RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES

Social Science Journal

WEB BASED CLOUD STORAGE FOR SECURING DATA SHARING AMONG THE PLATFORMS

SOWJANYA NAGANABOINA
sreenidhi institute of science and technology
The E-mail Author's: sowjanyanaveen202@gmail.com1,

ABSTRACT

Concerns about the security of customer data have grown in tandem with the proliferation of cloud computing. While client-side encryption/decoding seems like a great way to keep sensitive data safe, the current setup has three major flaws: terrible usability due to specialised software and plugins that need specific types of terminals, low security due to low-entropy PIN encryption, and traditional encryption algorithms make data sharing a pain. This work creates and deploys WebCloud, an effective browser-side encryption solution, using state-of-the-art Web technologies. Not only does it fix all three of those problems, but it also handles data quickly with disconnected encryption and re-appropriated decoding, as well as a robust and rapid client denial. More specifically, our solution works on any device—desktop, mobile, or otherwise—that has a Web user agent installed. We combine complicated cryptographic operations using WebAssembly and the Web Cryptography API. Additionally, we build a file management application called WebCloud based on ownCloud. We conclude that WebCloud is successful and cross-platform after comprehensive testing with many popular browsers, Android applications, and PC software. The technology known as the ciphertext-policy attribute-based key encapsulation mechanism (CP-AB-KEM) is an integral component of the design of WebCloud and has the potential to be utilised in a variety of other contexts.

Keywords: WebCloud, Secrecy; Web Cryptography, API, CP-AB-KEM.

1. INTRODUCTION

The decreased prices and greater data usage capabilities for users are driving the increased popularity of PUBLIC cloud storage services. Because of this trend, more and more people and businesses are storing sensitive information on public clouds without encryption and are sharing this data with others. You have to have faith that the server will protect your high-value data from unauthorised disclosure when you access it in the cloud.

This confidence is frequently misplaced due to the fact that there are numerous ways in which confidential data can be leaked, such as the data breaches that have been reported [1, 2], [3], [4], [5], and [6]. The client-side encryption and decryption method is one of the most promising remedies to the problem of data leaking. To be more precise, with client-side encryption, data can be encrypted before being sent to clouds and decrypted after it has been downloaded

from those clouds. This makes server-side data exposure more difficult, if not impossible, since clouds can only obtain encrypted data.The capacity to freely share files with a large number of users or a group of users is an essential component of cloud storage and must be fully supported.

On the other hand, the client-side encryption solutions that are now available have a number of drawbacks, particularly with regard to security, efficiency, and usability requirements. Encryption solutions that are known to be client-side. Existing solutions are examined, and the limits of such methods are highlighted.

Limited support or no support.

Google Drive and Dropbox are only two of several cloud storage platforms that do not enable client-side encryption. Files saved on the server are encrypted using server-side encryption, data in transit is encrypted using transport layer security (TLS), and user authentication is secured using two-factor authentication.

End-to-end encryption is supported for sensitive information stored in Apple I Cloud, such as Wi-Fi passwords and I Cloud Keychain login credentials. Server encryption is the only method that is utilised for other data that is uploaded to I Cloud.

Password-Based Solutions.

In order to encrypt the data of users, certain products [7], [8], and [9] employ symmetric encryption, which is commonly AES, and then upload the ciphertexts to cloud storage. In contrast, some techniques use a passphrase, password, or even a four-digit PIN to generate their cryptographic keys.

To rely on something with such a low entropy is considered to be risky [10]. Even more troublesome is the fact that the majority of password-based solutions only address the situation of encrypting and decrypting data for a single user, and thus do not offer any mechanism for file sharing. Specifically, [7] gives users the ability to produce a share link for every file that is secured by a password.

2. LITERATURE SURVEY

Data is fundamental to every company's identity, which is why it's typically considered the most important asset a company has. It is the main source from which one can derive the facts, figures, and, in due time, the wisdom that is required to make good decisions and execute proper actions.

One example of this might be assisting in the treatment of a sickness, increasing the profitability of a corporation, making a building more energy efficient, or being accountable for the accomplishment of goals and the enhancement of performance [11]. Furthermore, essential services for any organisation to enhance their performance include data storage, analysis, and sharing. On the flip side, organisations are under intense pressure to store the large volumes of data locally due to the data's rapid rise. Furthermore, data investigation has grown more challenging as a result of the limited resources. Most businesses have taken their operations to the cloud to provide these services because of all the benefits, such as on-demand service, scalability, reliability, flexibility, measurable services, disaster recovery, accessibility, and many more [12].

The concept of cloud computing is a paradigm that makes it possible to have enormous amounts of memory space and tremendous amounts of computation capacity at a low cost. Consequently, it provides customers with a significant amount of convenience by enabling them to receive the services they require across a variety of platforms, regardless of their location or the time of day. Moving the local data management system to the cloud and using cloud-based services allows users to save money and be more productive while managing projects and forming collaborations. As a result, more and more services are moving to the cloud, both for consumers and businesses [8].

In the not-too-distant future, it is not hard to think that practically all enterprises would be moved to the cloud. This is because cloud computing technologies are expanding at faster and faster rates.

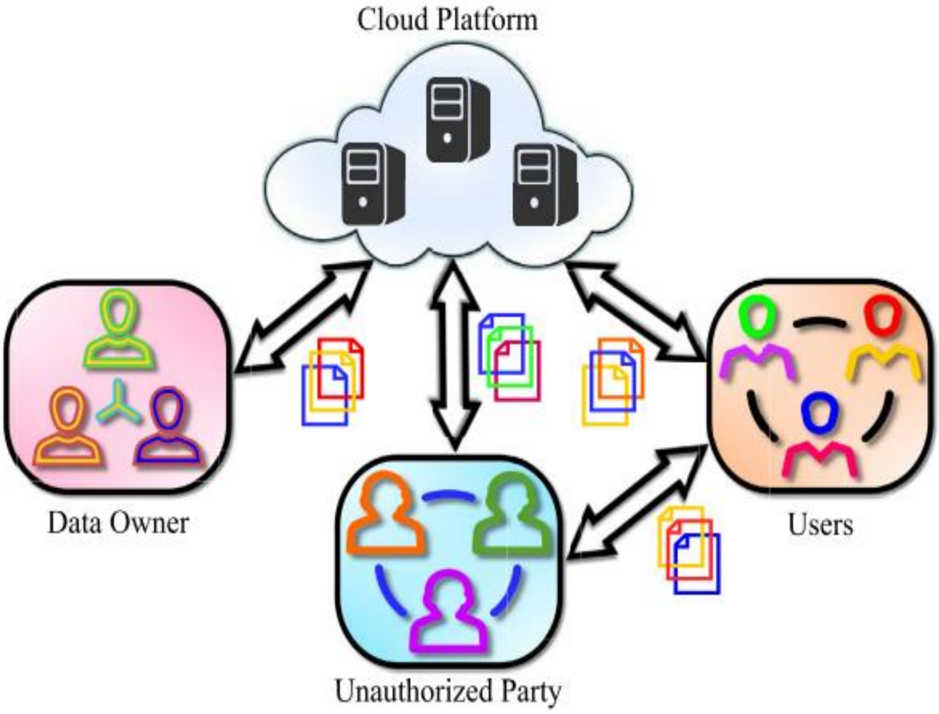


FIGURE 1. Block diagram of sharing environment.

In spite of the numerous benefits that cloud computing provides, it is confronted with a number of obstacles that have the potential to impede its rapid expansion if they are not addressed in an appropriate manner [10]. As an example of a real-world implementation, consider a company that encourages data storage and sharing across its employees or departments by utilising cloud computing platforms. Utilising the cloud allows the company to completely escape the responsibility of storing and managing the data on-premises. The major concerns of cloud users, however, centre on the fact that it is vulnerable to a variety of security threats [13]. The fact that users are no longer directly involved in the data's management is the first red flag when it comes to outsourcing to cloud servers. Because the data that is outsourced could contain important and private information, this makes the consumers nervous. Furthermore, it was demonstrated that the cloud server was susceptible to attacks [14].

This is because data sharing is typically implemented in an environment that is hostile and open to the public. Data owners in the scenario shown in Figure 1 are obligated to provide the cloud platform access to the organization's valuable data. The many benefits of cloud computing, coupled with the limited storage and computational capacity of organisations, make this a must. The data kept in the cloud is also shared among multiple users according to the different needs that are essential to its usefulness. Having stated that, once the information is collected, the recipient party is free to share it. Either the parties involved will divulge the information or an unauthorised third party will gain access to it and steal it. It is feasible to have both of these outcomes. If data were to be lost or disclosed, it might significantly threaten the organization's secrecy. Possible results include a fall in the company's status and standing, a reduction in shareholder value, and the annihilation of the enterprise's goodwill and image [15].

3. METHODOLOGY

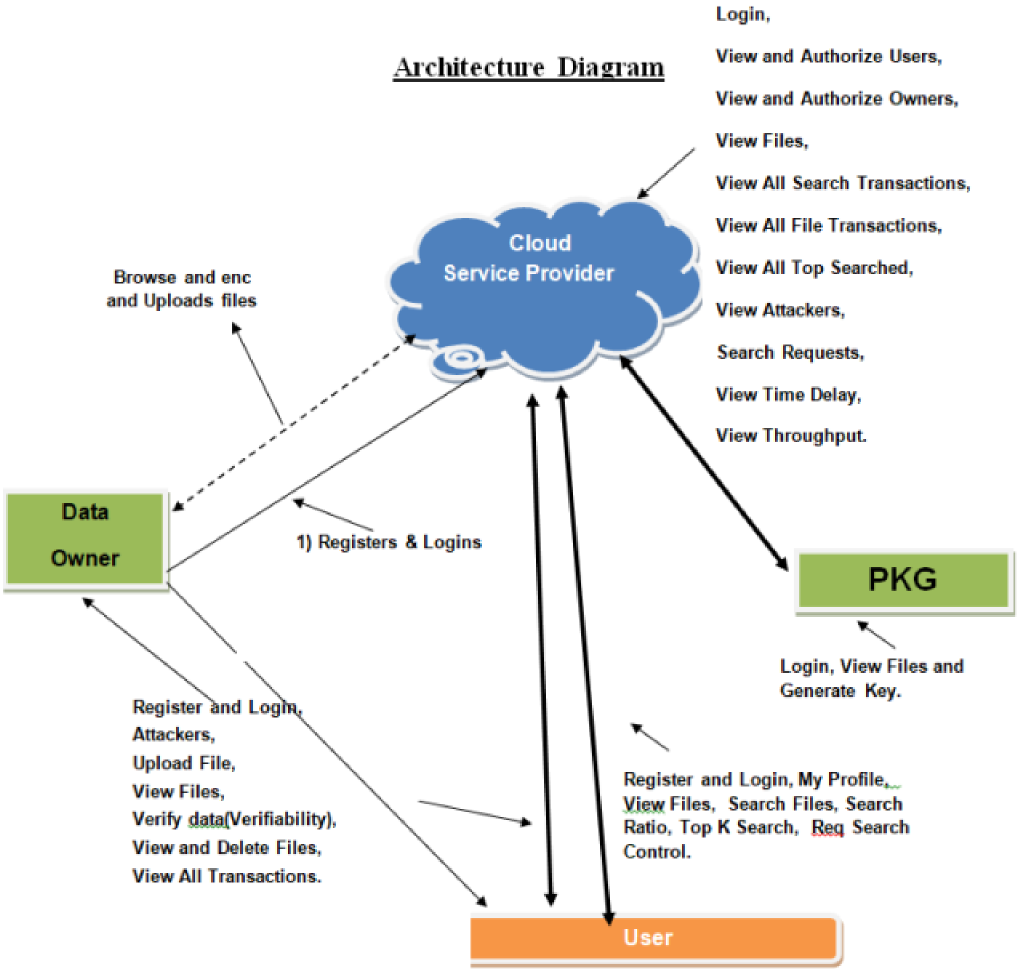


Fig 2: Architecture

The main architecture is shown in figure 2. It includes modules:

- **Data Owner**

This module allows the data provider to upload their encrypted data to the server that is associated with the cloud. A data file is encrypted by the owner of the data, and then it is stored on the server. This is done for reasons of security. It is possible for the owner of the data to demonstrate the ability to manipulate the encrypted data file and to carry out the following operations: Make sure you sign up and log in, Attackers. You are able to upload files, view files, verify data (also known as verifyability), view and delete files, and view entire transactions.

Cloud Service Provider

The data storage service that the Cloud server offers to the Data Owners is managed by the Cloud server. In order to make their data secure for users to access, data owners encrypt their files before storing them on the server. Data consumers are required to retrieve encrypted data files from the server, which will subsequently be decrypted by the server. The data consumers can now access the shared data files thanks to this. In the case that the user requests permission to view the file and performs the actions mentioned below—Login, View and Authorise Users, and Check for Authorization—the server will provide the aggregate key. You can view and authorise owners.

View the Files, Look at all of the search transactions, all of the file transactions, all of the top searches, all of the attackers, and all of the search requests. You may view the throughput and the time delay.

- **User**

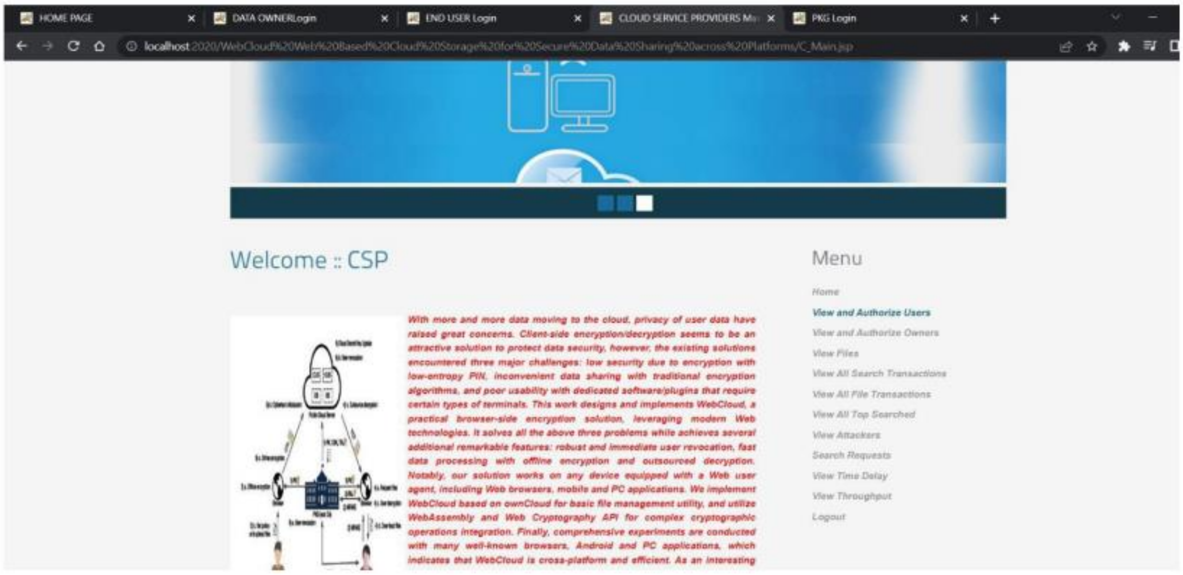
The user is only able to access the data file contained within this module if they have the secret key. The user has the option to search the file using a certain term. The user will obtain a response when the cloud server indexes the data that matches their unique keyword. Then, the following steps will be taken.

Sign up and log in, view your profile, and View Files, Search Files, Search Ratio, Top K Search, and Require Search Control are all feature options.

- PKG–

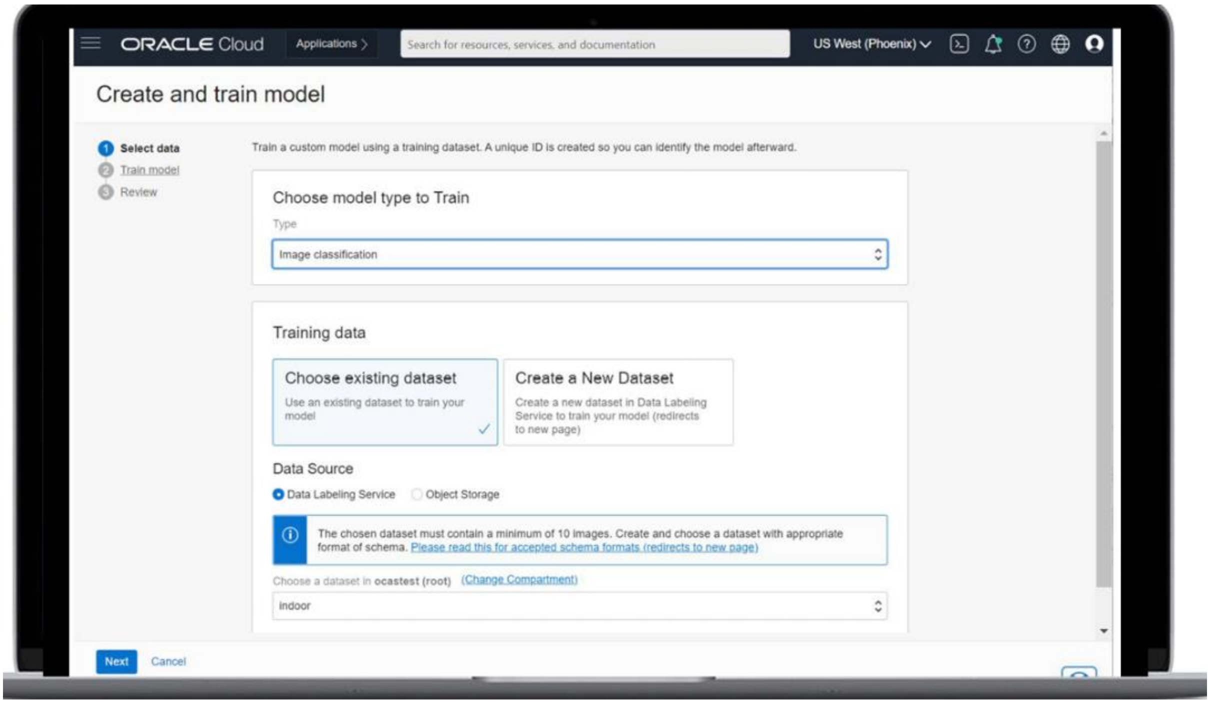
The individual in charge of reading files and generating keys.

RESULTS AND DISCUSSION


HOME PAGE
DATA OWNERLogin
END USER Login
CLOUD SERVICE PROVIDERS Ma
PKG Login
localhost:2020/WebCloud%20Web%20Based%20Cloud%20Storage%20for%20Secure%20Data%20Sharing%20across%20Platforms/C_Main.jsp
Welcome :: CSP
Menu
Home
View and Authorize Users
View and Authorize Owners
View Files
View All Search Transactions
View All File Transactions
View All Top Searched
View Attackers
Search Requests
View Time Delay
View Throughput
Logout

With more and more data moving to the cloud, privacy of user data have raised great concerns. Client-side encryption/decryption seems to be an attractive solution to protect data security, however, the existing solutions encountered three major challenges: low security due to encryption with low-entropy PIN, inconvenient data sharing with traditional encryption algorithms, and poor usability with dedicated software/plugins that require certain types of terminals. This work designs and implements WebCloud, a practical browser-side encryption solution, leveraging modern Web technologies. It solves all the above three problems while achieves several additional remarkable features: robust and immediate user revocation, fast data processing with offline encryption and outsourced decryption. Notably, our solution works on any device equipped with a Web user agent, including Web browsers, mobile and PC applications. We implement WebCloud based on ownCloud for basic file management utility, and utilize WebAssembly and Web Cryptography API for complex cryptographic operations integration. Finally, comprehensive experiments are conducted with many well-known browsers, Android and PC applications, which indicates that WebCloud is cross-platform and efficient. As an interesting

Fig 3: Cloud Main Page.



Create and train model

Train a custom model using a training dataset. A unique ID is created so you can identify the model afterward.

Choose model type to Train

Type: Image classification

Training data

Choose existing dataset ✓ — Use an existing dataset to train your model

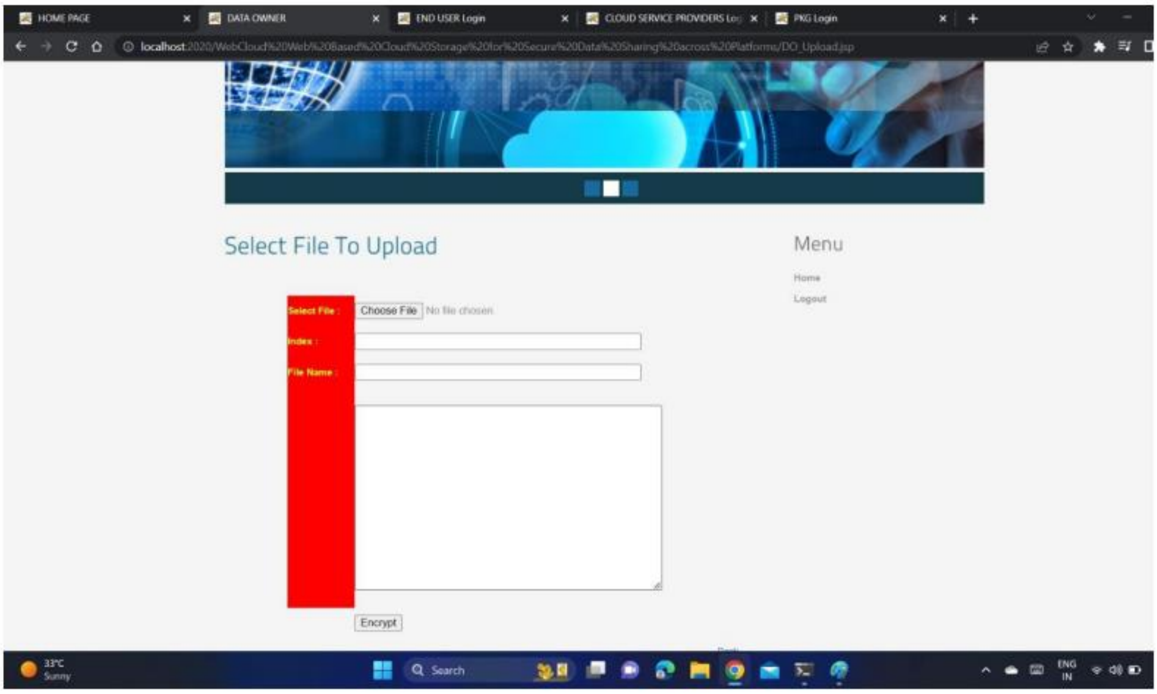
Create a New Dataset — Create a new dataset in Data Labeling Service to train your model (redirects to new page)

Data Source: ● Data Labeling Service ○ Object Storage

The chosen dataset must contain a minimum of 10 images. Create and choose a dataset with appropriate format of schema. Please read this for accepted schema formats (redirects to new page)

Choose a dataset in ocastest (root) (Change Compartment): indoor

Figure 4: UI for Custom Model Testing and Training


HOME PAGE
DATA OWNER
END USER Login
CLOUD SERVICE PROVIDERS Lo
PKG Login
localhost:2020/WebCloud%20Web%20Based%20Cloud%20Storage%20for%20Secure%20Data%20Sharing%20across%20Platforms/DO_Upload.jsp
Menu
Home
Logout
Choose File
Encrypt
33°C
Sunny
Search
ENG
IN

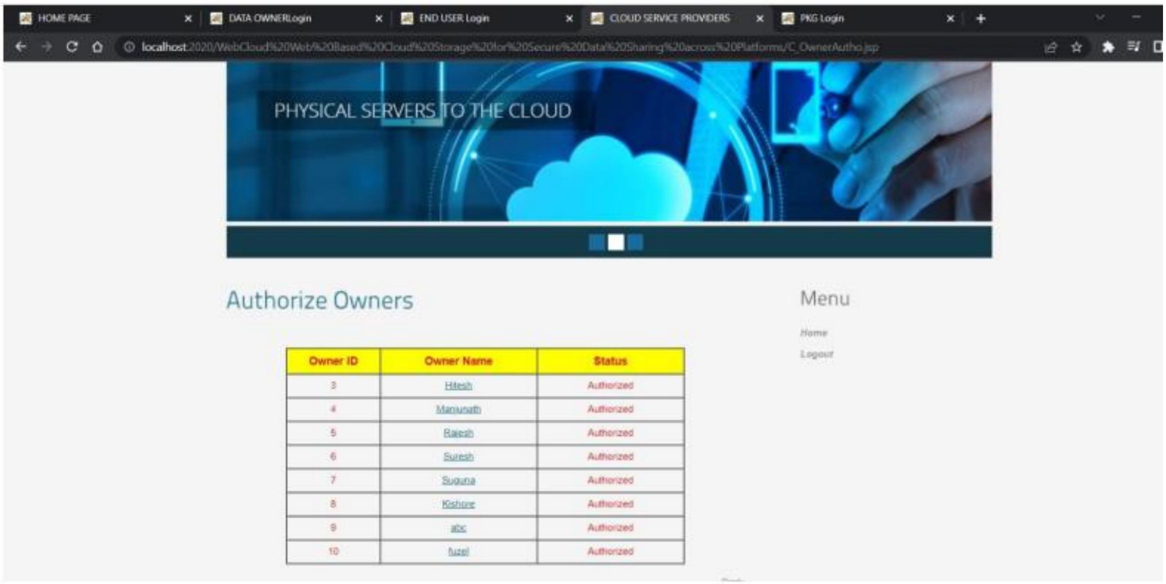
Select File To Upload

Select File : No file chosen

Index :

File Name :

Fig 5: Upload Files To Cloud

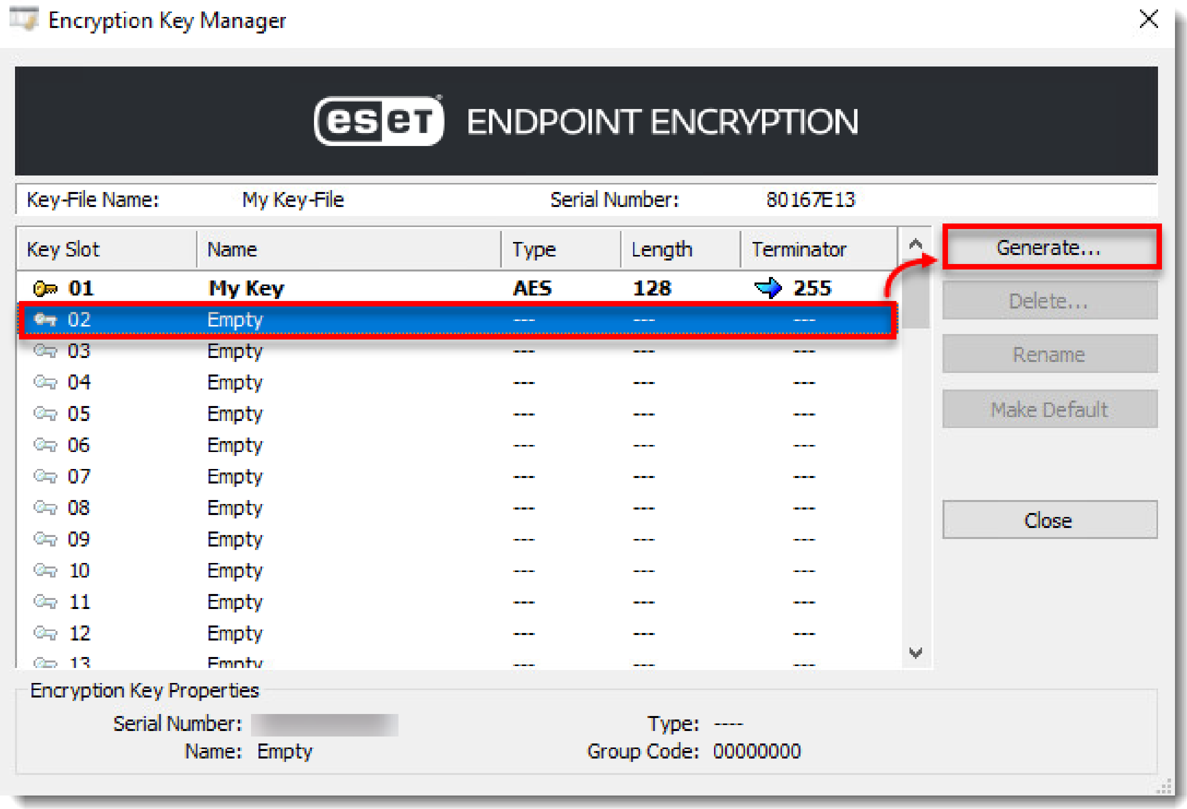


HOME PAGE
DATA OWNERLogin
END USER Login
CLOUD SERVICE PROVIDERS
PKG Login
localhost:2020/WebCloud%20Web%20Based%20Cloud%20Storage%20for%20Secure%20Data%20Sharing%20across%20Platforms/C_OwnerAutho.jsp
PHYSICAL SERVERS TO THE CLOUD
Menu
Home
Logout

Authorize Owners

Owner ID	Owner Name	Status
3	Hitesh	Authorized
4	Manjunath	Authorized
5	Rajesh	Authorized
6	Suresh	Authorized
7	Suguna	Authorized
8	Kishore	Authorized
9	abc	Authorized
10	fuzel	Authorized

Fig 6: Authorize Data Owners



Key-File Name: My Key-File Serial Number: 80167E13

Key Slot	Name	Type	Length	Terminator
01	My Key	AES	128	255
02	Empty	---	---	---
03	Empty	---	---	---
04	Empty	---	---	---
05	Empty	---	---	---
06	Empty	---	---	---
07	Empty	---	---	---
08	Empty	---	---	---
09	Empty	---	---	---
10	Empty	---	---	---
11	Empty	---	---	---
12	Empty	---	---	---
13	Empty	---	---	---

Encryption Key Properties

Serial Number: [redacted] Type: ----

Name: Empty Group Code: 00000000

Fig 7: Generating Key For Encryption

CONCLUSION

We propose Web Cloud, a web-based environment where users may perform cryptography solely in their browsers, as an efficient client-side encryption solution for public cloud storage. Web Cloud's security is evaluated, and we put it into practice by utilising our own cloud. Additionally, we do a comprehensive performance evaluation of Web Cloud. We proved the viability of our solution by analysing the experimental findings. Curiously, a specific CP-ABKEM scheme is intrinsic to the Web-Cloud architecture and finds utility in many other contexts.

REFERENCES

1. Mell P, Grance T (2012) The NIST definition of cloud computing. NIST Spec Publ 800:145. National Institute of Standards and Technology, U.S. Department of Commerce. Source: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Accessed on Oct 2012

2. Wikipedia definition of Cloud computing (2012). Source: http://en.wikipedia.org/wiki/Cloud_ computing. Accessed on Oct 2012

3. Healey M (2010) Why IT needs to push data sharing efforts. Information Week. Source: http:// www.informationweek.com/services/integration/why-it-needs-to-push-data-sharing-effort/ 225700544. Accessed on Oct 2012

4. Gellin A (2012) Facebook's benefits make it worthwhile. Buffalo News.

5. Riley DA (2010) Using google wave and docs for group collaboration. Library Hi Tech News.

6. Wu R (2012) Secure sharing of electronic medical records in cloud computing. Arizona State University, ProQuest Dissertations and Theses

7. Pandey S, VoorsluysW, Niu S, Khandoker A, Buyya R (2012) An autonomic cloud environment for hosting ECG data analysis services. Future Gener Comput Syst 28(1):147–154

8. Bender D (2012) Privacy and security issues in cloud computing. Comput Internet Lawyer 1–15.

9. Judith H, Robin B, Marcia K, Fern H (2009) Cloud computing for dummies. For Dummies.

10. SeongHan S, Kobara K, Imai H (2011) A secure public cloud storage system. International conference on internet technology and secured transactions(ICITST) 2011, pp 103–109.

11. A. K. Singh and I. Gupta, "Online information leaker identification scheme for secure data sharing," Multimedia Tools Appl., vol. 79, no. 41, pp. 31165–31182, Nov. 2020.

12. E. Zaghloul, K. Zhou, and J. Ren, "P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing," IEEE Trans. Big Data, vol. 6, no. 4, pp. 804–815, Dec. 2020.

13. I. Gupta and A. K. Singh, "GUIM-SMD: Guilty user identification model using summation matrix-based distribution," IET Inf. Secur., vol. 14, no. 6, pp. 773–782, Nov. 2020.

14. W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331–346, Feb. 2019.

15. I. Gupta and A. K. Singh, "An integrated approach for data leaker detection in cloud environment," J. Inf. Sci. Eng., vol. 36, no. 5, pp. 993–1005, Sep. 2020.