International Journal of Trend in Scientific Research and Development, Volume 1(4), ISSN: 2456-6470
www.ijtsrd.com

Enhancement of Cloud Resources Security Using Verification Code

Madamidola Olugbenga

Department of Computer Science, The Federal University of Technology Akure, Ondo State Nigeria

Abimbola Tolulope

Department of Computer Science and Information technology, Bowen University, Iwo Osun State, Nigeria

Afolabi Gboyega

Department of Computer Science, The Federal University of Technology Akure, Ondo State Nigeria

ABSTRACT

Cloud computing security or simply cloud security refers to a broad set of policies, technologies and controls deployed to protect data application and the associated infrastructure of cloud computing. The aim of this work was to address and minimize the problem of unauthorized access to information and applications on the cloud with the use of verification code, this project is targeted towards protecting user's privacy and also preserving the integrity of their information and also the integrity of the Cloud Environment. The work was accomplished with the creation of user registration phase, user login and authentication phase and password change and verification code change phase, this was accomplished with the use of certain tools such as PHP, JQuery, MySQL Database, Ajax, HTML5 and CSS. A system using an integrated development environment was developed and security was installed in the system using htdocs and htaccess which helps to prevent against IP address filtering, URL address switching and removes the channel of SQL injection.

Keywords: Cloud Computing, Security, Verification Code, Cloud Resources, Integrity

1. INTRODUCTION

The term "cloud" is used as a representation of the internet and other communications system as well as an abstraction of the underlying infrastructures involved. What we now refer to as cloud computing is the result of an evolution of the widespread adoption of virtualization, service-oriented architecture, autonomic and utility computing. Details such as the location of infrastructure or component devices are unknown to most end-users, who no longer need to thoroughly understand or control the technology infrastructure that supports their computing activities. The brief evolution of cloud computing are: Grid Computing, Utility Computing, SaaS and Cloud computing.

The National institute of Standards and Technology defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e. g networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction **(Mell, 2009).** Cloud computing security

or simply cloud security is an evolving sub-domain of computer security, network security and more broadly information security. It refers to a broad set of policies, technologies and controls deployed to protect data application and the associated infrastructure of cloud computing. Most of the time, cloud computing is concerned with accessing online software applications, data storage and processing power. In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. However, as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment is **(Kuyoro *et.al*, 2011).**

Despite the much attention given to the cloud, customers are still reluctant to deploy their business in the cloud due to security issues. Cloud computing has unique attributes that requires risk assessment in areas such as data integrity, recovery and privacy and an evaluation of legal issues in areas such as regulatory compliance and auditing. Organizations use the cloud in a variety of different service models (SAAS - Software as a Service, PAAS- Platform as a Service and IAAS- Infrastructure as a Service.) and deployment models (Private, Public and Hybrid), there are a number of security issues and concerns associated with cloud computing and these issues fall into two broad categories: security issues faced by cloud providers (organizations providing SAAS, PAAS or IAAS via the cloud) and security issues faced by their customers (cloud users). Other major security issues faced in cloud computing include governance and enterprise risk management, local and electronic discovery, portability and interoperability, application security e. t. c. This project intends to take a look at the major security issue of application and information security and proffer a solution to it.

2. RELATED WORKS

Akshay et.al, (2013), worked on FaceRecognition System (FRS) on Cloud Computing for User Authentication, in their work theyproposed the use of a biometric technique called "FACE RECOGNITION".Face recognition was based on both the shape and location of the eyes, eyebrows, nose, lips, and chin or on the overall analysis of the face image that represent a face as a number of recognized faces. Face Recognition System (FRS) enables only authorized users to access data from cloud server, the limitation of this work is that it will not work in the absence of camera also face features might become different depending on lighting conditions, time of the day

ALRassan and AlShaher (2013), worked on Securing Mobile Cloud Using Finger print authentication in their work they proposed an authentication mechanism using fingerprint recognition to secure access in mobile cloud. The proposed solution was employed to use a fingerprint recognition system to obtain the fingertip image through the mobile phone camera, the aim was to convert fingertip image obtained by mobile phone camera to fingerprint image and extract ridge structure from it to be as similar as possible with the ridge structure gained from fingerprint sensor. Of

course, mobile camera can't convert the image to be like the output image obtained and processed by using fingerprint sensor, but at least this process aim to export an acceptable output. The process will be achieved by the user initially, in the enrolment presenting his/her fingertip to the mobile phone camera to obtain a fingerprint sample and extracted features by pre-processing the sample.

Tirthani and Ganesan, (2013), worked on proposed a system for removing security threats in cloud architecture by using two encrypting techniques the Diffie Hellmann Key Exchange and Elliptic Curve Cryptography. To deploy these two methods, they proposed a new architecture which can be used to design a cloud system for better security and reliability on the cloud servers at the same time maintaining the data integrity from user point of view.

Wazed et.al (2012), worked on File Encryption and Distributed Server Based Cloud Computing Security Architecture, they proposed a model that uses the following security algorithms: RSA algorithm for secured communication, AES for Secured file encryption,MD5 hashing for cover the tables from user and One time password for authentication. In this model, all the users irrespective of new or existing member, needs to pass through a secured channel which is connected to the main system computer and RSA encryption algorithm was used for making the communication safe. In the proposed security model one time password was used for authenticating the user. The password was also used to keep the user account secure and secret from the unauthorized user. But the user defined password can be compromised. To overcome this difficulty one time password is used in the proposed security model.The limitation of this system is that if the user's email is hacked then the password is revealed.

3. METHODOLOGY

Security has become a major issue and with the invention of new and modern technologies, more security issues have come up. Cloud computing as a recent development also has a lot of security issues and threat to be careful about. This work looks at the security issue of unauthorized access to applications and information on the cloud and PHP, Java scripts and My SQL database are the major tools that was utilized.

A. Creation of a User Registration Phase:

Whenever a cloud user wants to access cloud resources and applications, the user has to first register on the cloud, the steps for the registration are as follows:

(i) The user provides his/her full name.

(ii) The user provides a valid email address, a username and password to the authentication server

(iii)Authentication server checks the email address against the availability of that email address. i.e the email address should not match or repeat with an existing user's email address.

(iv) The user answers a security question of their choice to serve as a backup in case of a future security breach.

(v) Once the email address has been checked, the authentication server sends a unique

verification code to the user's email in form of a link and which the user has to supply the answer to the security questions before the code is displayed.

(vi) Once the user supplies the correct answers and it has been checked by the server then the verification code is displayed for the user to see.

(vii) The user can then enter the verification code during log in for further authentication.

B. ***Creation of a User Login and Authentication Phase***: Whenever the user wants to access resources such as applications and information on the cloud, he/she has to login onto the cloud, the steps for login are as follows:

(i) User enters the registered username and password

(ii) The authentication server checks the username and password entered by the user with the one that has been provided at the time of registration

(iii) The user is then taken to another page and asked to enter the verification code that was sent to his/her mail for further authentication

(iv) The authentication server matches the verification code entered by the user with the one sent to the user's mail.

(v) After the verification code has been matched, the user will be authenticated and then gets access to applications and information

C. Creation of a Password Change and Verification Code Change Phase:

This phase is created in order to accommodate the need for change in password or verification code of the user due to security reasons. This phase will be created as follows:

(i) The user provides his/her email address.

(ii) The user supplies the correct answer to the security question he/she has previously answered in the registration phase.

(iii) The authentication server checks the supplied answer with the registered email address and answer supplied during registration.

(iv) After the email address and supplied answer have been matched, a new password is supplied by the user to the authentication server.

(v) A new verification code is generated and sent to the user's mail.

(vi) The password is updated successfully.

Other tools utilized in the work are PHP, jQuery, My SQL Database, Ajax, HTML5, CSS (Cascading Style Sheet), MTP (Simple Mail Transfer Protocol),

3.1 System Architecture

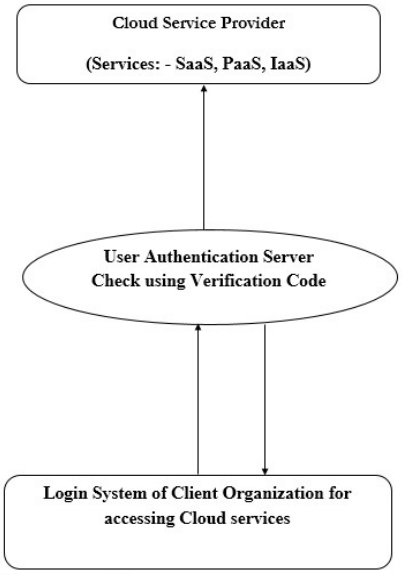

Figure3. 1: System Architecture

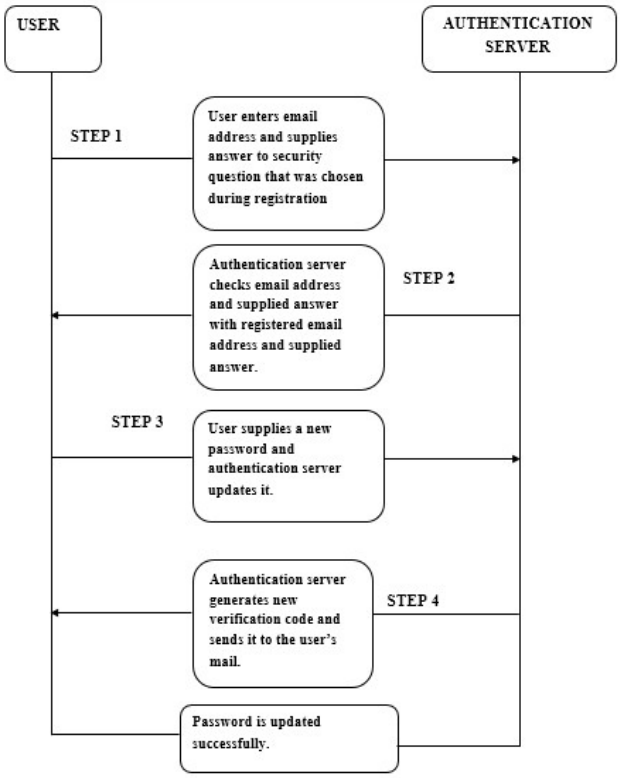

Figure 3.3 User login and authentication phase

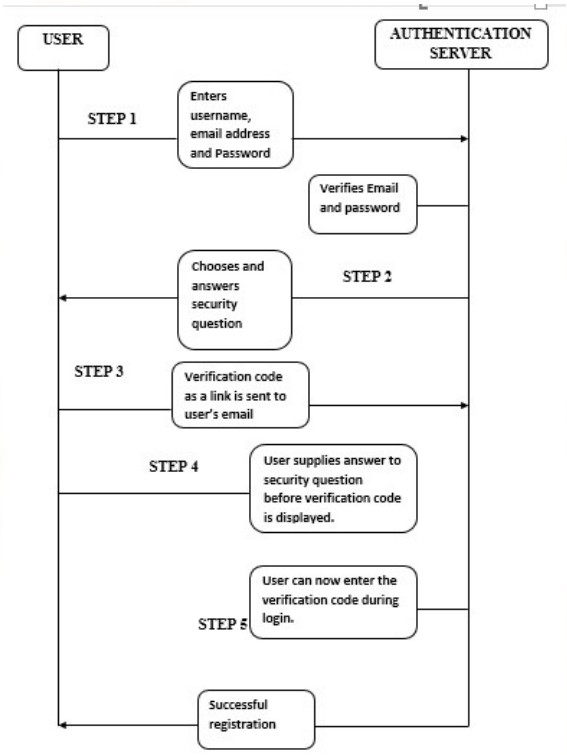

Figure3. 2: User registration phase

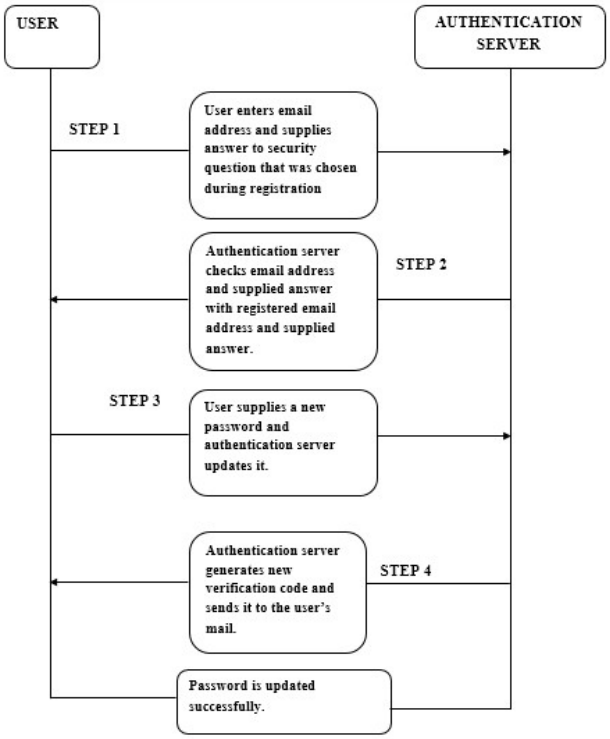

Figure3.4: Password change phase.

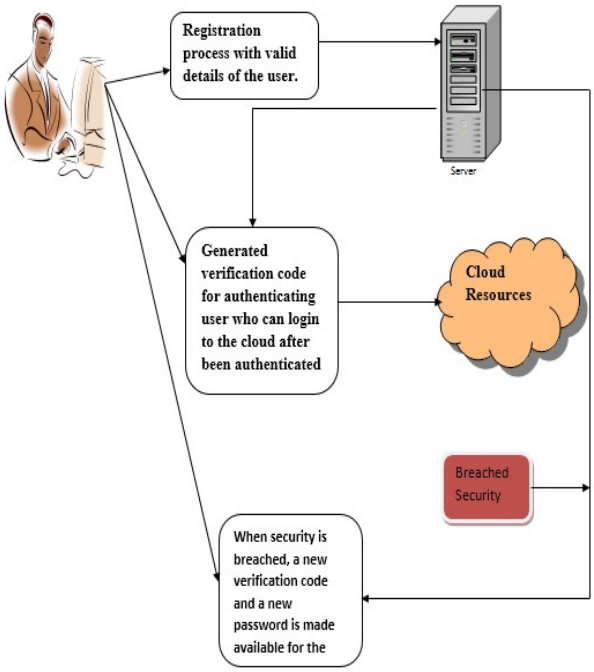

Figure 3.5: A use case diagram representing the proposed system.

4. IMPLEMENTATION

In order to carry out the implementation of this work, a system using an integrated development environment was developed. The system works by using a verification code which is a random set of numbers that is generated by the system to authenticate users. PHP programming language enhanced with other tools such as Ajax, htdocs, htaccess, SMTP server e. t. c was used in the development of the system. PHP was used in the development of the system as a result of the need to simulate web cloud security and security was installed in the development using htdocs and htaccess which help to prevent against IP address filtering, URL address switching and removes the channel of SQL injection. Also the application also provides security by retracting URL typographical errors to error 404 (not found).

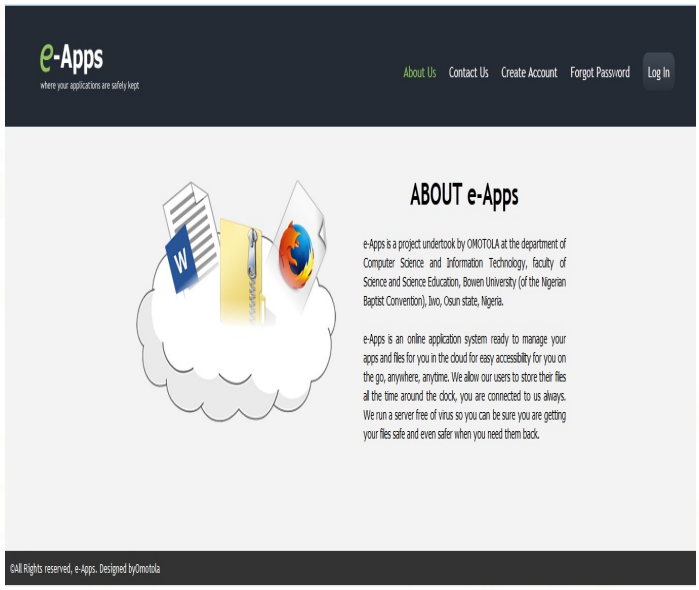

Figure 4.1: About interface

This interface that gives a brief introduction to users on what the application is all about and the services it offers and how to use the application.

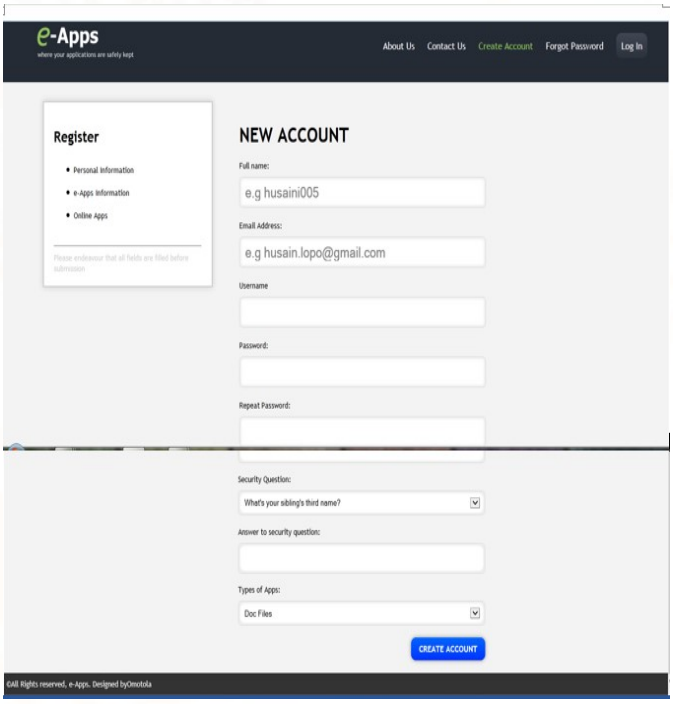

Figure 4.2: User registration

The above figure shows the user registration interface which consists of the steps to take and the fields to fill before becoming a registered user, after which the unique verification code of the user is generated and sent to the registered user's email.

Figure 4.3: First level of authentication

The Figure above shows the interface for which registered users who want to log in have to enter their user name and personal password as the first level of authentication.

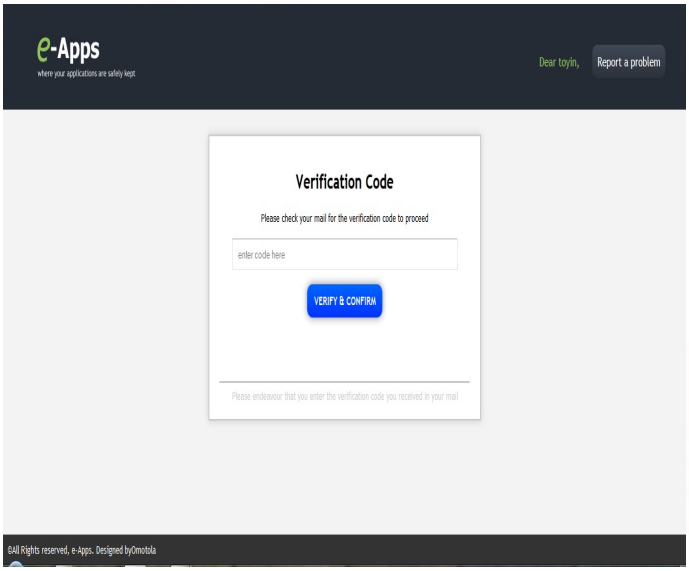

Figure 4.4: Second level of authentication

The above shows the interface for the second level of authentication that is presented to the user in which the user is to enter the verification code that was sent to their registered email address.

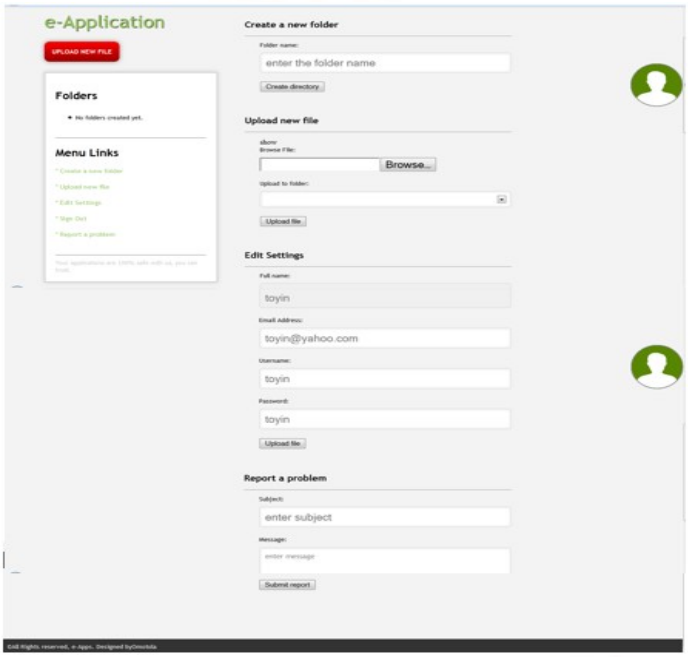

Figure 4.6: Upload page

The above shows the upload interface which is where an authenticated user is taken to and he/she can now manage their stored information and also add more information that they want to upload. Users can log out by clicking on the image by the right hand side.

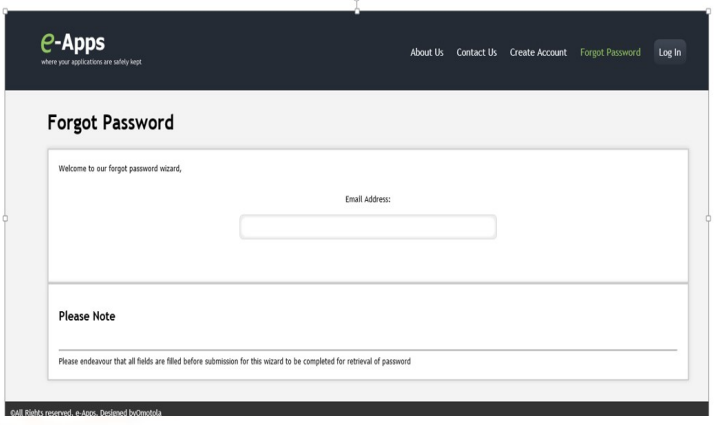

Figure 4.7: Password change step 1

The above shows the first step a user has to go through before they can change to a new password in case of anything happening to their previous password which is for the user to enter their registered email address.

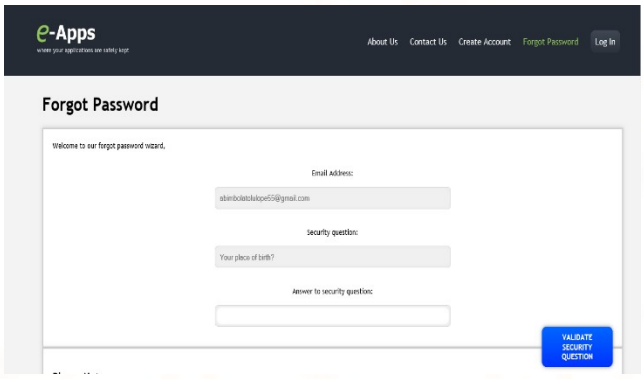

Figure 4.8: Password change step 2

The above shows the next step for users who want to change their passwords. After the user enters the right email address the user is taken to this page where he/she supplies the answer to the security question answered during registration and the authentication server validates the answer. If a wrong email is entered in step one the user is not going to be taken to step two.

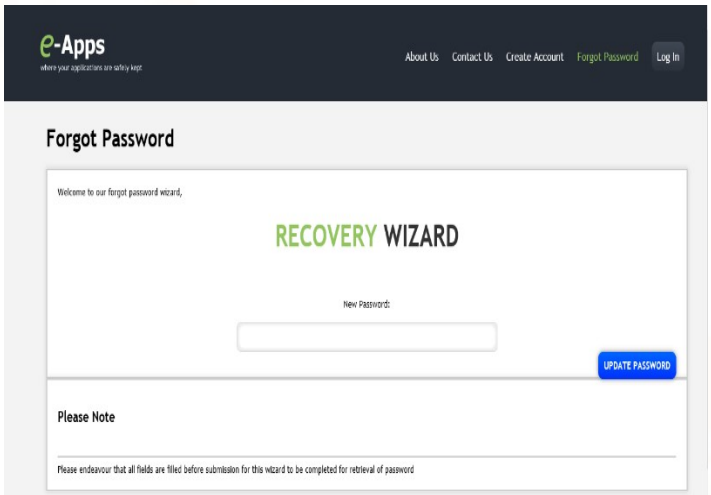

Figure 4.9: Password change step 3

The aboveshows the final step for users who want to change their password which is for users to enter the new password they would like to be using and the server updates the user's password after which a new verification code is supplied for the user.

CONCLUSION

The focus this work was to implement an application that addresses and provide a possible solution to the problem of unauthorized access to applications and information in the cloud environment, this was achieved by implementing a well secured system called **e-apps** for authenticating users and securing files and applications that are stored in the cloud. **E-apps** provides a secure environment with the use of a user-id, user's personal password and a uniquely generated verification code that is sent to the user's email, the verification code sent to the user's mail is protected with the security question answered during registration. The implementation shows that this work can support any type of file and application and that it works when user is connected to the internet. The architecture and the steps involved in the creation of the application has been discussed.The results are promising and demonstrates the suitability of e-apps for addressing the problem of unauthorized access to files and applications that have been uploaded and stored on the cloud.

REFERENCES

[1] Alvi, F.A. Choudar, B.S. Jaferry, N. and Pathan, E. (2012). *A review on cloud computing security issues and challenges.*

[2] ALRassan, I. and AlShahe, H. (2013). Securing Mobile Cloud Using Finger Print Authentication. *International Journal of Network Security & Its Applications (IJNSA), 5*(6).

[3] Akshay, A. and Pawar, P. (2013). Face Recognition System (FRS) on Cloud Computing for User Authentication. *International Journal of Soft Computing and Engineering (IJSCE), 3*(4).

[4] Atayero, A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. *Journal of Emerging Trends in Computing and Information Science, 2*(10).

[5] Bartholomew, D. (2009). *Cloud rains opportunities for software developers*. Retrieved from http://careerresources.dice.comcon/articles/tent/entry/cloud_rains_opportunities for software.

[6] Bogatin, D. (2006). *Cloud computing and advertising go hand in hand*. Retrieved from http://www.zdnet.com/blog/micro-markets/google-ceos-new paradigm cloud-computing-and-advertising-go-hand-in hand/369.

[7] Cloud security alliance (2009). *Security best practices for cloud computing*.

[8] Desisto, R.P. Plummer, D.C. and Smith, D.M. (2008). *Tutorial for understanding the relationship between cloud computing and SaaS*. Stamford, CT: Gartner.

[9] Demarest, G. and Wang, R. (2010). *Oracle cloud computing*. Oracle White Paper.

[10] Eze Castle Integration (2014). *The history of cloud computing*.

[11] Gartner. (2008). *Seven cloud-computing risks*. Infoworld.

[12] Gentry, C. (2009). *Fully homomorphic encryption using ideal lattices*. ACM.

[13] Gujar, V. Sapkal, S. and Korade, V. (2013). STEP-2 User Authentication for Cloud Computing. *International Journal of Engineering and Innovative Technology (IJEIT) Volume, 2*(10).

[14] Hamlen, K. Kantarcioglu, M. Khan, L. and Thuraisingham, B. (2010). Security Issues for Cloud
[15] Computing.*International Journal of Information Security and Privacy, 4*(2), 39- 51.

[16] Huth, A. and Cebula, J. (2011). *The Basics of Cloud Computing*. US-CERT.

[17] Kaufman L.M (2009). "*Data security in the world of cloud computing*". IEEE Security & Privacy: 61–64.

[18] Kim Kwang Raymond Choo (2010). *Cloud computing: Challenges and future directions*.

[19] Koblitz, N. (1987). *Elliptic curve cryptosystems*. Mathematics of Computation 48, 203-209.

[20] Kuyoro S.O, Ibikunle F. and Awodele O. (2011). Cloud Computing Security Issues andChallenges.*International Journal of Computer Networks (IJCN), 3*(5).

[21] Lori Macvittie (2013). *Application security in the cloud is still cloudy*. Retrieved from http://devcentral.f5.com/articles/application-security-in-the-cloud-is-still-cloudy.

[22] Marchany, R. (2010). *Cloud Computing Security Issues*. Virginia Tech.

[23] Mell, P. and Grance, T. (2009). *The NIST definition of cloud computing*. Retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[24] Miller. V (1985). *Use of elliptic curves in cryptography*. CRYPTO 85.

[25] Munir and Palaniappan (2013). *Framework For Secure Cloud Computing*.

[26] Rivest, R. Adleman, L. and Dertouzos, M. (1978). *On data banks and privacy homomorphisms. In Foundations of Secure Computation*. pp. 169–180.

[27] Siani Pearson (2012). *Privacy, Security and Trust in Cloud Computing*. UK: HP Laboratories.

Subashini, S. and Kavith, V. (2010). *A survey on security issues in service delivery models of cloud computing*. J Network Comput Appl.

[28] Srinavasin and Madhan (2012). *State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment*.

[29]Sun, T. and Wang, X. (2013). Research of Data Security Model in Cloud Computing Platformfor SMEs. *International Journal of Security and Its Applications, 7(6), pp.97-108*.

[30] Tirhatni, N. and Ganesan, R. (2013). *Data Security In Cloud Architecture Based On Dilfie Hellman And Elliptical Curve Cryptography*.

[31]Thomas, G. Jose, P and Afsar, P. (2009). *Cloud computing security using encryption Technique.*

[32] Tory Harris (2014). *Cloud Computing - an overview*.

[33]VMwarewhite paper (2009). *Securing the cloud: A review of cloud computing, securityimplication and best practices*. USA: VMware, Inc.

[34] Wazed, K. Kar, T. Hoque, S. and Hashem, M. (2012). A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture. *International Journal of Advanced Computer Science and Applications (IJACSA),3(10).*

[35] Web Security Journal. (2009). *Swamp computing aka cloud computing*.

[36]Ziyad, S and Rehman, S. (2014). Critical Review ofAuthentication Mechanisms in CloudComputing. *International Journal of Computer Science Issues (IJCSI), 11*(3).