International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

WEBCLOUD: INTERNET LINKED CLOUD REPOSITORY FOR PROTECTED INFORMATION EXCHANGE ACROSS SYSTEM

Mrs. Khutaija Abid[1*], Dr Karunakar Reddy[2], Asra Begum[3]
[1]Assistant Professor, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
[2]Assistant Professor, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
[3]Assistant Professor, Department of IT, MVSR Engineering College, Hyderabad.
khutaija@lords.ac.in

Abstract— With the rapid migration of data to cloud platforms, ensuring the privacy and security of user information has become a critical challenge. While client-side encryption/decryption offers a promising solution, existing approaches suffer from three key limitations: weak protection due to low-entropy PIN-based encryption, inefficient data sharing with conventional cryptographic schemes, and limited usability requiring dedicated software or plugins. To address these issues, we propose *Web Cloud*, a practical browser-based encryption framework that leverages modern web technologies to provide secure, efficient, and cross-platform data protection. Web Cloud introduces robust features including immediate user revocation, high-speed processing through offline encryption, and outsourced decryption to reduce computational overhead. The system operates seamlessly on any device equipped with a web user agent—ranging from browsers to mobile and desktop applications—ensuring broad accessibility without additional plugins. Our implementation, built on *ownCloud* for file management and enhanced with Web Assembly and the Web Cryptography API, integrates complex cryptographic operations efficiently. Experimental evaluation across popular browsers, Android, and PC applications demonstrates that Web Cloud achieves both high performance and strong security. Additionally, the framework inherently supports a practical ciphertext-policy attribute-based key encapsulation mechanism (CP-AB-KEM), extending its applicability to diverse secure data sharing scenarios

Index Terms—Web-Based Cloud Storage, Secure Data Sharing, Cross-Platform Encryption/Decryption Solution, Attribute-Based Encryption.

I.INTRODUCTION

Public cloud storage services are gaining widespread popularity due to their cost-effectiveness and ease of use. This trend has led both individuals and organizations to increasingly store unencrypted data in the cloud and share it with others. However, entrusting the cloud with high-value or sensitive data raises serious security concerns, as the server must be trusted to prevent unauthorized disclosures—a trust that has often proven misplaced given the numerous reported data breaches [1]–[6]. A widely recognized countermeasure is client-side encryption and decryption, where data is encrypted locally before being uploaded to the cloud and decrypted only after being downloaded. This ensures that the cloud server only handles ciphertext, thereby reducing the risk of data leakage. At the same time, effective cloud storage systems must also support flexible file sharing among
multiple users or groups. Unfortunately, existing client-side encryption approaches present significant drawbacks, particularly regarding security, efficiency, and usability. This section reviews current client-side encryption methods and highlights their limitations. Limited support or no support. Many cloud storage providers, including Google Drive and Dropbox, do The authors are with the State Key Laboratory of Information Security, Institute of Information

Engineering, Chinese Academy of Sci ences, Beijing 100093, China, and the School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China. Email: sunshuzhou mahui, songzishuai, r-zhang@iie.ac.cn. (Shuzhou Sun and Hui Ma contributed equally to this paper and are labeled as co-frist authors. Corresponding Author: Rui Zhang.) not provide support for client-side encryption. They adopt server-side encryption for files stored, TLS for data at transit, and two-factor authentication for user authentication. Apple iCloud supports end-to end encryption for sensitive information, e.g., iCloud Keychain, Wi-Fi passwords. For other data uploaded to iCloud, only server encryption is adopted. Password-Based Solutions. Some products [7], [8], [9] use symmetric encryption (typically AES) to encrypt users' data and then upload cipher texts to clouds. However, in these schemes, the cryptographic keys are derived from a pass word/passphrase or even a 4-digit PIN. Relying on such low entropy is considered unsafe [10]. Worse still, most password-based solutions only deal with the case of single-user file encryption and decryption, and do not provide any file sharing mechanism. Notably, [7] allows users to generate a share link for each password-protected file. However, users must manually send the share link through one channel, and password to all receivers through another secure channel, which is inconvenient and brittle. Hybrid Encryption Scheme. The cloud adopts a key encapsulation mechanism (KEM) and a data encapsulation mechanism (DEM), so called the KEM-DEM setting. Many public cloud service providers, including Amazon [11], Tresorit [12], and Mega, adopt the RSA-AES paradigm. Users generate RSA key pairs and apply for certificates from the providers, who build and maintain a Public Key Infrastructures (PKI). Users encrypt data under fresh sampled AES keys, which are further encrypted under all recipients' RSA public keys. This file sharing mechanism is inflexible and inefficient. A sender needs to obtain and specify the public keys of all receivers during encryption. Even worse, the size of the ciphertext and encryption workload are proportional to the number of recipients, resulting in greater bandwidth and storage costs and more user expenditure. Limitations of the Existing Solutions. Three drawbacks exist in above-mentioned solutions: 1)

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

comparatively poor security, 2) coarse-grained access control, inflexible and inefficient file sharing, and 3) poor usability. The first two are easy to see and we now elaborate the usability issue. Typically, users use different terminals to upload files, including desktop, Web and mobile applications. However, almost all the existing solutions require additional software or plugins, thus limiting users' devices and platforms. When switching to a new device, users need to repeat the boring installation process, which greatly increases users' burden thus decreases usability. Related Work In-Browser Cryptography. Both the Web community and security researchers understand the importance and useful ness of in-browser cryptography and have made remarkable efforts in this area. JavaScript cryptographic libraries were developed for ease of use of cryptography on browsers, for instance Many of these libraries have a large number of downloads for OpenPGP.js in total. The World Wide Web Consortium (W3C) noticed this trend of using in-browser cryptography and as a solution proposed a standard called Web Cryptography API The standard supports a few widely adopted standard algorithms, e.g., AES and ECDSA, which is convenient for building several secure Web applications including authenticated video services and encrypted communications via Web mail. Meanwhile, there are researches in the literature having explored the idea of running cryptographic algorithms on Web browsers. focused on using Identity-Based Cryptography for clientside security in Web applications and presented a JavaScript implementation of their scheme. They selected Combined Public Key cryptosystem as the Encryption scheme to avoid complex computations involved in bilinear pairing and elliptic curve. Shadow Crypt allows users to transparently switch to encrypted input/output for text-based Web applications. It requires a browser extension, replacing input elements in a page with secure, isolated shadow inputs and encrypted text with secure, isolated cleartext. implemented several Lattice-based encryption schemes and showed the speed performance on four common Web browsers on PC. Their results demonstrated that some of today's Lattice-based cryptosystems can already have efficient JavaScript implementations. Recently, constructed an efficient two-level homomorphic public-key encryption in prime-order bilinear groups and presented a high-performance implementation using Web Assembly that allows their scheme to be run very fast on any popular Web browser, without any plugins required. Attribute-Based Encryption. Attribute based encryption (ABE) was first introduced by Sahai and Waters under the name fuzzy identity-based encryption Goyal et al. extended fuzzy IBE to ABE. Up to now, there are two forms of ABE: key-policy ABE (KP- ABE) where the key is assigned to an access policy and the ciphertext to a set of attributes, and ciphertext-policy ABE (CP-ABE) where the ciphertext is assigned to an access policy and the key to a set of attributes. A user can decrypt a ciphertext if the set of attributes satisfies the access policy. In this work, CP-ABE is adopted as a building block of WebCloud: each file has an access policy to indicate the allowed receivers. The complex pairing and exponentiation operations in ABE are migrated by many works. Green et al. introduced outsourced decryption into ABE systems such that the complex operations of decryption can be outsourced to a cloud server, only leaving one exponentiation operation for a user to recover the plaintext. Further, online/offline ABE was proposed by Hohenberger and Waters, which splits the original algorithm into two phases: an offline phase which does the majority of encryption computations before knowing the attributes/access control policy and generates an intermediate ciphertext, and an online phase which rapidly assembles an ABE ciphertext with the inter mediate ciphertext after the attributes/access control policy is fixed. Meanwhile proposed two scenarios about the offline phase: 1) the user does the offline work on his smartphone. 2) A high-end trusted server helps the user with low-end device do the offline work. Traditionally, data exchange was limited to localized systems with confined communication channels. This scenario not only impeded the seamless flow of information but also restricted the accessibility of data beyond geographical boundaries. The advent of cloud computing drastically changed this landscape. Cloud- based repositories allowed data to be stored, accessed, and shared across various devices and locations, heralding a new era of flexibility and accessibility. However, this newfound convenience also raised concerns about data securit.[12].

WebCloud emerges as a response to the demand for secure and streamlined data exchange. Unlike traditional cloud storage solutions, WebCloud is designed with a laser focus on security. It acknowledges that the unrestricted flow of information must be accompanied by a robust fortress of protection mechanisms. This is particularly critical when dealing with sensitive information, such as personal data, proprietary business information, and classified documents. As digital landscapes evolve and data becomes the lifeblood of modern society, solutions like WebCloud emerge as beacons of innovation. This introduction has laid the groundwork for a deep dive into the world of WebCloud, where security and accessibility converge to usher in a new era of information exchange. The subsequent sections will unravel the technical marvels that make WebCloud possible and shed light on its potential to reshape industries, empower individuals, and safeguard the integrity of shared information.

II. LITERATURE SURVEY

This research explores the challenges and solutions associated with secure data sharing in webbased cloud storage platforms. The study reviews various encryption techniques, access control mechanisms, and authentication protocols to ensure data confidentiality and integrity. It also discusses emerging trends in secure data sharing across different platforms, highlighting the importance of user-friendly interfaces and seamless cross-platform compatibility.

It provides a comparative analysis of web- based cloud storage services for secure data sharing across multiple platforms. It evaluates the security features, performance, and user experience of popular cloud storage providers, such as Dropbox, Google Drive, and Microsoft OneDrive. The study aims to assist users and organizations in making informed decisions when selecting a cloud storage solution

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

that meets their cross-platform data sharing needs.This literature review examines the strategies and technologies employed to enhance data security in web-based cloud storage platforms, with a focus on facilitating cross-platform collaboration[14]. The research investigates encryption at rest and in transit, multi-factor authentication, and fine-grained access control as key components of secure data sharing. Additionally, it discusses the impact of compliance regulations on data sharing practices in a cross-platform context. In-Browser Cryptography. Both the Web community and security researchers understand the importance and useful ness of in-browser cryptography and have made remarkable efforts in this area. JavaScript cryptographic libraries were developed for ease of use of cryptography on browsers, for instance [13]. Many of these libraries have a large number of downloads, e.g., 423368 for OpenPGP.jsin total. The World Wide Web Consortium (W3C) noticed this trend of using in-browser cryptography and as a solution proposed a standard called Web Cryptography API The stan dard supports a few widely adopted standard algorithms, e.g., AES and ECDSA, which is convenient for building several secure Web applications including authenticated video services and encrypted communications via Web mail. Meanwhile, there are researches in the literature hav ing explored the idea of running cryptographic algorithms on Web browsers. focused on using Identity-Based Cryptography for client side security in Web applications and presented a JavaScript implementation of their scheme. They selected Combined Public Key cryptosystem as the en cryption scheme to avoid complex computations involved in bilinear pairing and elliptic curve. Shadow Crypt.This survey explores the integration of blockchain technology in web-based cloud storage to achieve secure and tamper-resistant cross-platform data sharing. The paper reviews existing literature on blockchain- based cloud storage solutions, highlighting their potential advantages and challenges. It discusses how blockchain can enhance data sharing security, establish trust among users, and provide an auditable record of data transactions across various platforms.

III. PROBLEM STATEMENT

The complex pairing and exponentiation operations in ABE are migrated by many works. Green et al. introduced outsourced decryption into ABE systems such that the complex operations of decryption can be outsourced to a cloud server, only leaving one exponentiation operation for a user to recover the plaintext. Further, online/offline ABE was proposed by Hohenberger and Waters, which splits the original algorithm into two phases: an offline phase which does the majority of encryption computations before knowing the attributes/access control policy and generates an intermediate ciphertext, and an online phase which rapidly assembles an ABE ciphertext with the intermediate ciphertext after the attributes/access control policy is fixed. Meanwhile, proposed two scenarios about the offline phase: the user does the offline work on his smartphone. A high-end trusted server helps the user with low-end device do the offline work[15].

Practical Encryption Solution for Cloud Storage. We introduce WebCloud, a practical clientside encryption solution for public cloud storage, which effectively combines modern Web techniques and cryptographic algorithms.

Web cloud involves of a key management mechanism, a dedicated attribute based encryption scheme and a high-speed implementation. More importantly, Web Cloud is cross platform (including major browsers, Android and PC) and plugin-free. Fine Grained Access Control Mechanism with ABE. It is widely-accepted that attribute-based encryption (ABE) is promising for finegrained access control of data. However, we find that the existing ABE schemes suffer from high computational overhead, or some vital missing functionalities, e.g., inefficient data encryption, robust and immediate user revocation, offline encryption and outsourced decryption simultaneously. To solve this problem, we propose a dedicated ciphertextpolicy attribute-based access control mechanism. The proposed scheme can also be used in other scenarios.

Rigorous Security Analysis. We present a security model of WebCloud, including the adversarial models for the Web and the cryptographic scheme simultaneously. The security analysis is then done in the proposed model, namely, the provable security of the proposed CP-ABE scheme and the reliability of the key storage in the browser side. Efficient Operation inside Browsers. We implement WebCloud based on ownCloud. The functionalities and performances are evaluated in major browsers on many devices, and applications on PC and Android devices. The benchmark result indicates that WebCloud is a practical solution. Most remarkably, in the Chrome browser on a 4-core 2.2 GHz Macbook machine, encrypting a 1 GB file takes 3.1 seconds, while decryption costs

AIM OF WEB CLOUD

The proposed system focuses on designing and implementing a practical, secure and cross-platform public cloud storage system. The proposed solution, WebCloud, is a Webbased client-side encryption solution. Users encrypt and decrypt their data using Web agents, e.g., Web browsers. The proposed system implemented Multi-Factor Authenticated Key Exchange which gives more security and safe. keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and performing the following operations Register and Login, My Profile, View Files, Search Files, Search Ratio, Top K Search, Req Search Control. **PKG–**responsible for viewing Files and Generate Key.

IV. IMPLEMENTATION

In this module, the data provider uploads their encrypted data in the Cloud server. For the security purpose the data owner

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Attackers, Upload File View Files, Verify data(Verifiability), View and Delete Files, View All Transactions.

Cloud Service Provider the Cloud server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as Login, 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.

User

Cloud Server Key-Exposure Resistance. The cloud secret key CSK is important to the revocation mechanism. If CSK leaks, the revocation functionality is useless. Thus, WebCloud introduces key-exposure resistance property for CSK. Concretely, the cloud updates CSK periodically (or when key is leaked). Meanwhile, it updates all stored ABE ciphertexts and deletes old ciphertexts when the CSK is updated.

V. IMPLEMENTATION RESULTS

Data Owner Register

Users provide essential information, such as their identity, contact details, and organizational affiliation. During registration, it's common for platforms to implement verification steps to ensure the authenticity of the data owner's identity.

Fig.1. Data Owner Login

Fig.1 shows the Data owner login involves accessing a platform or system where individuals with ownership rights over specific data can authenticate their identity. This process usually requires entering a username and password, with potential additional security layers like Multi-Factor Authentication.

Fig.2. Data Owner Login Home Page

Performance of WebCloud General Remarks. WebCloud has no specific requirement for the underlying cloud storage systems. It can be applied to all cloud storage systems. We implement WebCloud based on ownCloud (version 10.0.10), which is an open source cloud collaboration platform. We carefully review the codes of ownCloud on its PHP framework, file process, user management and debug method. Meanwhile, we also investigate a few third party open source projects that used in own Cloud, mainly jQuery file upload plugin and dav frame work

VI. CONCLUSION

We propose Web Cloud, a practical client-side encryption solution for public cloud storage in the Web setting, where users do cryptography with only browsers. We analyze the security of Web Cloud and implement Web Cloud based on own Cloud and conduct a comprehensive performance evaluation. The experimental results show that our solution is practical. As an interesting by-product, the design of Web- Cloud naturally embodies a dedicated CP-AB-KEM scheme, which is useful in many other applications.

VI REFERENCES

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

[2]. D. Lewis, “icloud data breach: Hacking and celebrity photos,”Duo Security, Tech. Rep., September2014.[Online].Available:https://www.forbes.com/sites/davelewis/2014/09/ 02/icloud-data-breach-hacking-and-nude-celebrity-photos

[3]. T.Hunt,“Hackeddropboxlogindataof68millionusersisnowforsaleonthedarkweb,”Tech.Rep.,September2016.[Online].Available:https://www.troyhunt.com/the-dropbox-hack-is-real/

[4]. “Amazon data leak,” Eleven Paths, 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., July2018. [Online]. Available: https://techcrunch.com/2018/07/20/ data-breach-level-one-automakers/
[6]. M. Grant, "$93m class-action lawsuit filed against city of calgary for privacy breach,"Tech.Rep.,October2017. [Online]. Available:http://www.cbc.ca/news/canada/calgary/ city-calgary-class-action-93-million-privacy-breach-1.4321257 (2020,April) Secure file transfer whisply.[Online].Available: https://whisp.ly/en
[7]. (2020, April) Cryptomator: Free cloud encryption for drop box and others. [Online]. Available: https://cryptomator.org/
[8]. (2020, April)Whitepapers from spider oak. [Online].Available:https://spideroak.com/whitepapers/
[9]. (2020, April) Aws sdk support for amazon s3 client-side encryption. [Online]. Available: https://docs.aws.amazon.com/ general/ latest/ gr / aws sdk cryptography.html
[10]. (2020,April)Cloud storage security secure cloud storage from tresorit. [Online]. Available: https://tresorit.com/security
[11]. W.Ma,J.Campbell,D.Tran,andD.Kleeman,"Password entropyandpasswordquality,"inFourthInternational Conference on Network and System Security, NS
[12]. 2010,Melbourne, Victoria, Australia, September 1-3, 2010,Y.Xiang,P.Samarati,J.Hu, W.Zhou,andA.Sadeghi,Eds.IEEEComputerSociety,2010,pp.583–587. [Online]. Available: https://doi.org/10.1109/NSS.2010. 18
[13]. (2020, April) Aws sdk support for amazon s3 client-sideencryption.[Online].Available: https://docs.aws.amazon.com/general/latest/gr/aws sdkcryptography.html
[14]. (2020,April)Cloud storage security- secure cloud storage fromtres or it .[Online]. Available: https://tresorit.com/security