INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 07 ISSUE: 04 | APRIL - 2023 IMPACT FACTOR: 8.176 ISSN: 2582-3930

CLOUDMOAP: Multilayer Security by Online Encryption and Auditing Process in Cloud

Dr. Anthony Raj
Associate Professor
Computer Science and Engineering
RGIT

Fathima Khanum
Computer Science and Engineering
RGIT

Dixitha R S
Computer Science and Engineering
RGIT

Kousalya N
Computer Science and Engineering
RGIT

Sarala Chaithra
Computer Science and Engineering
RGIT

Abstract— Each image is divided into squares by this module, from which the user selects one to serve as the pass-square. A 7 x 11 grid is used to split a picture. The password space increases as the discretized image size decreases. Yet, an excessively focused division might make it harder to operate the user interface on palm-sized mobile devices and cause problems with object detection. As 60 pixels is the optimal size for precisely selecting certain items on touch displays, a division was set at 60-pixel intervals in both the horizontal and vertical axes in our solution.

Index Terms— Online Encryption, Hash Code, Shoulder Surfing, Randomized Image Selection, Cipher Key, Data Security.

1 INTRODUCTION

In the realm of computers, cloud computing is a relatively new business model.Self-service on demand, extensive network access, resource pooling, fast flexibility, and quantifiable service are the five main characteristics of the cloud model. NIST lists three different categories of service models. The cloud provides four deployment models: hybrid, private, public and community as well as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS. Due to its adaptable and secure services, cloud storage is becoming more and more required and practical. As more people utilise cloud data services, they are becoming more concerned about various hazards. The security services offered by the Cloud Service Provider may appear insufficient to protect user data in such a situation. Mechanisms for user-level security aid in enhancing security and users' confidence in using cloud data services. In our system, it serves as user authentication through the use of online data encryption mechanisms and shoulder surfacing. It is utilised at the user level, encrypting data prior to transferring it to cloud storage. Internet data encryption speeds up the procedure and helps users save time. We have employed a robust data security approach that makes use of the user's data identifying credential in order to give improved data access control. Data identifying credentials, which make up a portion of the encryption key, are transferred to the cloud to be used in the data decryption procedure. In order to increase security, the decryption procedure is carried out at the user level using the help pin that will be produced when a file is uploaded. This solution uses more sophisticated and secure technology of containers to store data in the cloud while also freeing the user from important storage and administrative tasks

2.1 MOTIVATION

Use of cloud computing services has significantly increased today. In order to reach the end user, businesses of all sizes rely on cloud services. Because of the affordable security services offered by the cloud, even lone users are transferring from traditional storage to it. The hazards for cloud customers have escalated due to the services' widespread adoption. Seven common dangers to the cloud computing environment have been identified by Gartner. But, a lot has changed since then. As the number of people utilising cloud services has constantly expanded, new security threats, dangers, and issues have emerged. The study "Treacherous 12," which details the top 12 cloud computing vulnerabilities enterprises will face in 2016, was just issued by the Cloud Security Association (CSA) in January 2016. As new issues arise, new solutions must be developed in order to address them. Together with using the security services offered by Cloud Service Providers (CSPs), users should have their own security measures in place to protect themselves from the numerous risky circumstances that might arise in a cloud environment.

.2.2 PROBLEM DEFINITION

The "weakest link" in the authentication chain is thought to be human behaviour, such as selecting poor passwords and entering passwords insecurely. The shoulder surfacing attack and data privacy should be taken into consideration when it comes to user authentication because data security techniques like encryption have failed to prevent data theft attempts. In order to protect data in the cloud, offensive decoy technology should be used.

2.3 LITERATURE SURVEY

The usage of alphanumeric usernames and passwords is the most used computer authentication technique. It has been established that this approach has serious disadvantages. Users frequently choose passwords that are simple to guess, for instance. On the other side, a password that is difficult to guess is frequently also difficult to remember. Several researchers have created authentication techniques that employ images as passwords to solve this issue. This study performs a thorough analysis of the graphical password approaches currently in use. It divides these methods into two groups: those based on recollection and those based on recognition. We go over the benefits and drawbacks of each approach while also outlining potential future lines of inquiry. Apart from that, it attempts to address two crucial queries: "Are graphical passwords as safe as text-based passwords?" and "What are the main design and implementation difficulties for graphical passwords?" This poll will be useful for information security researchers and professionals seeking for alternatives to text-based authentication solutions.

In one technique, the user chooses the encrypted data from his or her local storage to upload. After the online services are activated, the user uploads the encrypted data to the cloud. The user can simultaneously upload data and perform encryption in the second manner. The first technique involves the user in an unnecessary laborious process, but the second way allows the user to save time. The second approach will be used by our suggested system. When the authentication procedure is complete, the user chooses which file or data to upload. In this instance, knowledge factor authentication will be applied. The chosen file is simultaneously uploaded to the cloud and encrypted. It uses this key to encrypt data. There is no register kept in order to record these keys. Typically, the user keeps the key registry on local storage, which raises the danger of insider assaults. In contrast, our solution will do away with the requirement for key storage, negating any chance of keys becoming lost or exposed and, eventually, personal data.

2.4 EXISTING SYSTEM

In a cloud computing environment, data can be uploaded in an encrypted manner and then downloaded after being decrypted using a user authentication request that will be issued when it is requested to download. The use of cloud data services is made more secure and user-friendly by user-level security mechanisms. Data may be uploaded to the cloud in one of two ways by the user. Data may be uploaded to the cloud in one of two ways by the user.

- Offline encryption
- Online encryption

The user chooses the files to upload from their local storage and encrypts them in the first technique. The user then launches the online tools and sends the encrypted data to the cloud. The user can simultaneously upload data and perform encryption in the second manner. The first technique involves the user in an unnecessary laborious process, but the second way allows the user to save time. The second approach was employed by our system. With our system, containers are utilised to store data on the cloud, enhancing its security. The system's overall flow is seen in Fig. 2. When the authentication procedure is complete, the user chooses which file or data to upload. In this case, knowledge factor authentication is applied. The chosen file is encrypted and uploaded to the cloud at the same time. To obtain the cypher key, the user's data identification credential (UDIC) token is obtained from the user and paired with salt. It uses this key to encrypt data. The next sections provide a thorough explanation of key creation and the encryption process. To keep track of these keys, there is no register kept. Key registries are often held locally by the user, which raises the danger of insider attacks. While there is no chance of keys being lost or exposed in our system since we have done away with the necessity for key storage.

2.5 DISADVANTAGES OF EXISTING SYSTEM

- Decoy technology is unable to provide robust security in terms of data privacy.
- Shoulder surfacing attacks make it exceedingly difficult to authenticate users.
- Just one video recording of the authentication procedure is made.
- Several videos document the full authenticating procedure.

2.6 GENERAL FLOW OF SYSTEM

The user must log in using their authenticated account while retrieving data. The user chooses the file to be downloaded after successful login. The One Time Password (OTP) is sent to the user's permitted email address when CSP receives this request for data retrieval. The data decryption procedure uses this OTP. The user's site is where the downloaded encrypted file is stored, and this is also where the decryption procedure is carried out. The user is only permitted to decrypt the file and view its contents after providing the proper OTP. OTP therefore offers data security.

2.7 PROPOSED SYSTEM

With a user authentication and user identification procedure, the cloud computing environment is more secure. In order to increase security, encryption is used while uploading files, and degradation as well as user authentication are used when receiving files.

• Offers a security plan for online encryption that ensures data privacy.

• To create a system that does not require key management or storage for cloud data storage, making the system more secure.

• To put in place a four-layer security approach that increases confidence in cloud service providers.

• Data integrity testing at the user level capable of providing great data privacy protection when it comes to decoy technology.

• The adoption of Randomized Picture Selection Algorithm to prevent the shoulder surfacing attack makes user authentication more safe.

2.8 ADVANTAGES OF PROPOSED SYSTEM

- When it comes to decoy technology, it is capable of ensuring strong security in terms of data privacy.
- User authentication is more secure because it uses age verification to defend against shoulder surfacing attacks like Naked eyes.
- Video records the entire authentication process multiple times.
- Honey bot technology is used to keep the data secure while downloading.

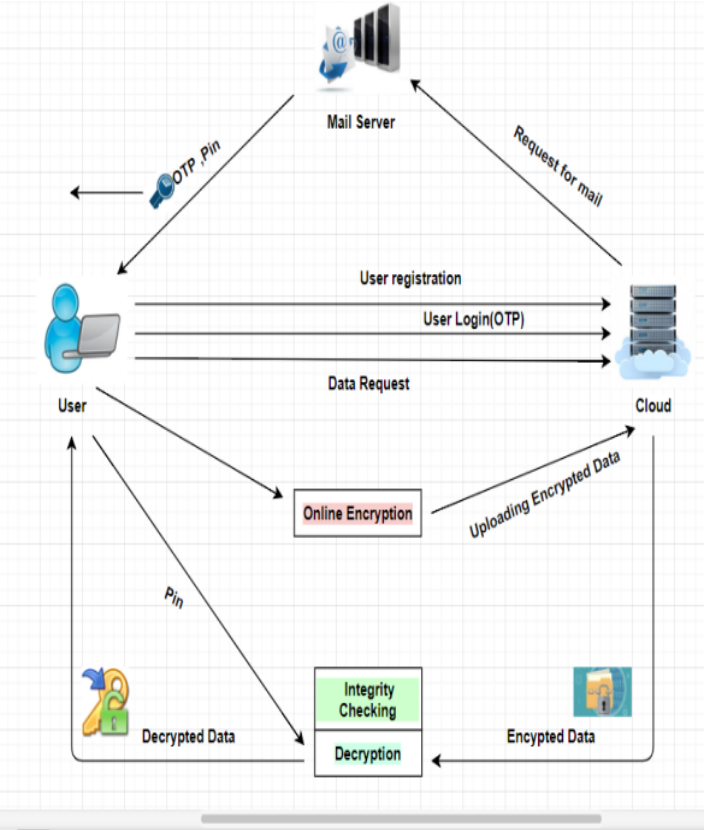


Fig 2.8 proposed System Frame work

3.1 DESCRIPTION OF MODULES

The following is a description of the modules:

3.1.1 User Registration

A user must first register in order to utilise this module by supplying information such as his userid, user name, password, legitimate email address, etc. The user will then receive three random pictures after entering this information, and one of the images' coordinate squares must be selected as the user's graphical password.The coordinate information for each photograph will be saved in the database for each user.

3.1.2 Module for Image Discretization

Each image is divided into squares, from which the users will choose one cell to act as the pass square.

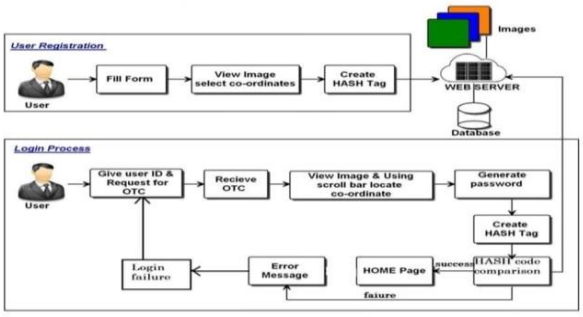
Figure 3.1.2 demonstrates the division of a picture into hash codes.

3.1.3 Hash Code Generation

The database will be updated with the user's information by concatenating the coordinates of all three photos, generating a hash code, and saving the data when the image coordinates have been correctly set.

3.1.4 Process for Logging In as a User

A One Time Password (OTP), which contains a random pair of and horizontal slider coordinate points for each of the three images, will be sent to the registered user's email if the userid and password are both valid. Registered users log in to the application using their userid and password. Three assigned images with sliders will be shown to the user following a successful login; the user must adjust the sliders for all three images



3.1.5 Generic Login Indicator Module

This module generates a login indication for users made up of different recognisable characters (like integers) or graphic elements (like colours and icons). We utilised a 7 x 11 grid and the letters A to G for our implementation. Because both letters and numbers are produced at random, a distinct login indication will be provided every time the module is invoked. The produced login indicator may be shown to the user visually or acoustically. The indicator in the first instance could appear directly on the display or through another specific graphic.

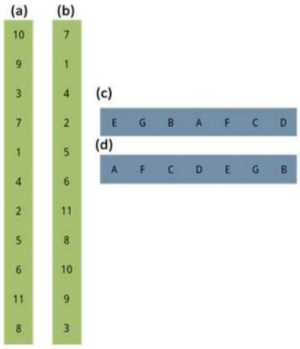
Fig. 4.8.5 Obtain the login indicator (E,11) directly., Obtain the OTC through a predefined image.

.

3.1.6 Control Module for Horizontal and Vertical Axes

The two scroll bars are a horizontal bar with a series of letters and a vertical bar with a series of numbers. This control module offers drag and fling features that allow users to manage both bars. By throwing either bar with their finger, they may change one alphanumeric at a time. They can also shift numerous checks at once by moving the bar far.

Given that both bars are circulative, turning the horizontal ba into a bar requires shifting it left three checks.



3.1.7 Module for Password Verification

During the authentication procedure, this module checks the user's password. A pass-square performs comparable duties to a password digit in the text-based password scheme.The user can only be regarded as authorised when each pass-square in each password is appropriately aligned with the login indication.

3.1.8 Communication Module

This module manages the data transferred between client devices and the authentication server.

The SSL (Secure Socket Layer) protocol protects against being overheard and intercepted during any conversation.

3.1.9 Admin

The administrator must access his account using the authorised user name and password. After successful registration, the administrator has access to each user's information.

3.1.10 Decoy paperwork

We propose an alternate approach that utilises offensive decoy technology to safeguard cloud-based data. We monitor data access in the cloud and search for odd data access trends. We initiate a deception assault by delivering the attacker a tonne of false information. This prevents misuse.

3.2 SYSTEM DEVELOPMENT

This chapter covers the system's architectural diagram, followed by descriptions of the modules and the development tools employed for the project.

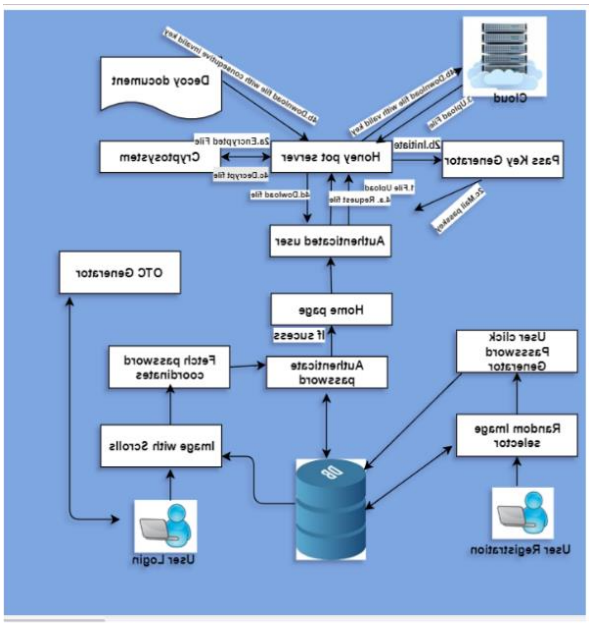


Fig 3.2 System Architecture

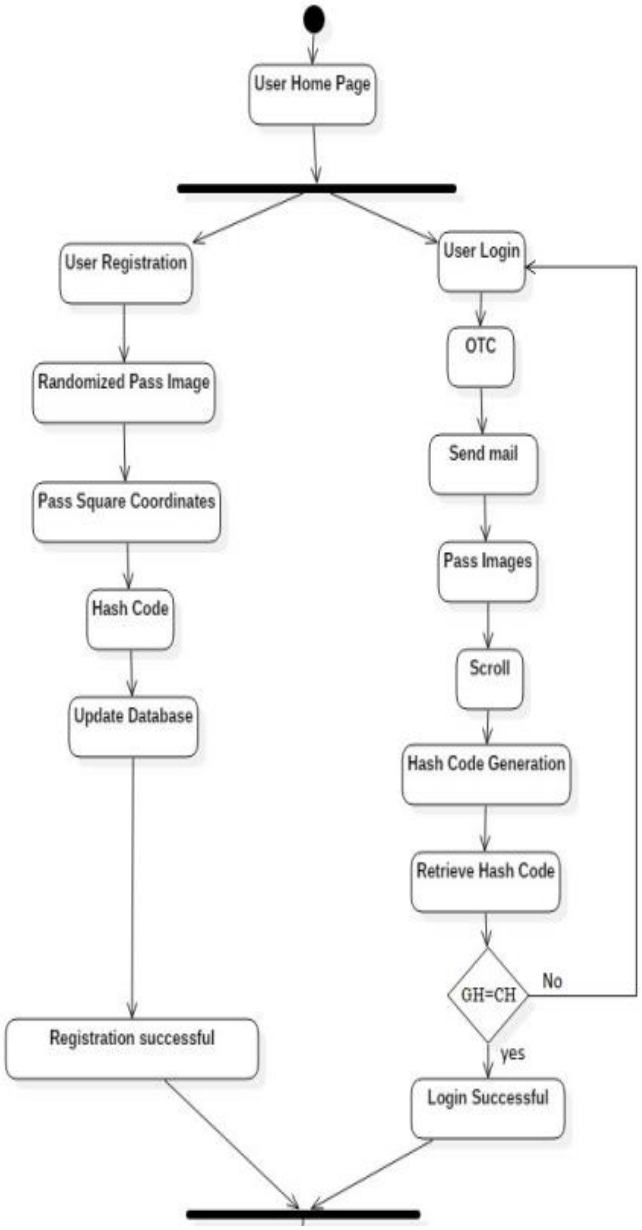


Fig.3.2.2 Activity diagram for Registration and Login

Data storage is one of the most popular cloud computing services. Although there are numerous advantages to this service, a cloud of privacy and security worries looms over it. Although CSPs promise to keep their customers' data secure, consumers are cautious to believe them and put off using cloud data services. Customers are hesitant due to different dangers to the cloud environment. Our technology addresses threats including data breaches, stolen credentials, compromised authentication, and malicious insiders. It also provides aid with investigations. The system performs a variety of functions, including user authentication, data auditing, online encryption, and private key creation for encryption.

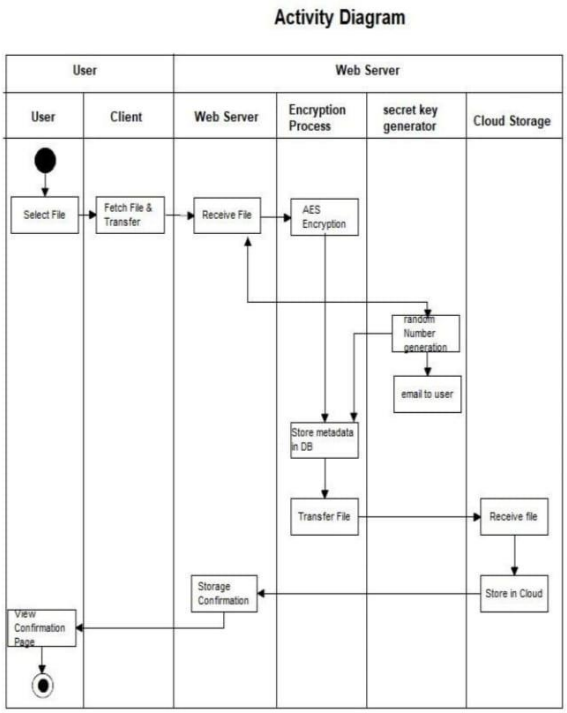


Fig 3.3.3 Activity Diagram

4 Algorithms

Algorithm 1. Randomized Image Selection

Step 1: Assume that Image Database has N images.
Step 2: Set M to the required number of password images.
Step 3:Initialize the integer array RAN[M] in step 3.
Step 4: C =1
Step 5: Create a random number between 1 and N and set it to R
Step 6: R must be present in the RAN array, t hen go to 5th step
Step 7 : RAN[C] = R
Step 8: C = C + 1.
Step 9: if C <= M at step 9, move on to step 5.
Step 10 : Stop

Algorithm 2. Password String creation & Secret Hash Code generation

Step 1: Let M represent the number of password pictures in step 1.
Step 2: C = 1 and password=""
Step 3: Assume that the user clicked a pixel on the image, P(X,Y).
Step 4: Use the Pixel to Co-ordinate function with P(X,Y) to obtain (RV,CV)
Step 5: Password = Password + RV + "," + CV (Step 5)
Step 6: C = C + 1
Step 7: go to Step 3 if C == M.
Step 8: Get the secret code by using the hashing algorithm on the password.
Step 9: Enter Secret Code Into Database
Step 10: Stop

Algorithm 3. Click Based Pixel to Co-ordinate conversion

Step 1: Let C represent the column offset (for example, C = 200).
Step 2: Let R be the Row offset (for example, R = 200).
Step 3: Assume that the user clicked a pixel on the image, P(X,Y).
Step 4: Let RV = CEILING(Extract Row value from P(X,Y)/R)
Step 5: Let CV=CEILING(Extract value from P(X,Y)/C)
Step 6: The coordinate value for the password picture is (RV, CV).
Step 7: Stop

Algorithm 4: One Time Code (OTC) Generation & SMS

Step 1: Let M represent the number of password pictures.
Step 2: Set C = 1 and OTC = "";
Step 3: Let K represent of columns in the image
Step 4: Let L be the number of rows in the picture.
Step 5: Create a random number between 1 and K and set it to R1.
Step 5: Create a random number between 1 and K and set it to R1.
Step 6: Choose R2 as the result of a random number generator between 1 and L.
Step 7: Change R1 into the alphabet (AR1), for example, 1 to A, 2 to B.
Step 8: OTC = OTC + AR1 + R
Step 9: C = C + 1
Step 10: If C=M, go to Step 5
Step 11: Choose the user's email address from the database.
Step 12: Send an email to the user's email ID.
Step 13: stop

Algorithm 5: OTC & Scroll Bar Mapping and Co-ordinate Generation

Step 1: Set K to be the number of columns in the illustration.
Step 2: Set L to the number of rows in the illustration.
Step 3: Assume that RA1 is the image's OTC column value.
Step 4: Assume R2 is the row value in the image's OTC.
Step 5: Pretend the user has positioned the scroll bar and the submit button.
Step 6: Assume that XR1 is RA1's current column position.
Step 7: CV = XR1
Step 8: Assume that XR2 is R2's current row position.
Step 9: RV = XR2 in Step 9.
Step 10: The OTC-mapped coordinate is (RV,CV).
Step 11: Stop

5. Study Of The Tools

Java

Java was used to build the front end. Windows 7 serves as the system's foundation. The programming language used in 5.6.1 is Java. The high-level programming language known as Java is characterised by the keywords straightforward, architecture agnostic,

object-oriented, portable, distributed, high performance, interpreted, multithreaded, resilient, dynamic, and secure.
It is divided into 2 sections:
The Java Virtual Machine (Java VM) and Java Application Programming Interface (JAPI) (Java API).
Java is well-known for a variety of reasons, including Portability
Portability is essential in the emerging realm of networked applications and business.
Java employs a number of programmes to tackle this issue.
The foundation of this strategy is the truth.
Secure: It is not possible to use explicit pointer variables in Java.
Even without explicit pointer variables, it is still feasible to access data illegally if a byte code has been updated suitably.
Due to the fact that the Java interpreter checks each byte of code before interpreting it, Java also protects against this type of security attack.

Eclipse
Java was used to construct Eclipse, which is an open source tool.
It provides functions like managing windows and menus, storing settings, and other services used often while creating desktop programmes. Moreover, it is the first IDE to support all of the JDK 5.0 features. For the Eclipse platform and IDE, Sun Microsystems offers free commercial and non-commercial support.
Eclipse is an open-source project with the aim of providing trustworthy software development tools (the eclipse IDE and the eclipse Platform) that are able to meet the needs of consumers, developers, and businesses who utilise eclipse as the basis for their own products.

Oracle Platform
The Eclipse Platform is a modular development environment for Java Swing desktop applications.
the Eclipse IDE's package
IDE for Eclipse
An integrated development environment that is free and open source is called Eclipse IDE.
The Eclipse IDE facilitates the creation of all Java application types right out of the box.

MySQL
The database in use is MySql. MySQL is the most widely used database in the world. platform that is created completely of software and runs on top of other hardware-based platforms. The Java platform consists of two parts: Java Virtual Machine (JVM) and Java Application Programming Interface (Java API) (Java API) It serves as the foundation of the Java platform and is supported by a wide range of hardware systems. GUI widgets are only one of the many helpful features provided by the Java API, which is a substantial collection of pre-made programme elements.
Packages, which are assemblages of related classes and interfaces, are how the Java API is organised.

Conclusion and Future Work
The concept of internet encryption has helped users save time. Data access management and privacy protection are improved by the security mechanism offered. Also, the system is devoid of key management and storage. Integrity An extra degree of protection will be added by user checking. Security risks such data breaches, stolen credentials, faulty authentication, and hostile insider attacks are nonexistent in the proposed system. Uploading several media files to the cloud can be used for future enhancement. Future upgrades might include an Auditor module, which would check the cloud provider's reliability as well. Attempting to contribute multimedia content can improve the project. It is possible to lift the file size constraints and work on the different algorithms to enhance the system's security and privacy.

REFERENCES:
[1] "Order and entropy in image passwords," Proceedings of graphics interface, Canadian Information Processing Society, Saranga Komanduri and Dugald R. Hutchings, 2008.

[2] M.C. Mont, S. Pearson, and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services," in Proceedings of the International Workshop on Database and Expert Systems Applications (DEXA), 2003, pp. 377–382.

[3] "Digital Color Picture Encryption Using RC4 Stream Cipher and Chaotic Logistic Map", Proceedings of the 2013 IEEE International Conference on Information Technology and Electrical Engineering.

[4] "Preventing Information Leakage from Indexing on the Cloud," in Proc. IEEE Int'l Conf. Cloud Computing, 2010.

[5] Xiaoyuan Suo and Ying Zhu G. Scott Owen, "Graphical passwords: a survey," 21st Annual Computer Security Applications Conference, 2005.

[6] An association-based graphic password design that is resistant to shoulder surfing attack was developed by Li, Qibin Sun, Yong Lian, and D. D. Giusto in 2005. (ICME).

[7] To achieve accountability, auditability, and trust in cloud computing, Ryan K. L. Ko1, Bu Sung Lee, and Siani Pearson wrote a paper in 2009 for the Cloud and Security Lab at HP Labs in Fusionopolis, Singapore.

[8] Y. Chen et al., "Oblivious Hashing: A Stealthy Software

Integrity Verification Primitive," in Proc. International Workshop Information Hiding, F. Petitcolas, ed., 2003, pp. 400-414.

[9] Design and Assessment of a Shoulder-Surfing Resistant Graphical Password System by Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget, Proceedings of Advanced Visual Interfaces, 2006 (AVI2006).

[10] Tari Furkan, A. Ant Ozok, and Stephen H. Holden, "A comparison of perceived and real shoulder-surfing dangers between alphanumeric and graphical passwords," Proceedings of the Second Symposium on Usable Privacy and Security, ACM, 2006.

[11] "Securing passfaces for description," Proceedings of the 4th Symposium on Usable Privacy and Security, ACM, Paul Dunphy, James Nicholson, and Patrick Oliver, 2008.