

# SkyLoader: Document Access over Cloud

Vinod Nadar, Vikas Yadav, Jyotsna Gharat

**Abstract**— This paper presents the working and functions of SkyLoader project. SkyLoader is a cloud based application service comprised of a Public cloud which can be accessed over a Desktop computer or an Android running device. In today's world where everyone has so much information to consume, remember and recall, it is possible to forget something or another, but what if it's an important Document required at an even more important place then it may lead to some serious problem. SkyLoader project will assist the clients to access personal Documents from anywhere at any time.

**Index Terms**— AES Encryption, Authentication, Cloud Computing, Openstack, OTP (One Time Password), QR code and Security.

## 1 INTRODUCTION

CLOUD computing is a model for enabling ubiquitous network access to a shared pool of configurable computing resources [1]. Cloud computing is one of the hottest buzzwords in technology. It appears 48 million times on the Internet [2]. The fundamental concept of cloud computing originated in the 1950s, when corporations and learning institutes prioritized the efficiency of their large-scale mainframe computers, allowing multiple users both physical access to the computer from multiple terminals as well as shared central processing unit time [3]. The expression cloud is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud and describes any set of things whose details are not inspected further in a given context [4]. It is not always possible to travel with every piece of paper around the world, especially when it's an important document like Identification documents. Skyloader eradicates this issue by making use of the Internet and every common man's weapon a Smart phone. With the help of a reliable Internet connection clients will be able to use the cloud services anytime from any place around the Globe and also as the stakes here are highly classified and important Documents we assure you that 'Security' is our first priority.

## 2 TECHNOLOGIES USED

### 2.1 Public Cloud

A cloud is called a "public cloud" when the services are provided over a network that is open for public use. Public cloud services may be free or offered on a pay-per-usage model. Technically there may be some or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Generally, public cloud

service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure at their data center and access is generally via the Internet. AWS and Microsoft also offer direct connect services called "AWS Direct Connect" and "Azure ExpressRoute" respectively, such connections require customers to purchase or lease a private connection to a peering point offered by the cloud provider [5].

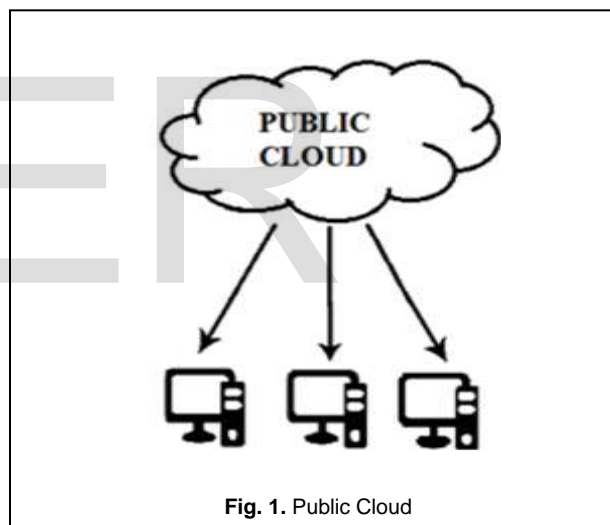


Fig. 1. Public Cloud

### 2.2 QR Code

QR Code is a Matrix code; the QR codes were developed in Japan in 1994 by Toyota subsidiary, DensoWave to help track automobile parts throughout production [6].

This technology has been around for over a decade but has since become popular as a medium for marketers to reach smart phone users.

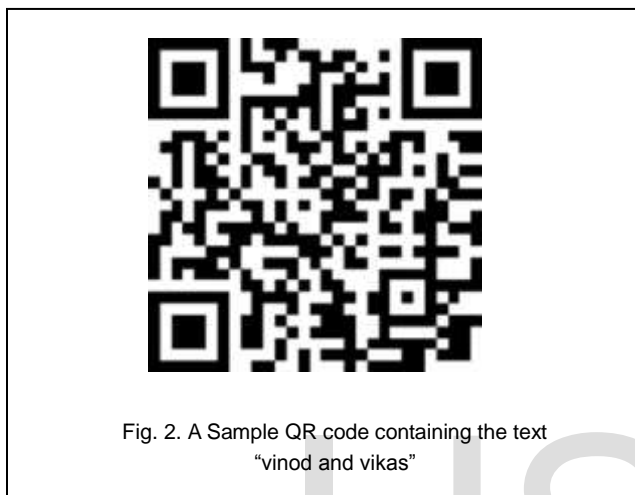
Bar codes have become widely popular because of their reading speed, accuracy, and superior functionality characteristics and their convenience universally recognized, the market began to call for codes capable of storing more information, more character types, and that could be printed in a smaller space. As a result, various efforts were made to increase the amount of information stored by bar codes, such as increasing the number of bar code digits or layout multiple bar codes. However, these improvements also caused this data. Think of it as an alternative way of getting data into your

- Vinod Nadar is currently pursuing bachelor's degree program in Information technology engineering in Mumbai University, India, PH-08108334808. E-mail: vinodselvinmadar@gmail.com
- Vikas Yadav is currently pursuing bachelor's degree program in Information technology engineering in Mumbai University, India, PH-09869985533. E-mail: vikasy060892@gmail.com
- Jyotsna Gharat holds master's degree program in Computer Engineering from Mumbai University, India, PH-09920326161. E-mail: jyots.584@gmail.com

phone (as opposed to typing it in manually) [6].

Here are some of the possibilities given below.

- a) Contact information
- b) Calendar event
- c) E-mail address
- d) Phone number
- e) Geo location
- f) SMS
- g) Text
- h) Wi-Fi network
- i) URL



### 2.3 OpenStack

OpenStack is a set of software tools for building and managing cloud computing platforms for public and private clouds. Backed by some of the biggest companies in software development and hosting, as well as thousands of individual community members, many think that OpenStack is the future of cloud computing. OpenStack is managed by the OpenStack Foundation, a non-profit which oversees both development and community-building around the project. The seven openstack's projects along with their respective code name are listed in table 1.

TABLE 1  
OpenStack Projects

Sr. No.	Openstack Project Name	Code Name
1	Compute	Nova
2	Object Storage	Swift
3	Identity	Keystone
4	Dashboard	Horizon
5	Block Storage	Cinder
6	Network	Neutron
7	Image Service	Glance

#### Components of OpenStack:

**2.3.1 Nova** is the primary computing engine behind OpenStack. It is used for deploying and managing large numbers of

virtual machines and other instances to handle computing tasks [8].

**2.3.2 Swift** is a storage system for objects and files. Rather than the traditional idea of referring the files by their location on a disk drive, developers can instead use a unique identifier referring to the file or piece of information and let OpenStack decide where to store this information. This makes scaling easy, and developers need not to worry about the capacity of a system, everything will be handled by OpenStack [8]. Swift store data in form of virtual containers [11].

The basic essential functionality of storing objects in containers, helps keeps track of stored objects, etc. swift provides additional features also, like replication, integrity audits, etc [11].

**2.3.3 Cinder** is a block storage component, provides the software to create and centrally manage a service that provisions storage in the form of block devices known as Cinder volumes.

Cinder provides storage with high availability, fault-tolerance and its APIs compatibility with other like Amazon EC2 APIs [11]. Cinder is more analogous to the traditional notion of a computer being able to access specific locations on a disk drive [8].

**2.3.4 Neutron** provides the networking capability for OpenStack. It is a system for managing networks and IP addresses. It helps to ensure that each of the components of an OpenStack deployment can communicate with one another quickly and efficiently.

**2.3.5 Horizon** (Dashboard) provides administrators and users a graphical interface to access, provision, and automate cloud-based resources [8]. Developers can access all of the components of OpenStack individually through an application programming interface (API), but the dashboard provides system administrators a look at what is going on in the cloud, and to manage it as needed.

**2.3.6 Keystone** provides identity services for OpenStack. It is essentially a central list of all of the users of the OpenStack cloud, mapped against all of the services provided by the cloud which they have permission to use [8]. It supports multiple forms of authentication including standard username and password credentials and token-based systems.

Mysql database server is used to maintain the keystone data [11].

**2.3.7 Glance** provides image services to OpenStack. In this case, "images" refers to images (or virtual copies) of hard disks. Glance is the only module that can add, delete, share, or duplicate images [9].

**2.3.8 Ceilometer** provides telemetry services, which allow the cloud to provide billing services to individual users of the cloud. It also keeps a verifiable count of each user's system usage of each of the various components of an OpenStack cloud [8].

**2.3.9 Heat** is the orchestration component of OpenStack, which allows developers to store the requirements of a cloud application in a file that defines what resources are necessary for that application. In this way, it helps to manage the infrastructure needed for a cloud service to run [8].

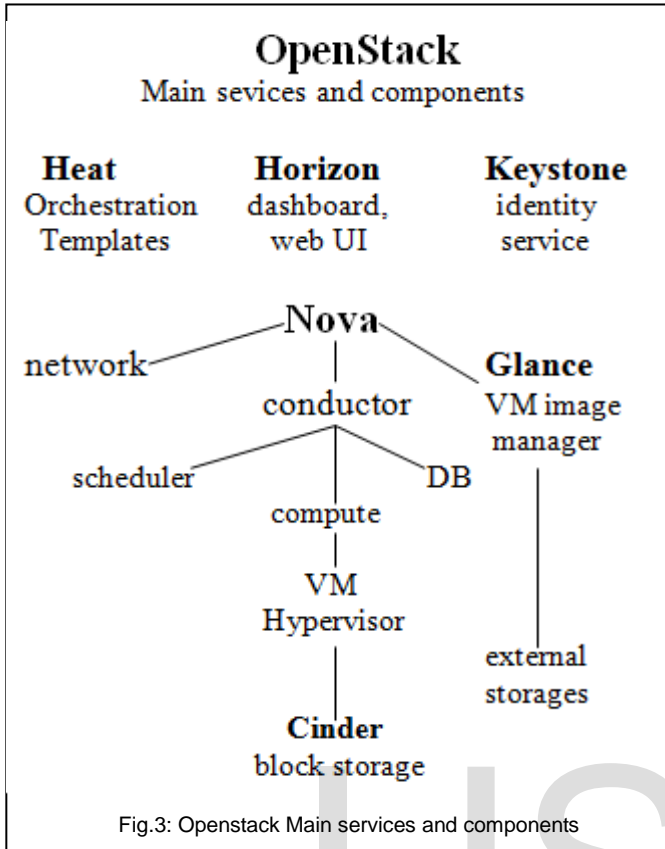


Fig.3: Openstack Main services and components

**2.4 OTP (One Time Password)**

One-time password is a password that is only valid for a single login session or transaction. Hence for each session the user wants to login or to access some file the new OTP is generated which is unique and Time based, means it will expire after some duration which helps preventing replay attacks, phishing attacks and other attacks on basic static passwords [9]. On the hand, one-time password schemes cannot be memorized by human beings. For this reason, they require additional technology in order to work [10]. Basically one-time password schemes can be classified into the following four categories:

- A. Based on the mathematical algorithm.
- B. Based on the smart card.
- C. Based on the time-synchronized token.
- D. Based on the Short Message Service (SMS) [10].

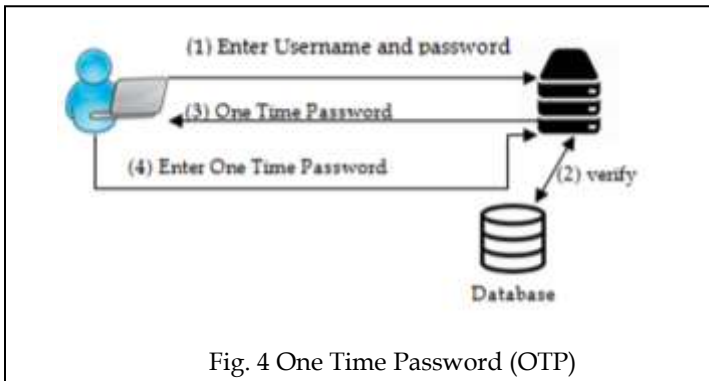


Fig. 4 One Time Password (OTP)

**3 PROPOSED SCHEME**

The QR technology plays an important role in our project. At a certain point in the authentication process of our project the user will be required to scan a server-generated QR code from their Smartphone if user is using a Smartphone. OTP is a password that is valid for only one login session or transaction. This OTP allow the user to get login into the system by entering their password with OTP.

OTP is an encrypted format, so users can't read it. Instead of that, user needs to forward that OTP with system logging password to the system. It avoids the unauthorized logging.

In our proposed approach is, after user entering the username and password web server generates the Encrypted OTP using AES algorithm and converted into QR image and it is available in that page. The user can make use of any normal QR Decoder/Scanner available for their mobile. After scanning the user will get new URL, which prompts user to enter OTP which will be available on the user message box of SkyLoader or it will be sent to the registered mobile number. After successful authentication the user can add/remove files easily.

**3.1 SYSTEM ARCHITECTURE**

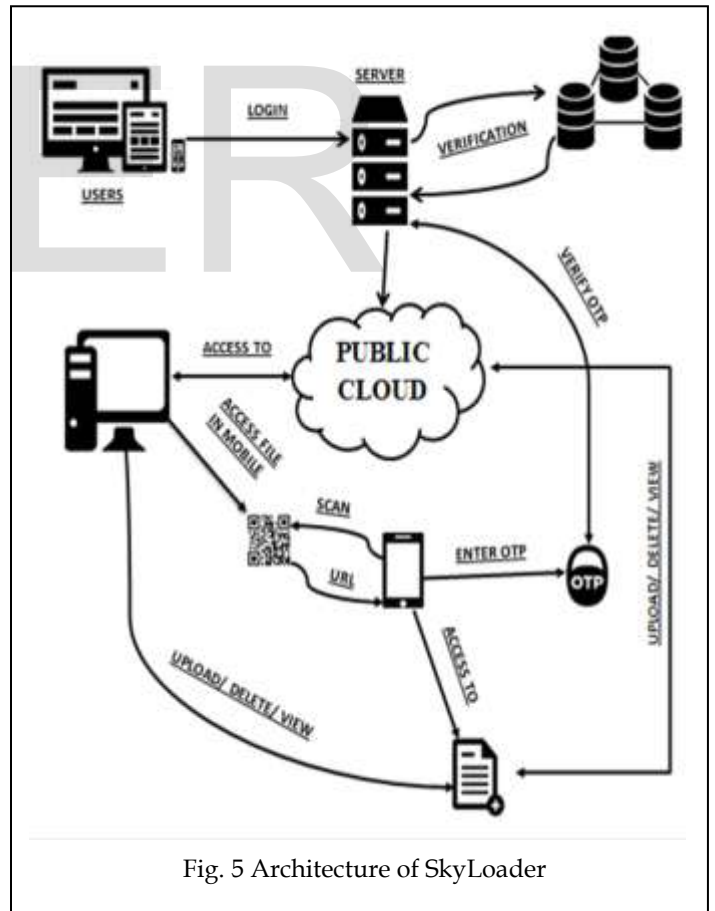


Fig. 5 Architecture of SkyLoader

**3.2 System Analysis**

**3.2.1 Registration**

In SkyLoader, the user will be asked to provide a username

and unique password set to register to SKYLOADER database. After the registration process the user can create an account on SKYLOADER cloud services and can upload and store the files (.JPG/.PNG/.PDF/.BMP/and other formats).

### 3.2.2 Login

After completion of registration process, user can login to SKYLOADER account using their login credentials. After the successful authentication the server will redirect the user to the homepage of the cloud, wherein the user will be asked to choose the mode of access i.e. if the user is using a Desktop or a handheld device (smartphone).

#### 3.2.2.1 Authentication: Phase-I

If the user chooses, a desktop computer as his device of operation then the user will be directly redirected to the account's homepage. Where a user will have the highest access to documents, user can create/delete/view or even close an account (temporarily or permanently).

#### 3.2.2.2 Authentication: Phase-II

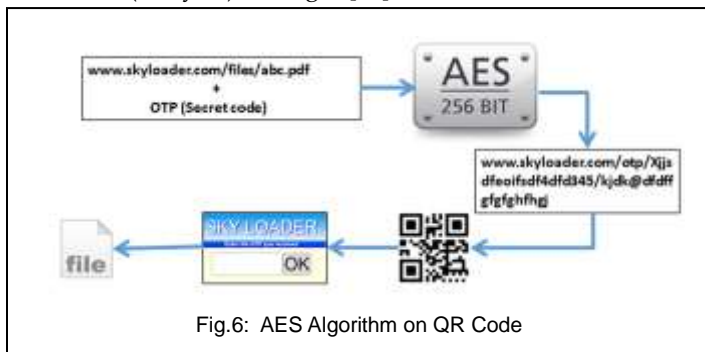
If a user wants to view the documents on a Mobile phone, i.e. the user has selected the Mobile option from the desktop then the Cloud server will start the phase-2 authentication process. In this authentication phase, a QR code will be generated on user's desktop screen for a certain period of time. If the user is not able to perform further process in that amount of time the QR code will expire. If the user scans the QR code from a smartphone in that given time-period, then an URL in the QR code will redirect to an OTP page on user's phone's browser. Also the required OTP will appear on user's desktop screen which user will be required to enter in user's Mobile phone's browser window. Now the user will be redirected to user's account page.

If the user is only using the Smartphone to login in the system, the server will recognize the device using his screen size (media query). Then there will be only one phase authentication process i.e. username and password. After which a user will be redirected to user's account page, where user can do update/delete/upload documents easily.

### 3.3 Encryption Algorithm

#### 3.3.1 AES algorithm

AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length [12].



This is called a symmetric encryption algorithm. Encryption algorithms that use two different keys, a public and a private key, are called asymmetric encryption algorithms. An encryption key is simply a binary string of data used in the encryption process. Because the same encryption key is used to encrypt and decrypt data, it is important to keep the encryption key a secret and to use keys that are hard to guess. Some keys are generated by software used for this specific task. Another method is to derive a key from a pass phrase [12].

## 4 RESULTS



Fig. 7. Home Screen of our Sky Loader website



Fig. 8. Click to generate QR-code



Fig. 9. QR-code scanned using QR-Scanner



Fig.10: OTP page

The term 128-bit encryption refers to the use of a 128-bit encryption key. With AES both the encryption and the decryption are performed using the same key [12].



## 5 Conclusion & Further work

The cloud computing is very popular and prevalent technology today which can be used to solve many day-to-day problems. SkyLoader is one example of that. Unlike other software applications for storing and accessing data online the users won't have to install the application on their device it can be accessed using any Web browser on their smartphones or a usual desktop. SkyLoader also uses many encryption algorithms to provide satisfactory security to the users with two-phase authentication process. We have proposed a secure and reliable authentication scheme for accessing documents on mobile through QR code based OTPs. The system is very user-friendly as user's does not require any technical pre-requisite.

The SkyLoader application will be designed in HTML5 using CSS3 as a front-end and PHP and MySQL as a back-end. The project mainly uses open source technologies which are free of cost. OpenStack will be used to create the Public Cloud.

The Skyloader application will be much easier than other cloud based applications and all the important documents will be at the tip of the fingers which will save users a lot of time and will be more secure than any other traditional methods.

## ACKNOWLEDGMENT

We would like to express our gratitude to our project supervisor **Prof. Jyotsna Gharat** for her guidance and support throughout the project. She has always directed us in the right direction and helped us to stick to our Project's domain all the time, which in fact helped us to complete this project with much ease and in time. We are truly thankful for our Head of Department (HOD) **Prof. Chhaya Narvekar** for allowing us to implement our idea into its practical form wherein there were a lot of interesting and challenging things to learn. We would like to express our sincere gratitude to the principal, **Dr. Y.D. Venkatesh**, for maintaining an environment of academic rigor along with providing us the required infrastructure for our project research and development. We would also like to mention and thank my friends and family for their constant support.

## REFERENCES

- [1] P. Mell and, T. Grance, "The NIST Definition of Cloud Computing," NIST (National Institute of Standard and Technology), Sept, 2011.
- [2] Who Coined 'Cloud Computing?. [Online]. Available at: "www.technologyreview.com/news/425970/who-coined-cloud-computing/". [Accessed 6th Aug 2015].
- [3] The history of cloud computing and what's coming next: A CIO guide. [Online]. Available at: "http://searchcio.techtarget.com/essentialguide/The-history-of-cloud-computing-and-whats-coming-next-A-CIO-guide". [Accessed 7th Aug 2015].
- [4] Software Reuse in the Emerging Cloud Computing. [Online]. Available at: "http://www.igi-global.com/chapter/software-reuse-emerging-cloud-computing/65173". [Accessed 8th Aug 2015].

- [5] Three Benefits of Public Cloud Computing. [Online]. Available at: "http://resource.onlinetech.com/three-benefits-of-public-cloud-computing/". [Accessed 11th Sep 2015].
- [6] A. S. Narayanan, "QR Codes and Security Solutions," International Journal of Computer Science and Telecommunications., Vol. 3, No. 7, 2012.
- [7] What are the components of OpenStack?. [Online]. Available at: "https://opensource.com/resources/what-is-Openstack". [Accessed 18th Jan 2016].
- [8] Chapter 9. Image service. [Online]. Available at: "http://docs.openstack.org/liberty/config-reference/content/ch\_configuring-openstack-image-service.html". [Accessed 19th Jan 2016].
- [9] A. Tandon, R. Sharma, S. Sodhiya, P. M. D. R. Vincent, "QR Code based secure OTP distribution scheme for Authentication in Net-Banking," International Journal of Engineering and Technology., Vol. 5, No. 3, 2013.
- [10] K. C. Liao, W. H. Lee, "A Novel User Authentication Scheme Based on QR-Code," Journal of Networks, Vol. 5, No. 8, 2010.
- [11] R. Kamboj, A. Arya, "Openstack: Open Source Cloud Computing IaaS Platform," International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 4, No. 5, 2014.
- [12] AES Encryption. [Online]. Available at: "https://townsendsecurity.com/sites/default/files/AES\_Introduction.pdf". [Accessed 18th Jan 2016].