WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Robust Protection Plug-in for Cloud Storage

Karthikeyan N[1], Mohamed Hashif H[1], Santhosh M[1],Dr. Anandraj P[2]

Department of Computer Science and Business Systems, E.G.S Pillay Engineering College, Nagapattinam, Tamilnadu, India

A B S T R A C T

With the increasing usage of cloud storage for personal and public, protection issues have turn out to be paramount. By giving protection from unauthorized access or security of the data then Client-side encryption is a common and better solution for ensuring end users that a third-party user cannot access the uploading data. This project is a browser extension designed to protect the data by using of encrypt the data. It operates with the aid of encrypting system using AES-256 encryption, ensuring that the user can encrypt and decrypt the data and get admission to the information. This extension model connects with cloud storage systems via API authentication and allowing customers to upload and retrieve encrypted files efficiently. It also helps batch processing permitting a couple of documents to be encrypted and uploaded concurrently

Keywords: Cloud security, end-to-end encryption, AES-256 encryption, data privacy, cloud storage protection, secure file upload, browser extension and API authentication.

INTRODUCTION

Cloud computing nowadays a big issue in this current development situation all over the world.Cloud computing is a business model that helps all type of organization like small, medium and as well as large organization to use the infrastructure with fast access and support.By the definition of National Institute of Standard and Technology (NIST), cloud computing is a model for empowering omnipresent, advantageous, on-request arrange access to a common pool of configurable registering assets (e.g., networks, servers, capacity, applications, and administrations) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].About 60% of the business people think that cloud is the best place to stock content and rest of the people, general people, think that cloud is the best place to stock data and retrieve the data virtually [2].

Although cloud computing has many benefits, there are still several barriers preventing its widespread use.Since clients and organizations data is combined on a platform which is accessible to everybody as they have given ownership of their information to a third party.As a result, there is a chance that someone who is not permitted will retrieve it resulting in data breaches [3].To protecting such vulnerability to the cloud data, this proposed model can improve the cloud data security by using of Client-side encryption.The data is encrypted by client-side which means that the only user can holds the encryption key and also decrypt and access the data.

It cannot give access like viewing the user data to cloud providers and unauthorized entities.It does not store encryption key on servers and this provides high security to the data.It is a browser extension that is mainly focus for end-to-end encryption and allowing users to encrypt files before uploading to the cloud storage and avoiding the third-party access.It integrates with cloud storage services via API authentication and it has a user-friendly drag-and-drop interface, batch encryption for upload multiple files.

LITERATURE SURVEY

A Novel Approach for Client Side Encryption in Cloud Computing-2019:

In this paper, they approach a Client-side encryption to give strong data protection and Client-side encryption is a common and better solution for ensuring end users that a third-party user cannot access the uploading data. Cloud service providers maintain different techniques to protect data but like google drive, most of the company do not use client- side encryption. It has a way to protect the data from hacking or losing when storing or uploading the data in the cloud server using the combination of Advanced Encryption Standard and Secure Hash Algorithm with Initial Vector.

Decentralized Network for Cloud Storage-2023:

This paper show case the decentralizing the cloud, which is currently a centralized entity, the authors attempt to improve cloud security. It is possible to solve these problems by deploying a decentralized cloud. Client software encrypts, fragments data, and then a client engine distributes the data among a number of hosting nodes (servers) spread throughout the world. As a result, the user has complete ownership of his data. In their study, the authors found that decentralizing cloud solved most of the problems of centralized cloud, since it increases the security of data by fragmenting and encrypting fragments.

Cloud Data Security using Hybrid Algorithm-2023:

In this paper, they propose a multilevel cryptography-based safety solution for cloud computing is designed. This paradigm is a combination of asymmetric & symmetric key cryptography techniques. The RSA and Data Encryption Standard (DES) are used in this proposed methodology to provide several levels of encoding and decoding at the sender & recipient side.

Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security-2023:

This research paper proposed solution encompasses a two-phase approach. In the first phase, dynamic Advanced Encryption Standard (AES) keys are generated, ensuring each file's encryption with a unique and ever-changing key. This approach significantly enhances file-level security, curtailing an attacker's ability to decrypt multiple files even if a key is compromised. The second phase introduces blockchain technology, where keys are securely stored with accompanying metadata, bolstering security and data integrity. Elliptic Curve Cryptography (ECC) public key encryption enhances security during transmission and storage, while also facilitating secure file sharing.

PROBLEM STATEMENT

Given that cloud computing stands as one of the pervasive technologies within the Information Technology (IT) sector, it presents a set of advantages which are: encompassing virtualization, extensive scalability, cost-efficiency, remote data processing, and the provision of on-demand clients centric sharing services [1].Additionally, traditional cloud storage have the lack of true end-to-end encryption which means that if the data is encrypted, the provider can still decrypt and access the information.This creates a vast security loophole to the users data and does not give privacy to the user data(confidential, financial and personally identifiable information (PII)).Cyberattacks, unauthorized government surveillance, data breaches and policy changes by cloud providers further increasing the risk of data exposure. Many existing encryption solutions are too complex to handle for average users and also lack of cloud integration and also require manual encryption processes that decrease the workflow.

There is a clear objective to the problem statement by giving a user-friendly with automated and highly secure encryption model that ensures only the user has access to their encrypted files without any storage of encryption keys. This project aims to bridge this security gap by providing easy of access and independent encryption mechanism. It provides that users contain full control over their encryption keys to protecting their files from unauthorized access.

PROPOSED DESIGN

This project is mainly focus on security, prevent unauthorized access or third-party access, and **user-friendly browser extension** that provides **end-to-end encryption** for files before it should upload to cloud storage services. The extension focuses on client-side encryption (CSE) and it gives the entire control to the user and it cannot be viewed or stored the keys to the third-party entities.It determine the eliminating the risk of unauthorized access.

System Architecture

The proposed design follows on modular architecture with the following key components:

I. User Interface (UI)

The extension have features such as simple and unique interface and it can also give users to encrypt their data and also decrypt their data.This User Interface can also directly uploading the encrypted files to the cloud storage.It can have input for a master password for encryption, view progress indicators, and receive notifications for errors or successful uploads.The UI is mainly designed for simple accessibility and also understandable for average users without requiring technical expertise.

II. Encryption Module

The encryption module contains data privacy and security by implementing AES-256 GCM encryption and decryption, Initialization vector (IV), PBKDF2 (Password-Based Key Derivation Function 2). It also enabling users for encrypted files seamlessly.The model can give access the only user to handle the encryption key. Additionally, file metadata is encrypted to prevent information leakage and encryption keys are derived from the user's master password, ensuring strong protection.

III. Cloud Integration Module

This model connects to Google Drive using API authentication (OAuth 2.0) to securely upload encrypted files. Unlike traditional cloud storage methods, this module should upload only the encrypted data is transmitted, preventing unauthorized access. The encrypted file should upload directly from the extension model.

IV. Secure File Management

To optimize security and efficiency,this model implements batch encryption while uploading and it should have multiple files to be processed simultaneously. The system also includes an automatic cleanup mechanism which deletes temporary encrypted files from the local device after a successful upload. Additionally, **checksum validation** is used to verify file integrity and detect unauthorized modifications.

V. Security Features

This model have the multiple security mechanism and Zero-knowledge encryption.It guarantees that encryption keys are never stored or shared or access by any third-party access. The system is also used **tamper detection** to prevent unauthorized modifications.

METHODOLOGY

The methodology of this browser extension makes a structured approach to designing, developing and implementing a client-side encryption system for cloud storage.It used to make that users can encrypt their files before uploading them, maintaining complete control over their sensitive data. It plays a vital role in ensuring the data remains secure and cannot view by unauthorized person. The extension determines that the strong encryption (AES-256(GCM)), cloud integration and automated file handling to enhance security while minimizing user effort.

Fig-1 User Interface (UI)

The above figure 1 representing the browser extension interface and it give the listing of the selecting files and indicating the strength of the password and encrypt by using of AES-256(GCM) and encrypt button used to download on the system storage and upload button used to directly uploading to the cloud storage and decrypt button used to decrypt or retrieve the original data from encrypted file with the password or encrypted key.

Use case diagram:

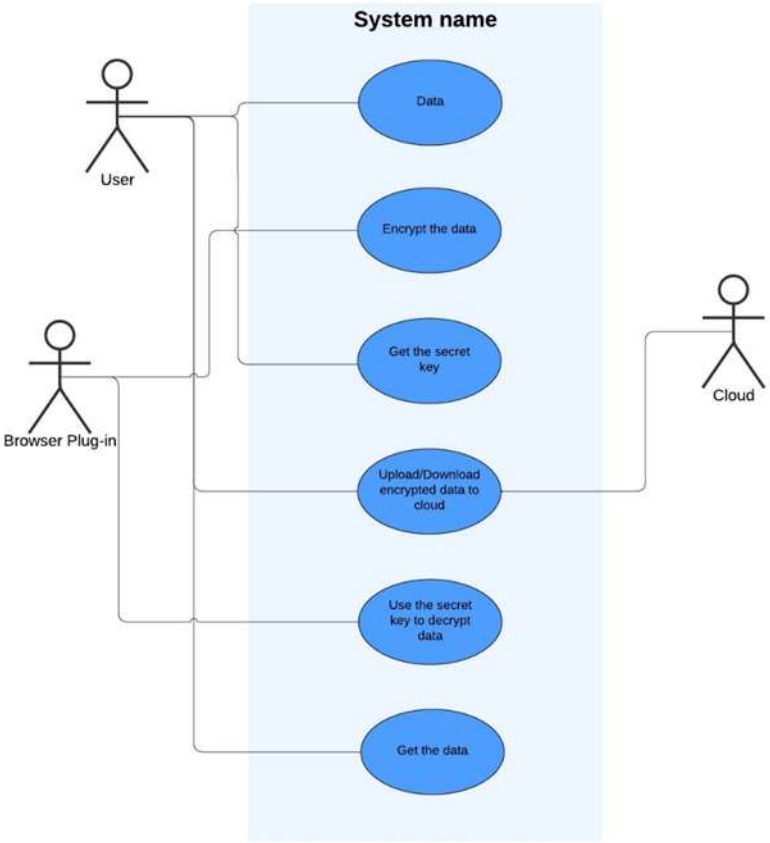

Fig-2 use case diagram

The above use case diagram defines the encryption and decryption process and also the uploading process of the extension. The user starts to setting a strong Password by indicating the strength for encryption and decryption purposes. Once set, they can select files to Encrypt using the AES-256 encryption algorithm. After encryption then the files are uploaded to the selected cloud storage. The extension communicates with cloud APIs, utilizing authentication for secure login to the cloud services.

System requirement:

HARDWARE REQUIREMENT

- **Processor**: Intel Core i3 or higher
- **RAM**: 4 GB or higher
- **Hard Disk**: 500 GB

SOFTWARE REQUIREMENTS

- **Operating System**: Windows 10/11, Mac OS, Linux
- **Browser** : Any browser that support extension
- **Cloud service** : google drive
- **Compression and Packaging Tools** : winrar, 7zip
- **Programming language**: HTML, CSS, Javascript

Working

The below flowchart represents the workflow of the extension and it is a client-side encryption before uploading files to cloud storage and provides secure decryption upon retrieval.The process starts with the user interacting through a web browser and the extension must installed to the browser.The user should have two primary options: selecting a raw file for encryption or choosing an already encrypted file for decryption.The user should give the raw or

original file for encryption and also give the valid strong password then it should ready for encryption.Once the data encrypted then the file is securely uploaded to cloud storage with the help of the extension and it gives that the user can decrypt it in the future.On the other hand, if the user selects an encrypted file then they must enter the correct or valid decryption password to restore the original file.The extension that have the correct encrypted file and the valid password then it should give decrption process and the file is decrypted and made available for download.It is the user workflow for the extension and it shows that easy to process,userfriendly, effective way of encryption the data. It have the simple process with the strong encryption system and also upload the encrypted data directly from the extension.

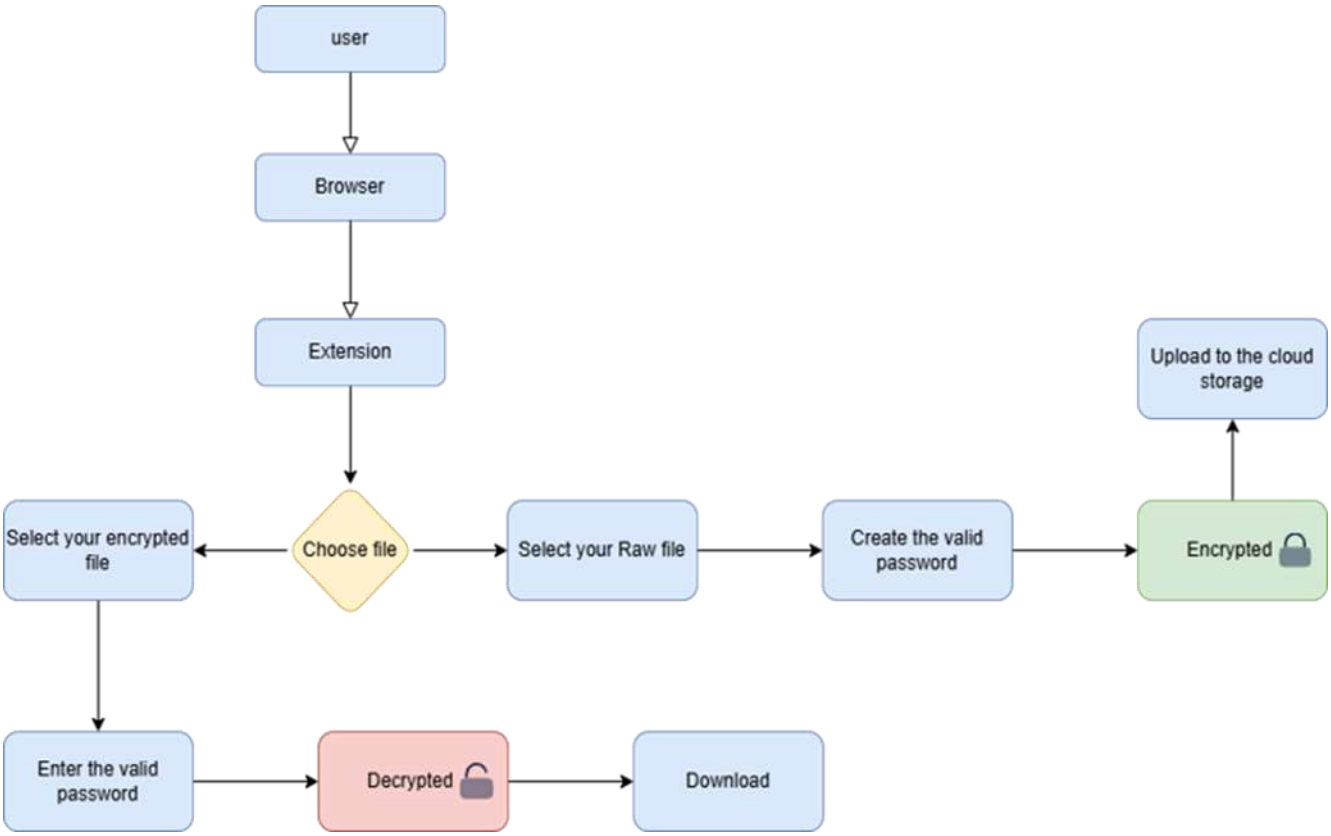

Fig-3 Flowchart

Conclusion

In this paper, the proposed design is used for stable and user-friendly solution for encrypting files before upload it to cloud storage.By implementing AES-256 encryption and OAuth 2.0 authentication to the extension and it need to keep that user have complete control over their encyption and it also preventing the unauthorized access .The effective and efficiency integration with extension offers that easy access to the cloud service and it also coupled with an automated encryption and decryption system.It makes this extension a preference to the users for prioritizing data security.The extension has effectively addresses the risks of data breaches, unauthorized access, and third-party vulnerabilities by by enforcing a zero-knowledge encryption method,where the user only holds the decryption key. Additionally, the extension should contains batch encryption, drag-and-drop support and automatic file cleanup to improve the usability while maintaining strong security measures.It establishes a strong foundation for secure cloud storage**,** ensuring data integrity, confidentiality, and accessibility.

As the demand for cloud computing, this extension will have several enhancements and feature upgrades to improve its functionality and security. Some of the updates include to improve the extension: Multi-Cloud Support,Mobile Compatibility, Enhanced Key Management–Introducing passwordless authentication methods like biometric encryption or hardware security keys (YubiKey, TPM integration) for better security. Security Audits and AI-Based Threat Detection will Implementing for AI-powered threat detection to monitor unusual activity and improve real-time security auditing.

REFERENCE

[1] W. A. S. Aldossary, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, no. 4, pp. 485-498, 2016.

[2] D. P. K. V. S. S. Bhukya, "Data Security in Cloud computing and Outsourced Databases," Data Security in Cloud computing and Outsourced Databases," International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), no. 5, pp. 2458-2462, 2016.

[3] Manmeet Kaur, Athira B Kaimal, Jasminder Kaur Sandhu, Rakesh Sahu, "Cloud Data Security using Hybrid Algorithm", 2023 3rd International Conference on Smart Data Intelligence (ICSMDI)

[4] Md. Mahidul Islam, Md. Zahid Hasan, Rifat Ali Shaon, "A Novel Approach for Client Side Encryption in Cloud Computing ", 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 7-9 February, 2019.

[5] Chirag N, Kshitij K, Gaurav Gupta, "Decentralized Network for Cloud Storage", 2023 2nd Edition of IEEE Delhi Section Flagship Conference (DELCON)

[6] Mohammed y. shakor, Mustafa ibrahim khaleel, Mejdl safran, Sultan alfarhood, and Michelle zhu "Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security",

[7] M. a. D. D.Vasumathi, "Query based computations on encrypted data through homomorphic encryption in cloud computing security," International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 3820-3825, 2016.

[8] M. Shah, M. Shaikh, V. Mishra, and G. Tuscano, "Decentralized cloud storage using blockchain," 4th International Conference on Trends in Electronics and Informatics, pp. 384-389, 2020.

[9] D. s. Tania Gaura, "A Secure and Efficient Client-Side Encryption Scheme in Cloud Computing," I.J. Wireless and Microwave Technologies, vol. 1, pp. 23-33, 2016.

[10] Tresorit.com. (2019). End-to-End Encrypted Cloud Storage for Businesses | Tresorit. [online] Available at: https://tresorit.com [Accessed 15 Jan. 2019].

[11] AL-Museelem Waleed, Li Chunlin, "User Privacy and Security in Cloud Computing", in International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352.

[12] Adnaan Arbaaz Ahmed, Dr.M.I. Thariq Hussan, "Cloud Computing: Study of Security Issues and Research Challenges" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, ISSN: 2278 – 1323 (2018).