International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Confidentiality Preserving Instant Runoff Voting System

Reena Kharat, P. Sanyasi Naidu, Shital Chattar

Abstract: ***Voting is a mandatory application in any democratic country for decision making. The E-voting gives the promise or confidence of giving or delivering a convenient, straight forward and economical results. E-Voting system used many cryptographic methods to reduce the security problems in the election process. Voting is one of the essential activity which is used in various applications from student's secretory elections, reality television shows, to national elections. With the goal of better efficiency, scalability, speed and lower cost, voting is currently changed from paper based to the use of electronic medium. This is targeted to meet better security, such that voting result gives true opinion of the voters. As of late in cryptography a few changes enable us to run troublesome calculations inside the encoded area. In democratic countries like India, Instant Runoff voting method is used in election of the President of India. In IRV, voter can vote by ranking the candidates in order of preference. To protect voter's privacy, encryption is mostly used to ensure security in open network such as the internet. The cryptosystem based on Elliptic curve cryptography (ECC) is becoming the latest technology of public key cryptography. In proposed E-voting system, voter's confidentiality is maintained by ECC, blind signature is used for ballot anonymity and authentication. This proposed scheme will effectively ensure confidentiality, anonymity and integrity of ballot in instant runoff voting method.***

Index Terms**: Online voting, encryption, decryption, confidentiality, public key, private key, Authentication server, vote counting server, ballot, Instant runoff, results, public key cryptography, blind signature.***

I.INTRODUCTION

Election is a mandatory process, in any democratic countries. The process of election provides an official mechanism to individuals to share their perspectives to the administrations. In past days, the method of voting is so extensive and tedious. Voter needs to come personally to cast a ballot at survey focus, as a result of this, low investment rate of casting a ballot. Another method of casting a ballot is Vote-via-mail .This technique is suitable for those voter, who live in populated region and who work far from the voting center. Now and again this technique is tedious for the expert to oversee on the grounds that it requires additional work for sending the mail, gathering and check the ticket physically.

Types of electrol systems are **plurality voting:**

Plurality voting is system in which the candidates with the more number of votes can win, there is no necessity to get a majority of votes. **Majority voting**: It could be a system within which the candidate got to receive a majority of votes from the remaining candidates**. Proportional voting:** It is electoral system within which division in associate degree electro rate are reflected proportionately within the electoral body. In E-voting citizens casts a ballot through a computerized framework instead of a paper. In IRV, casting a ballot procedure which is utilized in single situate election with very two applicants instead of select only for one up-and-comer. Voters in IRV elections will rank the candidates according to the preference. IRV has the result of avoiding split votes once multiple candidates earn support from similar voters.

A.Running example of IRV system

Table 1- Example

Number of Voters	5	7	8	3	10
1st choice	D	A	B	B	C
2nd choice	A	C	D	A	A
3rd choice	B	D	C	D	B
4th choice	C	B	A	C	D

There are a total of **5+7+8+3+10=33** votes, shown in **Table 1**

Using the basic plurality method, the winner would be Candidate B.

Step 1

A =7

B =8+3=11 (Notice 11/33=33.33%, not a majority)

C =10

D =5

Step 2-eliminate D

After eliminating candidate D, the vote count table shown in Table 2.

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author

Reena Kharat*, CSE Department, GITAM Institute Of Technology, GITAM University, Visakhapatnam

Computer Department, Pimpri Chinchwad College of Engineering, Pune, India.

P.Sanyasi Naidu, CSE Department, GITAM Institute Of Technology, GITAM University, Visakhapatnam

Shital Chattar, Computer Department, Pimpri Chinchwad College of Engineering, Pune, India.

Table 2- Count Table after deleting candidate D

Number of Voters	5	7	8	3	10
1st choice		A	B	B	
2nd choice	A			A	A
3rd choice	B				B
4th choice		B	A		

A =7+5=12(Notice 12/33=36.36%, not a majority)
B =8+3=11
C =10
D =0, shown in Table 2

Step 3-Eliminate C
After eliminating candidate C, the vote count table shown in Table 3.

Table 3- Count Table after deleting candidate C

Number of Voters	5	7	8	3	10
1st choice		A	B	B	C
2nd choice	A	C		A	A
3rd choice	B		C		B
4th choice	C	B	A	C	

A =7+5=12+10=22
B =8+3=11
C =0
D =0
The winner is A since with 22/33= 66.66% (Majority)

II. LITERATURE SURVEY

In [1]**,** the author clarify a protected obvious Ranked decision web based casting a ballot framework depends on homomorphic Encryption. In past day's elections is taken on paper. For that it requires bunches of assets and for that the elimination of forests, which ends up climate disintegration. To protect the privacy of the votes, every cast ballot is encrypted using the exponential ElGamal cryptosystem before submission. This methodology also called homomorphic tallying. Lastly, the tallied result can have decrypted by consideration of all authorities. This paper, e-casting a ballot framework comprises of the accompanying stages: instatement, enlistment, ticket casting, verification of voters, and check of tallies, counting and result uncovering. [1] In [2], the author proposes an Elliptic curve cryptosystem**.** The ECC is robust, fast, and public key cryptography for verifying constrained environment. Elliptic Curve Cryptography has been an ongoing examination area within the field of Cryptography [2], As compared to different cryptologic techniques, ECC furnishes larger amount of security with lesser key size. The author clarifies the procedure of encryption/decryption of content message. It is much impossible to aim a brute force attack to interrupt the cryptosystem victimization using ECC.
In [3], author propose a secure e voting for preferential election. E-casting ballot framework will significantly advance the power and without a doubt, the straightforwardness of national elections. This paper presents a case study of cryptologic protocols for secure evoting systems that use preferential voting strategies. In this paper, the size of electronic vote for preferential voting system is larger than 1-out-of-m voting system, when number of candidate's m increases. In preferential voting system, the size of the vote is at least log2 (m!) Bits.
In [4]**,** author propose a linked-list to deal with cryptographically secure elections using instant runoff voting. There are number of ways have been planned to lead cryptographically secure elections. A large portion of those conventions spend significant time in 1-out-of-n casting a ballot plans. We have a tendency to propose a linked list based theme that offers improved security over current plans, hiding citizen preferences that should not be disclosed. In [5]**,** author propose another technique relies upon cryptography to guarantee voters and candidate's confidentiality in the E voting referred as a NOTE system. In this framework, the election commission will be responsible for part of vote counting duties other than gathering and confirms the voter ID. The votes and the candidates' names are isolated into two sections during the counting process.EC will hold the candidates name secret before the tally comes up; the vote counting panel (VCS) just count the votes and isn't include in revealing the vote tally by virtue of the anonymity of the candidates. Only EC can disclose the final tally after VCC has tallied all votes without knowing who the votes are for during the vote counting procedure. This strategy effectively will guarantee voter's and candidate's confidentiality

III. SECURITY MECHANISMS IN E-VOTING

In this planned work, we have a tendency to built up an E-voting, which applies security mechanisms therefore on accomplish the protection needs essential for any election process. In this framework or system, voter's privacy is keep up by employing a blind signature for confidentiality.

A.*Elliptic curve cryptography (ECC)*

Elliptic Curve Cryptography or Cryptosystem (ECC) is sort of public-key cryptosystem. It was established by Victor Miller of IBM and Neil Koblitz of the University of Washington in the year 1985. ECC likely to be used an acronym for Elliptic Curve Cryptography. It is relying on the most recent arithmatics and gives a relatively more secure foundation than the first generation public key cryptography systems for example RSA. [2]

a. Encryption and Decryption

ECC can encrypt plaintext message, M, into cipher text, C, and decrypt the cipher text back into plaintext message, M.
The plaintext message M is first converted to a single large integer and then mapped to a point on the curve. The most important advantage of elliptical curve cryptography is the use of smaller keys providing the same level of security.
ECC can provide the same security with 164-bit key that other systems provide with 1024- bit key. It is mostly useful for mobile applications as it has the capability to provide high level security with low computing power and battery resource.

Using ECC i.e. public key cryptosystem used to generate public key and private key to encrypt and decrypt the message [7][8].

b. Key Generation

Key generation is most essential part where both public and private key have to generate. In this process the sender will convert the message into cipher text using receiver's public key and the receiver will convert again back into plain text using its private key. [10]

Select a number 'd' within the range of 'n'.

Generate public key using the equation Q=d*P

d=the random number chose inside the scope of (1 to n-1).

P is the point on the curve.

'Q' is the public key and'd' is the private key.

c. Encryption

Let 'm' be the message that sender wants to send to the receiver. Select k randomly from [1 to (n-1)]. Two cipher text generated i.e. c1 and c2

C1=k*P

C2=M+k*Q

C1 and c2 send to the receiver.

Decryption

For getting original message, calculate

M= C2-d*C1

M is the original message that sender sends.

Proof

M can be represented as 'c2-d*c1'

C2-d*C1=(M+k*Q)-d*(k*p)

=M+k*d*p-d*k*p

=M (Original Message)

B. *Blind signature*

A blind signature is fairly like to the digital signature. The distinction is that it provides permission to someone to induce another person to sign a message while not revealing the content of message [15]. Blind signature provides the confidentiality of voters. The signature is utilized to verify the voters without uncovering the substance of a ballot. Hence the specialist whose obligation is to check the qualification of a voter won't know whom a voter cast a ballot in support of[14][13]. In Evoting process a ballot is blinded to get the confidentiality of voter. A voter is essential to having a signature of authentication server (AS) when that voter votes. To acquire a secrecy of his ballot, a voter casts a ballot, B. Then encrypt a ballot using public key. Then blind a ballot using blind factor

$$m' = H(m)\, r^e \bmod n.$$

The blind version uses a random value r such that r is a prime i.e. gcd(r, n) =1.Consider {n, e} be the public key of authentication server and {n, d} is private key .The voter sends the following to the authentication server:

$$m' = H(m)\, r^e \bmod n$$

Then authentication server gives blinded sign on calculating

$$s' = (m')^d \bmod n.$$

s' is send back to the voter of a ballot, who can then remove the blinded factor or unblinds the ballot, to reveal the valid signature of message m by calculating the following.

$$S = s' . r^{-1} \bmod n = m^d$$

IV. EVOTING SYSTEM ARCHITECTURE

In this section we elaborate the overall architecture of online voting system. In proposed E-voting system, we have used two servers. One is Authentication Server (AS) and another is Vote Counting Server (VCS). The authentication server is responsible to check if voter is authentic or not. It is also responsible to authenticate ballot sent by the authentic voter during voting. The authentication server also checks the status of voting. If status is 0 then allow voter to vote otherwise not. This is made for avoiding the double voting. Vote counting server checks authenticity of ballot received. If the ballot is authenticated, then it is considered for counting. If the ballot is not authenticated, then this ballot will be discarded.

Our proposed E-voting system works in three phases

A. Initialization Phase

B. Voting Phase

C. Vote Counting Phase

Initialization Phase

Algorithm-1: Algorithm for Initialization Phase

1. Vote Counting Server (VCS) generates public key and private key pair using ECC cryptography.
2. Authentication Server (AS) generates public key and private key pair using RSA cryptography.
3. VCS sends the public key to the Authentication Server. Authentication Server also sends public key to Vote Counting Server.

The Architecture diagram for Key exchange between Authentication server and Vote Count Server is shown in fig 1.

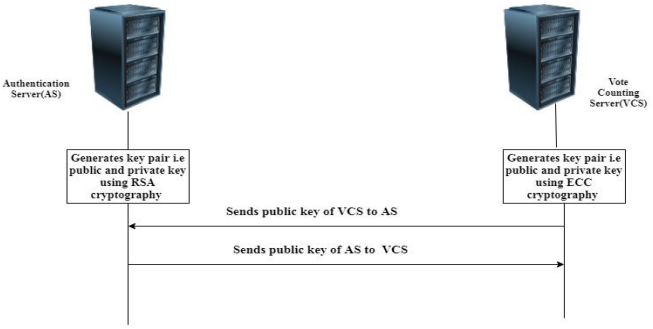

Fig 1. Key exchange between AS and VCS

Voting Phase

Algorithm-2: Algorithm for Voting Phase

1. Voter login into system using ID and password.
2. If the voter is an authentic voter and has not voted before then authentication server sends empty ballot, public key (e, n) of AS and public key of VCS to the voter.

3. The voter casts his ballot and encrypts the ballot using public key of VCS using following loop.
   for (i=1 to n candidates)
   Voter selects k randomly from [1 to (n-1)].
   Voter selects M as a choice.
   P – Point on curve
   Q- Public key of VCS

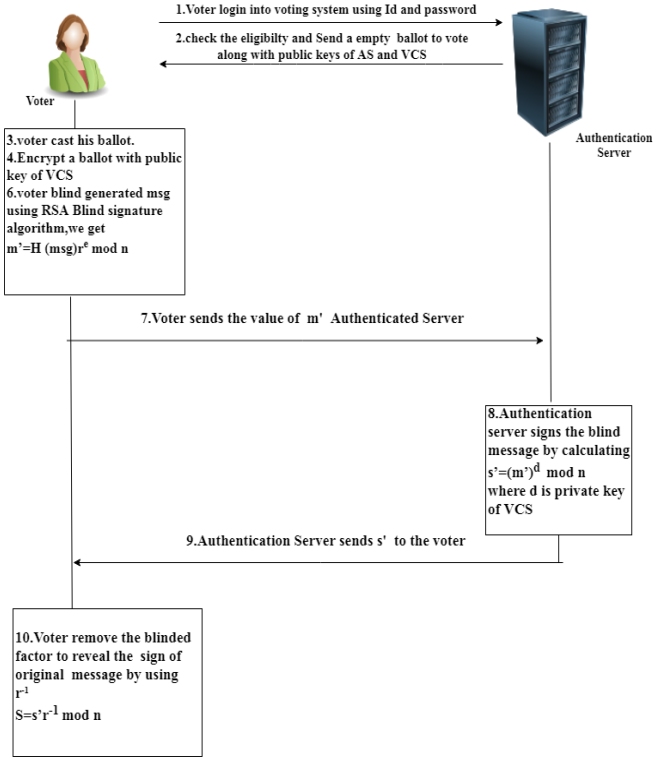

Fig 2. Data flow diagram of voter and Authentication server

   Msg= ""
   Compute c1i=k*P;
   Compute c2i=M +k*Q
   Return Msg= (Msg ||C_{1i}|| C_{2i})
   End for

4. After encryption, voter blinds generated message using RSA blind signature algorithm.
   Voter selects the value of r randomly such that gcd (r, n) =1.Voter blinds the message using the blind factor r as follows:
   $m' = H(Msg)r^e \bmod n$
   Voter sends m' to the Authentication Server to get blind signature.

5. After authentication of voter, the Authentication Server signs the blind message, by calculating
   $s' = (m')^d \bmod n$
   Where d is private key of Authentication Server.
6. Authentication Server sends signed blind message to the voter.
7. Voter unblinds the message to reveal the sign of original message, by using r-1.
   $S = s'. r^{-1} \pmod n = (H(Msg))^d \bmod n$
8. Voter sends the copy of signed message S along with C_{1i} , C_{2i} to the Vote Counting Server.

Vote Counting Phase

Algorithm-3: Algorithm for Vote Counting Phase

1. Vote Counting Server verify the signature of received message for authentication and tampering as follows, shown in fig 3:
   VCS decrypts signature using public key (e, n) of Authentication Server(AS).
   Decryptedmsg = $S^e \bmod n$.
   msg= ""

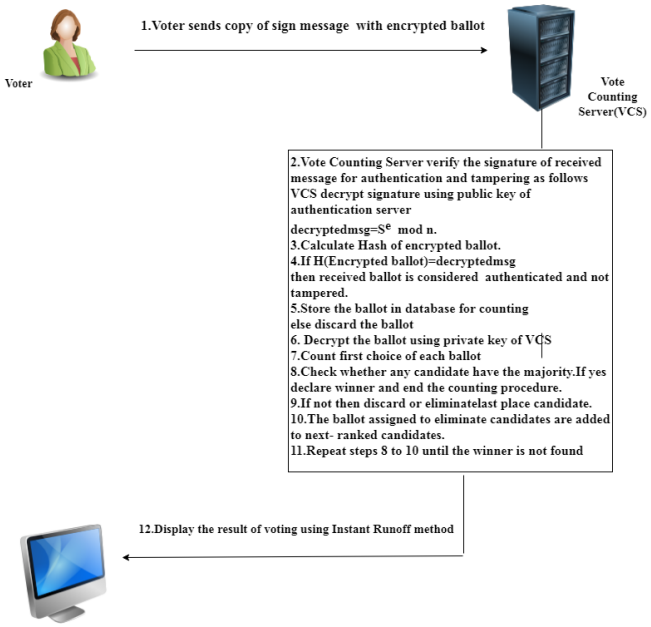

Fig 3. Data flow diagram of voter and Vote Counting Server

   for (i=1 to no. of choices)
   msg= (msg || C_{1i}|| C_{2i})
   end for
   If Hash (msg) =decryptedmsg
      Then received ballot is authentication and not tampered.Store the ballot in database for counting
   else
      Discard the ballot.

2. Decrypt authenticated ballot using private key of VCS

   Original ballot = $C_{2i} - d * C_{1i}$

3. Voter ranks the candidates in order of preference. They rank the candidates as 1st, 2nd, 3rd etc.
4. Count first choice of each ballot.
5. Check whether any candidate have the majority. If yes, then declare winner and end the counting procedure.
6. If not then discard or eliminate last place candidates.
7. The ballots assigned to eliminate candidates are added to next –ranked candidates.
8. Repeat steps 4 to 6 until the winner is not found.

V. RESULTS AND DISCUSSION

Instant-runoff voting (IRV) is a type of ranked preferential voting method. IRV is used in single-seat elections with more than two candidates.

In IRV, voters can rank the candidates in order of preferences, instead of showing support for only one candidate. Initially, ballots are counted for each voter's 1st choice. If a candidate has more than half of the votes i.e. majority among all, that candidate wins the election. If not, then the candidate with the fewest votes is discarded and added to the next ranked candidate. This process continues until a candidate has more than half of the votes. The casted ballot confidentiality is also maintained by using Elliptic curve cryptography. The voter's privacy is also achieved by using blind signature.

Initially, in proposed system the voter should be register by filling the personal information such as First name, Last name, Gender, Date of birth, Email Id and password.

The Voter registration form is shown in fig. 3

Fig 3. Voter Registration

After successful registration, voter will login into the system using Login-Id and password,shown in fig. 4

Fig 4. Voter Login

Voter successfully entered into the system, the Authentication server will send empty ballot to the voter for voting, shown in fig 5

Fig 5. Ballot for Vote

Registered Authenticated voter gives votes in order to the preferences. In vote count table, we get the information about voter's choices in order of 1st, 2nd 3rd etc., shown in fig. 6

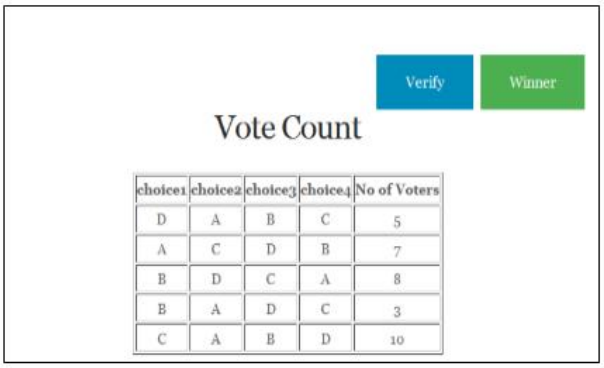

Fig 6. Vote Count Table

By applying Instant Runoff voting method, the winner of election is declared, shown in fig.7

Fig 7. Winner Declaration

VI.CONCLUSION

In this paper, a new secure e-voting system for instant runoff voting is presented. We have used Elliptical Curve Cryptography and blind signature. ECC provides confidentiality to casted ballot. In IRV, we cannot do counting without decrypting votes. This is because during counting process, if none holds majority then ballot added to eliminated candidate are to be assigned to the next preference ranked candidate.

For this purpose, we need to know all preferences of each ballot. The blind signature blinds the casted ballot to achieve anonymity and privacy of voter. It rejects the utilization of manual casting a ballot procedure and gives instant results in secure way. No one will forge votes on behalf of others and multiple times. This casting a ballot technique will Saves time and reduces human intervention. The system is flexible and secured to be used.

REFERENCES

1. Yang, Xuechao, et al."A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption." IEEE Access 6 (2018): 20506-20519.
2. Vanstone, Scott A. "Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments." Information Security Technical Report 2.2 (1997): 78-87.
3. Aditya, Riza, et al. "Secure e-voting for preferential
4. elections." International Conference on Electronic Government. Springer, Berlin, Heidelberg, 2003.
5. Keller, Jason, and Joe Kilian. "A linked-list approach to cryptographically secure elections using instant runoff voting." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2008
6. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223238. Springer, Heidelberg (1999).
7. W.Lu,A.L.Varna,andM.Wu‘‘Confidentiality-preserving image search: comparative study between homomorphic encryption and distance-preserving randomization,’’ IEEE Access, vol. 2, pp. 125–141, 2014
8. Parmer, Payal V., et al. "Survey of various homomorphic encryption algorithms and schemes." International Journal of Computer Applications 91.8 (2014)..
9. Ahmad, Tohari, Jiankun Hu, and Song Han. "An efficient mobile voting system security scheme based on elliptic curve cryptography." Network and System Security, 2009. NSS'09. Third International Conference on. IEEE, 2009.
10. Vanstone, Scott A. "Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments." Information Security Technical Report 2.2 (1997): 78-87.
11. M. Hirt and K. Sako, ``Effcient receipt-free voting basedonhomomorphic encryption," in Advances in Cryptology_EUROCRYPT. Bruges, Belgium: Springer, 2000, pp. 539_556. [Online]. Available:
12. Stalling, W., Cryptography and Network Security,3“ Edition, Prentice Hall, New Jersey, 2003
13. Ibrahim, Subariah, et al. "Secure E-voting withblind signature." 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.. IEEE, 2003.
14. Brickell, Ernest F. "A survey of hardware implementations of RSA." Conference on the Theory and Application of Cryptology. Springer, New York, NY, 1989.
15. Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." Proceedings of 2011 6th International Forum on Strategic Technology. Vol. 2. IEEE, 2011.
16. Chhabra, Aayush, and Srushti Mathur. "Modified RSA algorithm: a secure approach." 2011 International Conference on Computational Intelligence and Communication Networks. IEEE, 2011.
17. Hussein, Handy, and Hussein Aboelnaga. "Design of a secured evoting system." 2013 International Conference on Computer Applications Technology (ICCAT). IEEE, 2013.

AUTHORS PROFILE

Reena kharat is working as Assistant Professor in Compute Engineering department of Pimpri Chinchwad College of Engineering, Pune. Reena has completed her Masters of Technology in Computer Science & Engineering from Indian Institute of Technology, Bombay. Currently, she is pursuing her Ph.D. in Computer Science & Engineering department of GITAM Institute of Technology, from GITAM University, Visakhapatnam. She has total 15 years of teaching experience. She has guided seven post graduate student projects and 18 undergraduate student projects. She also worked in financial industry as software engineer for two years. Her area of interest is Information Security, data mining and data analytics. She has published 22 research papers.

P. Sanyasi Naidu is working as Associate Professor in Computer Science & Engineering department of GITAM Institute of Technology, from GITAM University, Visakhapatnam. He has completed his Ph.D. in Computer Science & Engineering from Andhra University. He has completed Masters of Technology in Computer Science & System Engineering from Andhra University. He has total 22 years of teaching experience. He has guided 18 post graduate student projects and 35 undergraduate student projects. Currently he is guiding 8 research scholar for Ph.D. His area of interest is information & Network Security. He has published 29 research papers. He is life member of ISTE.

Shital Chattar received the bachelor’s degree in Information Technology from Pimpri Chinchwad College of Engineering, PUNE University. She is currently pursuing M.E in Computer Science from Pimpri Chinchwad College of Engineering, PUNE University. Shital has total 6 years teaching experience of Diploma College (Pimpri Chinchwad Polytechnic) and working as visiting faculty in Pimpri Chinchwad Polytechnic for 1 year. Shital has experience in subjects- ’C’ Programming, Computer security, Network Management ,Computer fundamental, Professional practices, computer Architecture & management & Software Engineering etc. She has guided 12 groups of diploma students for their final projects. Her research interest includes cryptosystems, Information security, and data mining.