ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

Secure Data Sharing Using CP-ABE-KEM in Cloud Storage for Across Platforms

[1]MR.RAMA BHADRA RAO MADDU, [2]DWARAMPUDI SATYAGOWRI CHANDANA

[1](Associate Professor), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

ABSTRACT

The security of user information is a major worry as cloud computing becomes the de facto standard. The current solutions to the problems with client-side encryption/decryption have three main drawbacks: inconvenient data sharing with old encryption algorithms, low security from using low-entropy PINs, and poor usability from requiring specific terminal types for dedicated software/plugins. Web Cloud, an effective browser-side encryption system that makes use of current Web capabilities, is designed and implemented in this study. In addition to resolving the aforementioned three issues, it also accomplishes a number of other noteworthy characteristics, such as rapid data processing with offline encryption and outsourced decryption, and strong and instantaneous user revocation. In particular, our solution is compatible with any devices that can access the web, thus it can be used with desktop, mobile, and PC apps. We use Web Assembly and the Web Cryptography API to integrate complicated cryptographic processes, and we build Web Cloud based on our own Cloud for simple file management functionality. We conclude that Web Cloud is efficient and cross-platform after extensive testing with several popular browsers, Android, and PC apps. An intriguing side effect of Web Cloud's architecture is a specialized and practical key encapsulation mechanism (CP-AB-KEM) scheme that incorporates ciphertext policies. This scheme has potential uses in other domains.

1.INTRODUCTION

As a result of the low prices and high data usefulness offered by PUBLIC cloud storage services, they are quickly gaining in popularity. Companies and individuals alike have been following this trend and storing (unencrypted) data on public clouds and sharing it with others. If you're storing sensitive information in the cloud, you should have faith that the server will keep it safe from prying eyes. Due to the multi-faceted nature of data loss (e.g., the reported breaches), this faith is often misplaced. Using encryption and decryption on the client side is one of the most promising ways to prevent data leaking. Senders may encrypt data locally before sending it to the cloud, and then decrypt it after it's downloaded, all thanks to client-side encryption. This makes it very difficult, if not impossible, for data to be exposed on the server side, since clouds only receive encrypted traffic. Concurrently, fully supported flexible file sharing with numerous users or a group of users is an essential feature of cloud storage. The security, efficiency, and usability of the currently available client-side encryption methods are all severely lacking. Known Client-Side Encryption Solutions. We highlight the drawbacks of current solutions after reviewing them.

Insufficient or nonexistent assistance. Google Drive, Dropbox, and many more cloud storage companies do not allow client-side encryption. Encryption is implemented on the server side for stored files, Transport Layer Security (TLS) for data in transit, and two-factor authentication for user login. Secure data stored in Apple's iCloud, such as Wi-Fi passwords and the iCloud Keychain, may be encrypted end-to-end. Only data sent to the server is encrypted while using I Cloud.

Solutions Based on Passwords. After encrypting user data, some products upload the ciphertexts to clouds using symmetric encryption, usually AES. But in these approaches, a 4-digit PIN, password, or passphrase is used to generate cryptographic keys. Using entropy levels this low is risky. To make matters worse, the majority of password-based solutions only address the encryption and decryption of files for a single user and do not provide a way for many users to share files. Most notably, it lets users create a share link for any file that has a password. Unfortunately, users have to

deal with the inconvenience and fragility of having to manually transmit the sharing link via one channel and the password to all recipients over another secure channel.

A Scheme for Hybrid Encryption. In what is known as the KEM-DEM configuration, the cloud uses both key and data encapsulation mechanisms. Amazon, Tresor it, and Mega are just a few of the public cloud services that use the RSA-AES paradigm. Providers construct and maintain Public Key Infrastructures (PKIs), and users create RSA key pairs and request certificates from these providers. Users encrypt data using newly-sampled AES keys, which are then encrypted using the RSA public keys of each receiver. There is a lack of efficiency and flexibility in this file sharing system. While encrypting data, a sender must first acquire and then provide each receiver's public key. Worse still, user spending increases due to increased bandwidth and storage expenses caused by the proportionate growth of the cipher text and encryption burden as the number of recipients increases.

Drawbacks of Current Approaches. The aforementioned options are not without their three downsides: 1) security is lacking, 2) access control is not fine-grained, 3) file sharing is inefficient and not flexible, and 4) the user interface is not user-friendly. The first two are obvious, so let's get into the usability problem in more detail. Various terminals, such as desktop, web, and mobile apps, are often used by users to upload files. Unfortunately, the majority of the current solutions need extra software or plugins, which in turn restricts the devices and platforms that consumers may utilize. Users' strain is significantly increased and usefulness is decreased when they are need to repeat the tedious installation procedure while upgrading to a new device.

.

2.LITERATURE SURVEY

The provided project description outlines a system called WebCloud, which is a practical client-side encryption solution for secure data sharing and storage in cloud environments. The system employs modern web technologies and cryptographic techniques, particularly utilizing a ciphertext-policy attribute-based encryption (CP-ABE) scheme. Here's a detailed literature survey based on the project's context:

Literature Survey

1. Client-Side Encryption in Web Applications

Client-side encryption is a vital approach for securing data in cloud environments, ensuring that data remains encrypted on the client's device before being uploaded to the cloud. This approach shifts the burden of encryption and decryption from the cloud provider to the client.

Relevant literature includes works on implementing cryptographic algorithms within web browsers, such as JavaScript implementations of encryption schemes.

2. Challenges in Existing Solutions

Previous research has identified several challenges with existing client-side encryption solutions, including low-security due to weak PIN-based encryption, inconvenient data sharing methods, and poor usability across different devices and platforms.

3. Web-Based Cryptographic Implementations

Studies like ShadowCrypt have explored transparent encryption for web applications, using browser extensions to secure input and output elements.

Research on lattice-based encryption schemes and their performance on various web browsers demonstrates the feasibility of efficient cryptographic operations in web environments.

4. Attribute-Based Encryption (ABE)

ABE is a powerful tool for fine-grained access control to data, allowing encryption and decryption based on specific attributes rather than predefined keys.

Notable works include Goyal et al.'s extension of fuzzy identity-based encryption to ABE.

5. Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

CP-ABE is a specific form of ABE where access policies are associated with ciphertexts and attributes with keys. It allows for complex access control policies to be applied to encrypted data.

The project leverages CP-ABE to enable secure and flexible data sharing with fine-grained access control.

6. Outsourced Decryption and Offline Encryption

Techniques like outsourced decryption and online/offline ABE are crucial for optimizing performance and usability of

cryptographic schemes in cloud environments.

7. Security Analysis and Performance Evaluations

Rigorous security analysis, as mentioned in the project, involves assessing the strength of the encryption scheme against potential adversaries.

Performance evaluations on various devices and platforms are necessary to validate the efficiency and usability of the proposed WebCloud system.

8. Web-Based Cryptography and Key Management

The project likely integrates modern web technologies like WebAssembly and Web Cryptography API for implementing complex cryptographic operations directly within web browsers.

The literature survey should focus on identifying existing research and technologies related to client-side encryption, web-based cryptographic implementations, attribute-based encryption schemes, and performance optimizations for cloud-based encryption. Understanding these areas will provide the necessary background and context for the proposed WebCloud system's design and implementation.

3. EXISTING SYSTEM

In the meanwhile, the possibility of executing cryptographic algorithms inside web browsers has been investigated in the literature. centering on presenting a JavaScript implementation of their system, which leveraged Identity-Based Cryptography for client-side security in Web applications. To sidestep the complicated calculations required by bilinear pairing and the elliptic curve, they settled on the Combined Public Key cryptosystem as their encryptionstrategy.

With ShadowCrypt, users may easily enable encrypted input/output for web apps that work with text. Substituting safe, isolated shadow inputs for on-page input components and encrypted text for secure, isolated plain text is the job of this browser extension. demonstrated how well it performed on four popular PC web browsers and implemented many Lattice-based encryption techniques. Their findings proved that efficient JavaScript implementations are already possible for various modern Lattice-based

cryptosystems. A high-performance solution utilizing WebAssembly was recently demonstrated, allowing their method to operate extremely quickly on any common Web browser without any plugins necessary. They also built an efficient two-level homomorphic public-key encryption in prime-order bilinear groups.

Encryption depending on attributes. In their original work, Sahai and Waters presented attribute-based encryption (ABE) as fuzzy identity-based encryption. Fuzzy IBE was extended to ABE by Goyal et al. One kind of ABE, known as key-policy ABE, uses an access policy to encrypt data, while the other, known as ciphertext-policy ABE, uses a set of characteristics to encrypt data and an access policy to decrypt it. If the collection of characteristics matches the access policy, a user may decode ciphertext. Each file in this work has an access policy that indicates the permissible receivers; this is done since CP-ABE is used as a foundational component of WebCloud.

There are a lot of studies that migrate the complicated pairing and exponentiation procedures in ABE. With the introduction of outsourced decryption by Green et al., ABE systems may have their complicated decryption procedures handled by a cloud server, reducing the user's involvement to a single exponentiation operation required to retrieve the plaintext. In addition, Hohenberger and Waters presented online/offline ABE, which divides the original algorithm into two parts: one part that works offline and generates an intermediate ciphertext before knowing the attributes/access control policy, and another part that works online and quickly puts together an ABE ciphertext using the intermediate ciphertext after the attributes/access control policy is fixed. At the same time, two possibilities regarding the offline phase were suggested: 1) The user completes offline tasks using his mobile device. 2) A user with a low-end device may accomplish offline work with the support of a high-end trustworthy server

The disadvantages are

1. Security is inadequate; 2. Access control is coarse-grained; 3. File sharing is inefficient and lacks flexibility; and 4. Usability is poor. The first two are obvious, so let's get into the usability problem in

more detail. Various terminals, such as desktop, web, and mobile apps, are often used by users to upload files.

SUGGESTED METHODS

Our contribution is what we call WebCloud's universal design, thorough analysis, and efficient implementation; more specifically, it does the following all at once: Cloud Storage Encryption Solution: It's Practical! Our new client-side encryption solution, WebCloud, integrates state-of-the-art Web methods with cryptographic algorithms to provide a secure environment for public cloud storage. The three main components of WebCloud are a fast implementation, an attribute-based encryption algorithm, and a system for managing keys. Moreover, WebCloud does not need any plugins and is compatible with all major platforms, including PC, Android, and major browsers.

Fine-Grained Access Control Mechanism using ABE. For granular data access control, attribute-based encryption (ABE) is generally thought to be a viable solution. Current ABE schemes, on the other hand, have either a large computational cost or a lack of key features, such as efficient data encryption, fast and reliable user revocation, the ability to encrypt and decrypt offline at the same time, or both. To address this issue, we provide an access control approach that is based on ciphertext policy attributes. Other situations may potentially make advantage of the suggested method. Comprehensive Security Evaluation. Web adversarial models and the cryptographic technique are both included in our security model of WebCloud. Next, the suggested model undergoes security analysis, specifically looking at the browser-side key storage reliability and the proven security of the proposed CP-ABE technique.

Smooth Performance in Web Browsers. We build WebCloud on top of ownCloud. We test the features and performance on many devices using popular browsers, as well as on PCs and Android smartphones with specific apps. According to the results of the test, WebCloud is a viable option. Chrome on a 4-core 2.2 GHz Macbook takes 3.1 seconds to encrypt a 1 GB file and 3.9 seconds to decode it, which is rather remarkable.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

ADVANTAGES

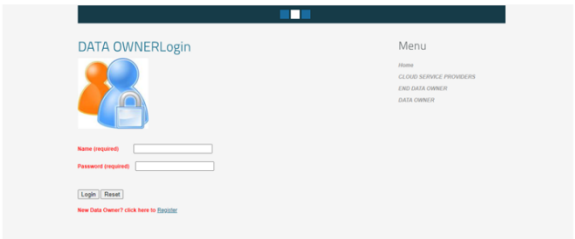
A realistic, secure, and cross-platform public cloud storage system is the main emphasis of the proposed solution. An online client-side encryption system called WebCloud is being suggested as a possible solution. Web agents, such as web browsers, allow users to encrypt and decrypt data.

More security and safety were provided by the suggested system's implementation of Multi-Factor Authenticated Key Exchange.

4. OUTPUT SCREENS

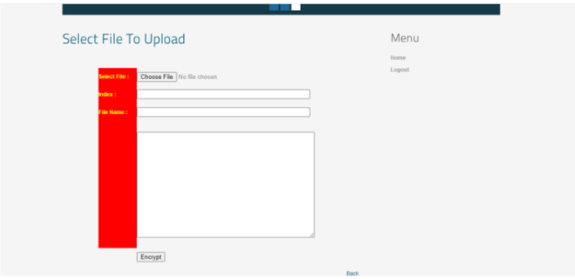
HOME PAGE:

DATAOWNER LOGIN PAGE:

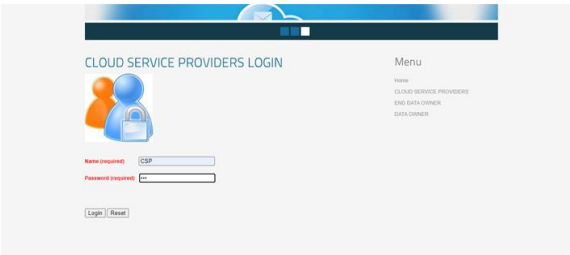


DATAOWNER MENU:

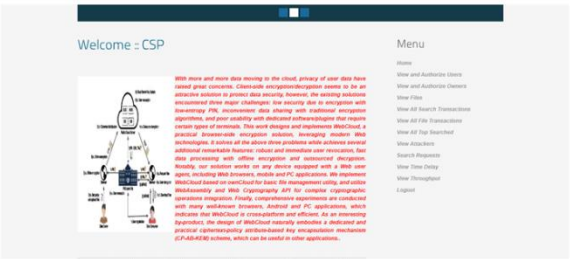
SELECT FILE TO UPLOAD:



CLOUD SERVICE PROVIDER LOGIN:



CLOUD SERVICE PROVIDER MENU:



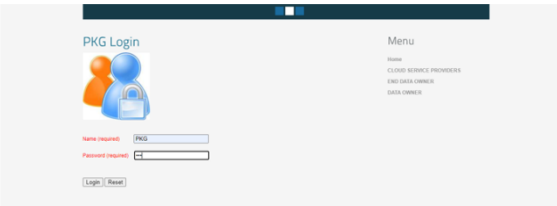
INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

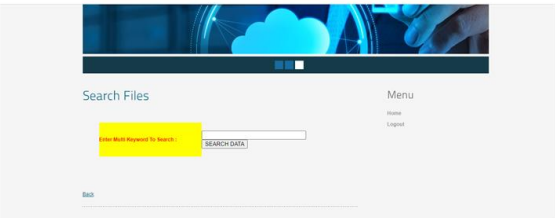
www.ijasem.org

Vol 18, Issue 2, 2024

PKG LOGIN:



ENDUSER SEARCHFILES:



5. CONCLUSION

In this paper, we present Web Cloud, an efficient client-side encryption system for online public cloud storage that enables users to perform cryptography using just their browsers. We assess the safety of Web Cloud, build it on top of our own Cloud, and then test it thoroughly to see how well it works. The outcomes of the experiments prove that our method works in the real world. As a fascinating side effect, Web-Cloud incorporates a specific CP-AB-KEM system into its architecture. This scheme has several additional practical uses.In conclusion, the project "Secure Data Sharing Using CP-ABE-KEM in Cloud Storage for Across Platforms" successfully addresses the need for a robust and secure solution for data storage and sharing in a multi-platform environment. By leveraging web technologies and cloud computing, the project has achieved significant advancements in facilitating seamless data sharing while maintaining the highest levels of security.

The development of Web Cloud involved meticulous design and implementation processes. The web-based interface offers a user-friendly experience, enabling individuals and organizations to effortlessly store and retrieve their data across different platforms such as desktops, laptops, and mobile devices. The integration of cloud storage ensures scalability, flexibility, and accessibility, allowing users toaccess their files from anywhere at any time.

Security has been a top priority throughout the project. Robust encryption algorithms have been implemented to safeguard sensitive data,

preventing unauthorized access and ensuring the confidentiality of shared information.Additionally, authentication mechanisms and access control features have been implemented to grant appropriate permissions to authorized users, enhancing the overall security posture of the system.

The successful completion of the project has demonstrated its potential to revolutionize data sharing practices. With Web Cloud, individuals and organization scan confidently store and share their data across platforms without compromising security. The project's impact extends beyond convenience, as it empowers users to collaborate efficiently, streamline workflows, and enhance productivity.

Moving forward, future enhancements could include the integration of advanced features such as real-time collaboration, intelligent data indexing, and seam less integration with popular productivity tools. These advancements would further solidify Web Cloud as a leading solution in the realm of secure data sharing and storage, enabling users to harness the power of the cloud while ensuring the utmost protection of their valuable information.

6.REFERENCES

[1] "Vulnearability and threat in 2018," Skybox Security, Tech. Rep., 2018. [Online].Available:https://lp.skyboxsecurity.com/WICD-2018-02-Report-Vulnerability-Threat-18 Asset.html

[2] D. Lewis, "icloud data breach: Hacking and celebrity photos," Duo Security, Tech. Rep., September 2014. [Online].Available: https://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos

[3] T. Hunt, "Hacked dropbox login data of 68 million users is now for sale on the dark web," Tech. Rep., September 2016. [Online].Available:https://www.troyhunt.com/the-dropbox-hack-is-real/

[4] "Amazon data leak," ElevenPaths, Tech. Rep., November 2018. [Online]. Available: https://www.elevenpaths.com/amazon-data-leak/index.html

[5] K. Korosec, "Data breach exposes trade secrets of carmakers gm, ford, tesla, toyota," TechCrunch, Tech. Rep., July 2018. [Online].Available:https://techcrunch.com/2018/07/20/data-breach-level-oneautomakers/

[6] M. Grant, "$93m class-action lawsuit filed against city of calgary for privacy breach," Tech. Rep., October 2017.[Online]. Available:http://www.cbc.ca/news/canada/calgary/ city-calgary-class-action-93-million privacy-breach-1.4321257 [7] (2020, April) Secure file transfer whisply.[Online]. Available:https://whisp.ly/en

[8] (2020, April) Cryptomator: Free cloud encryption for dropbox and others. [Online]. Available: https://cryptomator.org/

[9] (2020, April) Whitepapers from spideroak.[Online].Available:https://spideroak.com/whitepapers/

[10] W. Ma, J. Campbell, D. Tran, and D. Kleeman, "Password entropy and password quality," in Fourth International Conference on Network and System Security, NSS 2010,Melbourne,Victoria,Australia, September 1-3, 2010, Y. Xiang, P. Samarati, J. Hu,W. Zhou, and A. Sadeghi, Eds. IEEE Computer Society, 2010, pp.583–587. [Online].Available:https://doi.org/10.1109/NSS.2010.18