ENHANCING CLOUD COMPUTING SECURITY IN THE 21ST CENTURY USING ADVANCED WEB TECHNOLOGIES

By

MODESTA EZEMA*& NWAFOR CHRISTIAN IZUCHUKWU**

Abstract

Cloud computing is gradually replacing normal standalone computing. Almost all data processing today are done online with the assistance of cloud computing. Cloud computing offers numerous advantages to organizations such as cost savings, flexibility in capacity, time savings and effective use of computing resources, yet these focal points are most likely going to be undermined by the failure to ensure appropriate data security. There is urgent need to enhance data security since information kept online are prone to hacking especially in this digital age that cybercrimes is constantly on the increase. This project is aimed at enhancing cloud computing security using advanced web technologies. To achieve this, existing cloud computing security mechanism and technologies will be adopted. A model called CloudX was developed in this research work to handle web security. CloudX is a cloud-based security system that encrypts file paths, locks files and directories. Quick response code (QR) which is a form of authentication will be used to grant access to the cloud to curtail the breaches by unauthorized users. A user does not only need username and password before accessing his/her files. Identity management and authentication is a critical step towards securing the securing sensitive data in the cloud. Two different encryption algorithms; Attribute-based encryption (ABE), and advanced encryption standard (AES) will be utilized to build up the model to enhance these security flaws in the cloud. Each encryption algorithm has its pros and cons over the other in the role of data security. Several web development technologies were employed in the development of this software. They include: HTML5, CSS, PHP, JavaScript, AJAX and MySQL. Security and privacy being the two major factor that inhibits the growth of cloud computing were able to be enhanced through CloudX.

Key words: *CloudX, QR code, Encryption, Authentication.*

---

* Dr Ezema teaches in the Department of Computer Science, University of Nigeria Nsukka

**Department of Computer Science, University of Nigeria Nsukka

1. Introduction

Cloud Computing has turned out to be one of the most discussed technologies lately and has caught so many attentions due to its numerous advantages. These benefits include: cost savings, flexibility in capacity, time savings, manageability and effective use of computing resources. This innovation has taken enterprise search to another dimension and enables them to additionally lessen costs through improved usage, reduced administration and infrastructure cost. Cloud computing is not just useful to enterprises but an average person as well. It enables us to run software programs without installing them on our computer. Cloud computing enables us to store multimedia content through the internet and also to develop and test programs without essentially having server. Cloud computing according to [1] is a computing paradigm, where substantial pools of systems are connected in private or public networks, to give powerfully adaptable foundation to application information and file storage.

In spite of the numerous advantages that cloud computing can conceivably offer to organizations or individuals. Privacy and security remain major issue in the cloud and there have been no comprehensive solution to these issues. As cloud computing is dynamic and complex, the present security arrangement provided by cloud environment do not map well to its virtualized environments. The data security is provided to the data which is stored in the cloud by the use of various encryption algorithms. However, access revocation, user accountability, data processing speed issues are inherent in them. The simple passwords and One-time password (OTP) mostly used to authenticate cloud users are vulnerable to dictionary attacks and man-in-the-middle attack respectively. Access control issues due to the multi-tenancy nature of the cloud and easy accessibility of the cloud. Therefore, there is a pressing need to pay attention to several security issues in the cloud and introduce some security measures that can handle these problems.

This work focuses on developing a more efficient cloud computing security using already existing cloud computing security mechanism and technologies. A model called CloudX was developed in this research work to handle web security. CloudX is a cloud-based security system that encrypts file paths, locks files and directories. Quick Response code (QR) which is an authentication mechanism will be used to grant access to the cloud. Two different encryption algorithms; Attribute-based encryption (ABE), and advanced encryption standard (AES) were used to develop a model to

enhance this security flaws in the cloud. This model is aimed at curtailing breaches by external unauthorized users through the use of QR code authentication. This work does not cover developing a new cloud platform, hardware security issues in the cloud and legal issues in Cloud Computing. But it is intended to work with an existing cloud platform to enhance the privacy and the security of data in the cloud.

2. Cloud Computing Deployment Models

Cloud computing deployment can be classified into the following based on who owns the service and who uses the service. There four kinds of cloud computing deployment models according to NIST which are: private, public, community and hybrid [2]

3. Cloud Computing Service Models

According to NIST (2006), cloud computing offers three service model whose purpose is to provide easy, scalable access to computing resources and IT services. These services models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

4. Cloud Computing Threats

Threats refer to the hypothetical event wherein hackers utilize the vulnerabilities. Public cloud has made it feasible for associations to be considerably more productive, and to incorporate new innovations substantially more rapidly. Be that as it may, with every one of the advantages that public cloud conveys to the table as to highlights and usefulness, there are concerns when we consider the security of public cloud information and the availability of public cloud information when it exists in another person's data center. While there are numerous security worries in the cloud, [3] recognized that Cloud Security Alliance (CSA) has listed some of the dangers identified with the cloud out of which data breaches was identified as the highest security issue that needs tending to.

5. Literature Review

In the work by [4], where they we have analysed five different attribute-based encryption schemes like the ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, and HABE, MABE and compared their security, schemes and efficiency. Issues such as user revocation and scalability in key management become imperatively difficult towards accomplishing

cryptographically enforced data access control. When a user quits the system, the scheme cannot revoke his access right from the system directly because the attribute possibly belongs to multiple users. Therefore, there is need for a hybrid encryption algorithm and enhanced authentication method.

In the work by [5] "secure file storage on cloud using hybrid cryptography", a hybrid of 3DES, RC6 and AES was used to implement data security in the cloud. Data integrity, high security, low delay and confidentiality were achieved. But they used private key or symmetric cryptography which makes the data prone to attack when transmitting data from the client to the server.

RSA (Rivest-Shami-Adleman) and Attribute based encryption (ABE) for data security was proposed by [6]. This scheme ensured data security, secured data transmission and multiple accesses to authorized users. However, RSA has low data transmission speed compared to AES. Secondly, their model only encrypted data and data is not efficiently secure when the data paths and directories are unlocked. Lastly, an authentication system that will access control issues, user accountability and key revocation inherent in ABE was not considered in their model.

Using ABE with AES for sharing of personal health records in the cloud was proposed by [7]. ABE was used for efficient access control and AES was used to enhance the security of data in the server. Data was encrypted symmetrically with AES and the symmetric data key re-encrypted with ABE to allow for multiple access policy to the cloud. Emergency staff can equally access the data key in emergency situations. This model made secure and scalable sharing of personal health records in the cloud. But data cannot be efficiently secure when only the data is encrypted leaving the file path porous. The model also has poor authentication system and sharing of keys between the data owner and emergency staff is prone to attacks like man in the middle attack.

6. Authentication

Authentication confirms and ensures user identity. Conventionally this has been based on username-password and as result poses a security issues due to the fact that users choose simple and meaningful passwords which they can easily remember. These simple passwords are prone to dictionary attacks. One-time password (OTP) is another mechanism used to authenticate cloud users but vulnerable to man-in-the-middle attack [8].

One of the issues with these authentication mechanisms is that the right of access is controlled by an authentication system and once compromised, data can be hacked. To enhance access to the cloud, Quick Response code (QR) is used. QR code is a two-dimensional bar codes used to encode and decode the data between a text and image format.

7. Encryption Technologies

Ensuring the Security of data in the cloud must be provided for so that cloud users can willingly outsource sensitive data to the cloud for storage. There are many security concerns in the cloud which make it very difficult for one approach to prevent these threats in the cloud hence the use of multiple algorithms. Each encryption algorithm has its pros and cons and its distinct role to play in data security. Encryption is the process of encoding data in such that its confidentiality is protected from unauthorized users. There are many encryption algorithm that are provide excellent security features with high process speed, less memory space during implementation, etc. such as Advanced Encryption System (AES), Blowfish, RSA, etc.,. AES was used in the development of this system instead because:

Though AES and blowfish are furnishing amazing security highlights with high procedure speed, less memory space amid execution and numerous different points of interest, National Institute of Standards and Technology (NIST) expressed that AES is the stipulation of the encryption and decryption of electronic data [9].

On account of changing information type, for example, picture rather than content, it has been discovered that AES has favorable position over RC2, RC6, and Blowfish regarding time utilization [10]

8. Attribute Based Encryption (Abe)

Attribute based encryption which was introduced by Sahai and Waters in 2005 is broader category of identity based encryption (IBE) is a concept of functional encryption in the field of cryptography [4]. Attribute based encryption is a kind of algorithm in which the secrete key of a user and the ciphertext are dependent upon certain attribute such as position, place of residence and type of account. Decryption of a ciphertext is only possible here if the attributes of the client's key matches with the attributes of the ciphertext. Two major types of attribute-based encryption exist and they are Key-policy attribute based encryption (KP-ABE) and ciphertext-policy

attribute-based encryption (CP-ABE). One major advantage of ciphertext policy attribute-based encryption over Key-policy attribute based encryption is that it supports multiple of users of data at the same time provided the access policy defined tally with the user.

Some of the major issues in ABE are access revocation and user accountability. Access revocation simply means directly stopping a user from the system who quits the system given that each attribute possibly belongs to multiple users. User accountability is how to stop unauthorized user who was illegally given private key by authorized. The table below summarizes the advantages base on algorithms such as data confidentiality, scalability and secured access control.

Table: 1: Comparisons between CP-ABE and KP-ABE.

S/N	ALGORITHM	CP-ABE	(KP-ABE)
1	data confidentiality	yes	no
2	Scalability	yes	no
3	Secured access control	average	low

9. CloudX Encryption

This cloudX utilizes ABE and AES for encryption where necessary. The reason for this approach is to utilize the advantages of each technique and to make the cloud platform more secured. AES for example has robust security protocol but uses too simple algebraic structure. In this design, to encrypt file or directory paths, AES will be used. For data to be shared securely outside the platform then the ABE is applied.

The figure below shows the system architecture of the cloud computing security system. The mobile app QR code scanning does not need internet to work but when granting access, the internet is required.

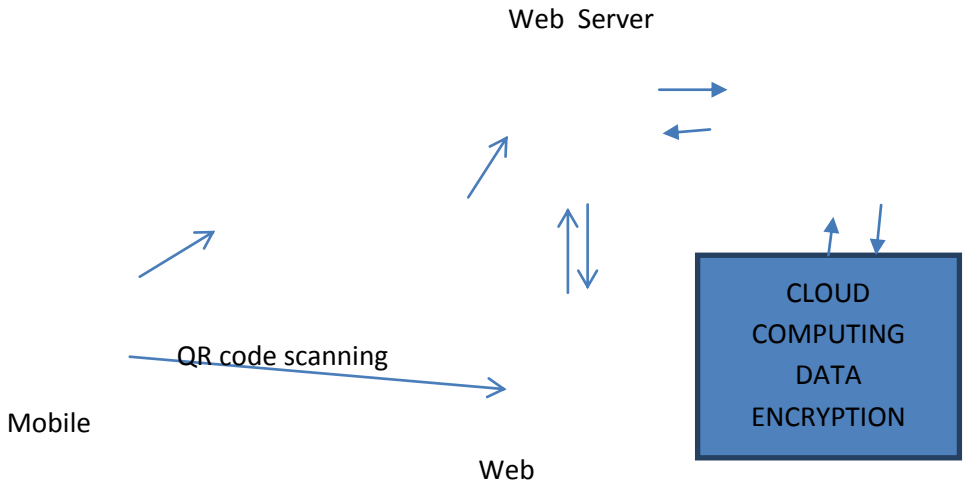

Fig. 1: Architecture of the proposed system

In the cloudX system itself, there are other encryptions developed based on base64 and base128. Both do not need keys for their encryption and decryption. The data encrypted using these methods can only be decrypted within the system, therefore no public or private key is need.

Writing and reading file

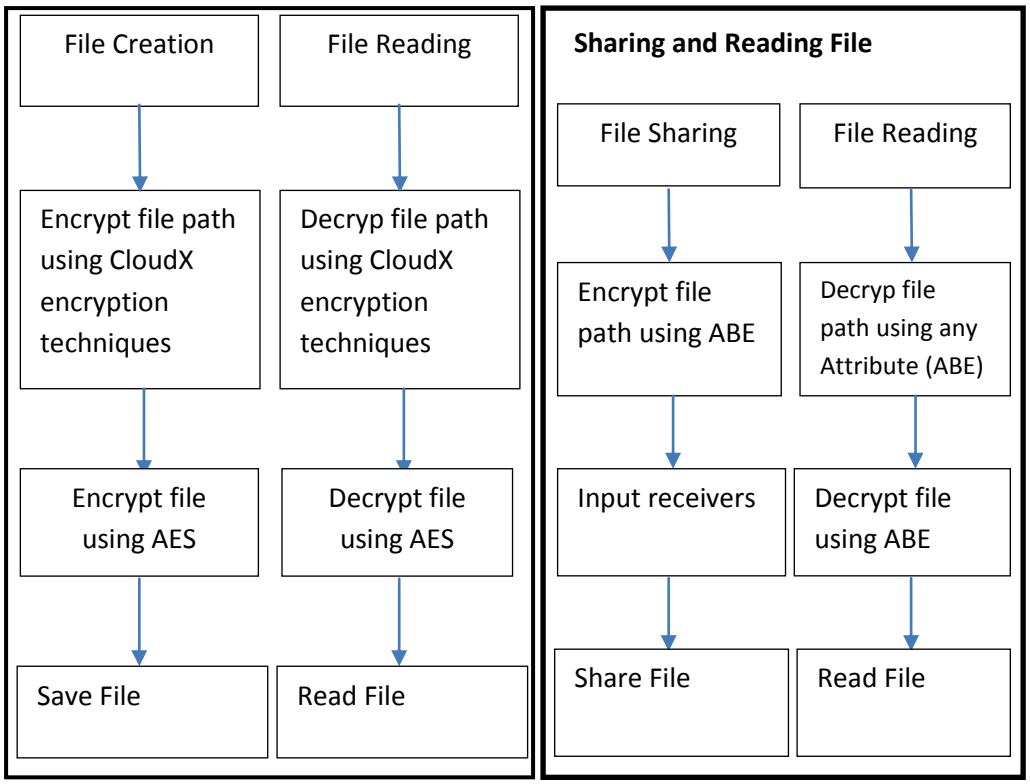

Fig. 2: Cloudx Encryption diagram

Figure 2 above shows the diagram of the CloudX encryption/decryption process. During writing of files, AES and CloudX new encryption technique are used. The file content is encrypted using AES and the password is derived from the username and session id of the person creating the file. That way the user must not memorize the file. The file name is encrypted using the CloudX Encryption which does not require password at all. Though the path can only decrypted within the system making using of CloudX security platform. If you copy the path elsewhere and decrypt it, you will not get the desired result.

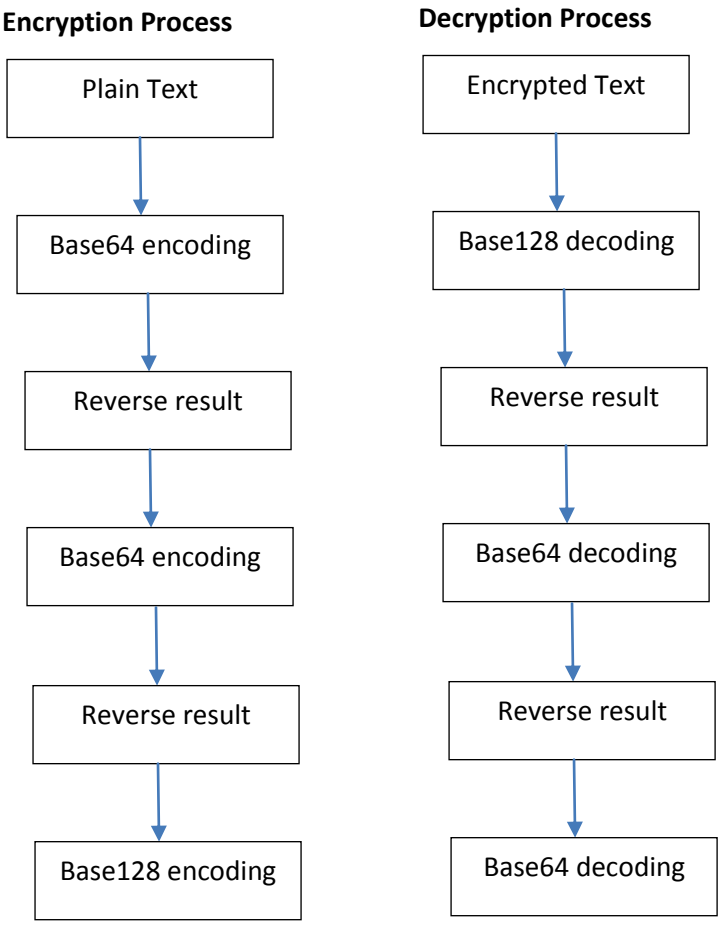

Fig..3 New CloudX Encryption based on base64 and base128

The encryption in fig. 3 is used in encrypting and decrypting directories and file paths and used in encrypting passwords. Before a password is used in AES, the password is encrypted first before it is used. This makes the password stronger and can never be guessed by anyone. The encryption method in fig. 4 can be used on file contents because the output is usually not a plain text.

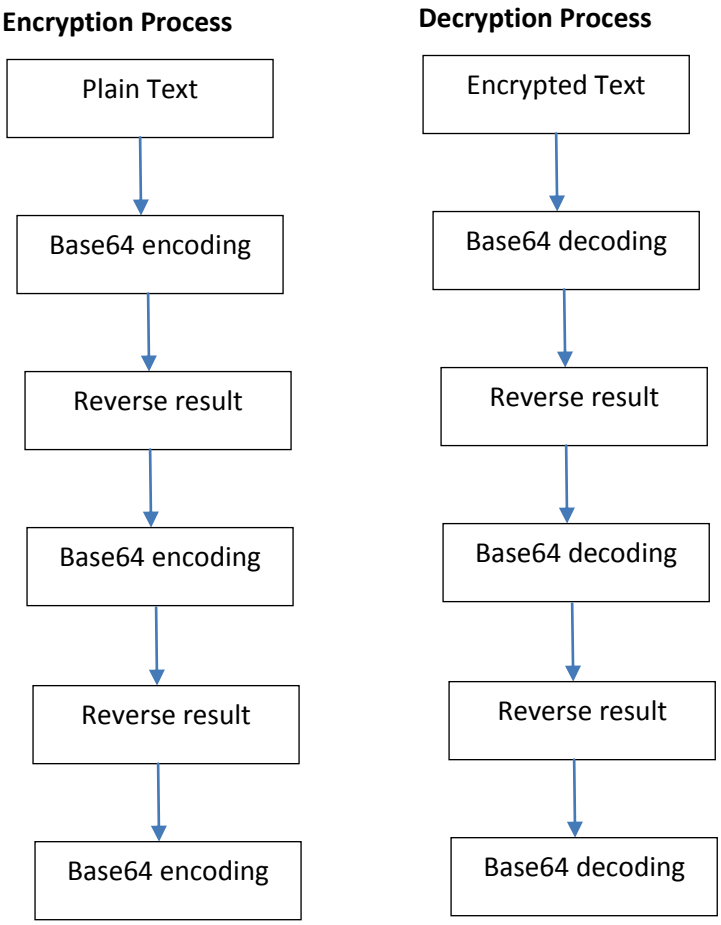

Fig. 4. New CloudX Encryption based on base64

10. Evaluation of the Proposed System in Comparison with the Existing Systems

Several works have focused on enhancing the security of cloud computing infrastructures yet there has been no comprehensive solution to the numerous security issues in the cloud. Some of the existing cloud computing services include but not limited to Amozon EC2, Google App Engine, Google Apps and Microsoft Office online.

Table: 2: Comparison between proposed system and Google Docs

S/N	PROPOSED SYSTEM	GOOGLE DOCS
1	Authenticates clients using username, password and QR code validation.	Authenticates clients using username and password mechanism.
2	Encrypts file paths, locks files and directories.	Encrypts only the data.
3	Re-encrypts encrypted password before use	Does not re-encrypt password.
4	Encrypts and decrypts shared files using users' access policies	Does not encrypt shared file

11. Detailed System Design

The proposed system aims at solving all the limitations in the existing system through username and password authentication, QR validation and cloudX encryption. CloudX which is a cloud-based security system that encrypts file paths, locks files and directories. The new system is broken into two parts: (i) web application and (ii) mobile application. The web application was designed first to demonstrate how to secure the login into any cloud computing platform using 2-factor authentication. The mobile app is basically QR code scanner that scans the QR code generated from the first phase of login through the web app. Both the mobile and web apps work hand in hand in securing system access.

The application was designed based on the existing system of authentication. In normal login, you supply your username and password and gain access to a system. In this one, you supply your username and password and you are authenticated. If the login is successful, a one-time password (OTP) is encoded into QR codes displayed as picture on the web page. The mobile app was designed to scanner the picture. The mobile app is configured to read the login of just one user. When the mobile app scans through the QR code, it reads the OTP and the username of the person. If the username matches the one in the mobile app then access is granted on the website. If the file is accessed without the security system then encrypted file will be shown. But when accessed with the authentication system, decrypted data will be shown.

In the file sharing, ABE was used because of the attribute based feature. When a file is to be shared within a company or organization,

anyone who has account within the system and also possesses one of the attributes of the company can decrypt the file. A security feature imposed in this area is that a file must be shared with you before you can decrypt it. If a file was not shared with you and you possess the attributes to decrypt such file, you still cannot decrypt it because it was never shared with you. The algorithm of the ABE remains the original one, nothing was added to it.

The main work done in this project is to smartly combine AES and ABE to add more security to cloud computing. A new encryption method was developed but not from scratch. It is a modification of base64 and base128. They do not require passwords. They were used in the area of encrypting and decrypting file paths and directories.

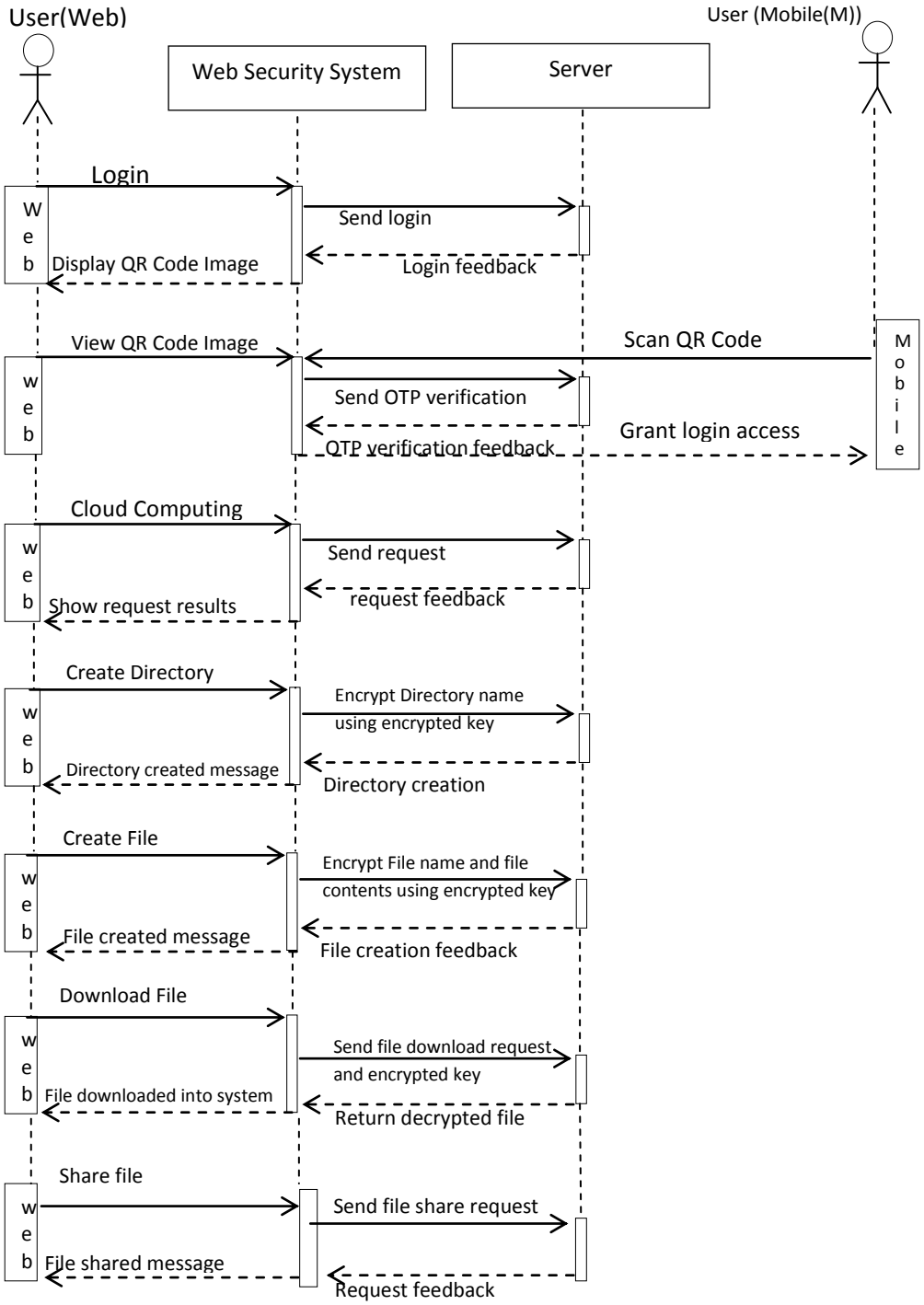

Fig. 5: Sequence diagram of the system

Fig. 5 above shows the sequence diagram of the system where there are 2 actors: the web user and the mobile user. The web actor is the one trying to login via web page. The mobile app actor is the one scanning the QR code for the authentication OTP.

12. Mobile Testing

The algorithm for the testing is shown below

1. Run app
2. App checks if there is existing system configuration
3. If configuration does not exist then

1.3.1 Open System configuration
1.3.2 Input cloud platform URL, username and password
1.3.3 Save the settings

2.1 Open Scan QR Code page
2.2 Tap the camera Icon on the bottom right of the app and
2.3 Scan the QR Code displayed on the web
3.1 If scan successful, send system access grant request to the server using the cloud platform URL that was stored in the phone.
3.2 End

The figure 6 to 9 below shows the mobile testing

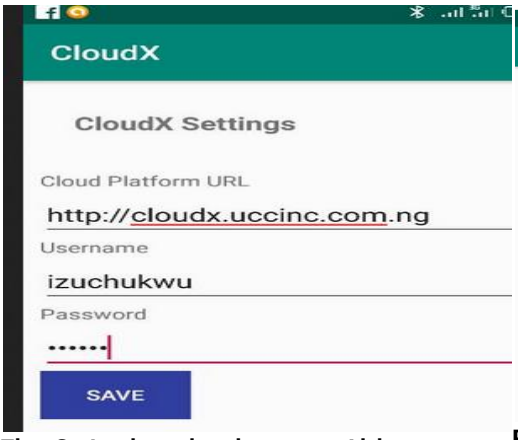

Fig. 6: Authenticating users' id.

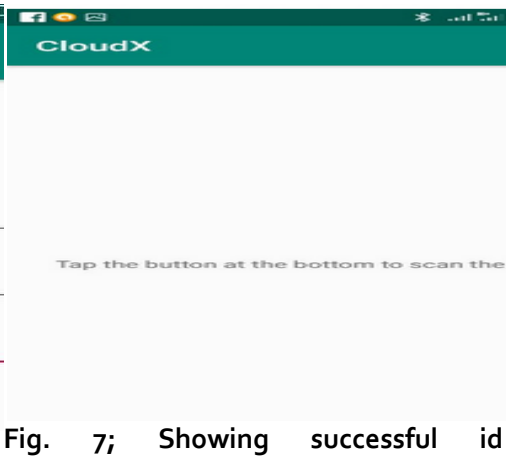

Fig. 7; Showing successful id authentication

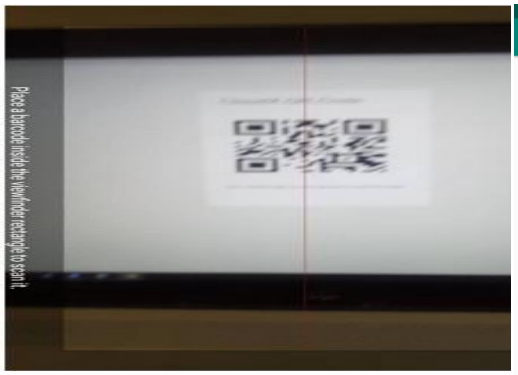

Fig. 8 showing mobile app scanning the web QR codes

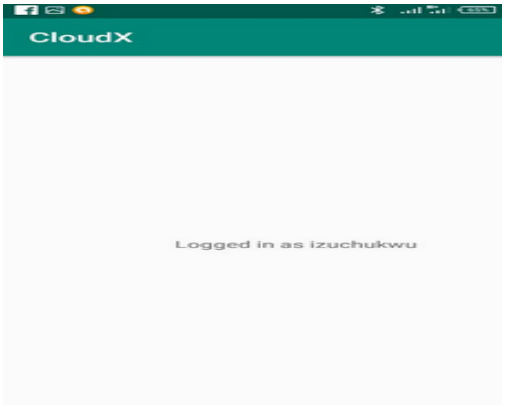

Fig. 9: showing successful login

13. Web App Testing

The web application was tested following the algorithm below:

1. Web login
2. Input username and password
3. If login successful go to 2.1 else back to 1.2

2.1 Generate QR Code Image
2.2 Scan QR Code with mobile app
2.3 If QR code authentication is successful go to 3.1 else back to 2.2
3.1 Grant access to cloud computing platform
3.2 Encrypt files and directory paths.
4.1 File Access
4.2 If file is accessed without the security system then show encrypted data else
4.3 show decrypted data

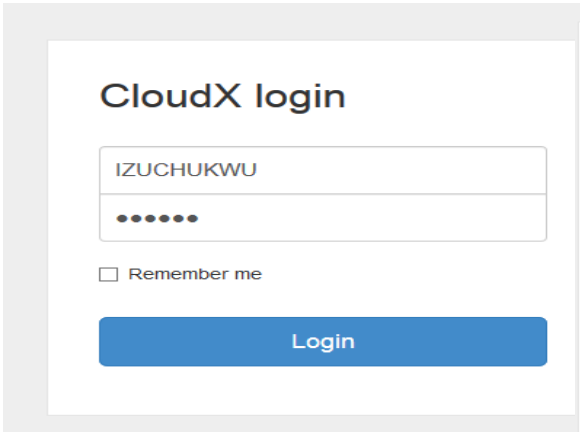

Fig. 10: the desktop app validating user id.

Fig. 11: showing cloudx scanning

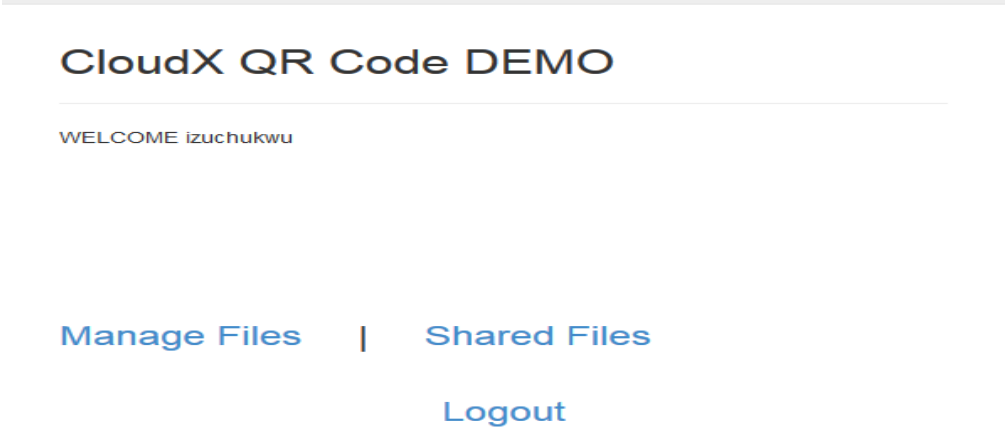

Fig 12: showing successful login

To test the encryption, login first and click manage file. Create folders and files and open the files directory in the CloudX package to see what is there. All the files and folders created are stored in **files** directory of CloudX. When you open the folder, what you will see is the encrypted folder's names and file's names. If you open the files you will see encrypted data. For the sake of testing, three folders were created and two files namely izu and encryption were created. The interface for created them is shown on fig. 13

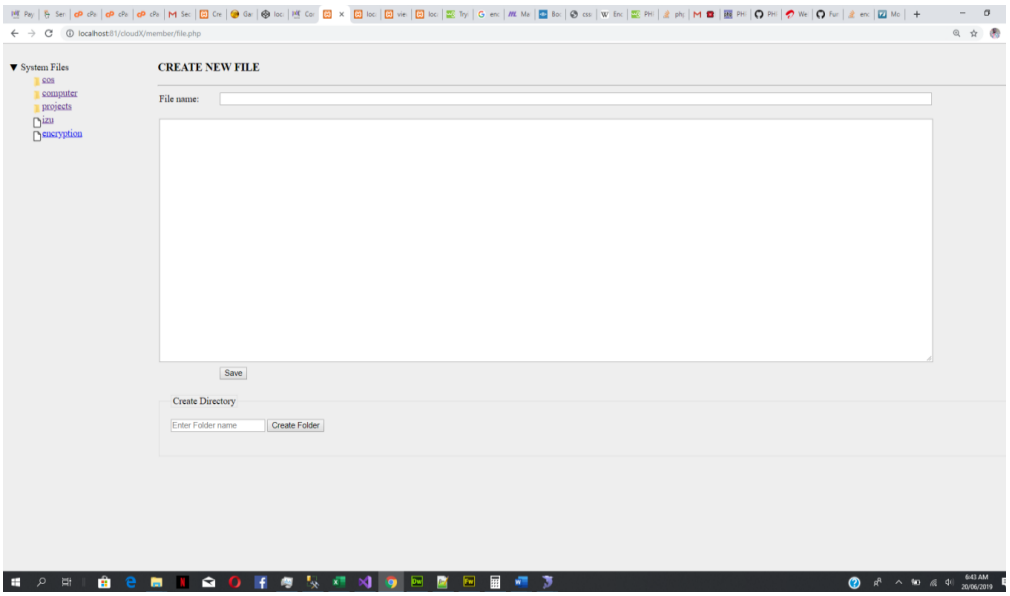

Fig. 13: File management page

To test the file share, login first and click manage file. Go to share file button and click on it and then click system files to show all the folders in the system with different files. When the file is selected as shown in fig. 14 below, a column for the email address of the file recipient shown but if left empty, file will be shared to all the members of the organizations whose email address are stored in the system.

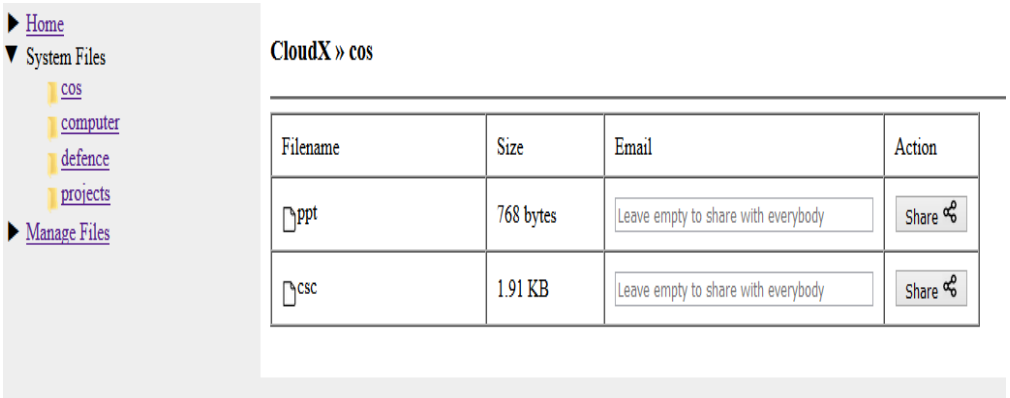

Fig.14: file share to all members of the organizations

The recipient of such file goes to his email account to download such file but the file can only be downloaded if the recipient put correctly the decryption

as shown in fig. 15 below. This data as stated earlier was encrypted at the process of sharing based on the users attribute and can as well be decrypted if the access policies match.

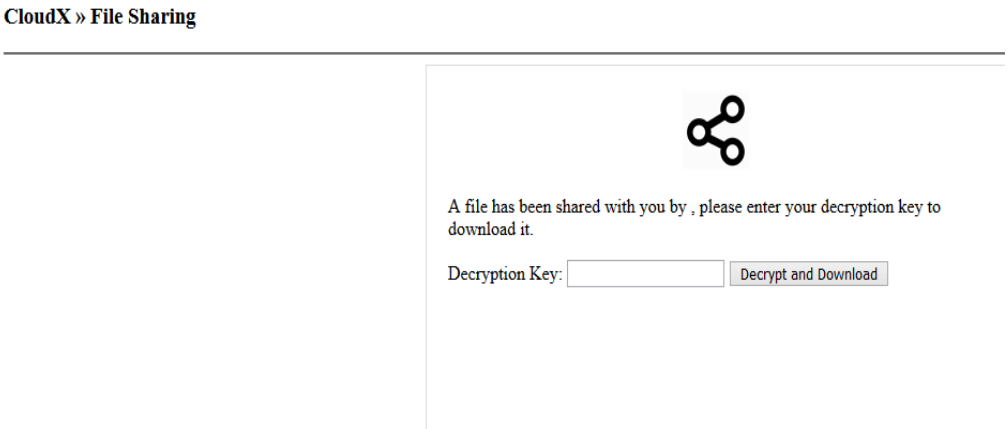

Fig. 15: Shared file requesting for decryption key before it is can be downloaded

14. Conclusion

Security and privacy have been the major issue militating against the wide adoption of cloud computing. Research has shown that there no one comprehensive solution to these challenges in the cloud. However this project employed the already existing security mechanisms to develop more enhanced security architecture for the cloud. The system makes of use username and password authentication and QR code validation to grant users access to the cloud. That is a two-level authentication which makes the authentication system more secured. With the information presented in this dissertation, it is pertinent to recommend that the system should be deplored to cloud computing platforms. Individuals, organizations and healthcare industries are assured of the security of their outsourced data in the cloud.

More research should be focused on this work towards a hybrid of advanced encryption standard, attribute based encryption and fully homomorphic encryption with a low computation overhead. This would allow for secure search on encrypted data and computation on encrypted data and protect data integrity

15. References

[1] T.-Harris, "CLOUD COMPUTING – An Overview" [available: https://www.thbs.com/downloads/Cloud-Computing-Overview]pdf. [Accessed: 03/05/2018]

[2] DIALOGIC "Introduction to Cloud Computing" [Available; https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp].pdf [Accessed: 03/05/2018]

[3] K. Walker "Cloud security alliance (CSA). The treacherous 12: cloud computing top threats in 2016". 2016. Feb. 29https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/.

[4] R.. Lakshmi, R. Laavanya, M. Meenakshi and C. Gana Dhas "Analysis of Attribute Based Encryption Schemes" International Journal of Computer Science and Engineering Communications. ISSN: 2347–8586 Vol.3, Issue 3, 2015, Page.1076-1081

[5] A. Poduval et al "Secure file Storage on Cloud Using Hybrid Cryptography", International Journal of Computer Science and Engineering. Vol-7, Issue-1, Jan 2019.

[6] S. Hemalatha and R. Manickachezian "Security strength of RSA and Attribute Based Encryption for data security in cloud computing", International Journl of Innovative Research in Computer Science and Engineering. Vol. issue 9, September 2014

[7] B. Varsha and P. Suryateja "Using Attribute Base Encryption with Advanced Encryption Standard for secure and scalable sharing of personal health records in cloud". International Journal of Computer Science and Information Technologies Vol 5(5), 6395-6399. 2014 *[Accessed: 05/02/2019]*

[8] S. Bharadwaj "A study on qr code based public cloud data protection**"** Indian Journal of Computer Science and Engineering (IJCSE) ISSN : 0976-5166 Vol. 8 No. 3 Jun-Jul 2017

[9] P. Prince "A comparison of symmetric key algorithms DES, AES, Blowfish, RC4, RC6: a survey" Vol. 6 No. 05 May 2015

[10] E. Abdul, H. Kader, and M. Hadhoud. " Performance Evaluation of Symmetric Encryption Algorithms." IJCSNS International Journal of Computer Science and Network Security 8.12 (2008): 280-286.