

Implementation of QR code on data protection of cloud computing

Sabah Shaikh

MCA, Post Graduate, V.E.S.I.T

Abstract - Cloud computing is basically an outsourcing project. Cloud computing has a number of other benefits too like online storage and users have the ability to increase or decrease space according to their requirements. Cloud computing lets you store information and use hardware and software remotely over the internet, based on where and when you need them. This unique attribute, however, poses many new security challenges which have not been well understood. In this paper we will study how QR code can be used for cloud computing as data protection.

Key Words: Cloud Computing, Security challenges, QR code.

1. INTRODUCTION

Cloud computing is a model for allowing convenient, on demand access from anywhere, to a shared pool of computing resources. These can include servers, storage, networking, applications and services that can be rapidly and easily provisioned and released. The cloud model includes five essential characteristics [1] On-Demand Self Service: This allows users to quickly and automatically get access to the IT resources that they want without requiring any additional human interaction. [2] Broad Network Access: This is the ability to access a service from any standard device that is connected to the network including PCs, laptops, mobile phones or tablets. [3] Resource Pooling: Computing networking and storage are pooled and shared across multiple customers. [4] Rapid Elasticity: This allows you to quickly scale or shrink the capabilities of your cloud to match the level of user demand. [5] Metering: This tracks and controls the level of resource usage or the cost of that usage.

A cloud data can be categorized by SaaS, PaaS and IaaS. Software as a service or SaaS allows users to access an application without having to manage or control the underlying cloud infrastructure. Platform as a service or PaaS gives users access to a software development environment to allow them to create their own cloud applications using programming languages, libraries services and tools. The user has control over these applications without having to manage or control the underlying cloud infrastructure. Most widely viewed as cloud

Infrastructure as a service or IaaS, allows a user to quickly and easily provision full computing resources including processing storage and networks without the user having to manage or control the underlying cloud infrastructure.

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.

QR code stands for Quick Response. It is very similar to a bar code. QR code is more versatile than barcode as it allows you to store more information than barcode. In fact, compared to barcode's 20 alphanumeric character limits, a QR code can hold thousands of characters of data. QR code was developed by Denso Wave in Japan in 1994. QR code is two-dimensional matrix format barcode. 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 directions which mean it could store more information up to 406 bytes than a normal barcode within a limited space. 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.

1.1 Structure

The structure of QR code consists of an encoding region (cell) and a functional pattern. Functional patterns are such as finder pattern, alignment pattern, timing pattern and a quiet zone which makes the reading of the data easier and provide an area for storage. Besides the finder pattern are located at three corners with intention to ease the location and identification of its position, size and inclination. Moreover the alignment pattern acts as a correction pattern that will correct the distorted QR code. While the black and white patterns allows the timing pattern to better identify and correct the central coordinate of the data cell at the time the QR code symbol is distorted. The quiet zone is the margin space needed for reading of QR code, while the data will be stored in the data area in the symbol. Currently there are 40 versions of QR code and four levels of error correction.

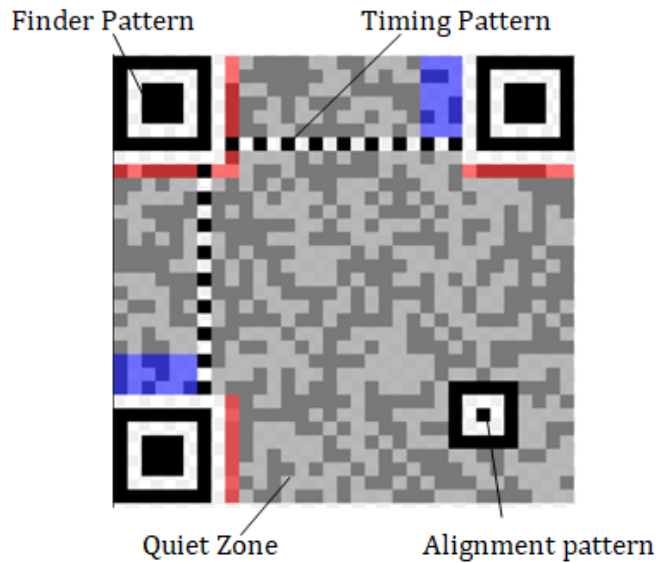


Fig -1: QR code

1.2 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 logo QR it incorporates a high level of design features.

	QR Code	PDF417	DataMatrix	Maxi Code
Developer(country)	DENSO(Japan)	Symbol Technologies (USA)	RVSI Acuity CiMatrix (USA)	UPS(USA)
Type	Matrix	Stacked Bar Code	Matrix	Matrix
Data capacity	Numeric	7,089	2,710	3,116
	Alphanumeric	4,296	1,850	2,355
	Binary	2,953	1,018	1,556
	Kanji	1,817	554	778
Main features	Large capacity, small printout size	Large capacity	Small printout size	High speed scan
Main usages	High speed scan	OA	FA	Logistics
Standardization	All categories	AIM International JIS ISO	AIM International ISO	AIM International ISO

Fig -2: Types of QR code

2. Related Work

Presently, much of growing interest has been pursued in the context of remotely stored data security David Pintor Maestre et al. [3] 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 IMEI number of smart phone with 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 pincode. They 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 security of QR code. Suraj kumar sahu et al. [7] describe “Encryption in QR code using stegnography” where cover image and QR data is embed and encrypted. Dong-sik oh et al. [8] consider creating 3 set of QR code by converting the single information into 3 versions of QR code and stored in distributed server system.

3. Proposed System

The proposed system, involve 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 used for creating a unique key for each user. Then the uploaded file is encrypted by homomorphic authentication and then combined with QR code. This combination of encryption code is stored in three different servers. A key is given to the user at time of download. The data is downloaded from servers if key is correct. The data is merged and decrypted before display to the user.

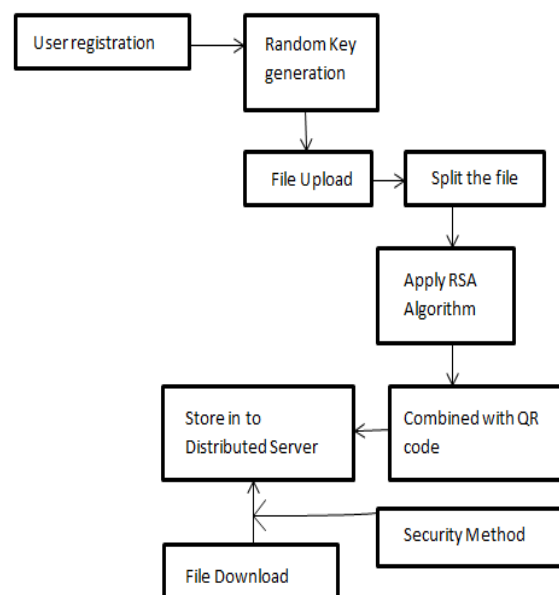


Fig -3: Flowchart

The pseudo code is given below:

```
// Module for uploading data
Upload ( )
{
    If (user authentication success)
    {
        Split and encode + combined QR;
        Distributed to servers
    }
    Else
        Return authentication failed;
}
// Module for downloading the data Download ( )
{
    If (key is ok)
    {
        Collect from the server;
        Decrypt the file;
    }
    Else
        Failed;
}
```

3.1 Working

Random key generation is the initial process. X_n is the random number. The next number assigned to the user is $X_{n+1} = (aX_n + b) \bmod m$. 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 . $e * d \bmod n = 1$. Here public key is n and e private key is d . plain text m , Encryption is $C(m) = m^e \bmod n$ and Decryption is $m(c) = c^d \bmod n$. Binary of QR code is XOR with every bit of Encrypted file F and result files F_n stored in to distributed server.

4. Conclusion

We thus conclude this proposed system saying that it will be a good technique for data protection which can be implemented in cloud computing 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] Denso-wave:
<http://www.densowave.com/qrcode/index-e.html>
- [3] David Pintor Maestre Universitat Oberta de Catalunya08018, Barcelona, Spain "QRP An Improved Secure Authentication method using QR codes".
- [4] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, SebastianSchrittwieser, Mayank Sinha, Edgar Weippl: "QR-Code Security". SBA Research, 2010.
- [5] Srikanth Bharadwaj A STUDY ON QR CODE BASED PUBLIC CLOUD DATA PROTECTION.
- [6] Wang, L., Laszewski, G., Kunze, M., Tao, J.: 'Cloud computing: a perspective study', New Gener. Comput., 2010.
- [7] Suraj Kumar Sahu: "Encryption in QR Code Using Stegnography". MATS University, Raipur
- [8] 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.