A STUDY ON QR CODE BASED PUBLIC CLOUD DATA PROTECTION

Srikanth Bharadwaj

Department of Computer Science
Bangalore Institute of Technology
Visvesvaraya Technological University
Bengaluru-04, India
srikanth.bharadwaj09@gmail.com

ABSTRACT

Cloud computing enables customers with limited computational resources to outsource their large computational workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner [5]. Treating the cloud as an intrinsically insecure computing platform from the viewpoint of the cloud customers, we must design mechanisms that not only protect sensitive information by enabling computations with encrypted data, but also protect customers from malicious behaviors by enabling the validation of the computational result [8].

Traditional cloud systems cannot convince the users that the data will be secure even if cloud servers are compromised and hence this study proposes a scheme which is QR code based Cloud data protection for the protection of the data on cloud using some of the advanced encryption algorithms.

Encryptions are done using public and private keys. These keys are not stored anywhere on the server side or the client side but only in the users' mobile devices in the form of QR codes. These QR codes can be used to decrypt the users' confidential information. Also, this scheme provides users with experience of managing the visible private keys by storing the keys into mobile phones and displaying them via QR codes. Thus, users' data are safely protected even if cloud servers are compromised.

Keywords: Cloud Data Protection, QR Code, Encryption

1. INTRODUCTION

Cloud services are very popular in the modern day. Users and enterprises prefer to upload their sensitive data onto the cloud servers because it is scalable, ubiquitous and easily accessible [6].

But cloud users do not trust the security and risk-management for cloud service providers is a huge factor.

The challenge for every cloud user is the concern of the security to upload their confidential data [2].

Cloud service providers claim to provide security. But it is difficult for service providers to convince the users [7] that the data is secure even if the cloud servers are compromised.

These sensitive data can include video recording and home surveillance videos as well. Such media files are not generally managed by the users. They are uploaded to the cloud servers. Sensitive behaviors may be unknowingly recorded which gets stored on cloud servers. Thus, if the online servers are compromised, such sensitive video can be accessed by the attackers.

Trade secrets by enterprises can also be considered as sensitive information. Uploading such data to cloud servers can reduce the costs of data management. But the risk of leakage of these trade secrets are greater. Business rivals or even the government may try to get access to these sensitive trade secrets with the help of professional hackers. Also, these trade secrets should not be accessible to unauthorized employees of the enterprise and hence these employees should be denied access to the cloud servers.

2. AUTHENTICATION

Cloud systems conventionally use username-password mechanism for authentication. Users with correct password get access to the data. Since password is something the user must remember and use it quite often,

they prefer to choose simple and meaningful passwords which are easy to remember. These simple passwords can be determined using methods such as dictionary attack. Also, it relies on precise recall of the secret information. If the user makes a small error entering the secret password, the authentication fails. Unfortunately, precise recall is not a strong point of human cognition.

Another mechanism used by cloud systems for authentication is one-time password(OTP). But users need to carry additional devices such as pager or mobile to receive the passwords. This can be inconvenient at times to the users. Receiving OTP at locations which do not have good network can also be inconvenient. Man-in-the-middle attack and OTP is as vulnerable to this as anything else. With this attack, the hacker sets up a fake interface for authentication (e.g., a fake web page, or an email phishing attack) [9]. Whatever you enter is passed on to the real interface, allowing the hacker to authenticate, and leave you with a failure message

One of the major problems with these authentications mechanisms is that the right of access is controlled by an authentication system. Hence if this authentication system is compromised, the data can be easily accessed by the attackers.

Encryption and decryption algorithms can be used to encrypt and secure the data. But the biggest challenge of this mechanism is the designing of key management for the keys used for encryption and decryption. The keys are generally stored in the system/PC where the data is encrypted and decrypted. Here though the data is secure, but the PC where the keys are stored will be accessed by many other users as well. Also, these keys are not portable hence using keys for encryption and decryption becomes inconvenient.

With all the above challenges, there is requirement of a secure and convenient mechanism to make the cloud users feel secure about their data.

This study proposes a mechanism to use encryption algorithms to encrypt users' data using users' public keys but the private keys used for encryption and decryption are not stored on any server or PCs. Instead these keys are stored in the users' mobile device in the form of QR code which is used to decrypt the data. Hence even if cloud servers are compromised, users can be convinced that their data cannot be accessed by attackers as they are encrypted and cannot be decrypted without presenting the QR code stored in their mobile device.

3. QR CODE

QR codes are a kind of two-dimensional bar codes. QR codes are used to encode and decode the data between a text format and image format. QR code is used to store information such as URL of web site, email address or phone numbers. QR code is a very easy to use technology as well. A QR code message can have a maximum size of up to 7089 characters in numeric format and 2953 bytes in binary format. QR codes also has fault tolerance and supports error correction. Different modes of QR codes can be used for different requirements. Level L mode provides 7% error correction rate while Level H provides a correction rate of 30%. Since QR codes provide fault tolerance, users need not try multiple times for decoding the QR code image. In recent times, since QR code technology and scanning the code is supported by many mobile phones such as Android and Apple phones (which are most widely used), it is adopted by various mobile applications, and most mobile users are familiar with it.

4. ARCHITECTURE

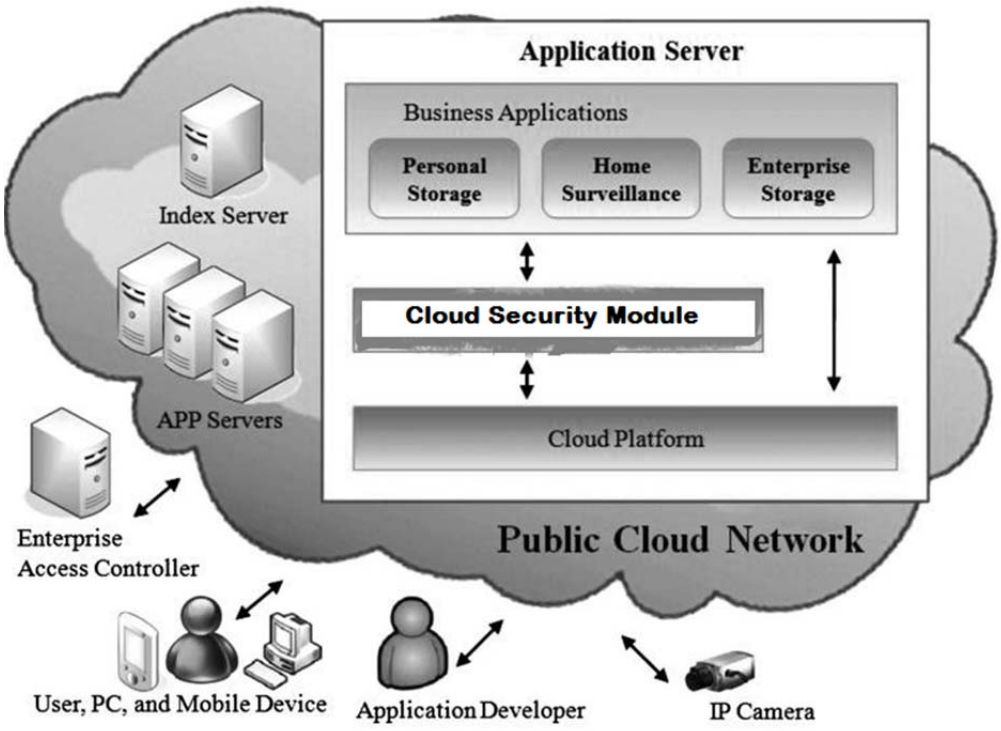

Fig 4.1 High-level Architecture

In the above architecture figure, the cloud security module is included as a middleware between applications and cloud platform to manage security issues.

The users can register their accounts with this security cloud application and generate their own public and private key pairs on their mobile application. The private key will be stored in their mobile alone in the form QR codes.

For personal usage scenario, the files with sensitive information can be encrypted by the users and upload onto the cloud. They can then be downloaded and decrypted using the QR code, which includes the private keys, stored in their mobile phone.

In case of home surveillance scenario, the IP cameras can encrypt the sensitive video with the public keys which can be stored on the cloud. The encrypted videos can be decrypted and viewed on PCs or mobile devices by extracting the private keys from the QR codes.

Finally, for the enterprise scenario, the Organization authentication controller can be used which provides the access control service to decide whether a user has access to other user's secret files.

5. ENCRYPTION

Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality, but also the key elements of security such as authentication, integrity and non-repudiation. Authentication is used to verify the origin of a message. Integrity

refers to the proof that the contents of a message have not been changed since it was sent and finally, non-repudiation ensures that the sender of a message cannot deny sending the message. Data, often referred to as plaintext, is encrypted using an encryption algorithm and an encryption key. This process generates cipher text that can only be viewed in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption. There is a course of wide range of encryption algorithms in use. The most well-known are DES, RSA, AES, Twofish and Blowfish.

This study proposes the use of Blowfish algorithm for the encryption of the data. Blowfish is a symmetric encryption algorithm, means that it uses the same secret key (private key) to both Encrypt and decrypt messages or data. Blowfish is also called as block cipher, means that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits. Messages which are not multiple of eight bytes in size must be padded. It takes a variable-length key from 32 bits to 448 bits. Blowfish consists of two parts: Data encryption and key-expansion. No attack is known to be successful against it. Blowfish has remained in the public domain to this day. Blowfish has 16 rounds. A simple encryption function is iterated 16 times. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. Due to the speed of the algorithm is more the throughput is also more. The power consumption is also less. Added functionality of key expansion makes it hard to crack. BLOWFISH is better than AES, DES, and other encryption algorithms in terms of throughput and processing time. BLOWFISH encrypts audio files at less speed. It also encrypts image most efficiently in comparison to AES. The key size is larger as it is difficult to break the code in the blowfish algorithm.

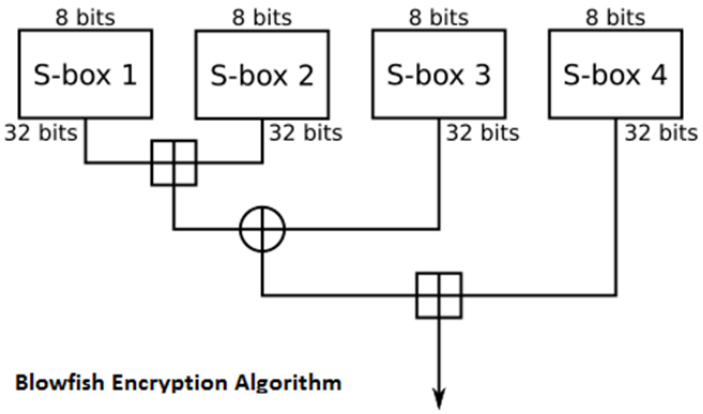

Fig 5.1 Representation of Blowfish Algorithm

6. DETAILED SYSTEM DESIGN

6.1. Upload Sequence

The user uses the Web Interface to provide his login credentials. The entered username and password is authenticated and the user is logged in if the authentication is successful. The Web Interface the sends a request for the file upload and allows the user to upload the file that contains the sensitive data. Once the upload is complete the uploaded file is encrypted and the encrypted data is stored on the cloud. Hence, even if the cloud storage is compromised the data is still secure as it is in an encrypted formatted. The private key needed for decryption is nowhere available on the cloud system.

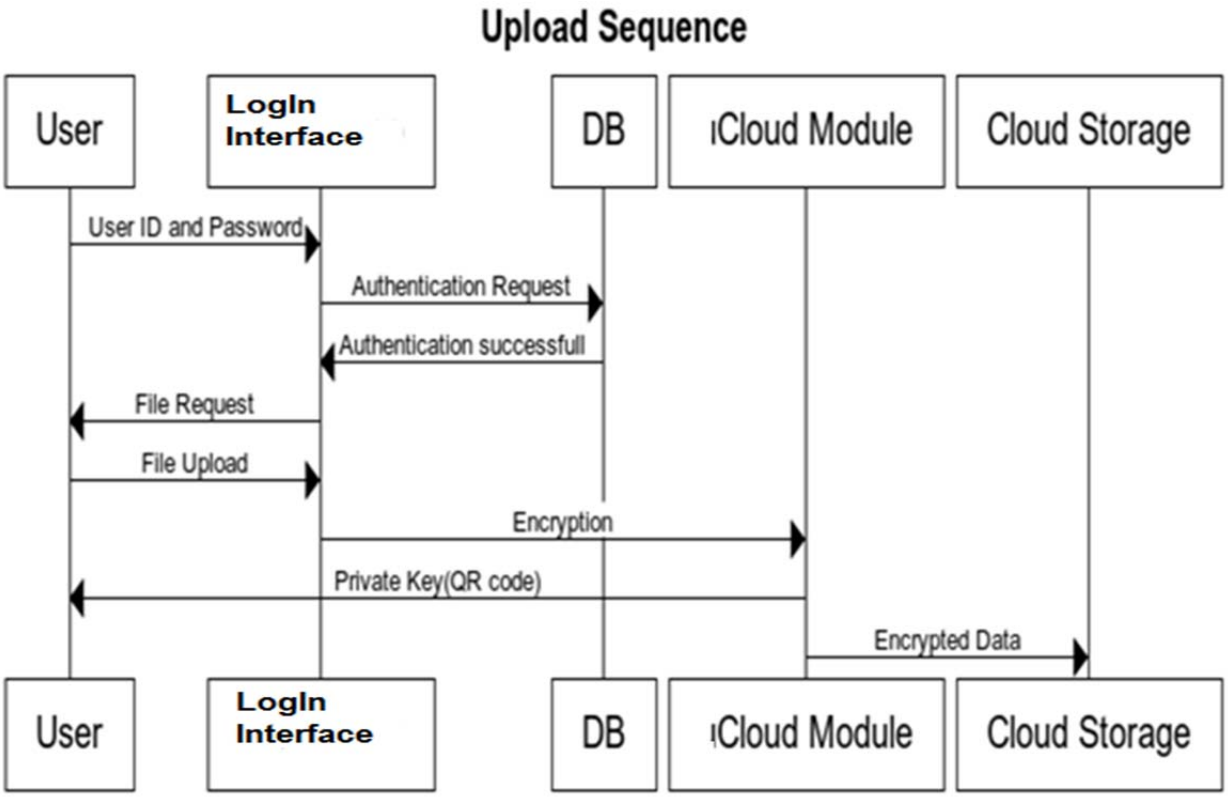

Fig 6.1 Sequence Diagram for Upload of a file

6.2. Download Sequence

The user here again uses the Web Interface and logs in using the credentials. On successful login, the user can enter the name of the file he wishes to retrieve. He is then prompted to display the QR Code. Once the user presents the QR code, the QR code is decoded and the private key is retrieved. The file is then downloaded from the cloud storage, decrypted using the decoded private key and the decrypted file is then downloaded onto the users' system. In case the user presents a wrong QR code, the decryption fails and the sensitive will not be available.

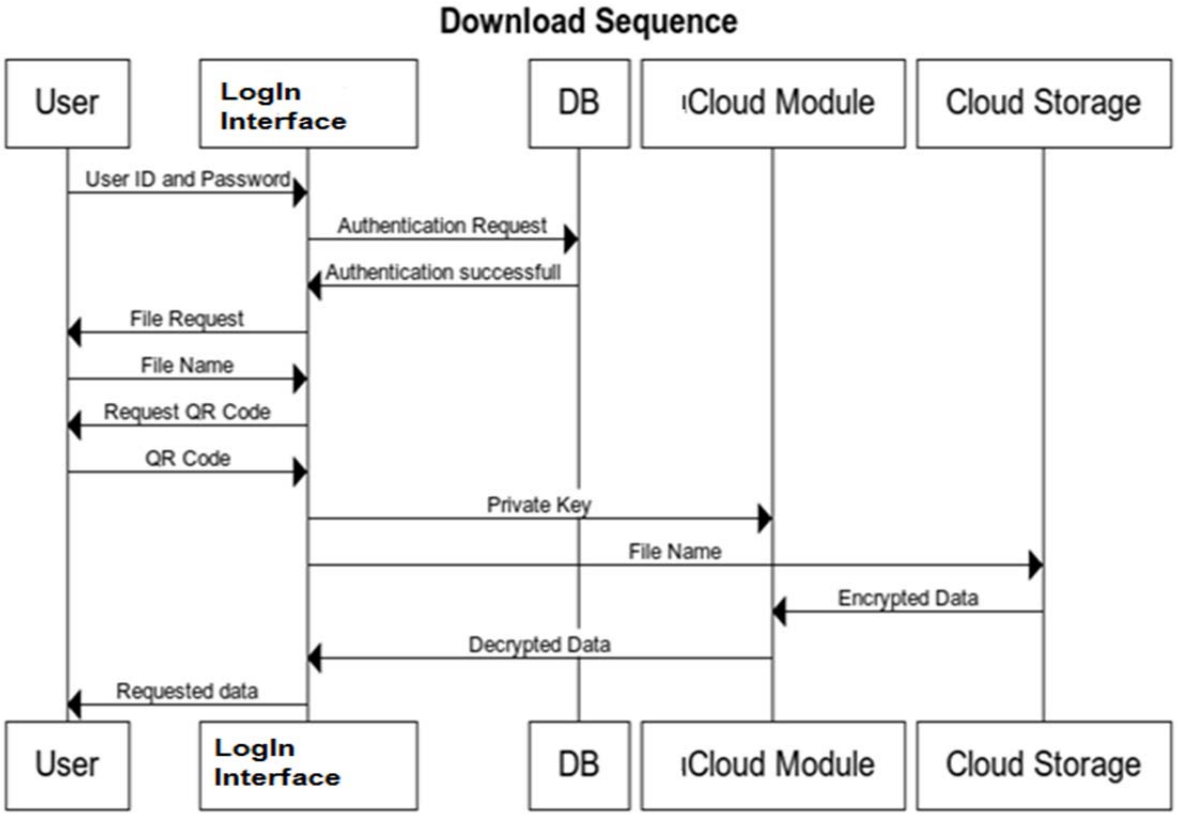

Fig 6.2 Sequence Diagram for Download of a file

7. RESULTS AND SNAPSHOTS

The method for cloud security presented in this study was implemented and a Proof of Concept was developed. This prototype was tested with different types of files such as text files, images and videos. The snapshots of the prototype are shown below.

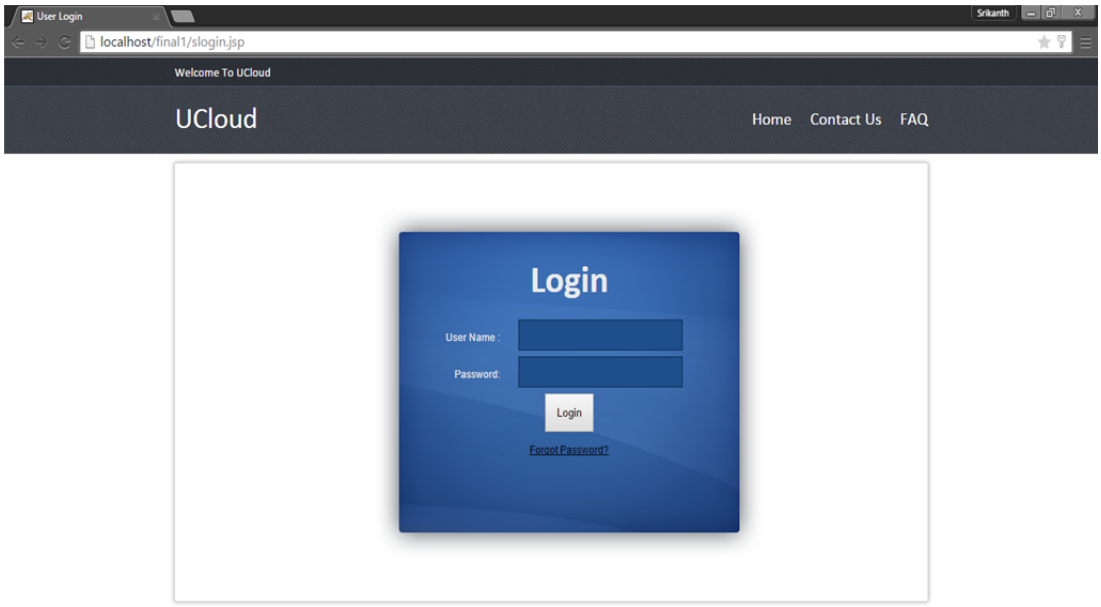

Fig 7.1 Login page for User authentication

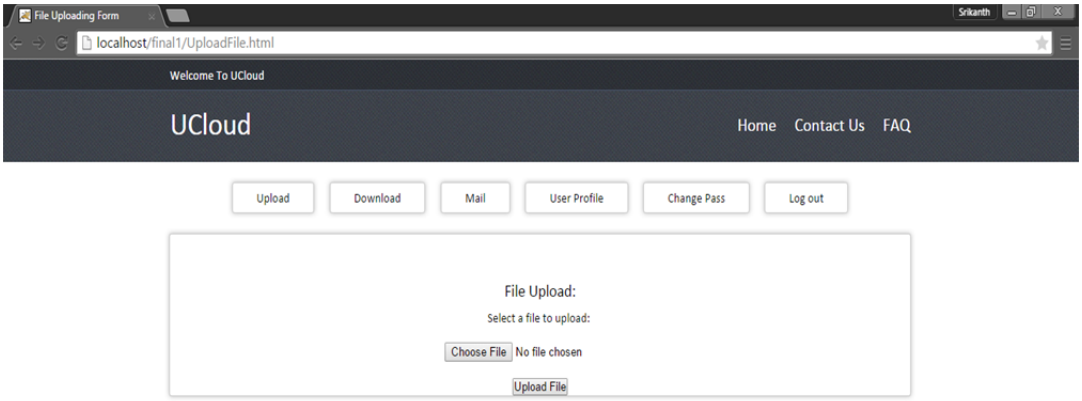

Fig 7.2 Request for the file with sensitive data to be uploaded

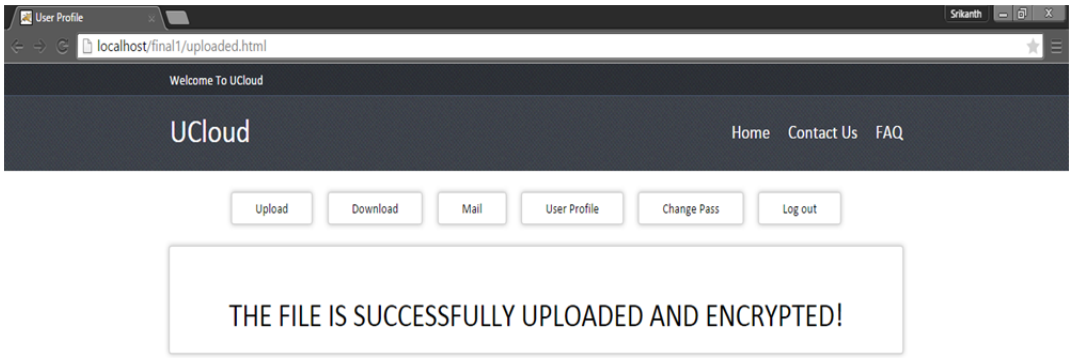

Fig 7.3 Successful Upload of the Encrypted file

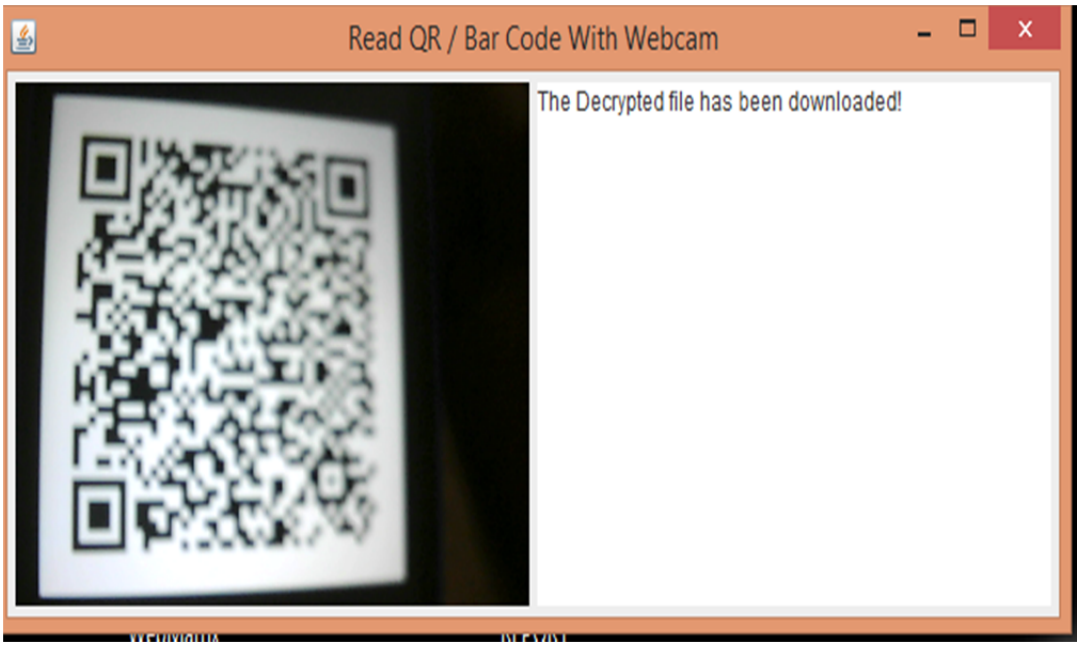

Fig 7.4 Decrypt and Download the file after scanning the QR Code via Webcam

8. CONCLUSION

Cloud computing has become a new trend in IT firms for its scalability, reduced cost, flexibility and availability. Even today cloud computing suffers from privacy and security issues. In this study, we try to make the data on a public cloud more secure by using robust encryption methods and user centric key management. The public key needed for decryption is stored in the form of a QR Code and is sent to the user, the private key is not stored anywhere in the cloud. This study proposes to use password authentication, QR code validation, hashing

function for authentication purpose and storing of the data on the cloud in an encrypted format. This enhanced form of security assures the users and thus helps in many more organizations to move to the cloud.

9. REFERENCES

[1] Chow, R., Golle, P., Jakobsson, M., et al: 'Controlling data in the cloud: Outsourcing computation without outsourcing control'. Proc. 2009 ACMworkshop on Cloud Computing Security, 2009.
[2] Heiser, J., Nicolett, M.: 'Assessing the security risks of cloud computing'. Gartner, Incorporated, 2008.
[3] Kandukuri, B.R., Paturi, R., Rakshit, A.: 'Cloud security issues'. Proc.Working IEEE SCC 2009: Int. Conf. Services Computing 2009 (SCC2009 WIP), 2009.
[4] Vouk, M.A.: 'Cloud computing – issues, research and implementations', J. Comput. Inf. Technol., 2008, 16, (4), pp. 235–246.
[5] Wang, L., Laszewski, G., Kunze, M., Tao, J.: 'Cloud computing: a perspective study', New Gener. Comput., 2010, pp. 137–146.
[6] Weiss, A.: 'Computing in the clouds', NetWorker, 2007, 11, (4), pp. 16–25.
[7] Kui Ren, Cong Wan, Qian Wang : 'Security challenges for public cloud', IEEE Internet Computing, 2012, 16, pp.69-73.
[8] Bernd Grobauer, Tobias Walloschek, Elmar Stocker : 'Understanding cloud computing vulnerabilities', IEEE Security and Privacy, 2011, 9, pp. 50-57.
[9] Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin, and Jean-Pierre Seifert : SMS-Based One-Time Passwords: Attacks and Defense. https://www.mulliner.org/collin/publications/mulliner_dimva2013.pdf