"QR CODE BASED CLOUD DATA PROTECTION USING RSA ALGORITHM"

Vipin Rawat Km Divya Deena Nath Devki Nandan Shukla

Student (M.Tech computer science UIET) ,

Department of computer science (M.Tech CS)

Babasaheb Bhimrao Ambedkar University Vidya Vihar Lucknow India

ABSTRACT:- Encryption and decryption is done by the asymmetric key encryption algorithm. Asymmetric key encryption means to encrypt and decrypt the data or file two different keys public key and private or secret key. The plain text is encrypt by the cipher text and encryption is done by the using of public key and decryption is done by the private key .In this paper we study proposes a system to secure the public cloud data protection using QR code and asymmetric key encryption algorithm. QR code is used to decrypt the encrypted text file and other files and also store the user details. cloud computing means to store the all data and information online. It is depend on the internet technology and in modern day cloud services is very popular for online data storage.

KEYWORDS :- Cloud computing, QR code, Encryption and Decryption, RSA algorithm , Results.

1. **CLOUD COMPUTING :-** Cloud computing is a modern technology which is used internet and servers to maintain the data like text file images, audio ,video and docs files and its applications. Cloud computing is a group of various computers and secret linked over the internet . In cloud computing designing, accessing and manipulating the applications online. The cloud computing allows consumers and businesses to use applications without installation access their personal file from any computer with the help of internet. Cloud computing means online data storage and application. Cloud computing architecture provides services via internet on demand and pay-per use access to a pool of shared resources for the network storage services and applications. Cloud computing is totally depend on the internet technology in which client data is stored and maintained in data centre of cloud provide likes google, amazon.

Advantages of cloud computing:-

1. Reduced cost.
2. Increased storage.
3. Highly automated.
4. Flexibility .

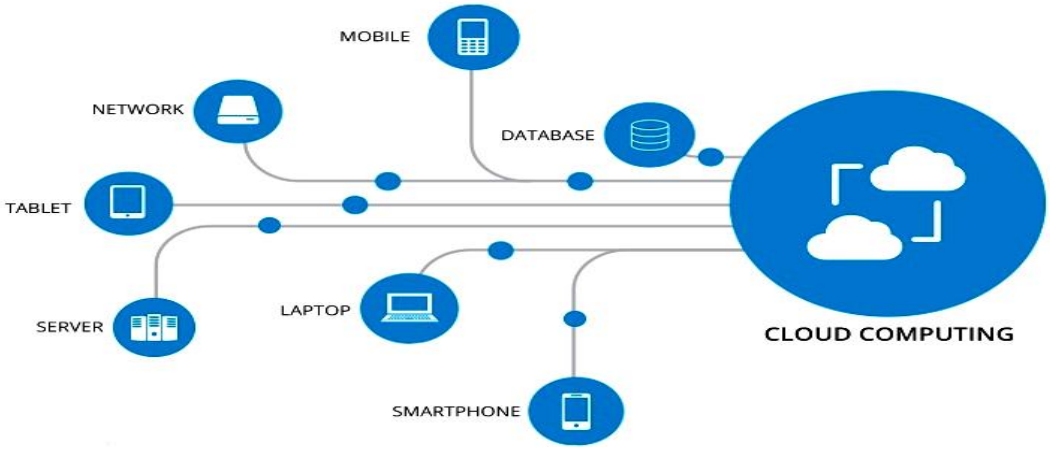


FIGURE NO :1 CLOUD COMPUTING

CLOUD MODELS:- IN the case of cloud models there are two type of cloud modes.

1. Services models

2. Deployment models.

1. Service model :

Service model can be defined as a reference model on which the cloud computing is based. This can be categorized into three types SAAS, PAAS and IAAS.

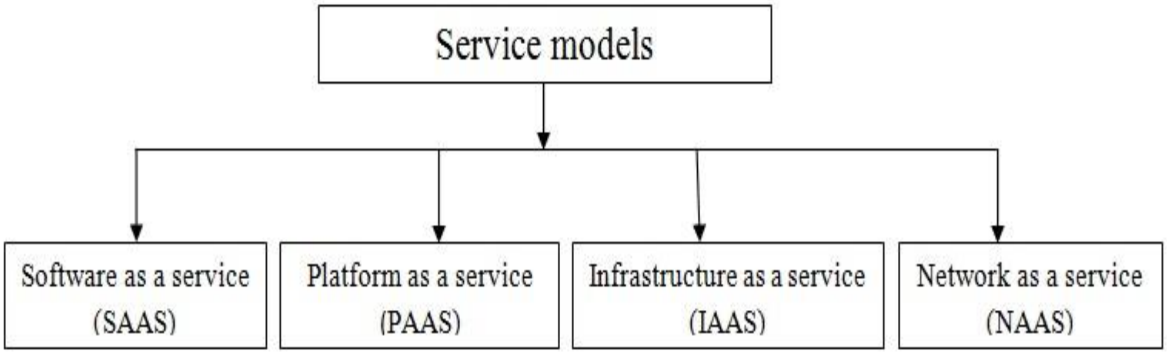

Service models
Software as a service (SAAS)
Platform as a service (PAAS)
Infrastructure as a service (IAAS)
Network as a service (NAAS)

FIGURE NO 2: SERVICE MODELS

A. **Software as a services:-**Different software applications are provided over the internet by the Application Service Provider (ASP).). SAAS model allows end user to use software applications as a service. With the use of SAAS, user will not have to install various on their own systems**. E.g.,** Google App.

B. **Platform as a services**PAAS provide the runtime environment for applications; development and deployment download or install software. PAAS also support Web-development interfaces such as simple object access protocol which allows the construction of multiple web services. **E.g.,** Google App Engine.

C. **Infrastructure as a services**

. The various services provided by the IAAS are-

1. Server Space
2. Network equipment
3. Memory
4. CPU Cycles
5. Storage Space

2. Deployment Model

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid and Community.

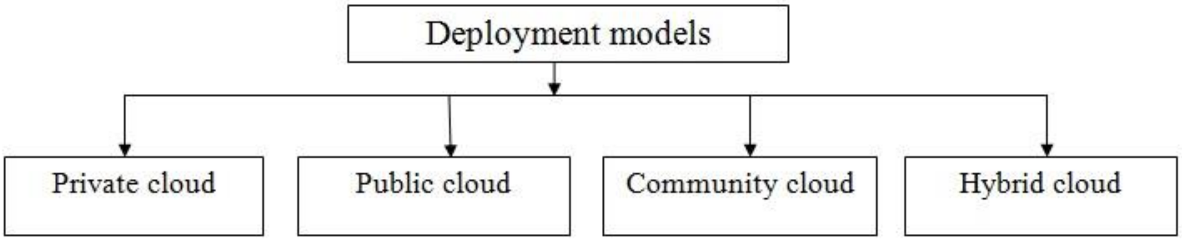


FIGURE NO 3: DEPLOYMENT MODELS

a. **Public cloud:-**The Public Cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail.

b. Private Cloud:-The Private Cloud allows systems and services to be accessible within an organization. It offers increased security because of its private nature.

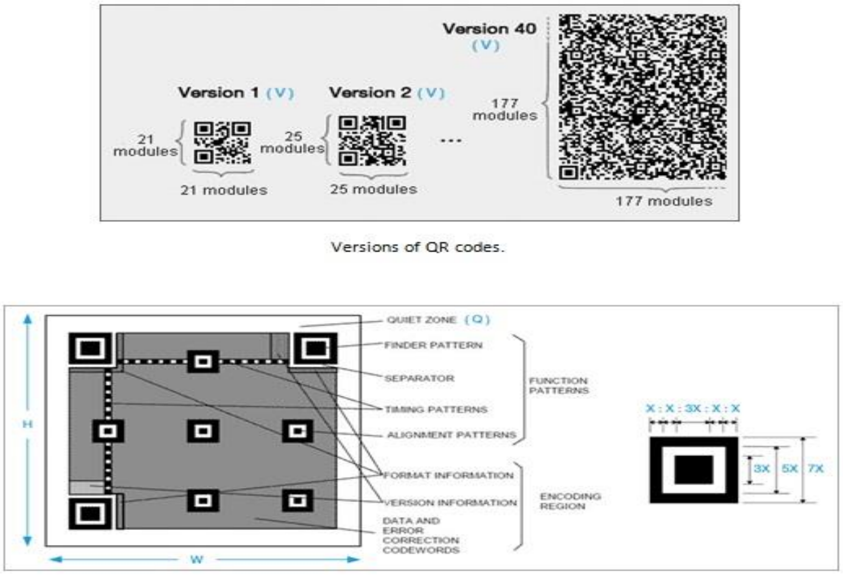
c. Community Cloud:-The Community Cloud allows systems and services to be accessible by group of organizations.

d.Hybrid Cloud:-The Hybrid Cloud is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud

2.QR CODE:-

QR code mean's quick response code .QR code is the trade mark for a type of matrix barcode. QR code are used to encrypt and decrypt the data in the form of text and images . QR code mostly used to store the user details such as name, password, URL of website and phone number 's. QR code is very easy to used for encryption of various type of messages and text files. QR code are-

a. The smallest size of QR code is 21*21 pixel s its also known as the version 1.
b. The largest size of QR code is 177*177 pixels its known as the version 40. And also support for error correction.



Versions of QR codes.

FIGURE NO 4: QR CODE ARCHITECTURE AND VERSIONS

Where
W: Width of QR code.
H: Height of QR code
X: The width of QR code module.
Q: Width of quiet zone q=4x

3.ENCRYPTION AND DECRYPTION

ASYMMETRIC KEY ENCRYPTION:- In the case of asymmetric key encryption process is done by the different keys are used for encrypting and decrypting the data and information is know as asymmetric key encryption .Asymmetric key encryption the both keys are different , they are mathematically related and hence retrieving the plain text is decrypt by cipher text is feasible. Asymmetric key encryption increases the security of the encryption system or process by using two separate keys such as public and private key. Public key is used for encrypt the data or information and private key is used to decrypt the secret messages and data. The given below diagram shows the asymmetric key encryption. In Asymmetric key encryption there are two related keys of a key pair . A public key is freely available to anyone who might want to send you a message .the private key is a secret key its only recipient know. Any message (text file ,binary file) that are encrypted by using the public key and the encrypted text file is decrypted by the secret or private key.

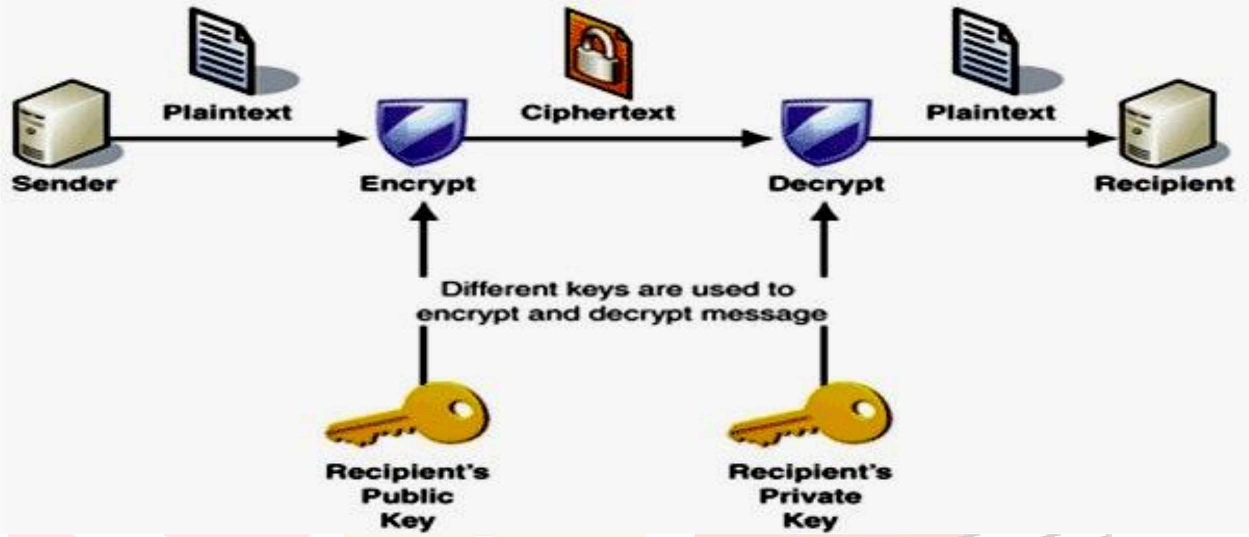


FIGURE NO 5: ASYMMETRIC KEY ENCRYPTION

The most important properties of asymmetric key encryption are-

1. Different pairs of keys are used for encryption and this is different than the symmetric key encryption.
2. Each receiver used a unique decryption key like private key or secret key.
3. Encryption algorithm is a very complex to attacker from deducing the plain text from the cipher text encryption.
4. The private key and public key are related mathematically ,it is not to be feasible to calculate secret key from the public key.

There are three type of asymmetric key encryption system

A. R.S.A (Ron rivest, adi Shamir,len adleman)
B. Elgamal system
C. Elliptic system

A. **RSA ENCRYPTION ALGORITHM**:- the R.S.A algorithm is invented by three scholar's Ron Rivest, Adi Shamir,Len Adleman. In R.SA algorithm there are two aspects

1. Firstly generation of key pairs.
2. Secondary is encryption and decryption algorithm.

1. **GENERATION OF R.S.A KEY PAIR**:- every participate in communication using encryption and decryption needs to generate a pair of keys such as public key and private or secret key. The given below process is shown in the generation of key pair.

1.1. Generate the RSA modulus (n)

a. Select two large primes, p and q.

b. Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.

1.2 Find Derived Number (e)

a. Number **e** must be greater than 1 and less than (p − 1)(q − 1).

b. There must be no common factor for e and (p − 1)(q − 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are co-prime.

1.3 Form the public key

a. pair of numbers (n, e) form the RSA public key and is made public.

b. Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.

1.4 Generate the private key

a. Private Key d is calculated from p, q, and e. For given n and e, there is unique number.

b. Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).

2. ENCRYPTION AND DECRYPTION:-

Once the key pair has been generated, the process of encryption and decryption are relatively straightforward and computationally easy.Interestingly, RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.

2.1 RSA Encryption

a. Suppose the sender wish to send some text message to someone whose public key is (n, e).
b. The sender then represents the plaintext as a series of numbers less than n.
c. To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as −

$$C = P^e \bmod n$$

a. In other words, the ciphertext C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.
b. Returning to our Key Generation example with plaintext P = 10, we get ciphertext C-

$$C = 10^5 \bmod 91$$

2.2 RSA Decryption

a. The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a ciphertext C.
b. Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$$\text{Plaintext} = C^d \bmod n$$

c. Returning again to our numerical example, the ciphertext C = 82 would get decrypted to number 10 using private key 29 −

$$\text{Plaintext} = 82^{29} \bmod 91 = 10$$

2.3 RSA Analysis

The security of RSA depends on the strengths of two separate functions. The RSA cryptosystem is most popular public-key cryptosystem strength of which is based on the practical difficulty of factoring the very large numbers.

A. **Encryption Function** − It is considered as a one-way function of converting plaintext into cipher text and it can be reversed only with the knowledge of private key d.

B. **Key Generation** − The difficulty of determining a private key from an RSA public key is equivalent to factoring the modulus n. An attacker thus cannot use knowledge of an RSA public key to determine an RSA private key unless he can factor n. It is also a one way function, going from p & q values to modulus n is easy but reverse is not possible.

4.Detailed system design:-

4.1 Upload file :- in the case of file uploading process we can create a web login page for the user authentication. The next step is create the database storage and last step is cloud data storage. working is in uploading process is firstly user login in login page now authentication request is performed and check the user is correct or incorrect. If user is correct then user access the database for uploading the various files. Databse request to upload the file . after upload the file automatically file is encrypted by the public key encryption alg rithm and generate the QR code of this encrypted text file.

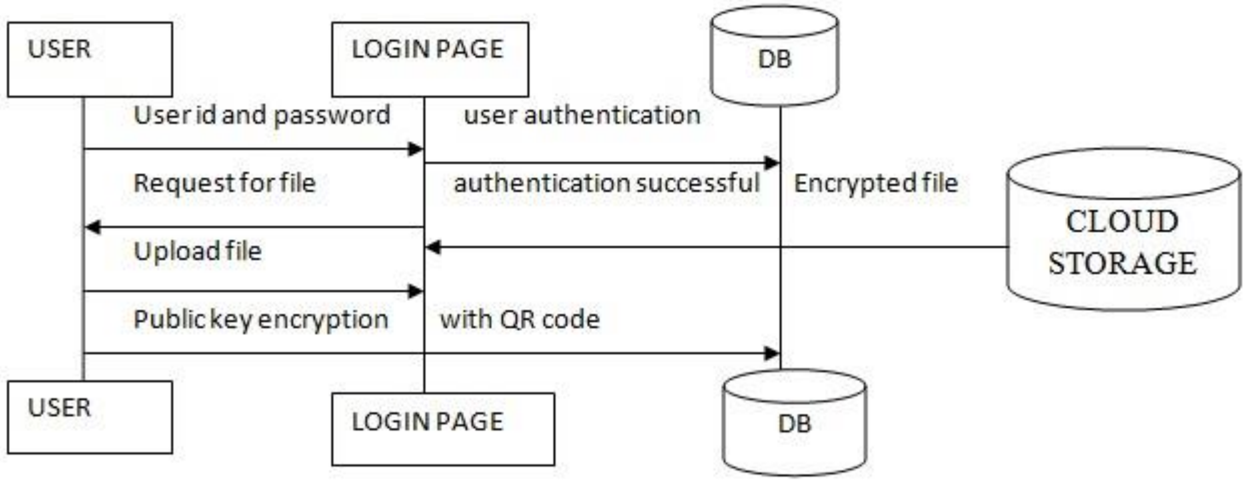


Figure no 4:- upload file system

5.1 Download the decrypted file:- the decryption is done by the private key with QR code. after file encryption user can download the decrypted files with QR code scan. User login in login page with right user name and password if user is authenticate then user access the data base and cloud storage.

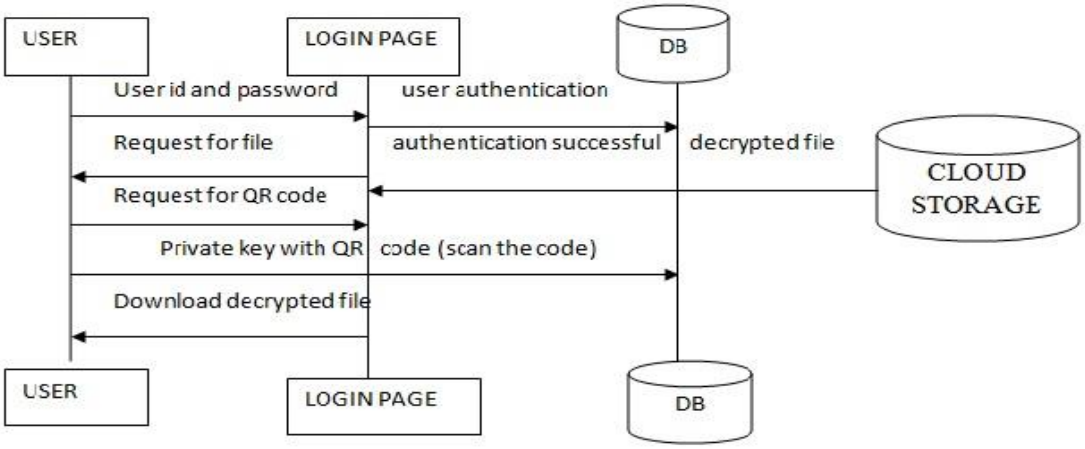
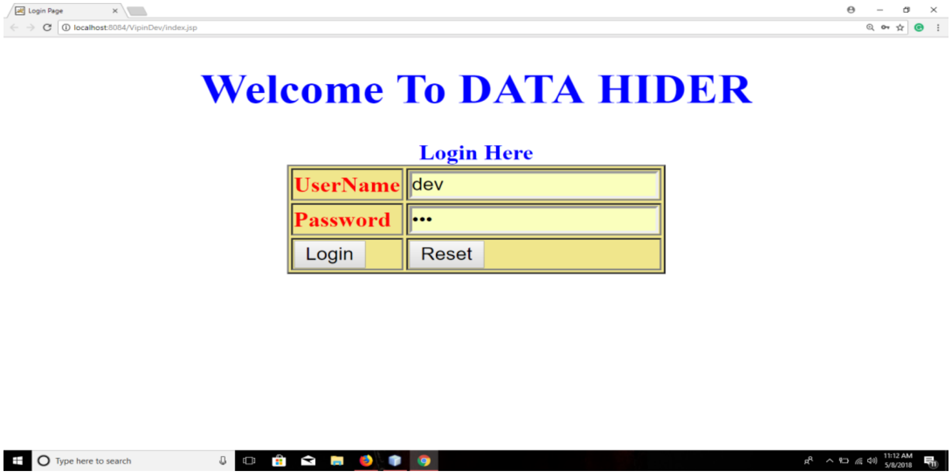


Figure no 5:- download page system

RESULT AND SNAPSHOTS:-

the public cloud data protection is successfully done by the QR CODE and encryption technique. the asymmetric key encryption algorithm is used for data encryption and decryption. We are developed a webpage for online public cloud data protection using QR code and asymmetric key encryption. The given snapshots is shows the working process of encryption and decryption.


Login Page

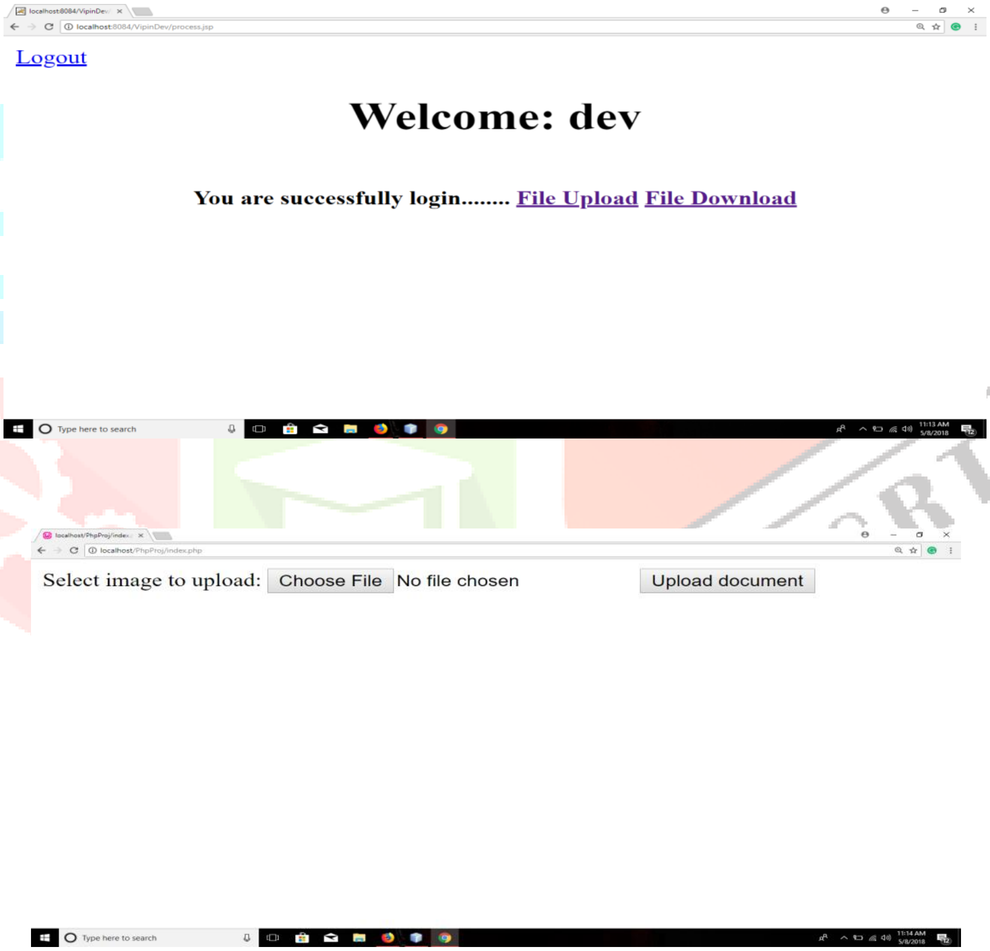
localhost:8084/VipinDev/index.jsp

Welcome To DATA HIDER

Login Here

UserName	dev
Password	•••
Login	Reset

FIGURE no 6 LOGIN PAGE


localhost:8084/VipinDev/process.jsp

Logout

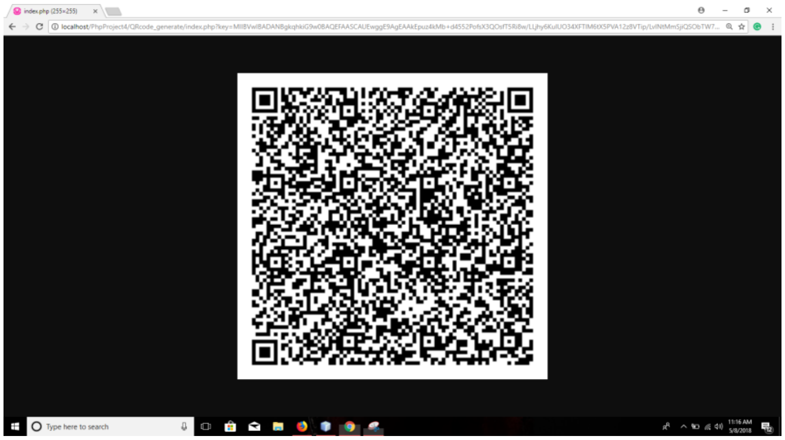
Welcome: dev

You are successfully login........ File Upload File Download

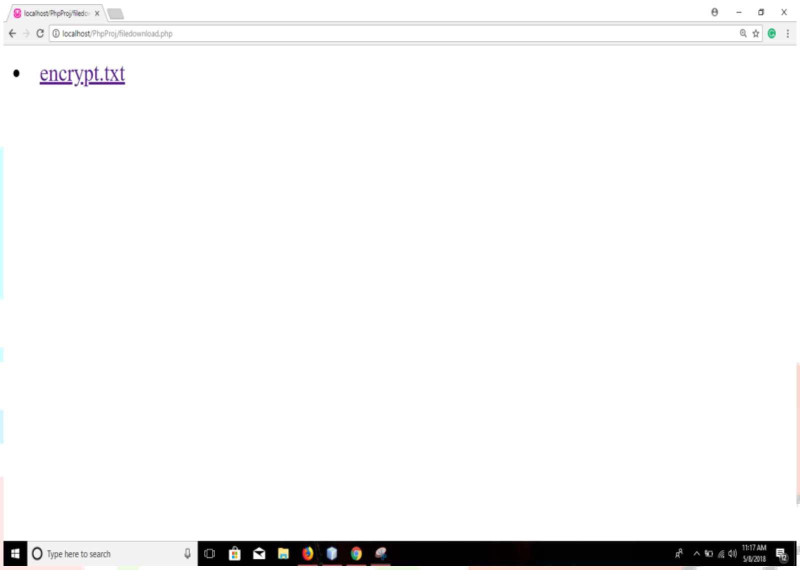
localhost/PhpProj/index.php

Select image to upload: Choose File No file chosen Upload document

FIGURE NO 7:- UPLOAD FILE PAGE

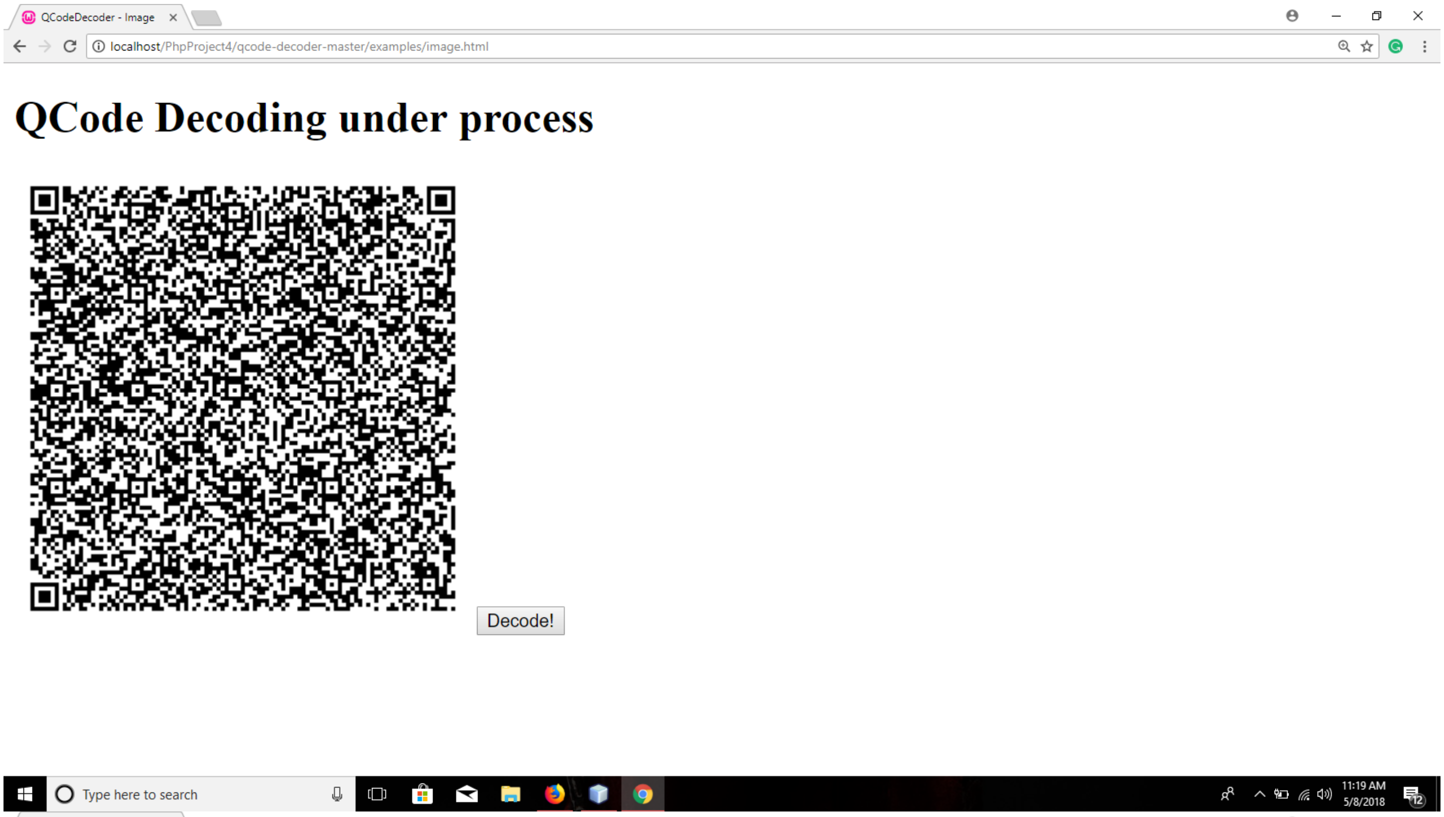

index.php (255×255)
localhost/PhpProject4/QRcode_generate/index.php?key=MIIBVwIBADANBgkqhkiG9w0BAQEFAASCAUEwggE9AgEAAkEpuz4kMb+d4552PofsX3QOsfT5Ri8w/LLjhy6KulUO34XFTIM6tX5PVA12z8VTip/LvINtMmSjiQSObTW7...
Type here to search
11:16 AM
5/8/2018

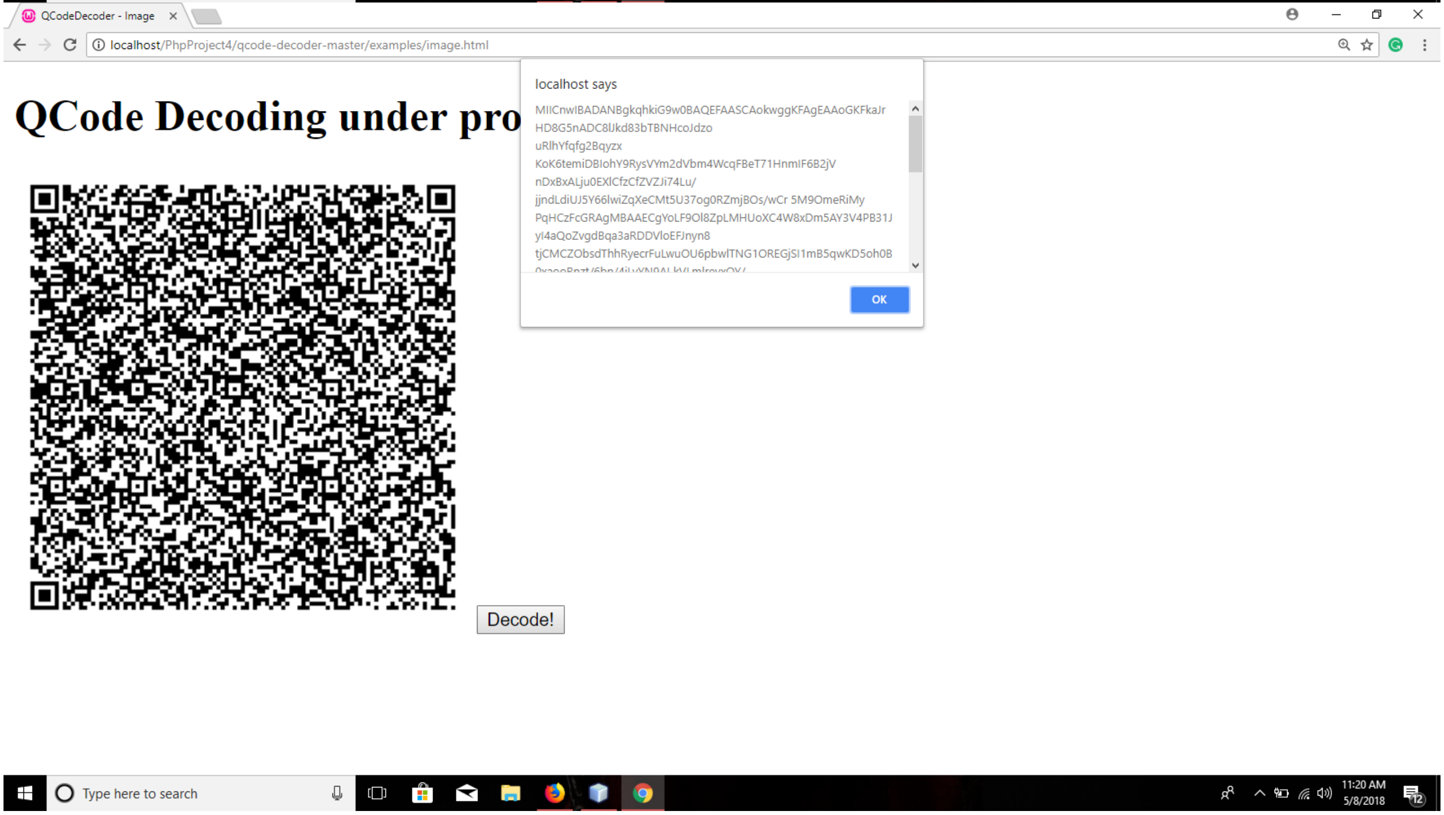
FIHURE NO 8:_ GENRATE qr CODE



- encrypt.txt

FIGURE NO 9:- ENCRPTED FILE


QCodeDecoder - Image
localhost/PhpProject4/qcode-decoder-master/examples/image.html
QCode Decoding under process
Decode!
Type here to search
11:19 AM
5/8/2018



localhost says

```
MIICnwIBADANBgkqhkiG9w0BAQEFAASCAokwggKFAgEAAoGKFkaJr
HD8G5nADC8lJkd83bTBNHcoJdzo
uRlhYfqfg2Bqyzx
KoK6temiDBIohY9RysVYm2dVbm4WcqFBeT71HnmIF6B2jV
nDxBxALju0EXlCfzCfZVZJi74Lu/
jjndLdiUJ5Y66lwiZqXeCMt5U37og0RZmjBOs/wCr 5M9OmeRiMy
PqHCzFcGRAgMBAAECgYoLF9Ol8ZpLMHUoXC4W8xDm5AY3V4PB31J
yI4aQoZvgdBqa3aRDDVloEFJnyn8
tjCMCZObsdThhRyecrFuLwuOU6pbwlTNG1OREGjSI1mB5qwKD5oh0B
```

FIGURE NO 10:- DECRYPTED THE FILE

COCLUSION AND FUTURE WORK:-

In this paper main goal is public cloud data protection using the asymmetric key encryption algorithm . The main concept of this algorithm encryption technique done by the public key and QR Code. After encryption the file is mostly secure and encrypted file is encrypted in QR code format. Decryption is done by the different key means private key and scan the QR code if QR code is correct the decrypted file is automatically downloaded . In this technique only text file is secure and easily encrypted . the future work is secure the various files such as docs audio video files.

REFRENCES:-

[1] P. Mell and T. Grance, “Draft nist working definition of cloud computing,” Referenced on Jan. 23rd, 2010 Online athttp://csrc.nist.gov/ groups/SNS/cloud-computing/index.html,2010.
[2] Cloud Security Alliance, “Security guidance for critical areasof focus in cloud computing,” 2009, online athttp://www.cloudsecurityalliance.org.
[3] C. Gentry, “Computing arbitrary functions of encrypteddata,”Commun.ACM, vol. 53, no. 3, pp. 97–105, 2010.
[4] Sun Microsystems, Inc., “Building customer trust in cloudcomputing with transparent security,” 2009, online athttps://www.sun.com/offers/details/sun transparency.xml.
[5] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H.Spafford, “Secure outsourcing of scientificcomputations,”Advances in Computers,vol. 54, pp. 216–272,2001.
[6] Ning Cao, Zhenyu Yang, Cong Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving query over encrypted graph-structured data in cloud computing." In Distributed Computing Systems (ICDCS), 2011 31stInternational Conference on, pp. 393-402. IEEE, 2011.
[7] Cong Wang, Kui Ren, and Jia Wang. "Secure andpractical outsourcing of linear programming in cloudcomputing." In INFOCOM, 2011 Proceedings IEEE,pp. 820-828. IEEE, 2011.2043–2047.
[8] D. Luenberger and Y. Ye, Linear and Nonlinear Programming, 3rd ed.Springer, 2008
[9] Dimitrios, Zissis and Dimitrios Lekkas. "Addressingcloud computing security issues." Future Generationcomputer systems 28, no. 3 (2012): 583-592.
[10] R. Gennaro, C. Gentry, and B. Parno, “Non-interactive verifiablecomputing: Outsourcing computation to untrusted workers,” inProc. of CRYPTO, Aug. 2010.
[11] D. Coppersmith and S. Winograd, “Matrix multiplication via arithmetic progressions,” in Proc. of STOC‟87,1987, pp. 1–6.
[12] MOSEK ApS, “The MOSEK Optimization Software,” Online at http: //www.mosek.com/, 2010.
[13] Ronald Petrlic, "Proxy re-encryption in a privacy preserving cloud computing DRM scheme." InCyberspace Safety and Security, pp. 194-211. SpringerBerlin Heidelberg, 2012.