DATA SECURITY FOR ANY ORGANIZATION BY USING PUBLIC KEY INFRASTRUCTURE COMPONENTS AND MD5, RSA ALGORITHMS

Ruchi Verma[1], Shikha Agrawal[2]

[1]M.Tech. Scholar, [2]Assistant professor, Computer Science & Engineering, CSIT Durg, Chhattisgarh, India,
ruchi.verma393@gmail.com, shikhaagrawal@csitdurg.in

Abstract

In Digital world all type of information are moved around the whole world in the digital form. Securities of these digital data are very necessary from the intruder, enemies, and unauthorized individuals for any government and non-government organizations. Security is the protection against danger, criminals and loss. There are many features to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. Cryptography is one essential feature for secure communications. There are two techniques are used in cryptography one is secret key cryptography and another is public key cryptography. A PKI does not a particular business function; it is providing a foundation for other security services. The primary function of a PKI is to allow the distribution and use of public keys and certificates with security and integrity. The components of public key infrastructure are certification authority (CA), certificate revocation, registration authority (RA) and digital certificate. PKI contain complete information and identifications of there sender and receiver for authentication. In the basis of these identities PKI provide certificates and authentication for secure communication. In this paper study different components of PKI and there uses for secure any type of data. This paper presents the performance of a secure application for private organizations that offers services to both owner and other members of the same organization. The primary focus of this paper is better implementation of PKI with the help of there algorithms.

Index Terms: *Security, Cryptography, Encryption, Decryption, Public key, Private key, Public Key Infrastructure (PKI), Digital Certificate, Certification Authority (CA), Revocation, Registration Authority (RA).*

----------***----------

1. INTRODUCTION

Every open and private network needs data and network security for transactions of secret and confidential data among the government agencies, business and private organizations. Every sender wants to send there data securely, without any changes and duplicate of there respective data. In the same way every receiver wants to receive accurate and exact data sender to be send. For information security we need privacy or confidentiality, authentication, message integrity and non-repudiation. Every user want to authentication for secure transaction of data means that unauthorized person should not access, intercept and copy of these data. Sender and receiver have all the information about together for the identification of authenticate sender and receiver. Message integrity means assuring the receiver that the received message should not been altered it means receiver receives the original data. Non-repudiation is a mechanism to prove that the sender really sent this message and sender is authenticate sender. Cryptography is the science of writing in secret code and hides the message [1]. Cryptography is not only used for protect data from theft or alteration or copied, but can also be used for authentication of sender and receiver. There are three type of cryptographic algorithm are used for security of data: symmetric/secret key cryptography, public key cryptography and hash functions [1]. This technique is used in application of advanced societies, security of ATM cards, electronic commerce and computer passwords. In cryptography the basic concepts are: cipher, key, plaintext and cipher text. Cipher is the encryption algorithm, key is a secret value which is used by cipher, and plaintext is the original message which is send by sender and cipher text is the result of encryption of the plaintext [2]. Secret key cryptography is used single private key for both encryption and decryption. The secret key is known to both the sender and receiver [3]. At all time sender have risk to send there secret/private key to the open network. The biggest problem of this algorithm is the distribution of the private key. Secret key cryptography is not practical for internet, it is suitable for encrypt private data and its encryption speed is very fast [4]. The development of the Internet provides the way in which the world communicates, but the Internet has also new problems of Internet communication are trust, privacy and Security. All sectors of economy need some formula for trusted and private secure transmission of electronic data between any two parties. The way of overcoming these problems are Public Key Infrastructure. Public key cryptography is based on two key systems. In public key cryptography without any sharing of secret key sender and receiver are perform secure communication over unsecure network [5]. In public key cryptography use one key

for encryption and other key for decryption. The sender used receiver's public key which is known to every one for encryption. The encrypted data is sent to the receiver, receiver decrypt this data with his private key. Only receiver can decrypt the data because no one else has the private key. In this algorithm the sender only need to know the receiver's public key and the receiver's private key is keep secret. Public key cryptography is slower but more secure than to the secret key cryptography. Public key cryptography fulfills all four aspects or requirement of security. Public Key Infrastructure is a system of digital signature; digital certificates, Certificate Authorities, and other registration authorities these components are used for verify and authenticate the validity of each entity involved in an online transaction. PKI can be used for email communication, web browsing, and online banking. Public Key Infrastructure is the combination of hardware, software, and people policies with aim to manage, create, issue, modify, store and remove digital certificates. The main benefit of the PKI is that it provides a system for distributing and managing digital certificates, in other words it manages transmission and storage of Public/Private keys.

2. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography is asymmetric key cryptography in this technique use two keys. When sender use this algorithm one key is used for encryption and other key is used for decryption. PKC is more secure than the secret key cryptography. PKC have all security requirements for secure communication. Symmetric key cryptography uses same key/secret key for both encryption and decryption. The advantages of symmetric key cryptography are – it is easy to implement, much faster than PKC and processing power of symmetric key cryptography is less [6].

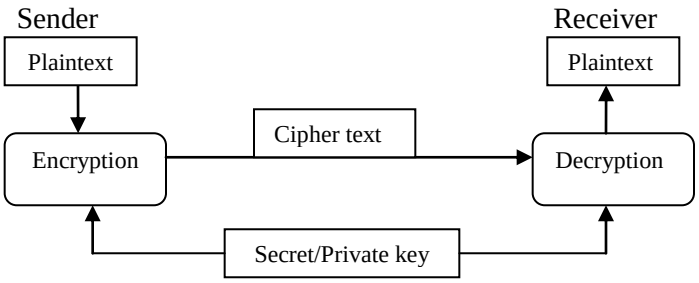

Fig-1: Symmetric key/same key/private key cryptography.

In symmetric key cryptography single key is used in which two parties sending there messages to each other must agree to use the same private key [3]. Now as single key are used between two parties for secure information transmission, they need a secure environment for that which is almost impossible, sharing of private key is risky and unsecure, it is disadvantage of symmetric key cryptography but in public key cryptography public key is used for encryption and it does not need to remain secure. That's why this type of key is called public because it does not matter other people know about it.

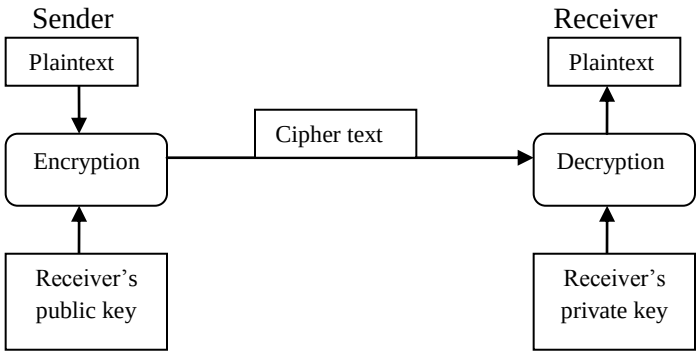

Fig-2: Asymmetric key/ public key cryptography.

PKC provides data integrity, message authentication, and privacy and non-repudiation aspects for security with digital signature. Digital signature is component of public key infrastructure which is used for certification and authentication of messages. Public Key Infrastructure (PKI) is a set of hardware, software, product, policies and procedures to create secure information and secure communication [7]. PKI provide frame work for components and applications to combine and achieve the requirement of security.

3. PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure is group of people, procedure, hardware, software and policies. All the requirement of security is fulfillment with the help of PKI components. With security and integrity, the functions of PKI allow the distribution and use of public key and certificates [8]. For the building of other applications, network and data security components, PKI is playing the role of foundation. In open network communication when we send any data electronically, the PKI gives guarantee of the privacy of that data and guarantee of correct source and destination of that data. PKI has application for communication and transactional security is – SSL, IPsec and HTTPS, and for email security is – S/MIME and PGP [9].

If two parties want to transact business securely and they not have ever met. In this case they use public key cryptography for secure transaction services; they must be able to receive each other's public keys and identities. They may be performed this type of secure transaction and if they will conduct business with more parties then they must rely on a trusted third party to identity authentication for corresponding key pair owners and distribution of these public keys [10]. Public key cryptography uses the technique of PKI (Public key infrastructure). In PKI digital signature technology are used that makes it important as a basis for security function in public key distribution.

4. COMPONENTS OF PKI

The basic components of public key infrastructure are certification authority, registration authority, digital signature, repositories and archives.

4.1 Digital Signature

In public key cryptography two different keys are used for encryption and decryption. If sender want to uses his/her private key for encryption and public key for decryption. Sender sends encrypted data with there public key to decrypt this data. In secure transaction of data message integrity are necessary for authentication of users, digital signature provide data integrity for the receiver to receive the original public key from the original sender, it means it proving that a message is effectively coming from a given sender. In Digital Signature message is digitally signed with Hash function. Hash function is used for message digest. These digest message are encrypted by sender's private key and than message is digitally signed and this digitally signed message is attached with original message, it is called digital signature, is send to the receiver. From receiver side for successful decryption of message we need verification of digital signature. Verification means that no doubt that it is sender's private key which is used for encryption of data. From Fig-3 we can easily understand the process of digital signature.

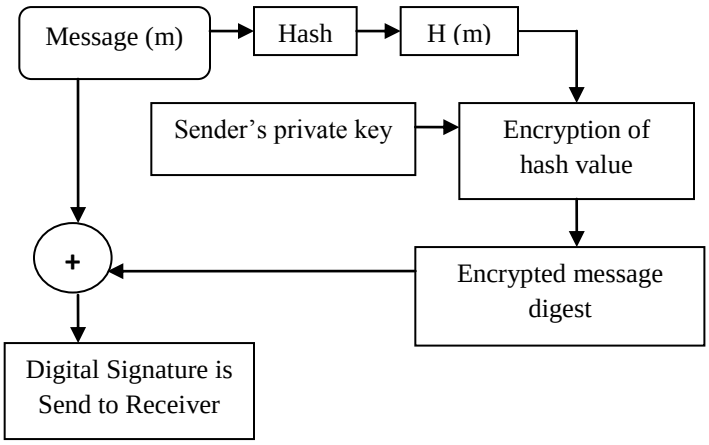

Fig-3: Digital Signature (Encryption) in sender side.

In the receiver side, receiver separates original message (m) and encrypted message digest. After separating, receiver apply Hash algorithm to the message (m) for message digest H (m). In another side receiver decrypt the digital signature with the help of sender's public key and get message digest H (m). If both sided message digest H (m) are equal, it means that there is no doubt that it is sender's private key that encrypted the message. Fig-4 shows the receiver end process of verifying of digital signature.

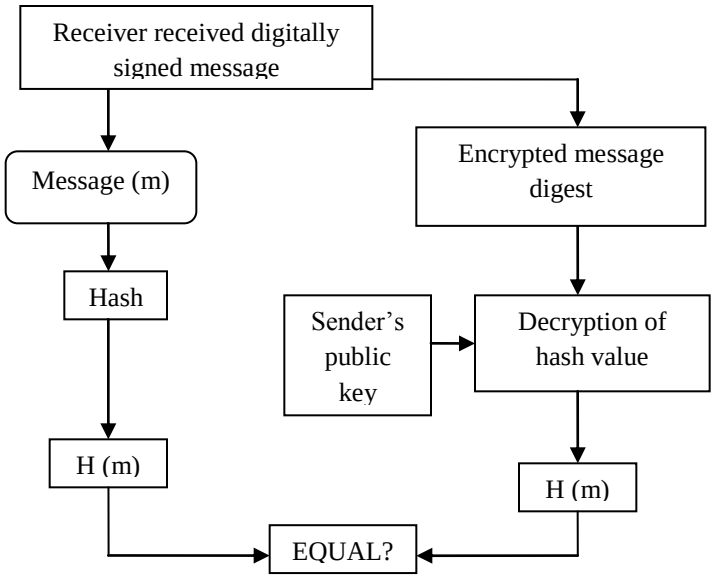

Fig-4: Digital Signature verification in receiver side.

From Fig-3 and Fig-4 we easily understood the digital signature technology for user authentication and for data integrity.

4.2 Digital Certificates

A digital certificate is data; the function of digital certificate is like a physical certificate. It's included with a person's public key that helps others to verify that a key which is used for encryption is sender's private key or not. Digital certificates are used to thwart attempts to substitute one person's key for another [11].

A digital certificate has three things:

- A public key of sender.
- One or more digital signatures.
- Identification of users, like name, user ID, etc.

The purpose of digital signature on a certificate is that the information of certificate is attested by trusted third party called certification authority. A certificate is basically a public key with forms of ID attached and cheerful stamp of approval from trusted third party [11].

4.3 Certification Authority

Certification Authority (CA) is a piece of information that issues and verifies the certificates. CA proves the identity of public key's owner. The trusted third party CA signed and delivered certificates securely. The CA is operated by the collection of software, hardware and people.

CA performs four basic PKI functions [10]:

- Creates and signs the certificates.

- Issues CRLs and maintains certificate status information.
- Publishes its current certificates and CRLs
- Maintains archives of status information about the expired certificates that it issued.

A certificate contains:

- The identification of CA.
- The identification of owner.
- The owner's public key.
- The expiry date of certificate.
- The CA's signature of that certificate.

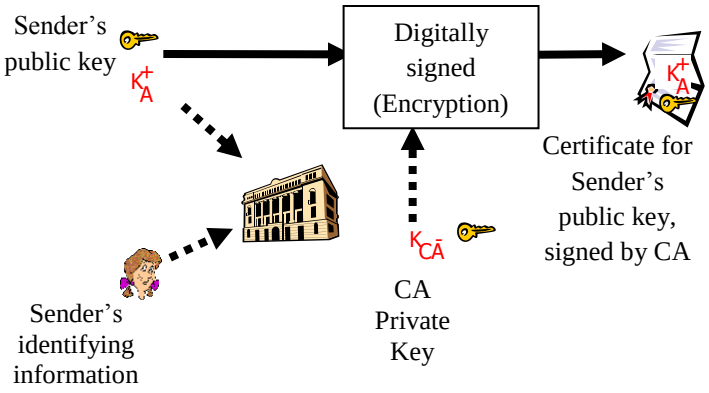

Fig-5: CA provide certificate for sender's public key.

CA provides certificate to the sender's public key. It means this public key is certified public key which is used for the decryption of message in PKC. When receiver receives certified public key he/she assure for the public key it means the public key authentic key which is send by authentic sender.

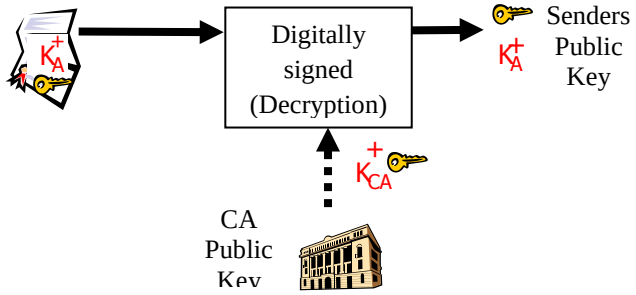

Fig-6: Certificate is decrypted by CA's public key

Send signed public key to the receiver which is certified with CA's private key. The certified public key is decrypted by CA's public key and receiver receives the original sender's public key. It prevents modification of the details contained in the certificate. The CA can be a unit within a organization, a company or an independent entity [8].

4.4 Registration Authority

Registration authority is intermediate between user and CA. RA is used for user's identifications. RA submits the certificate requests to the CA and verifies certificate contents for the CA. RA may also reflect information provided by a third party. The quality of this authentication process determines the level of trust that can be placed in the certificates [11]. CA identifies an RA with its name and public key. RA sends message along with its own signature, CA verify the RA's signature and satisfy that the message is provided by RA. RA's signature is important for sufficient protection of its own private key.

5. RSA ALGORITHM

The RSA algorithm is named after Ron Rivest, Adi Shamir and Leonard Adleman, who invented it in 1977 [8]. RSA is most widely used public key algorithm. It supports encryption and digital signature. In RSA algorithm multiply large prime number together. The multiplication of large prime number is easy but the factor of product of two prime numbers is difficult. It is easy to understand and implement. The public key and private key in RSA are based on very large prime numbers. The RSA algorithm consists of key generation, encryption and decryption algorithm.

5.1 Key Generation

1. We choose very large prime integers numbers randomly p and q.
2. Compute n: n = a * b.
3. Compute x: x = (a-1) * (b-1).
4. Choose an integer e (encryption exponent), Where 1 < e < x, such that: gcd (e, x). gcd- greatest common divisor.
5. Compute d (decryption exponent), 1 < d < x, such that: e * d = 1 (mod(x)).

In RSA Key generation there are some important factors –

- The public key is - (n,e).
- The public key is - (n,d).
- The values of p, q and x are private.
- "e" is the public.
- "d" is the private.

5.2 Encryption

Sender represents the plaintext message as a positive integer m, 1 < m < n and does follows-

1. Obtains the receiver's public key (n,e).
2. Computes the cipher text C = m^e mod n.
3. Sends the cipher text C to the recipient.

5.3 Decryption

Receiver follows:
Receiver uses his own private key to decrypt the message from cipher text.

$$m = c^{\wedge}d \bmod n$$

6. HASH FUNCTION

The message authentication is one important requirement for security of any data. It is used to verify the integrity of message. It is a procedure to verify that received message is come from the authenticate sender and messages have not been altered [8]. Hash function is most common cryptographic technique for message authentication.

Hash function is a cryptographic function that maps a message of any length into a fixed size bit string called cryptographic hash value [8]. When we create a digital signature we use hash function that is digest any message into fixed & manageable size. Hash function is mathematical function that takes input data and produced fixed size output which is called message digest. Hash function H accepts messages of any length and one-bit digest fixed length outputs are produced. If the input is even number of character the digest message returns H=0 and if the message input has odd number of character the digest message returns H=1 [13].

There are two cryptographic hash functions are used- MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm 1). MD5 has an arbitrary input length and produces a 128-bit digest and SHA1 has input messages of any length less than 2^ 64 bits and produces a 160-bit digest. SHA1 stronger than MD5 but speed of MD5 is faster than SHA1.

7. METHODOLOGICAL STEPS

The proposed methodology is concern with my previous papers presentation [14]. In this project first we create infrastructure for the collection of various set of public keys. In java secure socket extension used truststore and keystore file to provide secured transaction between the client and server.

The Keytool command is used to stores the keys and certificates in a keystore file. Keystore file protects private keys with a password.

7.1 Create Keystore File

The keytool command is used to create the keystore file which contains public or private key. It allows users to manage their key pairs and certificates. For creating java keystore file there are three steps are follows [15]:

1. Create the java key store file (.jks) that only contains the private key.
2. Generate Certificate signing request (.csr) and have a certificate generated from it.
3. Import certificate to the keystore.

Keytool is enables users to manage their own key pairs (public/private) and for self-authentication it uses certificates. Authentication and data integrity services using digital signatures, it certifies the user to cache the public keys of there respective peers. Keytools commands are already discussed in my previous publication on international conference in IRnet "Analysis of Public key Cryptographic Systems RSA and MD5 for Information Security" [16].

7.2 Working Steps

1. Symmetric Encryption: Encrypt the data by using a symmetric key. After create keystore file the first step of algorithm is symmetric encrypt.
   Symmetric – encrypt:
   a) Generate a DES key.
   b) Create the cipher.
   c) Initialize the cipher for Encryption.
   d) Initialize the cipher for decryption.
2. Encrypt the symmetric key using the receiver's public key.
3. Store a public key in the set of public key.
4. Create a Message Digest of the data to be transmitted.
5. Sign the message to be transmitted using digital signature.
6. Send the data over to an unsecured channel.
7. Validate the Signature using certificate authority.
8. Decrypt the message using Receivers public key from the set of key to get the Symmetric Key. (Call Import-key & Test Key pair)
   Import – key:
   a) Receive a certificate.
   b) Validate the certificate
   c) Provide a authorize key to user
   Test-key-pair:
   a) Receive a key from import key
   b) Test the key against
   c) If true
   d) Return
   e) Else
   f) False
9. Decrypt the data using the Symmetric Key.
10. Compute Message-Digest of data + Signed message.
11. Validate if the Message Digest of the Decrypted Text matches the Message Digest of the Original Message.

8. RESULT

The result of this work is providing secure and authenticates transaction in between organization and there employees. In an organization the key distribution is very difficult for unsecure medium, to overcome this problem use asymmetric key cryptography and public key infrastructure. In this work uses PKI for provide confidentiality, message integrity, authentication and non-repudiation. RSA is one of the algorithms of asymmetric key cryptography. In this work we use RSA for loading the key, X.509 certificate, DSA for generating key pairs, MD5 for message digest and AES for generating symmetric key. These all algorithms are make transaction more secure, less cost and faster than other cryptographic system. In this system employees decrypt encrypted data in less time. PKI have many advantages over secret key cryptography, for these reason we use this infrastructure for our system

CONCLUSIONS

Public key infrastructure is highly scalable. PKI users maintain their own certificates and keys. It provide delegated trust, a user who has obtained a certificate from a recognized and trusted certificate authority can authenticate himself to a server. The very first time he connects to that server, without having previously been registered with the system. In this paper we describe working of Public key cryptography, PKI and their components. In this discussion we discuss about how to create infrastructure for certificates and digital signatures. The advantages of public key system are that they provide authentication and digital signatures. In PKC, key distribution and private key sharing problem is finished for secure transactions. So we use PKC in our work.

ACKNOWLEDGEMENTS

I want to thank Mrs. Shikha Agrawal for guiding me and supporting me in my research work. I want to thank God, my family and friends, who made all things possible.

REFERENCES:

[1]. SECURITY AND CRYPTOGRAPHY, A tutorial for cryptography.
[2]. Stallings, W. Cryptography and Network Security: Principles and Practice, 4th ed. Englewood Cliffs (NJ): Prentice Hall, 2006.
[3]. Bill Anderson, Certicom Corp, "A Modern Approach to Information Security", published in Messaging Magazine, September/October 1998.
[4]. A seminar report on "Public key infrastructure".
[5].www.facweb.iitkgp.ernet.in/~sourav/PublicKeyCrypto. pdf
[6]. Ayushi, "A Symmetric Key Cryptographic Algorithm", Lecturer, Hindu College of Engineering H.No:438, sec-12, sonipat, Haryana, 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15.
[7]. A.Jancic and M.J.Warren," PKI - Advantages and Obstacles", School of Information Systems, Faculty of Business and Law, Deakin University, anaj@deakin.edu.au; mwarren@deakin.edu.au.
[8]. Dr. Mahesh Motwani, a book on, "Cryptography & Network Security", Associate Professor, Department of Computer Engineering & Deputy Secretary Rajiv Gandhi Technical university, Bhopal.
[9]. Joel Weise, "Public Key Infrastructure Overview", SunPS Global Security Practice, Sun BluePrints™ OnLine - August 2001.
[10]. D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang, "Introduction to Public Key Technology and the Federal PKI Infrastructure", National Institute of Standards and Technology, 26 February 2001.
[11]. Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", IJCST Vol. 2, Iss ue 2, June 2011, Dept. of CS & IT, MERI College of Engg. & Tech., ASANDA (near Sampla), Bahadurgarh, Haryana, India.
[12]. Ray Hunt, "PKI and Digital Certification Infrastructure", Proceedings of the 9th IEEE International Conference on Networks (ICON.01), Associate Professor, Department of Computer Science, University of Canterbury, New Zealand.
[13]. John Edward Silva, "An Overview of Cryptographic Hash Functions and Their Uses", January 15, 2003, GIAC Security Essentials Practical, Version 1.4b Option 1.
[14]. Ruchi Verma, Vinti Nanda, "A Novel Approach For Public key Infrastructure", Int. J. Tech, 2011 ; vol.1; Issue 2, pg 112-116, Chhatrapati Shivaji Institute of Technology, Durg, C.G.
[15]. Ruchi Verma, Vinti Nanda, "ANALYSIS OF PUBLIC KEY CRYPTOGRAPHIC SYSTEMS RSA AND MD5 FOR INFORMATION SECURITY", International Conference on Recent Trends in Control, Communication and Computer Technology RTCCCT, Raipur, 25th November, 2012.
[16]. Ruchi Verma, Vinti Nanda, "A Novel Approach for Information Security and public key infrastructure", National Conference on Innovative Trends in Management, Science & Technology ITMAST 2012 , on 8th April 2012 in CCEM, Raipur, C.G.

BIOGRAPHIES:

Ruchi Verma receives the degree of B.E. in Computer Science and Engineering from Raipur Institute of Technology, Raipur C.G. India in 2010 and she is currently pursuing M.Tech in Computer Science and Engineering from Chhatrapati Shivaji Institute of Technology, Durg C.G. India. Her research interests include cryptography and information security.

Shikha Agrawal is Assistant Professor of Computer science and Engineering at Chhatrapati Shivaji Institute of Technology,Durg, C.G, India. She receives the degree of B.E. in Computer Science and Engineering from Chhatrapati Shivaji Institute of Technology, Durg C.G. India in 2009 and M.E in Computer Technology and Application from Shri Shankaracharya College of Engineering and Technology, Bhilai, C.G. India in 2012. Her research interests include image processing and data mining.