key Exchange (ECDH)

Public: Elliptic curve and base point B=(x, y) on curve
Secret: Alice's private key 'a' and Bob's private key 'b'

- Alice and Bob want to agree on a shared key.
- Alice and Bob compute their public and private keys.

Alice:
Private Key = a
Public Key = $P_A = a * B$

Bob:
Private Key = b
Public Key = $P_B = b * B$

- Alice and Bob send each other their public keys.
- Both take the product of their private key and the other user's public key.

Alice → $K_{AB} = a(bB)$
Bob → $K_{AB} = b(aB)$
Shared Secret Key = $K_{AB} = abB$

4 Implementation Details

Registration: First the voter will register on the website ucshivam.5gbfree.com/registration and after registration successful, it will generate a unique id for the voter which will be sent to the user's mail.

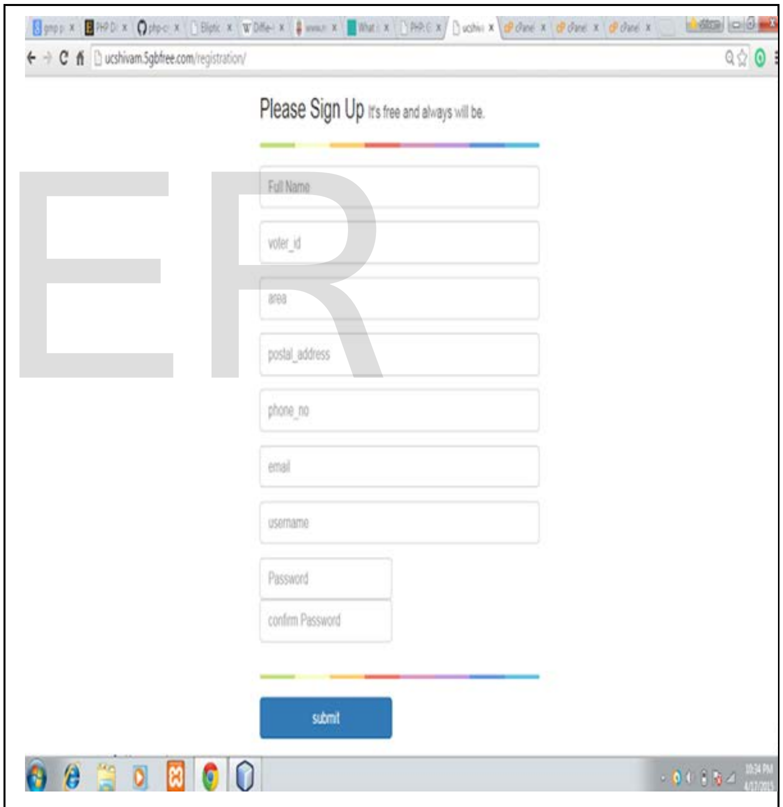
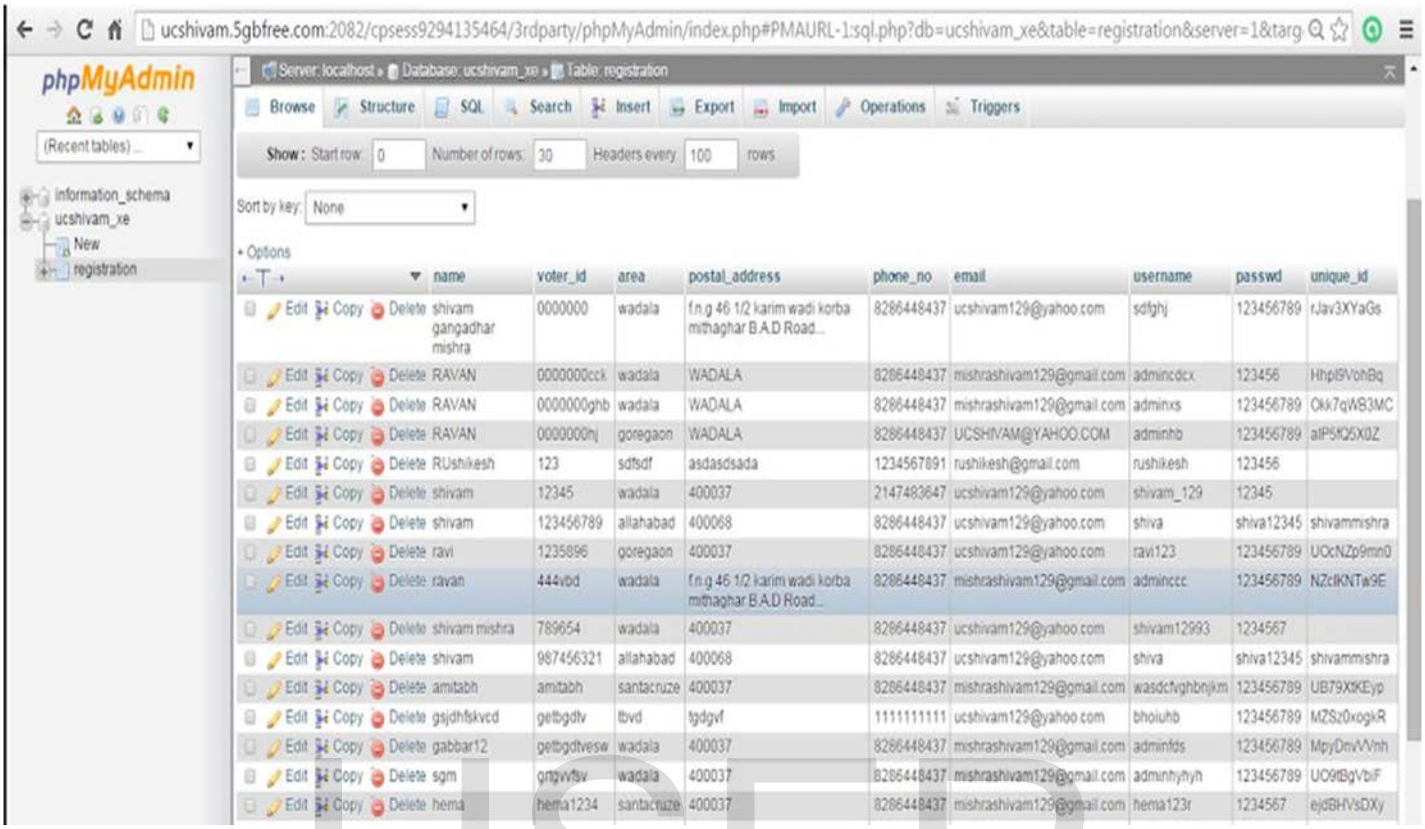


Fig. 3. Online Registration Webpage.

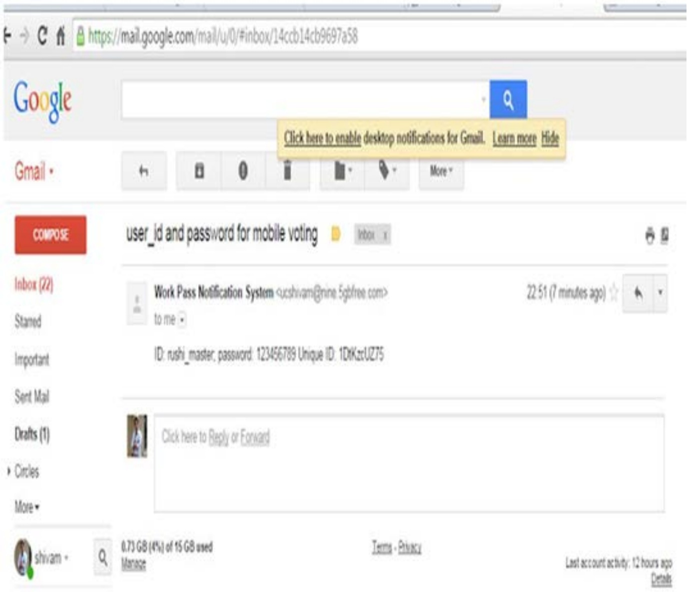
Once the user submits all the entered details will be stored into the database server which is our database server as shown in figure 4.


ucshivam.5gbfree.com:2082/cpsess9294135464/3rdparty/phpMyAdmin/index.php#PMAURL-1:sql.php?db=ucshivam_xe&table=registration&server=1&targ
phpMyAdmin
(Recent tables) ...
information_schema
ucshivam_xe
New
registration
Server: localhost » Database: ucshivam_xe » Table: registration
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Triggers
Show : Start row: 0 Number of rows: 30 Headers every: 100 rows
Sort by key: None
+ Options

	name	voter_id	area	postal_address	phone_no	email	username	passwd	unique_id
Edit Copy Delete	shivam gangadhar mishra	0000000	wadala	f.n.g 46 1/2 karim wadi korba mithaghar B.A.D Road...	8286448437	ucshivam129@yahoo.com	sdfghj	123456789	rJav3XYaGs
Edit Copy Delete	RAVAN	0000000cck	wadala	WADALA	8286448437	mishrashivam129@gmail.com	admincdcx	123456	Hhpl9VohBq
Edit Copy Delete	RAVAN	0000000ghb	wadala	WADALA	8286448437	mishrashivam129@gmail.com	adminxs	123456789	Okk7qWB3MC
Edit Copy Delete	RAVAN	0000000hj	goregaon	WADALA	8286448437	UCSHIVAM@YAHOO.COM	adminhb	123456789	alP5fQ5X0Z
Edit Copy Delete	RUshikesh	123	sdfsdf	asdasdsada	1234567891	rushikesh@gmail.com	rushikesh	123456	
Edit Copy Delete	shivam	12345	wadala	400037	2147483647	ucshivam129@yahoo.com	shivam_129	12345	
Edit Copy Delete	shivam	123456789	allahabad	400068	8286448437	ucshivam129@yahoo.com	shiva	shiva12345	shivammishra
Edit Copy Delete	ravi	1235896	goregaon	400037	8286448437	ucshivam129@yahoo.com	ravi123	123456789	UOcNZp9mn0
Edit Copy Delete	ravan	444vbd	wadala	f.n.g 46 1/2 karim wadi korba mithaghar B.A.D Road...	8286448437	mishrashivam129@gmail.com	adminccc	123456789	NZclKNTw9E
Edit Copy Delete	shivam mishra	789654	wadala	400037	8286448437	ucshivam129@yahoo.com	shivam12993	1234567	
Edit Copy Delete	shivam	987456321	allahabad	400068	8286448437	ucshivam129@yahoo.com	shiva	shiva12345	shivammishra
Edit Copy Delete	amitabh	amitabh	santacruze	400037	8286448437	mishrashivam129@gmail.com	wasdcfvghbnjkm	123456789	UB79XtKEyp
Edit Copy Delete	gsjdhfskvcd	getbgdtv	tbvd	tgdgvf	1111111111	ucshivam129@yahoo.com	bhoiuhb	123456789	MZSz0xogkR
Edit Copy Delete	gabbar12	getbgdtvesw	wadala	400037	8286448437	mishrashivam129@gmail.com	adminfds	123456789	MpyDmVVnh
Edit Copy Delete	sgm	grtgvvfsv	wadala	400037	8286448437	mishrashivam129@gmail.com	adminhyhyh	123456789	UO9tBgVbiF
Edit Copy Delete	hema	hema1234	santacruze	400037	8286448437	mishrashivam129@gmail.com	hema123r	1234567	ejdBHVsDXy

Fig. 4. Database Server.

The unique id which is generated after registration is send to the user's email id as shown in figure 5.


https://mail.google.com/mail/u/0/#inbox/14ccb14cb9697a58
Google
Click here to enable desktop notifications for Gmail. Learn more Hide
Gmail
More
COMPOSE
Inbox (22)
Starred
Important
Sent Mail
Drafts (1)
Circles
More
shivam
Inbox
Click here to Reply or Forward
0.73 GB (4%) of 15 GB used
Manage
Terms - Privacy
Last account activity: 12 hours ago
Details

user_id and password for mobile voting

Work Pass Notification System <ucshivam@nine.5gbfree.com> 22:51 (7 minutes ago)
to me

ID: rushi_master, password: 123456789 Unique ID: 1DtKzrUZ75

Fig. 5. Email containing unique ID, Email ID, password.

Now when voting application is run on android phone, user is asked to enter login id and password as shown in figure 6.

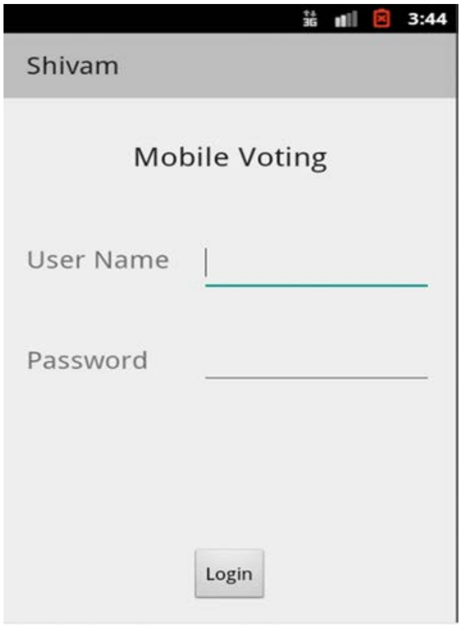


Fig. 6. Mobile Interface for Login.

On successful login, the mobile application asks for the unique id. Here, at the backend the application will match the entered unique id with the one in the database. If the id matches it will display the candidate list as shown in figure 7 and figure 8.

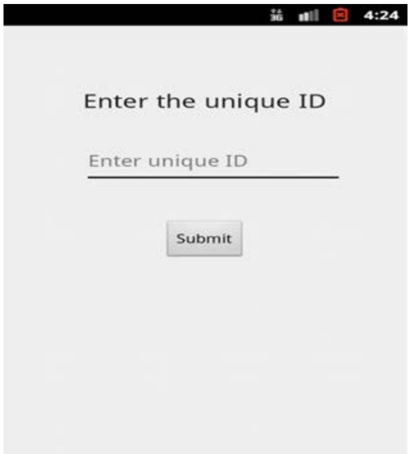


Fig. 7. Mobile Interface for unique ID verification.

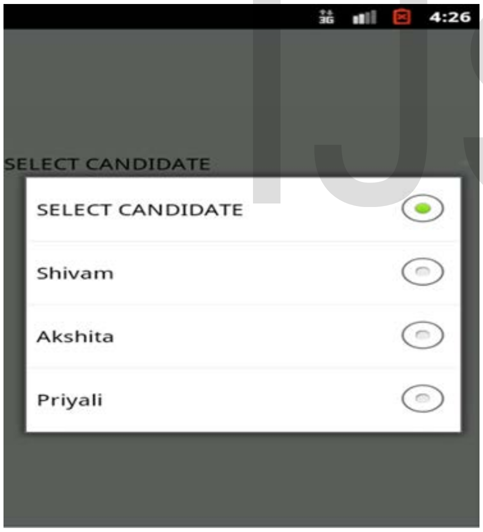
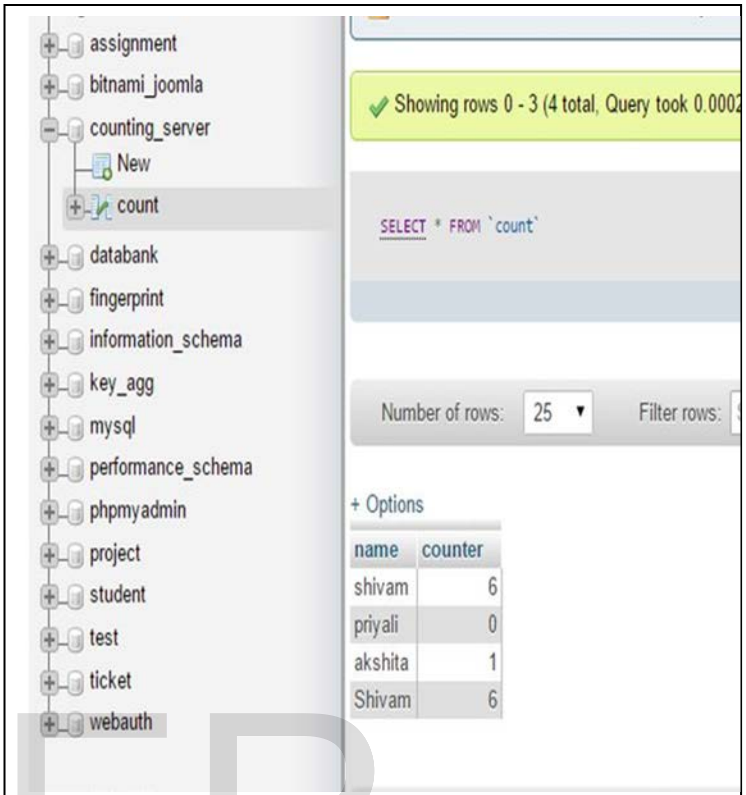


Fig. 8. Mobile Interface for Candidate List.

After user selects one of the candidate from given list, at the counting server, the voter's vote gets stored as shown in figure9.

On Successful increment in the vote count at counting server, user will get "voting successful" message as shown in figure10.

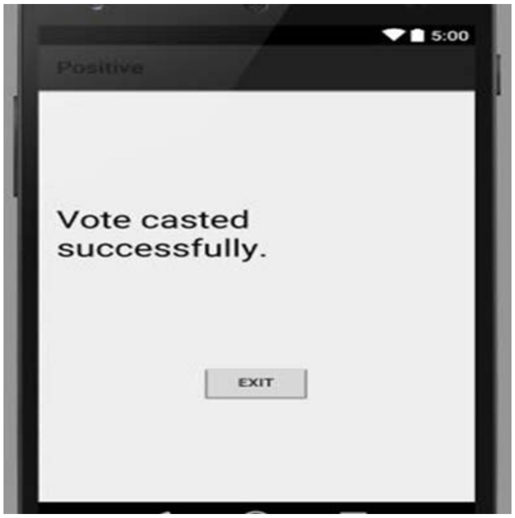


✓ Showing rows 0 - 3 (4 total, Query took 0.0002

```
SELECT * FROM `count`
```

name	counter
shivam	6
priyali	0
akshita	1
Shivam	6

Fig. 9. Counting Server Database.



Vote casted successfully.

Fig. 10. Mobile Interface for "voting successful" message.

5 Conclusion

The paper presents secure mobile voting system based on ECC which ensures secure voting requirements of privacy, integrity, anonymity. As compared to traditional voting systems, mobile voting will be more convenient, user friendly and quick as voter can vote at any time from any place through his mobile device. ECC is used in mobile voting over RSA, DES, Diffie-hellman and other encryption algorithms as its inverse operation gets harder, faster, against increasing key length than do the inverse operations. Our scheme enhances the security and provides more mobility and convenience to voters, where the voters' privacy is protected by applying ECC.

References

[1] Manish Kumar, T.V.Suresh Kumar, M. Hanumanthappa, And D Evangelin Geetha: "Secure Mobile Based Voting System".

[2] Chun-Ta Li1, Min-Shiang Hwang: "A Secure and Anonymous Electronic Voting Scheme Based on Key Exchange Protocol", International Journal of Security and Its Applications Vol. 7, No. 1, January, 2013.

[3] Dr.R.Shanmugalakshmi and M.Prabu:" Research Issues on Elliptic Curve Cryptography and Its applications", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.

[4] Dr.M.Kamaraju, P.V.Subba Rao and T.Venkata Lakshmi "A NOVEL VOTING SYSTEM USING SMS".

[5] Tarun Narayan Shankar, G.Sahoo:"CRYPTOGRAPHY WITH ELLIPTIC CURVES", International Journal of Computer Science and Applications Vol. 2, No. 1, April / May 2009.

[6] Debdeep Mukhopadhya: "Elliptic Curve Cryptography.pptx".

[7] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[8] http://cr.yp.to/ecdh.html (Daniel Bernstein)

[9] Aditya Babel:"Elliptic Curve Cryptography".

[10] Ikshwansu Nautiyal, Madhu Sharma:" Encryption using Elliptic Curve Cryptography using Java as Implementation tool", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1, January 2014.

[11] Konstantinos Chalkias, George Filiadis, and George Stephanides:" Implementing Authentication Protocol for Exchanging Encrypted Messages via an Authentication Server based on Elliptic Curve Cryptography with the ElGamal's Algorithm", International Journal of Computer, Information, Systems and Control Engineering Vol:1 No:7, 2007.

[12] Lokesh Giripunje, Sonali Nimbhorkar:" Comprehensive Security System for Mobile Network Using Elliptic Curve Cryptography over GF (p)", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May2011.