An Approach for Amplifying the Cloud Environment Security

Sumita Lamba
Department of Computer Science Engineering
Uttarakhand Technical University
Dehradun, Uttarakhand, India

Ajay Kumar
Department of Computer Science Engineering
DIT University
Dehradun, Uttarakhand, India

ABSTRACT
Many people consider "CLOUD" as the buzzword for internet and utility computing, but this innovative paradigm of computing is imparting new designs of computing platforms. Being a pool of ample of resources, cloud computing allows the access to the users through internet. It has greatly emerged as a computing standard where the computing infrastructure is served as internet services and has made an effective change in the way of computation and services for its customers. There is a need of such a cloud which doesn't compromise with any of the following: Integrity, reliability, flexibility and elasticity, and ensure security for storing and transmitting the data. In cloud, the user's data is stored tenuously and they have no control over it, so security issues have always been dilemma here. In this paper, we have proposed a new practical approach to secure the cloud environment for data storage by blending authentication with hashing and encryption algorithm. We aim to develop a secure cloud environment which ensures the standards of user and data authentication, data confidentiality and user oriented access control.

Keywords
User and data authentication, data confidentiality, user based access control.

1. INTRODUCTION
Although cloud computing is not a new term to the world these days, but still it will be appropriate to understand a little about it before moving further. It is this generation development based on internet technology. It gives innovative ways of providing, deploying and managing the computing resources to the users like CPUs, storage systems and databases. Many leading vendors like Google, Amazon, IBM, Microsoft and salesforce.com offer their own cloud infrastructure for these services. Cloud computing eliminated the daily computing problems of hardware, software and availability of resources faced by customers. Cloud brings the servers and lots and lots of storage space together in just an instance on the command of its customer. The main concern in cloud computing is privacy, security and integrity of end user's data from unauthorised entity. From the data security perspective, which has always been an important aspect of quality of service, Cloud Computing indistinguishably poses new challenging security threats for number of reasons. Firstly, we could not directly adopt the traditional cryptographic primitives for the purpose of data security protection as users lose control over the data under cloud and are unaware of the location of their data stored. Therefore, without any explicit knowledge of data, verification of correct data storage in cloud must be conducted. Secondly, Cloud Computing is not just a third party data warehouse. When the data is stored in the cloud, it is customarily updated by the users, which may include uploading, downloading, modification, appending, etc. Hence it is paramount importance to ensure storage correctness under dynamic data update. However, this dynamic feature makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, data center empower the deployment of Cloud which runs in a virtualized, simultaneous and distributed manner. Users' data is stored redundantly at multiple physical locations which lead to reduce the threats on data integrity. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world.

Some necessary definitions we should know are: (i) Users- Who has data to be stored and interact with CSP (Cloud Service Provider) [2] to manage their data in cloud. (ii) CSP- has major resources and expertise in building and managing distributed cloud storage servers. A CSP offers storage or software services to users available via internet. (iii) Storage server- where the user's password, data and other information is stored.

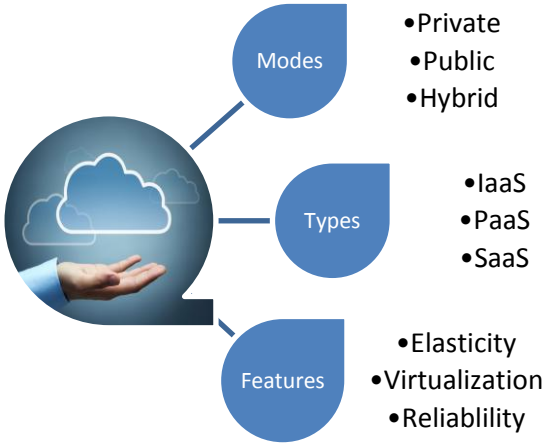

Fig. 1 Cloud Computing Overview

We have introduced a new approach for secure data storage by securing the cloud environment using cryptographic techniques, providing authentication, confidentiality and user

oriented access control. A web application specific Cloud Computing model is designed which is based on the principle of resource sharing using Oracle Server 10g and J2EE application programming software.

The rest of the paper is structured as follows: Next section (2) contains related work. Section 3 frames proposed secure cloud environment. Finally Section 4 accounts conclusion and future work.

2. RELATED WORK

Rohit Bhadauria et al. [1] have elaborated and analyzed the numerous unresolved issues threatening the cloud computing adoption and diffusion affecting the various stake-holders associated with it like application level security including DoS attack, session hijacking, cookie poisoning [1], etc.

Edward S David et al. [2] has explained the promises and challenges of cloud computing, which gives some benefits of implementing cloud computing and some challenges encountered doing so. He has also explained the different models and types of cloud.

S.Sabarish et al. [4] gave an approach that enables CSP's to provide a highly secured environment. Three security mechanisms: Digital signature, Message authentication and Iris scanning are used to provide security to private cloud as well as public cloud environment.

Mr. Prashant Rewagad et al. [7] have used three ways protection scheme. Firstly Diffie Hellman algorithm is used to generate keys for key exchange step. Then digital signature is used for authentication, thereafter AES encryption algorithm is used to encrypt or decrypt user's data file.

Pradeep Bhosale et al. [8] gave a model for data storage where at client side user select the parameters reactively between CIA and before actual storing the data in cloud a digital signature is created using MD 5 Algorithm and then RSA Encryption algorithm is applied then it stored on cloud.

3. PROPOSED APPROACH

We have proposed a web application in which users can store and transit the data securely. This web application named "Impregnable Store", allows user to access the data from anywhere at any time. Users can upload, download or view the data (either it is file, document, videos or photos) easily. The proposed web application is HTTPS enabled and provides a secure environment to store and safeguards all the data. The proposed cloud environment ensures authentication, data confidentiality, user oriented access control and availability.

At the time of registration users enter some details like name, email address, password, secret code, date of birth etc. All the entered fields are checked for the integrity such as password should case sensitive containing case-sensitive characters (64) using digits 0-9 and letters A-F, Users must be 18 and above age and email address must be valid for future reference. The email address should be unique i.e. no two users can have same email id.

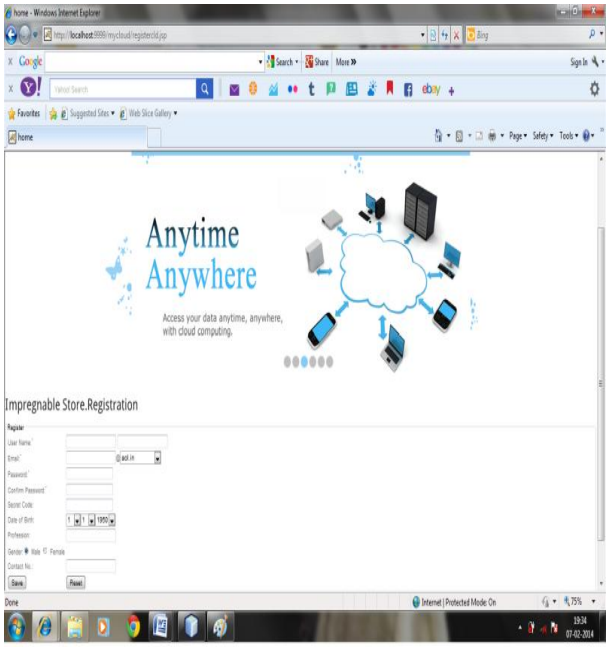

Fig. 2 Impregnable Store registration page

Once all the fields are verified by the cloud storage server, a mail is sent to the users from where they can get their Unique ID and password (plain text) for further communication.

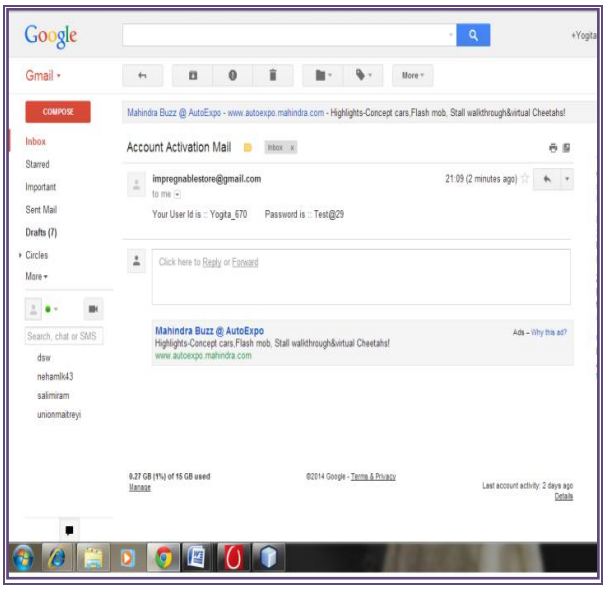

Fig. 3 Mail sent by the web application to a user

The password entered by the verified user is stored in hashed form in the cloud storage server. The cryptographic function we have used to hash the password is SHA-3 with salting. Salting is a random string which is concatenated with the password entered by the users. The salted password is hashed using SHA-3.It uses a sponge construction and generates a 512 bit length hash from the salted password. Then the salt and calculated hash is stored in the server database. Salting makes dictionary attack more difficult and by adding hashing to the salt makes SQL injection attack nearly impossible.

3.1 Hash generation algorithm:

1. Select the password entered by the user.

2. Generate a long random string; concatenate it with the password selected.

3. SHA-3 hashing is applied over the message concatenated.

4. Output: New hash of the password.

Example: Password entered: - Test@29

Salt String: - JH7P0IY21EA5HQUMJTEBNF7Y1HCR6SKYWGT7

Generated Hash: - 0ABF2E426E4550D58F75A718E2D081B00028A20CF5139895679496ABEFD4147DECBN8N5F7Y9E240A7284F2CEDTU&D4G6JF7J8JT9BG074O97SR5

After successful registration, users can login into the cloud using the Unique ID, their email address and password.

At the time of login, Users have to enter the captcha code. We have used captcha at the time of login for authentication purpose. "Captcha: Completely Automated Public Turing test to tell Computers and Humans Apart[10] " is a sort of challenge-response test used to determine whether the user is human or not. It is used to prevent the brute force attacks.

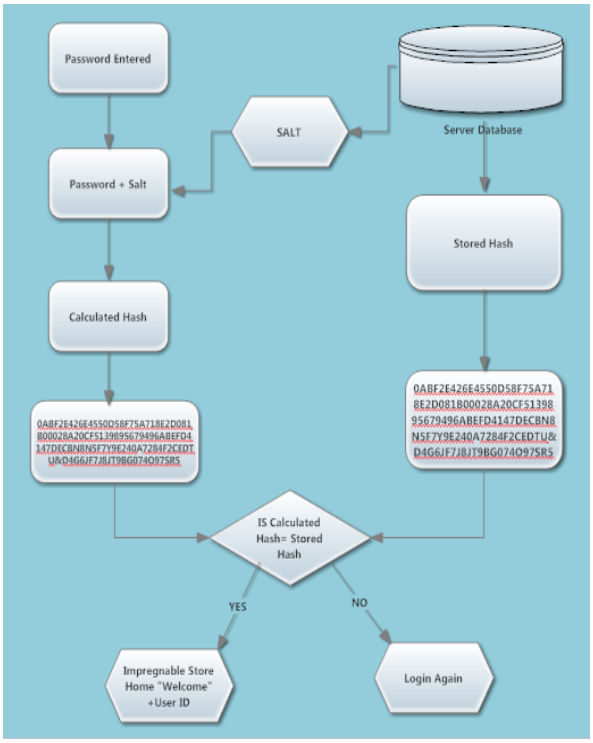

Fig. 4: Hash comparison (Salting the password)

3.2 Captcha algorithm:

1. A background image is created containing different patterns (horizontal/vertical lines, rectangles and parallelogram) of random size, colors and position.

2. 8 random characters from set [a-z A-Z 0-9] are selected.

3. Each character is placed over background image (created in step 1) by rotating each character with random angle between -5° to 5°.

4. Final Captcha image is generated.

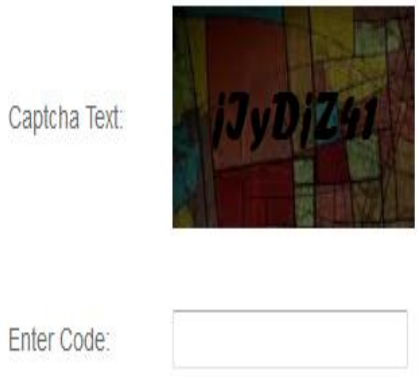

Fig 5 Generated Captcha Image

The fields (Unique ID, email ID, password and captcha code) are then verified at the back end database server. The hash of the password entered by the user is calculated and is compared with the hash stored at the database. To do so, the salt stored at the database server is extracted and concatenated with the password. Now the hash of the salted password is calculated. If both the hashes come out to be same and all entries are valid, user is grant access and directed to home page otherwise access is denied.

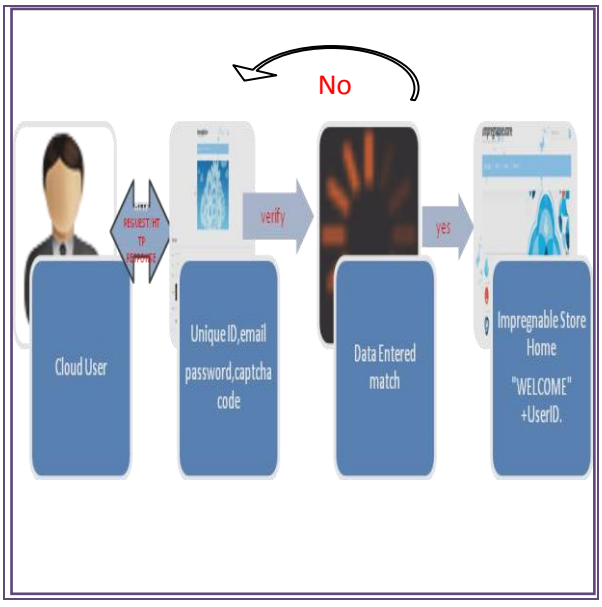

Fig. 6 User login process flow

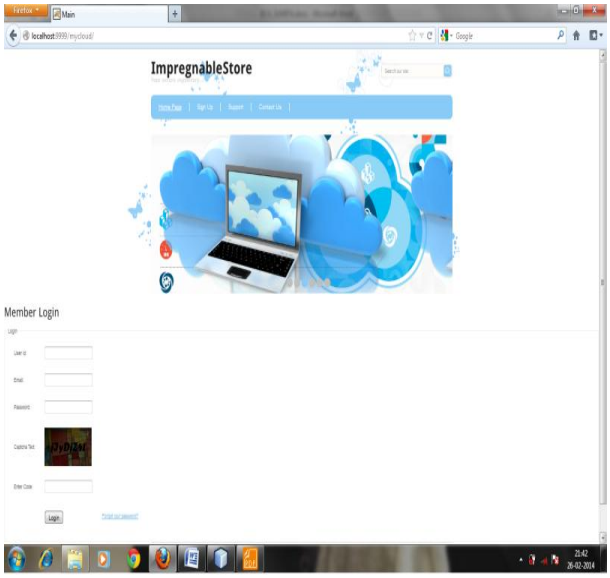

Fig. 7 Login page

Once the users get into the cloud, they can perform various functions like storing the data (documents, files, photos, videos, etc.) at storage server, downloading the data from the server, viewing the data, editing the stored data, managing their circles or their profiles.

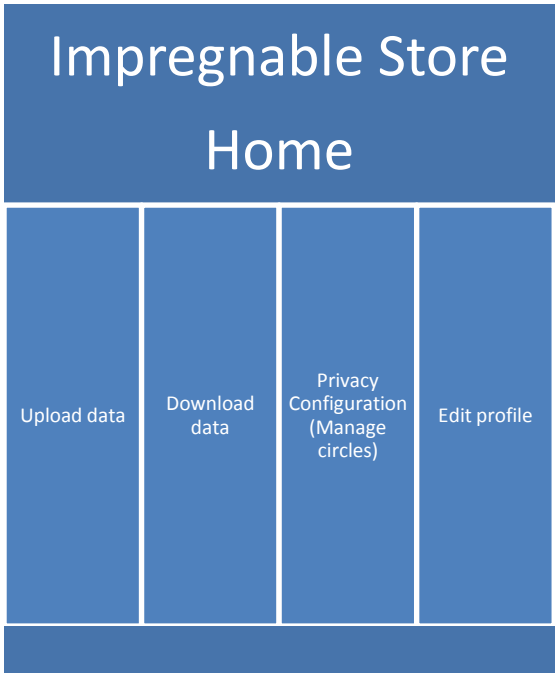

Fig. 8: Impregnable Store services

The files are encrypted before storing at storage server. The algorithm used for encryption/decryption is AES. We have followed a user oriented data handling approach. Users have full control over their data and over the people viewing it. Users have the right to allow only those users from the cloud whom they want their data to be accessed. Users can choose single person or group of people from the cloud who can access their data after decryption. User can manage their circles where they can select the other users from the cloud or can delete the selected users who have the shared secret key and will be able to decrypt the data. By doing so, they become sure that no one authorized is accessing their data. They can also manage their profiles where they can make changes in their password, secret code, email address, etc.

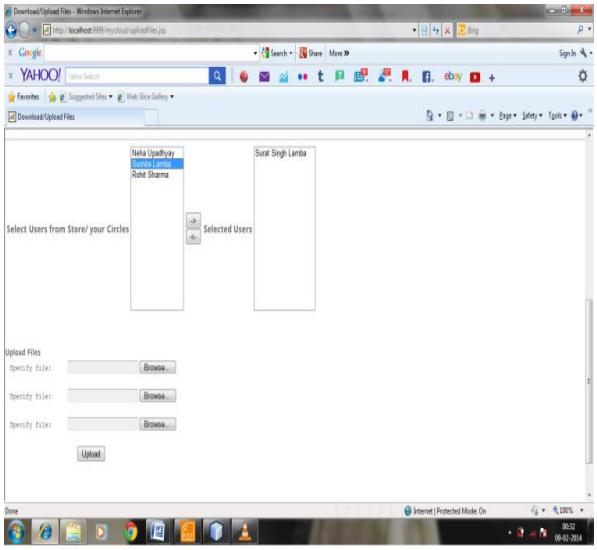

Fig. 9 Upload files Page

On the Upload files page, user first selects the other users from cloud who can download the uploaded file. Multiple file upload option is given so that if user wants, he can upload more than one file at a time. The selected user will be able to decrypt and download the files. This provides the full control to the user over their data. The user can delete the file he has uploaded at any point of time.

On the Download files Page, user views the data only for which he has been selected and can download after decrypting it using the secret key.

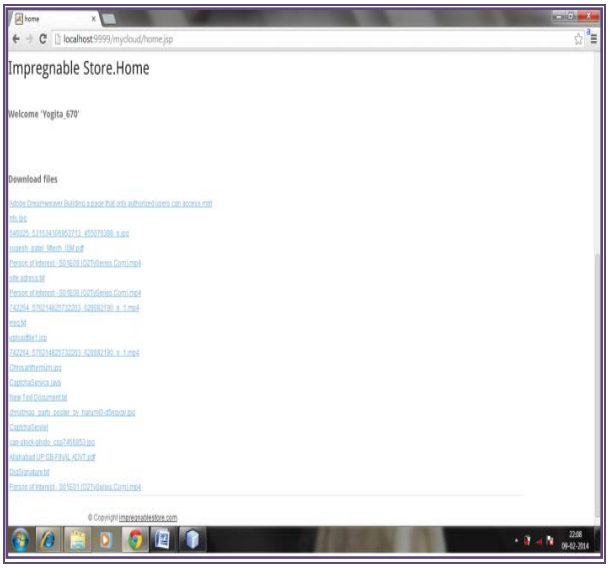

Fig. 10 Download files page

It is very important to keep the data confidential as we don't want an intruder to access our data. The password confidentiality and integrity is maintained by SHA-3 hash technique with salting method. Captcha is used to distinguish between human and machine. Encryption and decryption is done using AES algorithm which provides confidentiality of data stored in the cloud.

4. CONCLUSION AND FUTURE SCOPE

We have shown that the proposed work is a practical approach to secure the cloud environment for data storage. This is done by blending authentication technique with hashing and encryption algorithm. The purpose of the paper is to develop such a cloud environment which is not only secure but also fulfils the following standards: authentication, data confidentiality and user oriented access control. Authentication is delivered by Captcha, Password and its storage become more secure using SHA-3 and AES maintains the data confidentiality. In future, we will explore the penetration power of the proposed application and test the cloud environment.

5. REFERENCES

[1] Rohit Bhadauria. "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques" International Journal of Computer Applications (0975 – 888) Volume 47– No.18, June 2012.

[2] Edward S David. Promises and Challenges of Cloud Computing. International Journal of Computer Applications (0975 – 8887) International Conference on Current Trends in Advanced Computing "ICCTAC-2013".

[3] Anup Mathew. "Survey Paper on Security & Privacy Issues in Cloud Storage Systems", EECE 571B, Term survey paper, April 2012.

[4] S.Sabarish, G.Basha & A.Padmashree, Tirupur M. King, B. Zhu, and S. Tang. "Secured cloud environment with a new approach", "Optimal path planning," *Mobile Robots*, vol. 8, no. 2, pp. 520-531, March 2001.

[5] Priyanka V. Mogre, Girish Agarwal, Pragati Patil ."Data Security and its techniques in Cloud Storage – A Review" International Journal of Engineering Research and Technology Vol. 1 (02), 2012, ISSN 2278 – 0181.

[6] Sanjoli Singla, Jasmeet Singh. Cloud Data Security using Authentication and Encryption Technique International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323 Volume 2, Issue 7, July 2013.

[7] Mr. Prashant Rewagad, Ms.Yogita Pawar. "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing" International Conference on Communication Systems and Network Technologies,2013.

[8] Pradeep Bhosale, Priyanka Deshmukh, Girish Dimbar and Ashwini Deshpande. Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012.

[9] Ankit Kumar Sahu. "Java Web Deployment in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 75– No.15, August 2013.