ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (35-41), Month: October - December 2021, Available at: www.researchpublish.com

Efficient and Secure Data Storage in Cloud Computing

[1]Gutta Ranjitha, [2]Mithila G, [3]Harshitha Reddy S, [4]Sai Divya H,
[5]Professor Bindu Madavi K.P

[1,2,3,4]Dept. of CSE, Dayananda Sagar University, Bangalore, Karnataka

[5]Assistant Professor, Dept. of CSE, Dayananda Sagar University, Bangalore, Karnataka

Abstract: **Cloud computing has been intended as the next age group architecture of IT Enterprise. In contrast to traditional results, cloud computing moves the application of software and databases to large data centers, where the organization of the data and services may not be fully truthful. So, this paper attentions the need for users to trust the commercial cloud provider's and security issues of storing data in cloud storage service. The cloud storage is one of the projecting services presented in cloud computing. This is a implemented paper and proposes a method for cloud storage that allows user to store and access the data securely using SHA256 algorithm and implementing it in Amazon Web Services (AWS) Cloud. In this paper we have proposed a solution which uses a mechanism of hash function along with various cryptography tools to provide better security to the data stored on the cloud (AWS).**

Keywords: **Integrity, Amazon Web Service (AWS), Cloud Computing, Storage, Security, SHA256 Algorithm.**

1. INTRODUCTION

The main call for cloud computing is that the user can only utilize what they required and the user's only pay for what they use. One of the most important service offered by cloud is cloud storage, which refers to the online space where the user can store the data securely. Cloud computing will bring several advantages to the market and the three most important are security, effectiveness and scalability. Cloud storage is a service model in which data is preserved, managed and backed-up remotely and made accessible to user over a network. The biggest concern about cloud storage is security and which is considered as a key requirement of a cloud. The main risk in cloud is that there is no proper security inside the cloud and it's fails to protect, the risks using cloud services that can lead to higher costs and mostly potential loss for business. Security of data remains a concern in computing and this problem arises from the fact of sensitive data. To overcome this, we have proposed a solution which generates a hash values using SHA256 algorithm which helps us to secure data in the cloud. SHA256 stands for Secure Hash Algorithm and this algorithm is used for cryptographic security and produce's unique hash values and this algorithm mainly focuses on the speed of generating the key.

2. LITERATURE SURVEY

Vaidehi M [1] They proposed a technique and algorithm used to ensure security, SHA256 has been applied. It handles 256 bits known as digest length. This does not use any keys. Secure hash algorithm is commonly used in data security for various applications and this convert actual data into encrypted form if the input data of hash changes then the output hash also changes. They have detailed about data distributed on three levels, that is network, host and application level. And also they mentioned it is important to satisfy the requirements which is related to security to store data, which includes integrity, availability and confidentiality.

Rajendra Patil [2] In this paper they have suggested the mechanisms and algorithms used are cryptographic encryption and strong authentication mechanism and also blowfish encryption algorithms are used, message authentication code and effective auditing mechanism is used. It is required to satisfy security requirements to store data.

Dr. P Sasikala [3] They have been explained about the storage techniques which are prototype of searchable encrypted data file sharing to requisite storage and flexibility and also they have recommended a methodology termed as intelligent cryptography through which cloud servers could not directly attain partial data. Attribute based encryption for ensuring security and attained reliable fine-grain file access control in cloud storage scheme and also mentioned about data dynamics and public auditability to facilitate storage security. Here they have mainly focused on security problems which includes trust, data confidentiality, data privacy, data availability and also mentioned about cloud storage structure which consists of four layer: Access layers, application layer, basic management layer. This paper emphasizes the modern studies concerning storage and ensuring data security, dynamic ways of data storage and optimum cloud storage system.

Mohamed Ismail [4] The key objective of this paper is to identify different security threats related to store data, system development using advance encryption standard algorithm for data encryption and authentication scheme valid user's verification and prevention of unauthorized access to all functional units of the system. The main issue in data storing are data control, security threat and application suitability.

Manisha Thakur [5] In this paper they have specified about the storage on cloud with inexpensive storage and backup option small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of the data and they have been detailed about deployment models such as hybrid cloud. And it also mainly focuses on security are privacy, legal issues and have more concern related to these issues.

3. PROBLEM STATEMENT

Cryptographic approaches might significantly reduce the efficiency of the cloud system and makes the deployment of traditional data utilization service difficult. It is desirable to build cryptographic approaches to achieve the security goals without introducing significant overhead for the cloud system. In this project we mainly concentrate on data storage and retrieval in cloud computing. Data breaching one of the main performance issues faced in cloud computing. The main aim is to maintain integrity of data (videos, images) so, we have proposed a solution which includes a mechanism of hash function using various cryptographic tools to provide better security to the data which is stored.

4. SYSTEM MODEL

4.1 Existing Method

Cloud storage is being widely adopted due to popularity of cloud computing, recent reports indicate that data loss can occur in cloud storage providers. So the problem of checking the integrity of data in cloud storage, which we refer to as secure cloud storage, has attracted a lot of attention. On the additional side, networking coding, which was planned to expand the network capacity, also faces the problem of integrity checking. A transitional router may purposefully infect codewords, which outcomes in decoding failures at the endpoints. Glance through the integrity of codewords is referred to as safe network coding problem.

4.2 Proposed Method

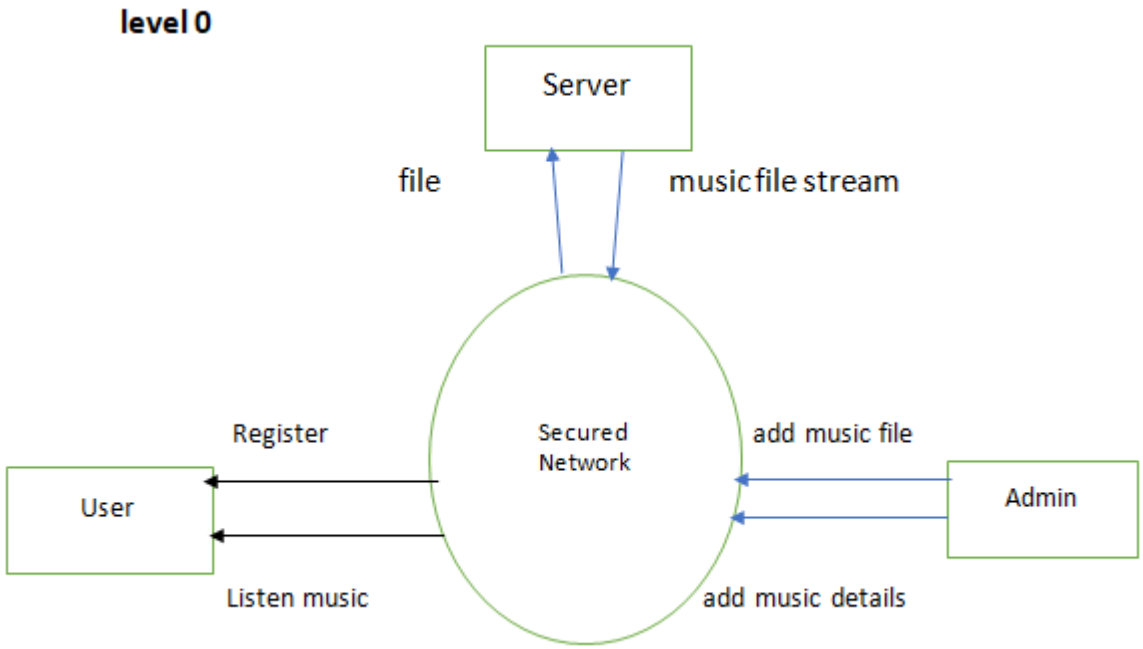
The proposed method contains two parts that is file upload and file download. This is executed in local host as well as in Amazon Web Service platform.

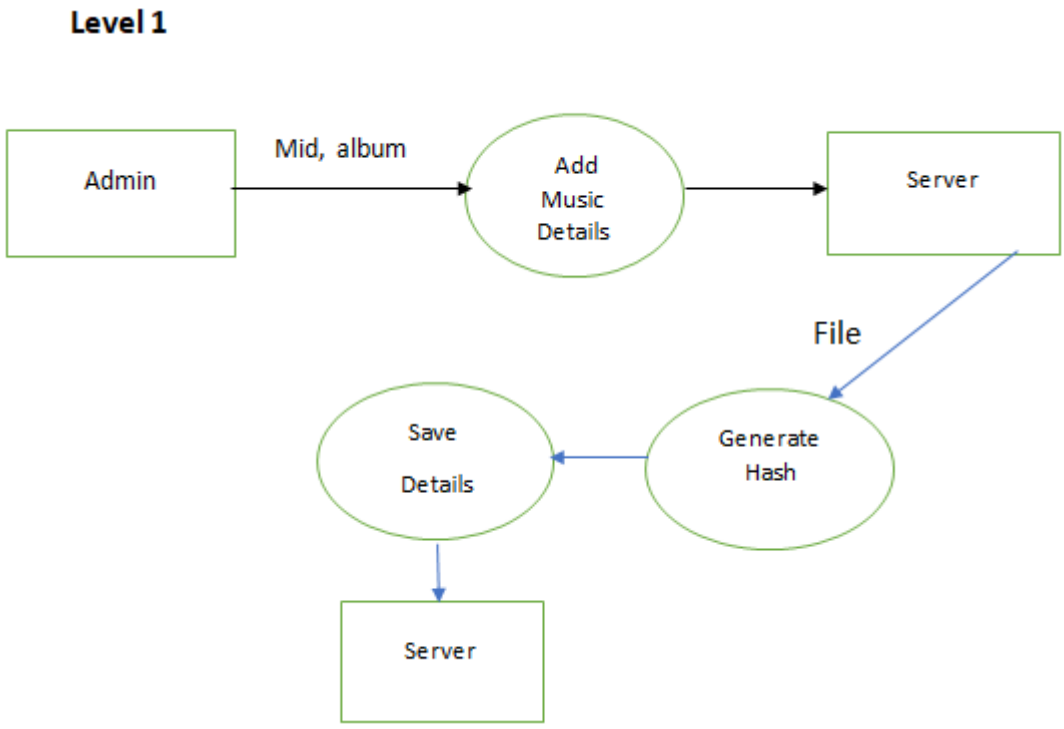
- **File upload**: The file upload allows the admin to login into the portal using user id and password. Server verifies the login credentials and if it's a successful login then admin can add video details. Once the video details are uploaded then admin can select the video file and upload. Server once receives the video file generates the hash of the file using SHA256 algorithm.

- **File download**: In file download user can register into the portal by providing his/her details. Then the details are saved into the database then the user can login using login credentials and can search for videos. When the user sends the request to the server for a video file, server gets the details of the file. Then the server checks the file id's, file hash and server generates the hash value of the file using SHA256 algorithm and compares it with the hash that was saved in the database while uploading.

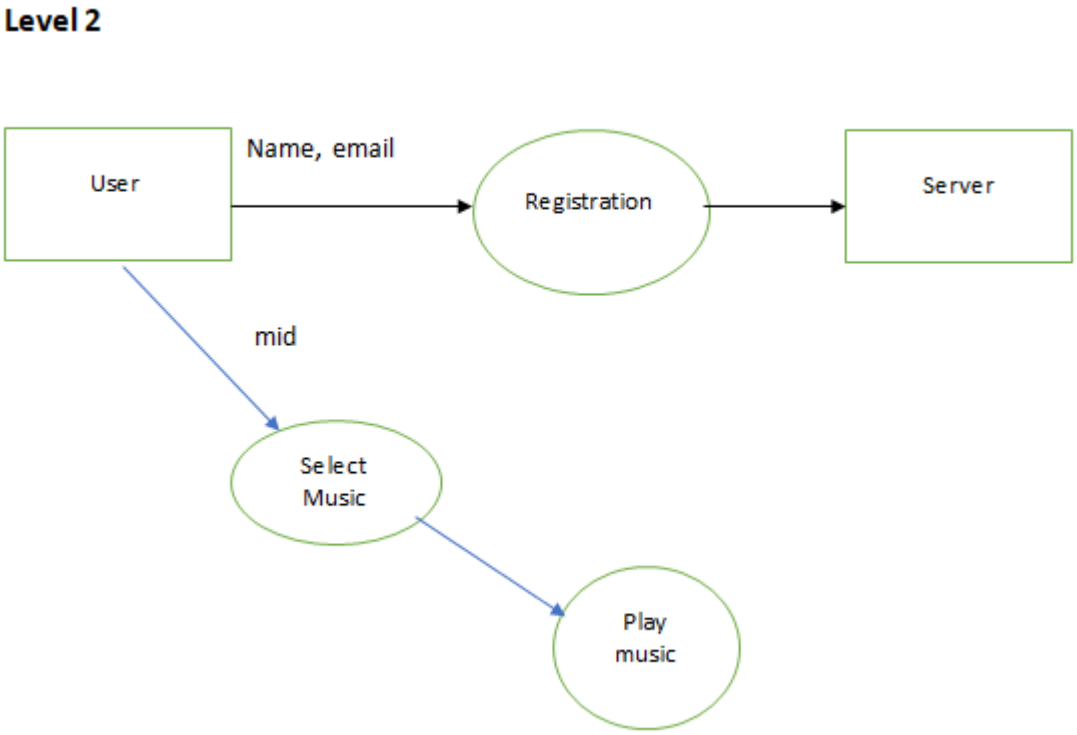
ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (35-41), Month: October - December 2021, Available at: www.researchpublish.com

4.3 Data flow Diagram





ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (35-41), Month: October - December 2021, Available at: www.researchpublish.com

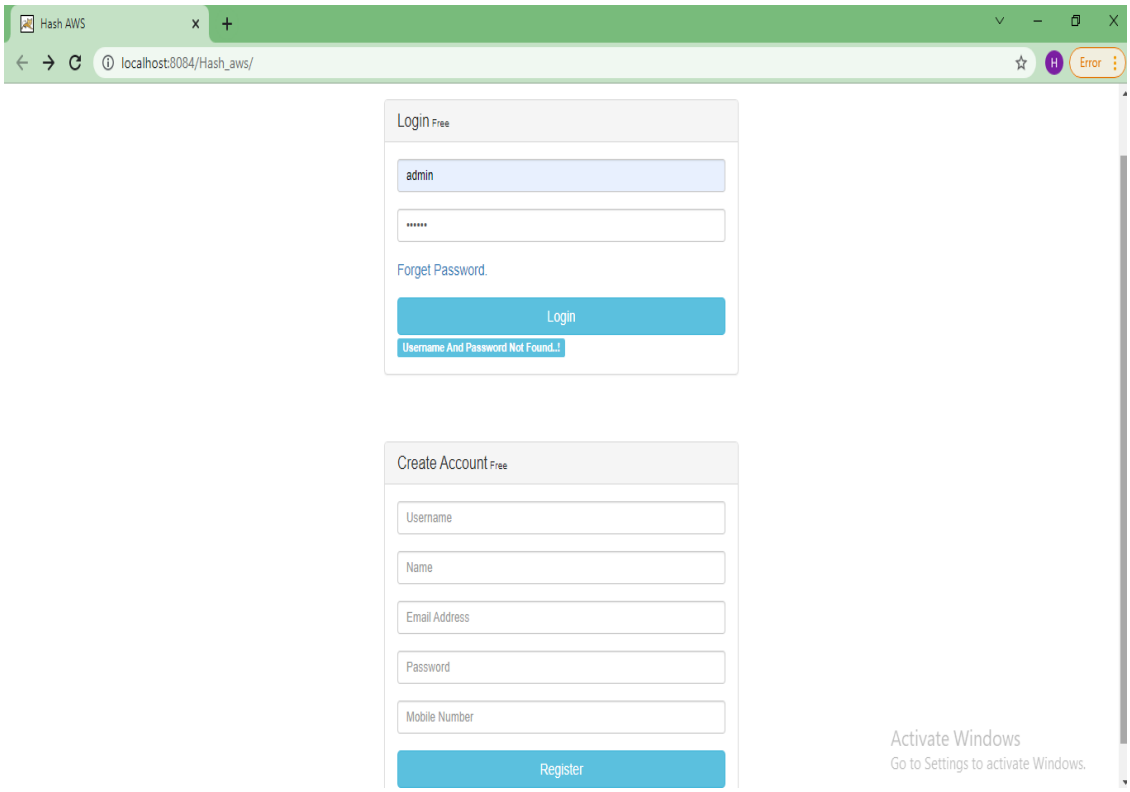


5. METHODOLOGY

In this proposed schema, to ensure security the SHA256 algorithm been used and the same is implemented in AWS platform. SHA256 or secure hash algorithm that is commonly used in data security for various applications.

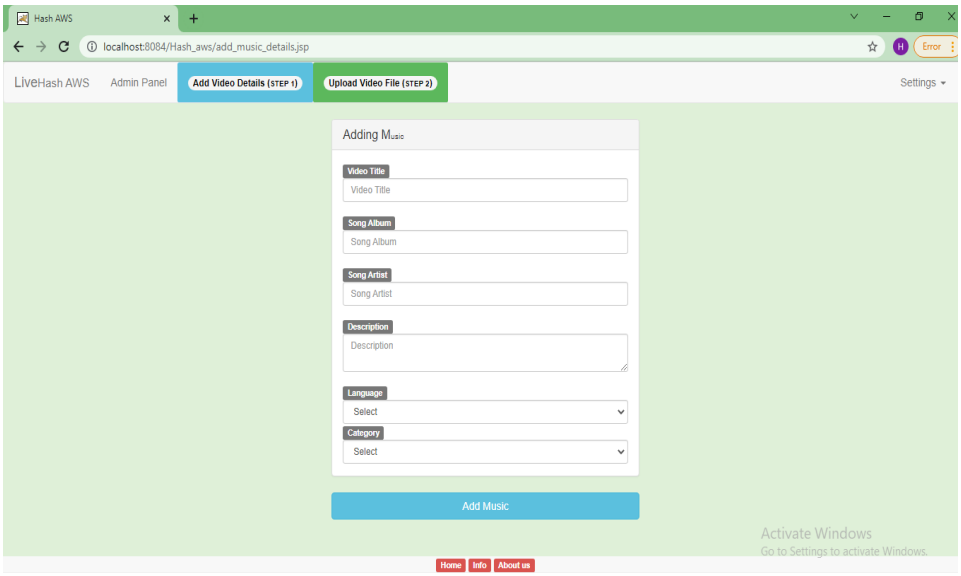
6. SAMPLE RESULTS

Step 1: Create account and login with user id and password.

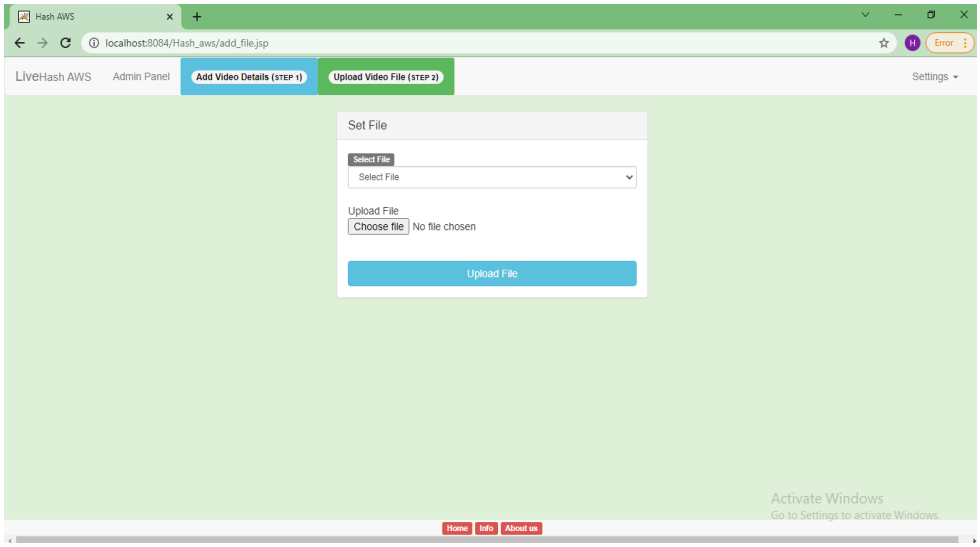


ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (35-41), Month: October - December 2021, Available at: www.researchpublish.com

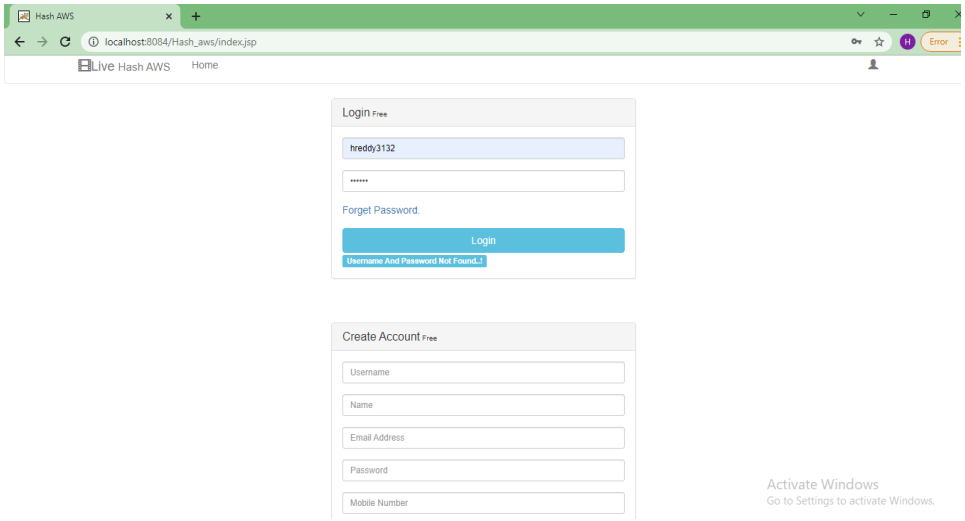
Step 2: In this admin panel, here the admin can add video details.



Step 3: Here admin can select file and upload the video.

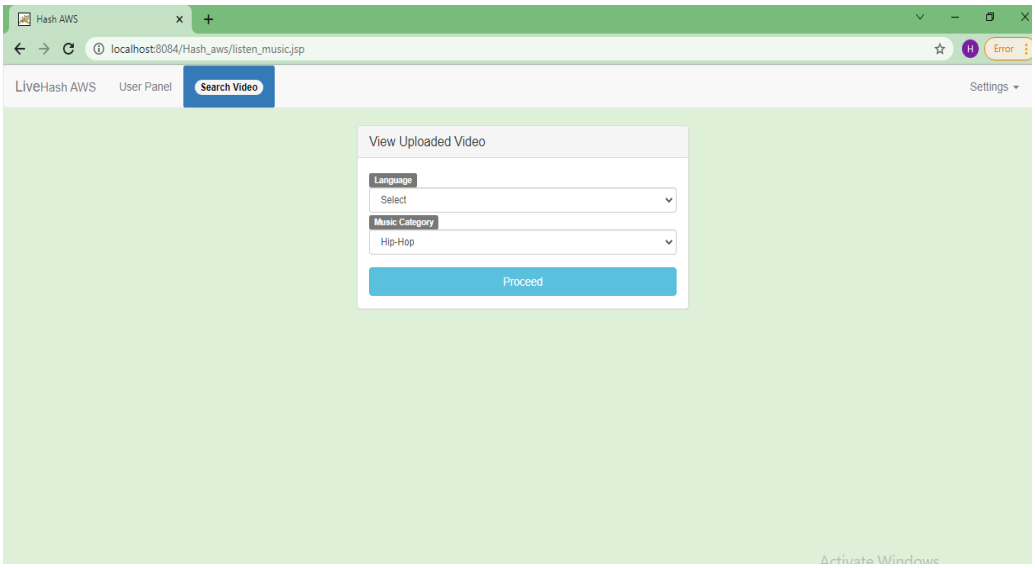


Step 4: User can create their account and login with the username and password.

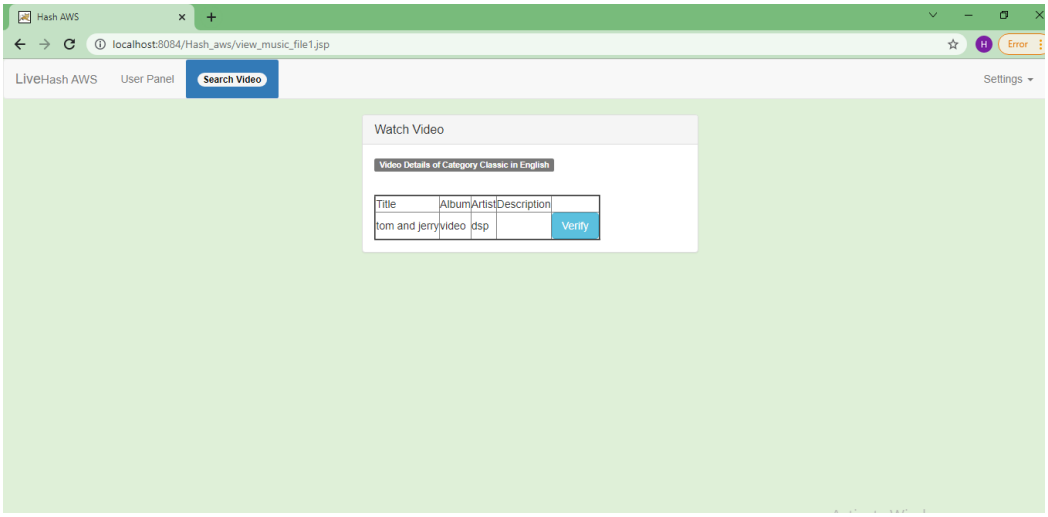


ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (35-41), Month: October - December 2021, Available at: www.researchpublish.com

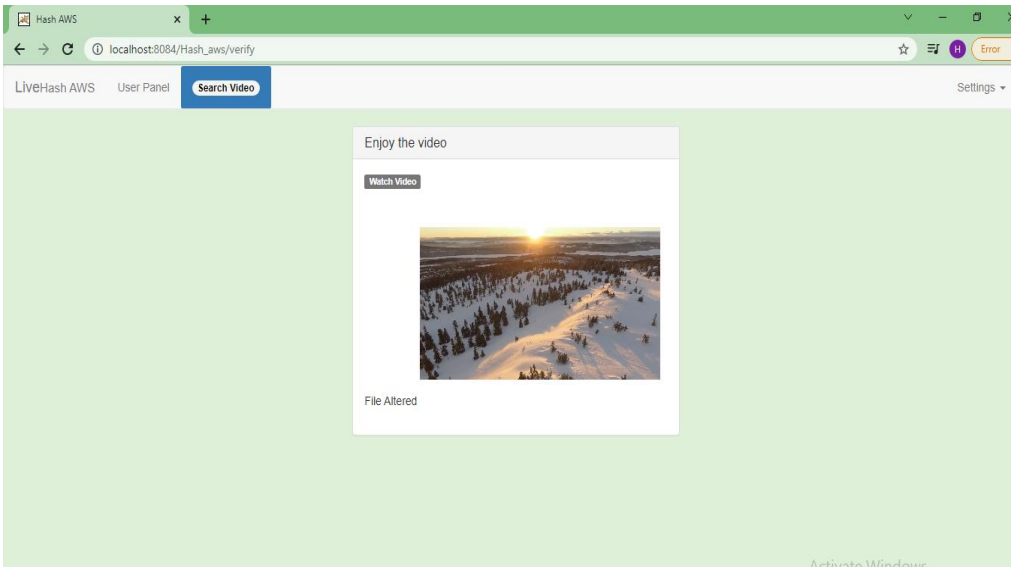
Step 5: User can view the uploaded videos of their choice.



Step 6: The user can see the details of the video and verify it.

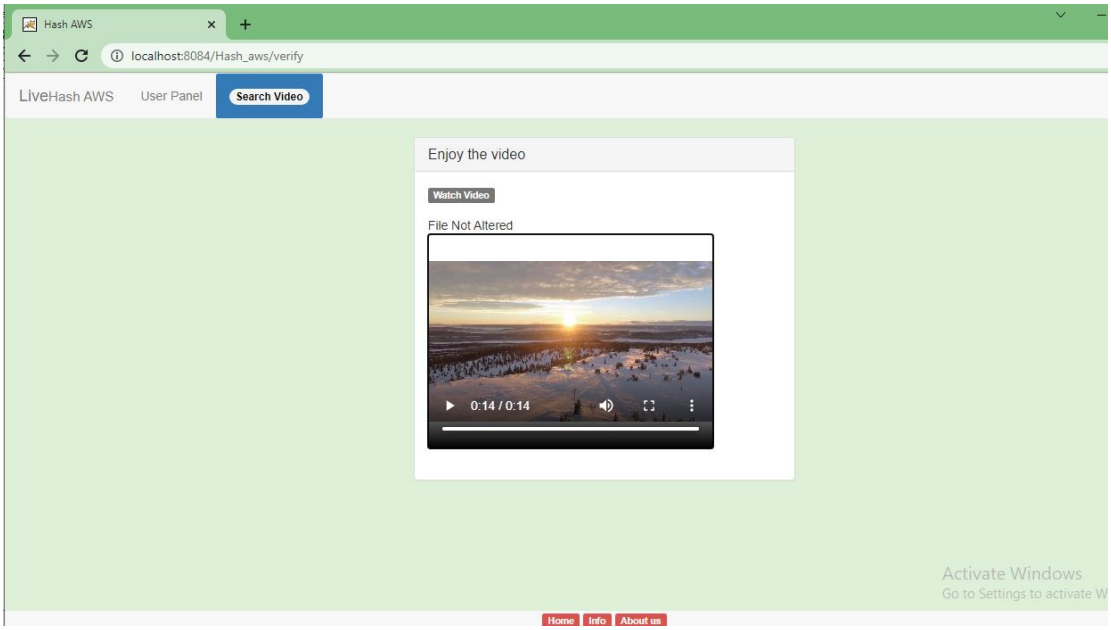


Step 7: The user can watch the video and you can see the file altered here because we modified the value of Hash.



ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (35-41), Month: October - December 2021, Available at: www.researchpublish.com

Step 8: The user can watch the video and you can see the file not altered because the Hash value remains same.



7. CONCLUSION

We have introduced a SHA256 schema for fine-grained access control in cloud computing and to ensure flexibility and scalability in it. Using this hashing algorithm, which has 256 bits key length this results in higher security, rather than using a traditional AES and a DES algorithms are of smaller in key sizes this results in lesser security. SHA256 algorithm generates a hash value for the data stored in the cloud, if the data uploaded in cloud changes then the hash value also changes.

REFERENCES

[1] R. Dinesh Arpitha and Shobha R. Sai International journal of research and analytical reviews(4)(2019)data storage, security and techniques in cloud computing.

[2] Manisha Thakur and Dr. Neeru Bhardwaj International journal of computer science and mobile computing IJCSMC, Vol.8, Issue 5,May 2019,pg23-31 A Review paper on cloud Computing and security Issue.

[3] Athira A R and Dr. P Sasikala journal of Information and computational science,Survey on distributed secure data storage in cloud computing.

[4] Vinayaka pujari and Rajendra Patil Conference paper- February 2020, A Study of Data Storage Security Issues in Cloud Computing

[5] H. Guesmi, C. Ghazel and L.A. Saidane International journal of engineering research and technology (IJERT) Securing Data Storage in Cloud Computing.

[6] Mohamed Ismail and Badamasi Yusuf Conference: ASCENT 2019, Ensuring Data Storage Security In Cloud Computing With Advanced Encryption standard (AES) and Authentication Scheme (AS).

[7] Naresh Vurukonda and B. Thirumala Rao, Academic research paper on Computer and information sciences. A study On Data Storage Security Issues In Cloud Computing.

[8] Manish M Saunshi, Manoj N, M Ramesh, Nithyashree B.T, Vaidehi M, International Research Journal of engineering and Technology(IRJET).Efficient and Secure Data Storage in Cloud Computing.