ISSN: 0975-833X

*Available online at http://www.journalcra.com*

*International Journal of Current Research*
*Vol. 10, Issue, 04, pp.68018-68020, April, 2018*

**INTERNATIONAL JOURNAL OF CURRENT RESEARCH**

## RESEARCH ARTICLE

# QR CODE BASED PUBLIC CLOUD DATA PROTECTION: A REVIEW

***Vipin Rawat and Ram sringar verma**

Department of Computer Science, M. Tech Computer Science UIET, Babasaheb Bhimrao Ambedkar University, Vidya Vihar Lucknow, India

**ARTICLE INFO**

***Article History:***
Received 18th January, 2018
Received in revised form
24th February, 2018
Accepted 20th March, 2018
Published online 30th April, 2018

***Key words:***
Cloud computing, Encryption and Decryption , Quick response code, Cloud data protection, Authentication.

**ABSTRACT**

Encryptions and Decryptions are done using the public key and private key. These both keys are not stored on the client side or server side but only in the users devices like mobile, tablet in the form of Quick Response (QR) codes. This quick response codes can be used to Decrypt the users information and data. The Cloud computing standard as a new computing model which aim to provide reliable, Custom and quality of service certification in dynamic computing for the end users. Cloud computing enables customers with limited computational resources to out resource with their Big computational workload to the cloud, and storage, bandwidth power and even relevant software that can be shared in pay- per –use way. In this paper we must design a mechanism for protect information or data by using the encryption and decryption technique. And also protect the customers data and information from malicious Attacks or Behaviors.



**Citation: Vipin Rawat and Ram sringar verma, 2018.** "QR Code based public cloud data protection: A review", *International Journal of Current Research*, 10, (04), 68018-68020.

## INTRODUCTION

In the modern day the cloud services are very popular. Cloud service offers claim to provide security. The user can upload their information data like document and media files because the cloud servers are scalable easily accessible and all over. In the case of cloud security the users do not trust the security of cloud data. Every cloud users the biggest challenge of the cloud data security like data recovery, data location, regulatory compliance and privileged users. But it is very difficult for service providers to prove the users that the data is secure even if the cloud servers are agreed. These sensitive information, data like document images audio video files and more media file as well. Such media files are not managed by the users. these files are uploaded to the cloud servers.

**Essiential characterstics of cloud computing can be define as the given bellow**

- On-demand self service.
- Broad network access.
- Rapid elasticity.
- Resource pooling.
- Measured service.

**Corresponding author:* **Vipin Rawat,**
Department of computer science, M. Tech computer science UIET, Babasaheb Bhimrao Ambedkar University, Vidya Vihar Lucknow, India.

**On-demand self service**

User can unnaturally provision computing capabilities like server time and network storage is automatically without requiring human interaction with each service provider. The On demand service is a delivery model in this model computing resources are made available to needed as per user requirement.

**These resources maintained by the user enterprise and made available by a cloud service provider**

**Broad network access:** In the broad network accessed through the standard mechanisms that promote use by different thin and thick client platforms.eg. laptops and mobile phones.

**Rapid elasticity:** Rapid elasticity capabilities can be elastically released and provisioned, in some cases automatically to scale rapidly outward and inward sufficient with demand.

**Resource pooling:** The resource pooling providers computing resources are pooled to serve the multiple users or customers using a multilevel model, with different virtual resources and physical resources can dynamically assigned and reassigned according to the customer demand. Example of resources include memory, processing, storage and network bandwidth.

**Measured service:** In the case of measured service the cloud systems automatically control and optimize resource use by averaging metering capability at some level of abstraction proper to the service. Example storage, memory and processing.

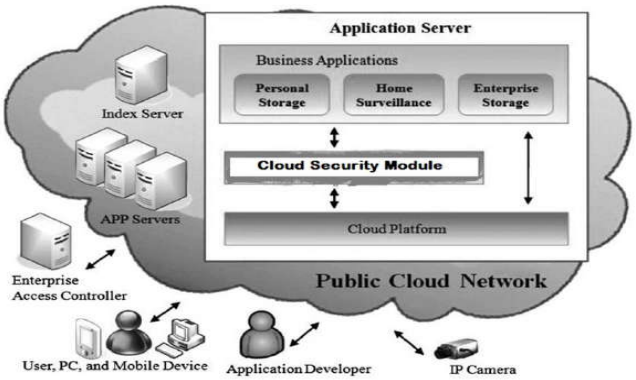


**Figure no 1. Cloud architecture**

**Cloud computing models**

**There are two type of cloud computing models**

- Service Models.
- Deployment models.

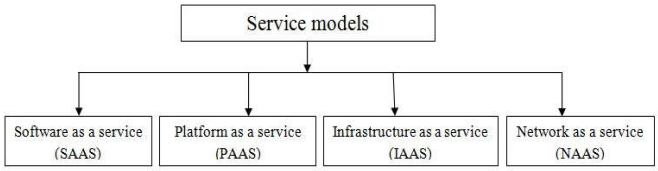


**Figure no 2. Service models**

**Software as a service (SAAS):** Applications are accessible from various customers or client devices through a thin client interface, such as web browser like email based, or a program interface. The consumer does not control and manage the cloud infrastructure including servers, network, storage and operating systems.

**Platform as a service (PAAS):** Platform as a service provide the runtime environment for applications, development and deployment and download install software. It is also support to web-development interfaces such as simple object protocol which allows the multiple web services.

**Infrastructure as a service (IAAS):**

**In infrastructure as a service provided the various services are**

- Memory.
- Storage space.
- CPU cycle.
- Network equipment.
- Server space.

**Network as a service (NAAS):** Networks as a service involves the optimization resource allocations by considering network and computing resources as a unified whole. The traditional network as a service include the flexible and extended virtual private network with bandwidth on demand.

**Deployment model**

**Private cloud:** private cloud is opposite of public cloud. private cloud allows systems and services only with an organization.

**Public cloud:** In public cloud allows the easily accessible cloud systems and services to open general public. Its operated and managed by a business, academic, and government organization.

**Community cloud:** Community cloud means to access the services in various group of organizations.

**Hybrid cloud:** Hybrid cloud is the combination of the public and private cloud. Its provides the both features scalability private and public scalability.

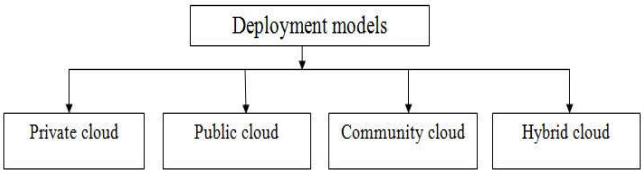


**Figure no 3. Deployment models**

**Quick response code (QR Code)**

QR codes are two dimensional barcodes (matrix codes).QR code used to encrypt and decrypt the various information and data in the format of text format and image format. In QR code we store the information such as email address, URL of website, phone numbers and various identity of users. QR code is a very easy to use technology for hidden the information of the customers or client. The smallest size of QR code pixel is 21*21 and the largest size of QR code pixel is 177*177 .Size of QR code pixels is called versions. 21*21 pixel size of QR code is version 1 and 25*25 pixel size of QR code is version 2 and 177*177 pixel size of QR code is called version 40.its also support for error correction. There are four levels of error correction Level L modes provides 7% error correction rate and level M provides the 15% error correction rate and 25%error correction rate is level Q and level H provides the error correction rate is 30%. In present time QR code technology and scanning the code is supported by many mobile phones and devices such as Android phones and apple phones. In android phones we are used the various applications for scan the QR code.

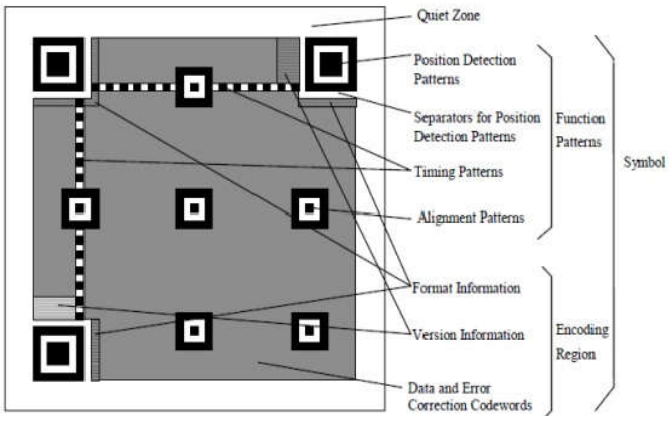


**Figure no 4. QR Code architecture**

**User authentication**

In cloud systems use the user name and password for user authentication. User authentication technique use for verify the correct user. If users gives the correct password then access to the data. If the user input the small error entering the secret password, the authentication is fails and user cannot access the data. In cloud systems an another mechanism used for user authentication is one time password (OTP). For one time password user need the extra devices such as mobile or pager for receive the conformation code or passwords.


**Figure NO 5. User authentication**

**Encryption and decryption**

Encryption means to hide or encode the secret Data. Decryption means to decode the encrypted or encoded data with the help of Encryption and Decryption algorithms. There are various encryption algorithms such as RSA, AES, DES, BLOWFISH, Encryption and Decryption is done by the public and private key.

**Related work**

Cloud data protection using the QR code and encryption algorithm is already done. This study proposes the use of algorithm for encryption of the data using the blowfish algorithm.

Blowfish algorithm is a symmetric key encryption algorithm. Symmetric key algorithm means the user public and private key is same

**Conclusion**

The goal of this survey paper is highly secure the cloud data using the user authentication and QR code based technique. In modern day the cloud data suffers from the various privacy and security issues. We try to more secure the cloud data using the asymmetric encryption algorithm. Asymmetric algorithm is used to both encryption and decryption after using the asymmetric algorithm the cloud data is more secure because user encrypt the data using public key and decrypt using the private key both key are different.

## REFRENCES

Bernd Grobauer, Tobias Walloschek and Elmar Stocker, 2011. 'Understanding cloud computing vulnerabilities', IEEE Security and Privacy, 9, pp. 50-57.

Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, 2012." Toward secure and dependable storageservices in cloud computing." Services Computing, IEEE Transactions on 5, no. 2: 220-232.

Heiser, J., Nicolett, M. 2008. 'Assessing the security risks of cloud computing'. Gartner, Incorporated, 2008.

Kandukuri, B.R., Paturi, R. and Rakshit, A. 2009. 'Cloud security issues'. Proc. Working IEEE SCC: Int. Conference Services Computing 2009 (SCC2009 WIP), 2009.

Kui Ren, Cong Wang, and Qian Wang, 2012. "Security challenges for the public cloud." *IEEE Internet Computing,* 16, no. 1: 69-73.

Tout, Sverdlik, and Lawver, 2009. "Cloud Computing and its Security in Higher Education," In Proceedings of the Proc ISECON 2009.

Wang, L., Laszewski, G., Kunze, M. and Tao, J. 2010. 'Cloud computing: a perspective study', New Gener. *Comput.,* pp. 137- 146.

Yunqi Ye, Liangliang Xiao, I-Ling Yen and Farokh Bastani, 2010. "Secure, Dependable, and High Performance Cloud Storage", 29th IEEE *International Symposium on Reliable*.

*******