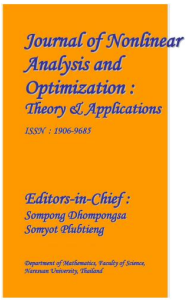
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



WEB CLOUD INTERNET LINKED CLOUD REPOSITORY FOR SECURE EXCHANGE OF DATA

Mr. K. Shekhar, ***Assistant Professor CSE, Vaagdevi College of Engineering (Autonomous), India***

Ch.Divija, ***UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India***

Ch.Divya, ***UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India***

A.Adithya, ***UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India***

B.Bhavana, ***UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India***

ABSTRACT

In the rapidly evolving landscape of digital communication and information exchange, the demand for secure and efficient cross-system data sharing has become increasingly paramount. This paper introduces "WebCloud," a novel internet-linked cloud repository designed to facilitate protected information exchange across diverse systems. By integrating advanced encryption and authentication mechanisms, WebCloud offers a robust platform that ensures the confidentiality, integrity, and accessibility of shared data. This paper presents the architecture, key features, and security protocols employed by WebCloud, highlighting its potential to redefine secure information interchange in a connected world. The proliferation of interconnected devices and systems has ushered in a new era of information exchange, but it has also brought forth unprecedented challenges in maintaining the privacy and security of shared data. Traditional methods of data storage and transmission are often vulnerable to unauthorized access and breaches. In response to these challenges, this paper introduces "WebCloud," a groundbreaking solution designed to address the intricacies of secure data sharing across various platforms. By amalgamating the power of cloud computing and internet connectivity, WebCloud offers a comprehensive framework that prioritizes data protection without compromising accessibility. This paper elucidates the motivation, objectives, and organization of the subsequent sections, which delve into the technical aspects, security measures, and potential applications of the WebCloud system.

1. INTRODUCTION

In the dynamic landscape of modern information exchange, where data flows ceaselessly across networks, the need for secure and efficient data sharing has become paramount[1]. Organizations and individuals alike seek mechanisms that allow them to seamlessly exchange information across systems[2] without compromising the confidentiality, integrity, and accessibility of their data[3]. The advent of cloud computing and its integration with internet-linked repositories has brought forth a new paradigm for data storage and sharing. In this context, the concept of "WebCloud" emerges as a pioneering solution that endeavors to revolutionize the way protected information is exchanged across diverse platforms[4].

The accelerated pace of digitalization has interconnected systems spanning the globe, catalyzing an exponential surge in data generation and sharing. From personal communications to intricate business transactions, the digital landscape has become a conduit for the flow of valuable information[5]. However, this data-driven evolution has not come without challenges. Cybersecurity threats, unauthorized access, data breaches, and privacy concerns loom as persistent threats that require innovative solutions[6].The essence of WebCloud lies in its potential to address these challenges head-on. By amalgamating the power of cloud computing and the ubiquitous reach of the internet, WebCloud introduces a comprehensive platform that facilitates secure and efficient information exchange[7]. With a robust architecture, advanced encryption techniques, and stringent authentication mechanisms, WebCloud positions itself as a transformative solution for safeguarding the confidentiality of shared data[8].

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[9]. 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 security[10].

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[11]. As digital landscapes evolve and data becomes the lifeblood of modern society, solutions like WebCloud emerge as

beacons of innovation. This introduction[12] 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 [13].

2. LITERATURE SURVEY

This research explores the challenges and solutions associated with secure data sharing in web-based cloud storage platforms[14]. 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[15].

This paper 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 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. The research investigates encryption at rest and in transit, multi-factor authentication, and fine-grained access control as key components of secure data sharing[16]. Additionally, it discusses the impact of compliance regulations on data sharing practices in a cross-platform context[17].

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[18]. It discusses how blockchain can enhance data sharing security, establish trust among users, and provide an auditable record of data transactions across various platforms[19].

3 PROBLEM STATEMENT

The complex pairing and exponentiation operations in ABE are migrated by many works. Green et al. [19] 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 [20] 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, [20] 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[21].

3.1 limitation of system

Comparatively poor security, Coarse-grained access control, inflexible and inefficient file sharing, and 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.

4. WEB CLOUD

Practical Encryption Solution for Cloud Storage. We introduce WebCloud, a practical client-side encryption solution for public cloud storage, which effectively combines modern Web techniques and cryptographic algorithms. WebCloud involves of a key management mechanism, a

dedicated attribute based encryption scheme and a high-speed implementation. More importantly, WebCloud is crossplatform (including major browsers, Android and PC) and plugin-free.Fine-Grained Access Control Mechanism with ABE[22]. It is widely-accepted that attribute-based encryption (ABE) is promising for fine-grained 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 ciphertext-policy attribute-based access control mechanism[23]. 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 [23]. 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 3.9 seconds[24].

4.1 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 Web-based 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.

5. IMPLEMENTATION

5.1 Data Owner

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

5.2 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.

5.3 User

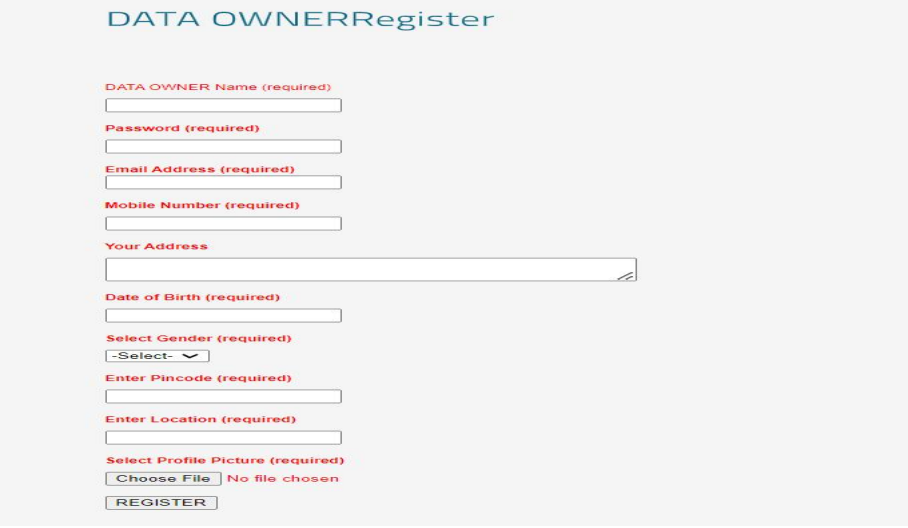
In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and performing the following operations Register and Login, My Profile, View Files, Search Files, Search Ratio, Top K Search, Req Search Control.

PKG–responsible for viewing Files and Generate Key.

6. IMPLEMENTATION RESULTS

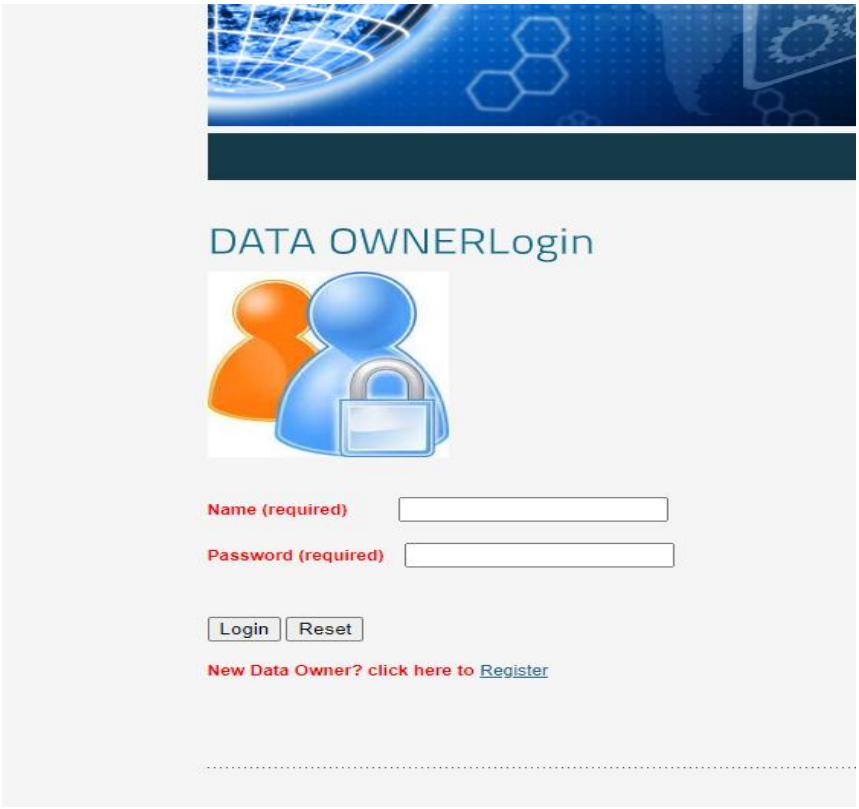
6.1 Data Owner Register

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.



6.2 Data Owner Login

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 (MFA)[25].



7. 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.

8. FUTURE SCOPE

In the evolving landscape of data exchange and storage, WEBCLOUD, an internet-linked cloud repository for secure information sharing across systems, presents a promising future. With a growing emphasis on data security, WEBCLOUD offers enhanced protection, ensuring the confidentiality and integrity of sensitive information. Its cross-platform compatibility is poised to become increasingly valuable in a world where seamless data sharing between diverse systems is

essential. Integration with emerging technologies such as IoT and AI positions WEBCLOUD as a central hub for managing the vast data generated by these innovations.

9. 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 celebrityPhotos," 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 forsale 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., November2018. [Online]. Available: https://www.elevenpaths.com/amazon-data-leak/index.html

[5] K. Korosec, "Data breach exposes trade secrets of carmakersgm, 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 cityofcalgary for privacy breach," Tech. Rep., October 2017.[Online].
Available:http://www.cbc.ca/news/canada/calgary/city-calgary-class-action-93-millionprivacy-breach-1.4321257

[7] (2020, April) Secure file transfer — whisply. [Online].
Available:https://whisp.ly/en[8] (2020, April) Cryptomator: Free cloud encryption for dropboxand 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 entropyand password quality," in Fourth International Conference onNetwork 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

[11] (2020, April) Aws sdk support for amazon s3 client-sideencryption. [Online].
Available: https://docs.aws.amazon.com/general/latest/gr/awssdk cryptography.html

[12] (2020, April) Cloud storage security - secure cloud storage fromtresorit. [Online]. Available: https://tresorit.com/security

[13] (2020, April) Mega - secure cloud storage and communication.
[Online]. Available: https://mega.nz/

[14] E. Bocchi, I. Drago, and M. Mellia, "Personal cloud storage: Usage,performance and impact of terminals," in 4th IEEE InternationalConference on Cloud Networking, CloudNet 2015, Niagara Falls,ON, Canada, October 5-7, 2015. IEEE, 2015, pp. 106–111. [Online].
Available: https://doi.org/10.1109/CloudNet.2015.7335291

[15] "Web cryptography api," the Web Cryptography WG ofthe W3C, Tech. Rep., January 2017. [Online]. Available:https://www.w3.org/TR/WebCryptoAPI/

[16] A. Haas, A. Rossberg, D. L. Schuff, B. L. Titzer, M. Holman,D. Gohman, L. Wagner, A. Zakai, and J. Bastien, "Bringing theweb up to speed with webassembly," in ACM SIGPLAN Notices,vol. 52, no. 6. ACM, 2017, pp. 185–200.

[17] B. Waters, "Ciphertext-policy attribute-based encryption: Anexpressive, efficient, and provably secure realization," inInternational Workshop on Public Key Cryptography. Springer,2011, pp. 53–70.

[18] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attributebasedencryption from r-lwe," Chin. J. Electron, vol. 23, no. 4, pp.778–782, 2014.

[19] M. Green, S. Hohenberger, B. Waters et al., "Outsourcing thedecryption of abe ciphertexts." in USENIX Security Symposium,vol. 2011, no. 3, 2011.

[20] S. Hohenberger and B. Waters, "Online/offline attributebasedencryption," in International Workshop on Public KeyCryptography. Springer, 2014, pp. 293–310.

[21] R. Zhang, H. Ma, and Y. Lu, "Fine-grained access control systembased on fully outsourced attribute-based encryption," Journal ofSystems and Software, vol. 125, pp. 344–353, 2017.

[22] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based datasharing with attribute revocation," in Proceedings of the 5thACM symposium on information, computer and communicationssecurity, 2010, pp. 261–270.

[23] (2020, April) owncloud - the leading opensource cloudcollaboration platform. [Online]. Available: https://owncloud.Org/

[24] (2020, April) Openpgp implementation for javascript. [Online].
Available: https://github.com/openpgpjs/openpgpjs

[25] E. Stark, M. Hamburg, and D. Boneh, "Symmetric cryptography injavascript," in Computer Security Applications Conference, 2009.ACSAC'09. Annual. IEEE, 2009, pp. 373–381.