

Data Protection in Cloud Computing Using QR Code

Sandha* and M. Ganaga Durga**

ABSTRACT

Data protection in outsourced data is challenging task in cloud computing. In cloud environment the critical data should be masked or encrypted. This paper suggests QR code , a two dimensional code with RSA based homomorphic Algorithm can be used for secure authentication between client and server at the time of storage and auditing .Which is authenticate the client with encrypted split file combined with user identity QR code and by storing distributed server system of cloud computing environment. It helps to make user data protect effectively.

Keywords: Cloud computing, Homomorphic encryption, QR Code

I. INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it. The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter. Cloud Computing has been defined as the new state of the art technique that is capable of providing a flexible IT infrastructure, such that users need not own the infrastructure supporting these services. This integrates features supporting high scalability and multi tenancy. Moreover, cloud computing minimizes the capital expenditure.

Authentication is an important process in cloud computing. Data security is very big problem in public storage. In order to prevent this a proper, effective authentication system must be implemented which prevents data leakage or loss a new technique called QR code.

A Quick Response code is a 2 dimensional bar code Which was developed by Densa-Wave. Basic of this technology is tracking the information. Two types of QR codes are there Static QR code and dynamic QR code. It can store and digitally present much more data than other barcode. Data is aligned in vertical and horizontal direction. Information is retrieved by a photograph of the code using QR code Reader with a camera. QR can be read from any position. QR code scanner decodes the image through three squares present in the corner of the image.

(A) Structure

The three large squares highlighted in green are the Finder pattern. These enable the decoded software, and to recognize the QR Code and determine the correct orientation. The small brown square is an alignment marker it will add more if the code size increased. Separators used to separate Finder pattern for the actual data . Timing pattern contained alternate red & yellow module. Format information is 15 bit data next to

* Research Scholar, Bharathiar University, Assistant Professor, Department of Computer Application, St. Michael College of Engineering and Technology Kalayar Koil, *E-mail: Yazhini98@gmail.com*

** Research Supervisor, Bharathiar University, Assistant Professor, Department of Computer Science, Government Arts College for Women, Sivagangai, *E-mail: mgdurga@yahoo.com*



Figure 1: QR Code

separators it contained about error correction level. Pink color squares are used to encode the version data. Blue color Data part is in 8 bit size.

(B) Types

The 4 different types of QR codes [1] differ with the view and features. QR code model 1 and model 2 are the first type of QR code. Up to 1167 numerals can be stored in Largest version of model 1 and Up to 7089 numerals can be stored in Largest version of model 2. The next type is a micro QR code. It differs from the regular QR model by position detection pattern and size. IQR Code is next type. The same size of the IQR Code as an existing QR Code can hold 80% more information than the latter. SQR Code is used to store private information there is no difference from regular code in appearance. The next type is logoQR it incorporates a high level of design features.





	QR Code	PDF417	DataMatrix	MaxiCode
				
Company	Denso Wave	Symbol	CI Matrix	UPS
(Country)	(Jap)	(USA)	(USA)	(USA)
Method	Matrix	Scotkudo bar code	Matrix	Matrix
Number	7,089	2,710	3,116	138
Muneral	4,206	1,850	2,355	93
Binary number	2,953	1,018	1,556	
Chinese character	1,817	554	778	
Major function	Mass storage Space-saving Fast data-processing	Mass storage	Space-saving	Fast data- processing

Figure 2: Two dimensional code

II. RELATED WORK

Recently, much of growing interest has been pursued in the context of remotely stored data security David Pintor Maestre *et al.* [4] consider secure authentication using QR code in their defined “A Improved secure authentication method using QR codes” develop an authentication method using 2 factor authentication.. In their scheme, they utilize an IMEI number of smart phones with a random number of QR code for secure authentication, thus private data security is achieved. The problem here is, the server must have a copy of the user’s private key in order to generate the same pin code.

Thiyagarajan M, Dinesh Kumar K, *et al.* [2] consider authentication of consumer product can be done with QR codes . They achieve the security by QR code along with the public key encryption algorithm. But the normal QR code can be easily retrieved using any smart phone. They do not consider the security of QR code. Suraj kumar sahu *et al.* [5] describe an “ Encryption in QR code using stegnography” where cover image and QR data is embedded and encrypted. Dong-sik oh *et al.* [6] consider creating 3 sets of QR code by converting the single information into 3 versions of the QR code and stored in the distributed server system.

III. PROPOSED SYSTEM

The proposed system Fig. 2 involved various steps in the process of storing and retrieving the data secured in a cloud computing environment. First achieving initial authentication by the secure random number generation is used for creating a unique key for each user.

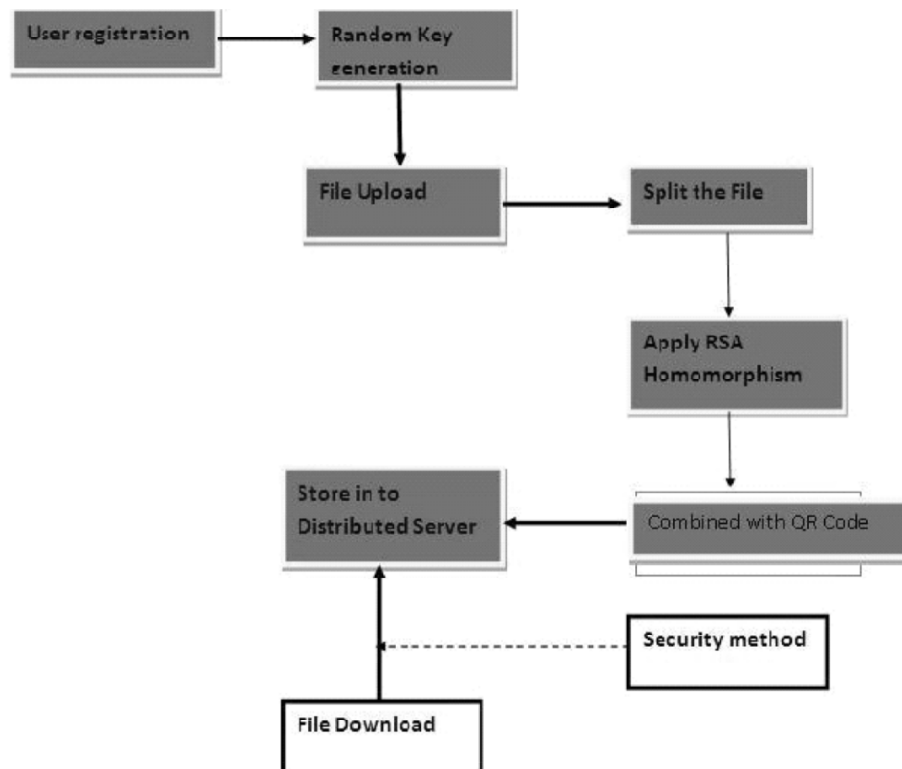


Figure 3

The uploaded file encrypted by homomorphic authentication and combined with QR code. It will store in the three different server which is purchased by us. The Key is getting from the user at the time of download. If the key is correct then the data is downloaded from servers .Before display to the user it merged and decrypted.

The pseudo code for our proposed system is

Shown below

```

// Module for upload the data
upload()
{
  If(user authentication success)
  {
    Split & Encode+combined qr;
    Distributed in to servers
  }
  Else
  Return authentication failed;
}
// Module for download the data Download()
{
  If (key is ok)
  {
    Collect from the server;
    Decrypt the file;
  }
  Else
  Failed;
}

```

IV. SIMULATED WORK

PHP is server side scripting language introduced in 1994 by Rasmus Lerdorf. Latest major PHP version named PHP 7. It is the best tool for developing desktop, mobile and web application quick and easy manner. Compatible on all Operating System, fast data processing and flexibility are benefits of PHP. Large applications can be managed easy and efficient way of approaches. Missing feature in PHP can be plug in by us.

Random key generation is the initial process . X_n is the random number. The next number assigned to the user is $X_{n+1} = (a X_n + b) \text{ mod } m$. Here a, b, m are large integers. This random number is a password for the user to access the cloud. $N = X_n$, N is Individual user. RSA Based homomorphic algorithm used for encrypt the data Key generation in RSA, P and r are distinctive prime numbers . Find the value of n , $n = p * r$ product is $n = (p-1)(q-1)$.Find Co prime(e) for n and modular multiplicative inverse d . $e * d \text{ mod } n = 1$. Here public key is n and e private key is d .plain text m , Encryption is $C(m) = m^e \text{ mod } n$ and Decryption is $m(c) = c^d \text{ mod } n$. Binary of QR code is XOR with every bit of Encrypted file F and result files F_n stored in to distributed server.

1. CLOUD ACCESS

To implement this work we purchased three web domains which is considered as a three different public servers. We can use this for storing split files.

Before entering in to the secure cloud storage system client should register their details to confirm the authenticated user. The authentication of clients can be done with the email id as user id and password is given by the user. A Unique random number is assigned for every user and is sent to the registered mail id. The key which is sent to the client is an authentication message, for downloading files. The uploaded file is split into three parts and encrypted by homomorphic then combined with user identity QR code. Security is maintained by storing three files in to distributed systems. Not only stored in to public cloud, but also in private cloud.

3. SCREEN SHOTS

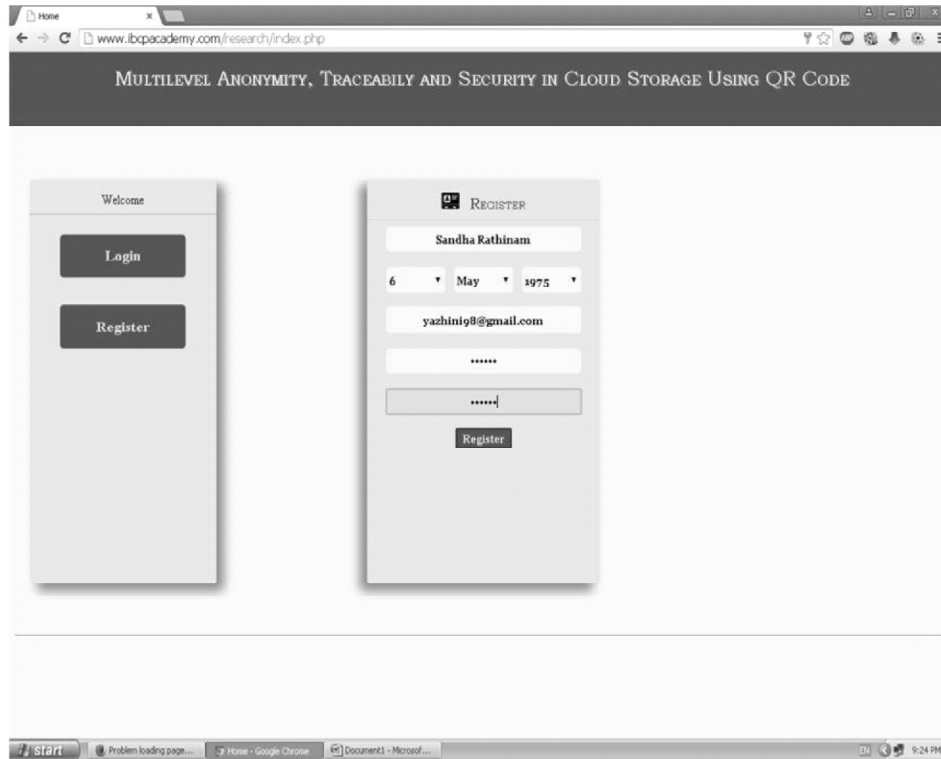


Figure 3: User Registration

Fig. 3 is the user registration screen in this simulation. This page is designed using php and getting information will transfer to the database. Name, Email Id, Password, date of birth and are collected on this screen. Email id of user will use as a user Id for further access of cloud. Random number generation is used for creating key for each user and send to the appropriate user Mail Id.

For accessing cloud ,user needs to login the screen Registration confirmation will display on this screen and Authentication get success if he is the valid user. we can get unique id from mail, which is used for store and retrieve the file from the cloud storage.

Uploaded file is split and then stored into three different servers. Before storing the file, Homomorphic algorithm [11] work for encrypting the data and then combined with QR code. Keeping a copy on file in local server is considered as a private data. The key for each user is stored in key server ,which is used for retrieving their file from public and private cloud.

In screen Fig. 7 Stored files are collected from three servers and decrypted and waiting for user key for proper authentication. File can be downloaded from public server and also private server if the key is correct.

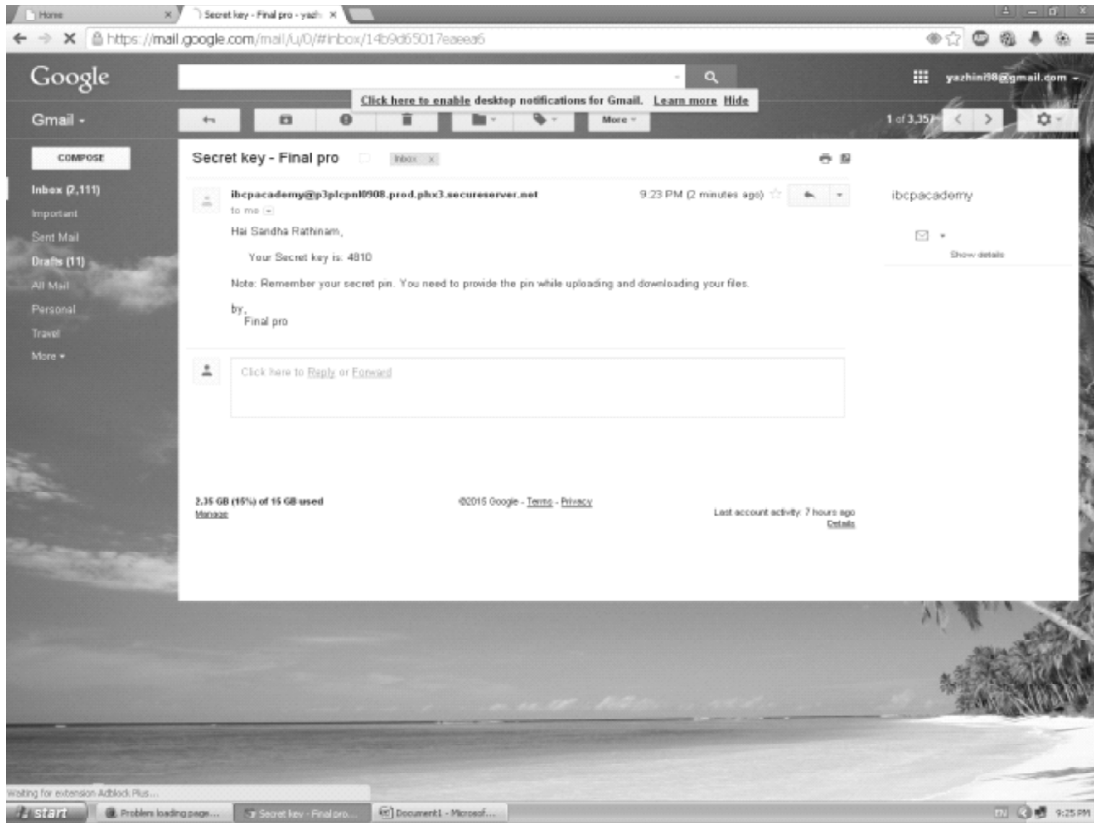


Figure 4: Key Generation

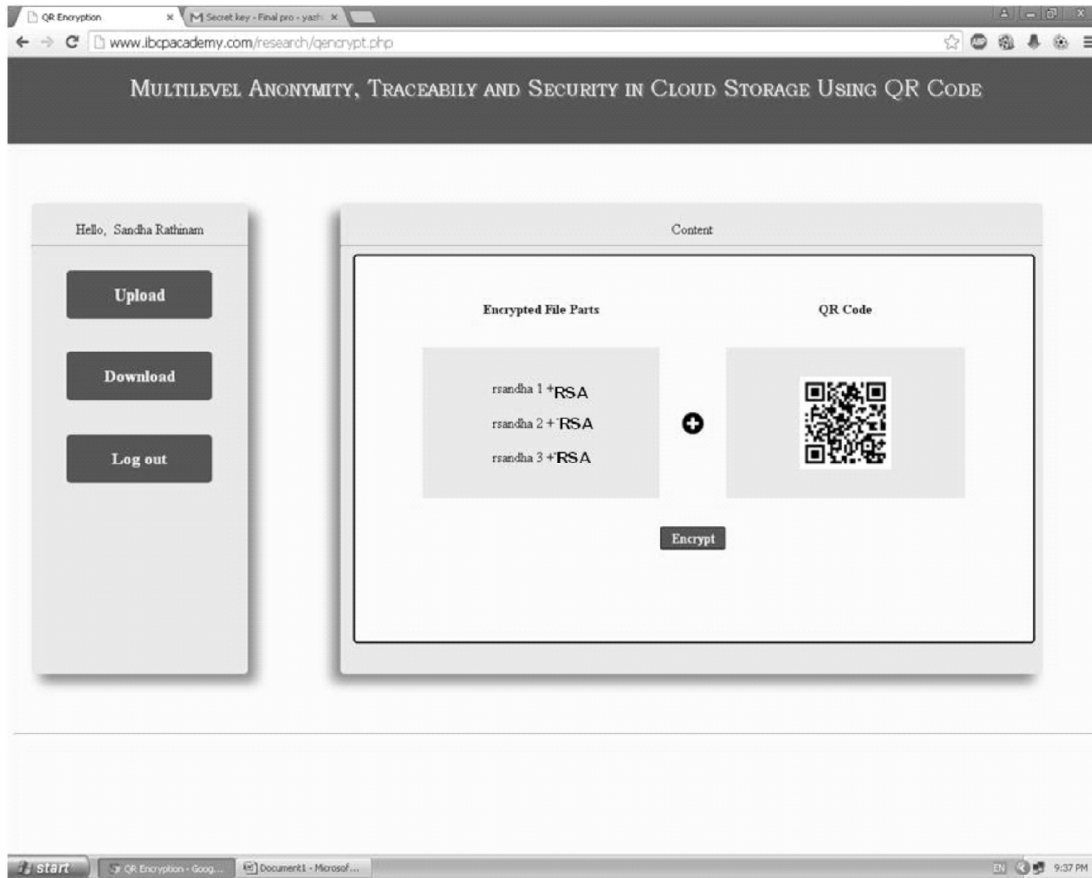


Figure 5: Upload Screen

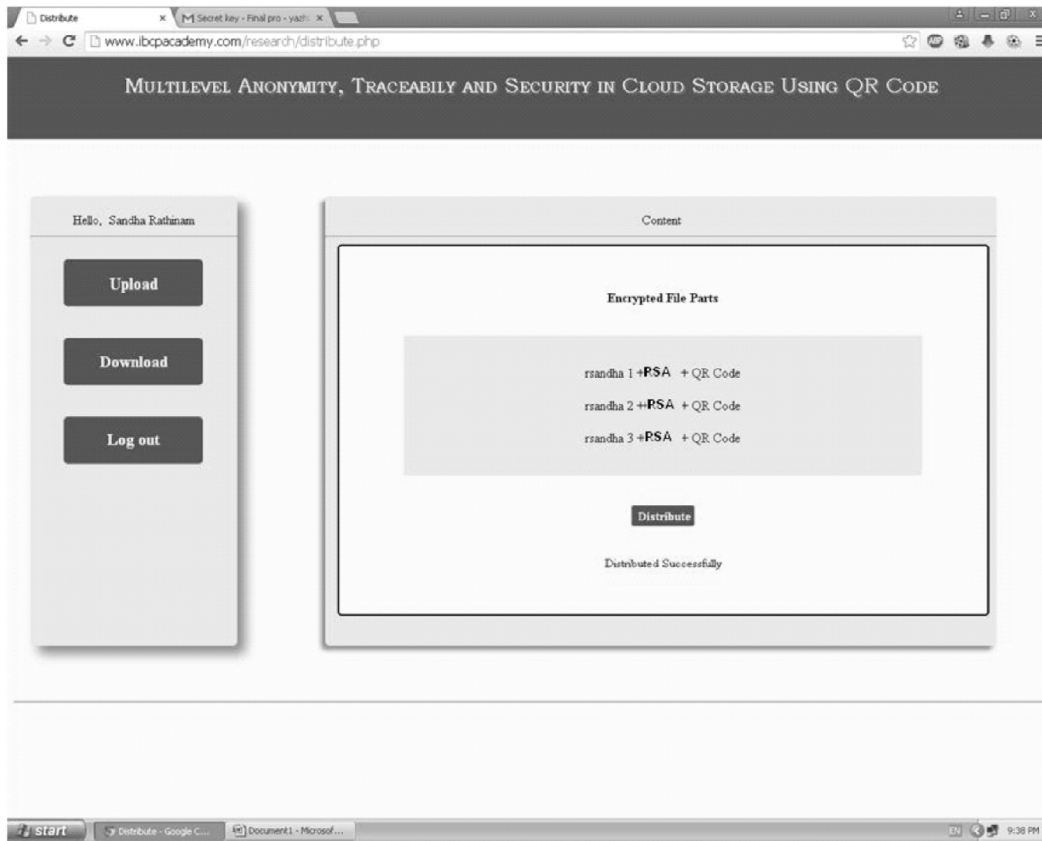


Figure 6: File Distribution

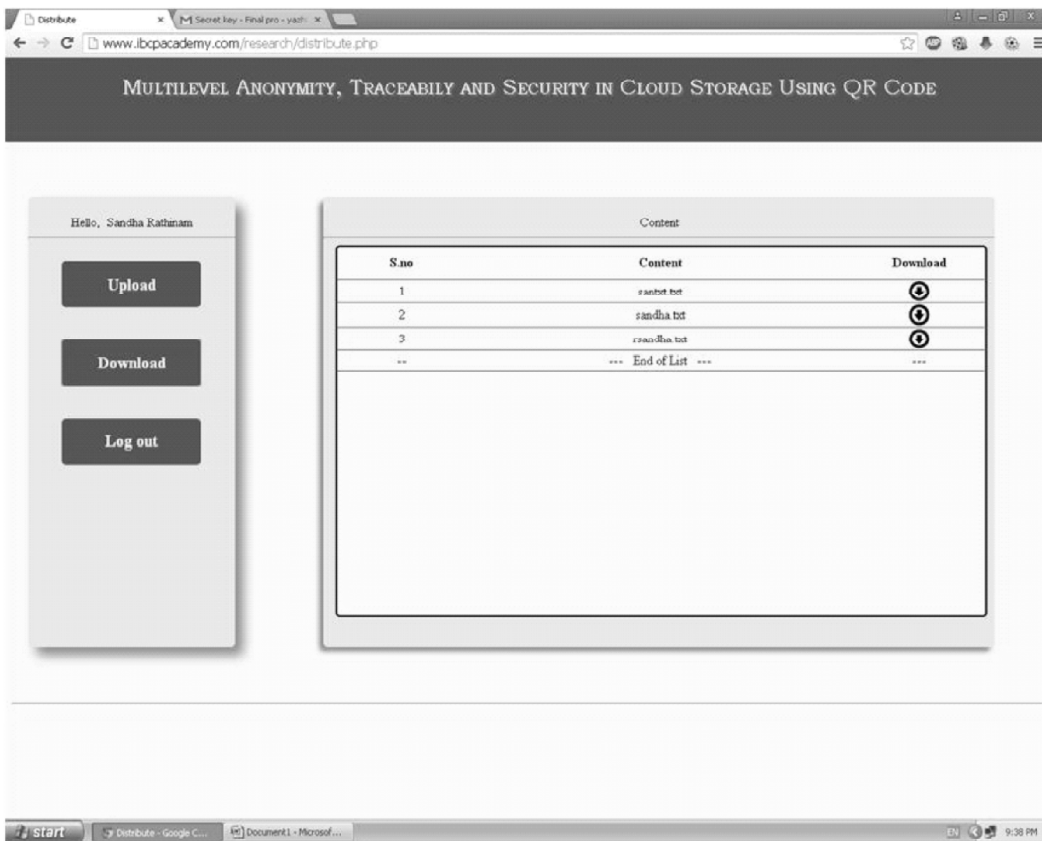


Figure 7: File display

V. CONCLUSION

We thus conclude this proposed system saying that it will be a best data protection model can be implemented in cloud environment to avoid the cloud storage problem and improvise the security . Future enhancement of this work is to apply additional mechanism to increase the speed of access of data from the cloud environment

REFERENCES

- [1] <http://www.qrcode.com/en/codes/>
- [2] Thiyagarajan M, Dinesh Kumar K” Qr code authentication for product using cloud computing”journal of global research in computer science, Volume 3, No. 2, February 2012.
- [3] Denso-wave: <http://www.denso-wave.com/qrcode/index-e.html>
- [4] David Pintor Maestre Universitat Oberta de Catalunya08018, Barcelona, Spain “QRP An Improved Secure Authentication method using QR codes” 2012.
- [5] Suraj Kumar Sahu: “ Encryption in QR Code Using Steganography “. MATS University, Raipur.
- [6] Dong sik-oh, Bong han-kim and Jae- Kwang Lee : “A Study on Authentication System using QR code for Mobile cloud computing Environment”. Hennam University Daejeon, Korea.
- [7] Young Sil Lee; Nack Hyun Kim; Hyotaek Lim; HeungKuk Jo; Hoon Jae Lee: “OnlineBanking Authentication System using Mobile-OTP with QR-code”. Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference,Nov.-Dec. 2010.
- [8] Kuan-Chieh Liao; Wei-Hsun Lee: “A Novel User Authentication Scheme Based on QR-Code”. *Journal of Networks*, Vol 5, No 8 (2010), 937-941, Aug. 2010.
- [9] Craig A. Shue and Brent LagesseCyberspace Science and Information Intelligence Research “Encryption in QR Code Using Steganography” 2013.
- [10] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, SebastianSchrittwieser, Mayank Sinha, Edgar Weippl: “QR-Code Security”. SBA Research, 2010.
- [11] Sandha, Dr. M. Ganaga Durga, “ Study on Data Security Mechanism in Cloud Computing” 2014 ,IEEE digital Library.
- [12] Sandha, Dr. M. Ganaga Durga, “Effective Data Security Mechanism in Cloud Computing Using QR Code” 2015.