ZKG INTERNATIONAL ISSN: 2366-1313

WEBCLOUD: WEB-BASED CLOUD STORAGE FOR SECURE DATA SHARING ACROSS PLATFORMS

[1]Mr. B. NARSINGAM, [2]K. VIMAL KUMAR, [3]K. NIMESH REDDY, [4]K. SANDEEP REDDY

[1](Assistant Professor) ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

[234]B,tech scholar ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

ABSTRACT

The need for effective and safe cross-system data sharing has grown in importance due to the quickly changing digital communication and information exchange landscape. This paper presents "WebCloud," a new cloud repository connected to the internet that is intended to enable secure information sharing between various platforms. WebCloud provides a strong platform that guarantees the confidentiality, integrity, and accessibility of shared data by including so phisticated authentication and encryption techniques. This article highlights WebCloud's potential to revolutionize safe information transfer in a connected society by presenting its architecture, essential features, and security protocols. A new era of information exchange has been brought about by the development of interconnected devices and systems, but it has also presented previously unheard-of difficulties in preserving the security and privacy of shared data. Conventional techniques for transmitting and storing data are frequently open to intrusions and illegal access. This study presents "WebCloud," a novel solution to these problems that tackles the complexities of safedata sharing across several platforms. WebCloud combines the strengths of cloud computing and internet access to provide a complete framework that puts data security first without sacrificing usability. The purpose, goals, and structure of the following sections—which include the WebCloud system's technical features, security precautions, and possible uses—are explained in this document.

ISSN: 2366-1313

1. INTRODUCTION

Problem Statement: In the dynamic landscape of modern information exchange, the incessant flow of data across networks has underscored the critical need for secure and efficient data sharing mechanisms. More and more people and organizations are looking for ways to maintain the confidentiality, integrity, and accessibility of their data while facilitating easy information sharing. The amalgamation of cloud computing and internet-connected repositories has brought about a fundamental transformation in the methods of storing and sharing data. Nevertheless, there are a lot of obstacles in the way of this development, such as privacy issues, unauthorized access, cyber security risks, and data breaches. To tackle these obstacles, creative solutions are needed that put security first without sacrificing usability. Description: Global system interconnection brought about by the quick speed of digitalization has resulted in an exponential increase in data generation and sharing activities. Information can be exchanged for important purposes across the digital world, from personal chats to complicated economic transactions. Still, there are a number of issues with this data-driven progress, such as privacy concerns and cyber security weaknesses. Asa result, Web Cloud shows up as a trailblazing solution ready to transform data sharing procedures. Web Cloud makes use of the capabilities of cloud computing and the extensive reach of the internet to enable safe and effective information sharing between various platforms. Web Cloud protects the privacy of shared data with its strong architecture, cutting-edge encryption methods, and strict authentication procedures.

WebCloud is created with a laser-like focus on security, in contrast to standard cloud storage solutions. It recognizes the necessity for a strong fortress of protective systems to preserve confidential data. Data interchange was formerly restricted to localized systems with few communication channels, which hampered the smooth transfer of information and limited the accessibility of data. This environment has changed with the introduction of cloud computing, which makes it possible to store, access, and share data across several devices 2and places. Nevertheless, worries over data security continue, which is why WebCloud and other solutions have been developed. As digital environments change and data becomes more essential to contemporary life, creative solutions like WebCloud stand out as

examples of innovation. Through tackling the urgent problems with data exchange, WebCloud hopes to transform sectors, give people more control, and protect the confidentiality of shared data. This introduction lays the groundwork for a more thorough examination of WebCloud's technological wonders and its ability to bring about the advent of a new era of accessible and secure information exchange.

2. LITERATURE SURVEY

In various delivered plans a user concede possibility only within financial means approach dossier if a user gangs the set of attestations or attributes. Currently, the only designfor sanctioning such tactics search out engage a trustworthy server to store the dossier and intercede approach control. However, if some server locking away the dossier is marred, before the secrecy of the data will be jeopardized. In this paper we present a plan for earning complex approach control onencrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By utilizingour methodsencrypted dossier maybe observed confidential even though the depository attendant is untrusted .Moreover, our orders are secure against collusion attacks. Previous Attribute Based Encryption wholes secondhand attributes to specify the encrypted dossier and buxom policies into consumer's answers; while in our arrangement attributes are used to interpret a user's attestations, and a body encrypting dossier decides a policy for the one can decipher. Thus, our systems are conceptually tighter to usual access control orders in the way that Role-Based Access Control (RBAC). In addition, we support an exercise of our system and present conduct calculations. Wireless Body Area Networks (BANs) be necessary to play a critical part inpatient energy monitoring in the forthcoming future. Establishing secure media middle from two points BAN sensors and outside consumers is key to discussing the widespread security and solitude concerns

.In this paper, we suggest the barbaric functions to implement a secret-giving located Ciphertext- Policy Attribute-Based Encryption (CP_ABE) blueprint, that encrypts the data established an approach building particularized for one dossier beginning. We also design two obligation stosolidly save the impressionable patient dossier from a BAN and tell the sensors in a BAN. Our study indicates that the projected blueprint is doable, can specify meaning genuineness, and cancounter possible big

ISSN: 2366-1313

attacks to a degree conspiracy attacks and assault-tiring attacks. In this paper, we intend a delivered Prediction-based Secure and Reliable beating foundation(PSR) for emerging Wireless Body Area Networks (WBANs). It maybe joined accompany in gas pecific crushing obligation to improve the latest's dependability and avert data dose attacks all along dossier communication. In PSR, utilizing past link condition measurements, each bud anticipates the characteristic of every related link, and accordingly any change in the neighbor set also, for the next future. When skilled are multiple attainable next hops for bundle forwarding(in accordance with the conquering code used), PSR selects the individual accompanying the highest called link value between them. Specially-tailor-made inconsequential beginning and data confirmation designs are employed by knots to secure dossier ideas. 4Further, each growth adaptively enables or immobilizes beginning authentication in accordance with predicted neighbour set change and guess veracity so as to fast clean false beginning authentication requests. We display that PSR considerably increases routing dependability and effectively withstand dossier injection attacks through meticulous safety analysis and thorough simulation study

3.SYSTEM DESIGN

3.1 SYSTEM ARCHITECTURE

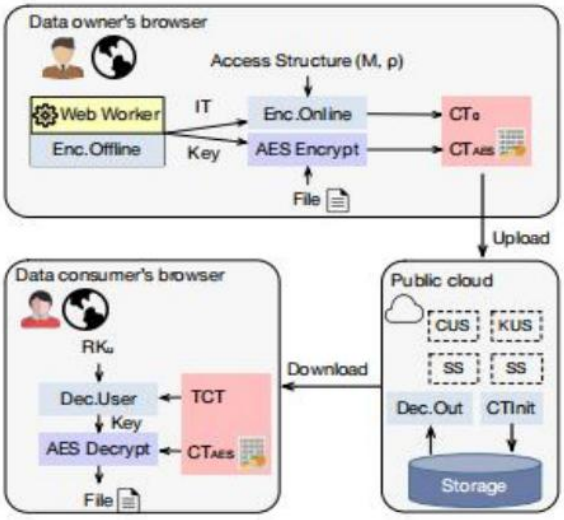

Figure 3.1 System Design of WebCloud

The WebCloud system architecture aims to offer a stable and expandable frame work for safe data exchange and storage on many platforms. It is made up of a number of inter connected components, each of which has a distinct function in promoting easy communication and guaranteeing user data security. The Data Owner Module, which enables users to start and oversee safe data storage and sharing operations, is at the center of the system architecture. The Cloud Service Provider Module, which is in charge of setting up and maintaining the underlying infrastructure needed for the WebCloud platform, communicates with this module.

ISSN: 2366-1313

The Cloud Service Provider Module uses so phisticated security procedures and compliance checks to safeguard user data, ensuring the platform's availability, scalability, and security. Furthermore, the User's Module facilitates user registration, authentication, and data access by acting as an interface between individual users and the WebCloud platform. After completing the authentication process successfully, users work with the Data Owner Module to safely upload, arrange, and manage access to their data. Sensitive data is encrypted before being stored by the Data Encryption Module, and data security is increased by the Key Management Module, which guarantees safe key production and storage. 10In addition, the Data Management Module integrates critical management features to support data security protocols and is essential in managing encrypted data storage and retrieval. The integration of these modules results in a unified system design that guarantees user data availability ,confidentiality, and integrity within the WebCloud platform, offering users a reliable and effective environment for exchanging data.

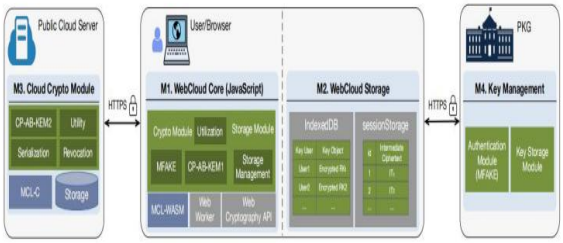

Figure 3.2 System Architecture of WebCloud

A webpage for accessing and storing data in Web user agents is provided by the public cloud server. It also provides the following services

:• PKG creates, sends, and receives system keys and parameters to other entities. It also gives the cloud instructions on how to remove a user. PKG serves as the primary Certificate Authority (CA) and manages the Public Key Infrastructure (PKI). We emphasize that sincekey distribution and certificate issuance are finished simultaneously, this only slightly increases PKG's burden.

•he browser and server (B/S) architecture is adopted by the WebCloud. A public cloud server, a private key generator (PKG), data owners, and data consumers are the four parties involved. The following are each entity's roles: Data owners establish access controls and encrypt data in accordance

ISSN: 2366-1313

withthesepoliciesbefore uploading it to the public cloud. We note that it is not difficult to locate a trusted party (acting as PKG), for example, largebanksor government agencies.

- Data consumers download encrypted data from the public cloud server and decrypt it locally.

- o Transformation keys and encrypted data are reliably stored by Storage Service(SS).

o To reduce the computational burden of decryption for consumers, the

Out sourced Decryption Service (DS) pre-processes the ciphertext and verifies if a data consumer has been revoked. o When the current cloud secret key (CSK) is leaked or updated on a regular basis, Key Update Service (KUS) is triggered. o New CSK is added to ciphertexts via the Ciphertext Update Service (CUS). 11Security Notions: For cloud storage systems, WebCloud's security objective is to shield user data from server-side disclosure. We take the cloud to be sincere but inquisitive. In an honest manner, the cloud offers storage services and outsources decryption services, for example. Users' data is not altered by adversaries. While the majority of data consumers are truthful, a small percentage may be dishonest and collaborate by sharing their secret keys. PK Gand data owners, however, are taken to be completely trustworthy. TLS provides security for all the communications. We examine the adversary models listed below: Passive Man-in-the-Middle. The opponent does not carry out any active attacks, such as changing network packets; instead, they passively read all network traffic. Web Attacker Model. The common security model for web applications is this one. According to this concept, an adversary can send emails and other messages, access any open Web application, obtain its client-side code, and create their own (malicious) Web apps. The adversary is unable.

ACTIVITY DIAGRAM

Activity Diagrams in UML offer visual depictions of dynamic workflows, detailing the sequence and conditions of activities within a system or business process. They consist of nodes, representing actions or decisions, and transitions, illustrating the flow between these nodes. Initial and final nodes denote the activity's commencement and conclusion, respectively. Control flows connect Decision Nodes: Enable branching in the workflow based on conditions

- **Control Flows:** Connect nodes, defining the sequence of execution.

ISSN: 2366-1313

- **Initial and Final Nodes:**

Indicate the start and end points of the activity.

- **Transitions:**

Depict the flow of control between nodes.

- **Nodes:**

Represent actions or decisions within the workflow.

• actions, dictating the order of execution, while decision nodes enable branchingbased on conditions. Additionally, forks and joins manage parallel flows, andswimlanes partition activities among different entities for clarity.

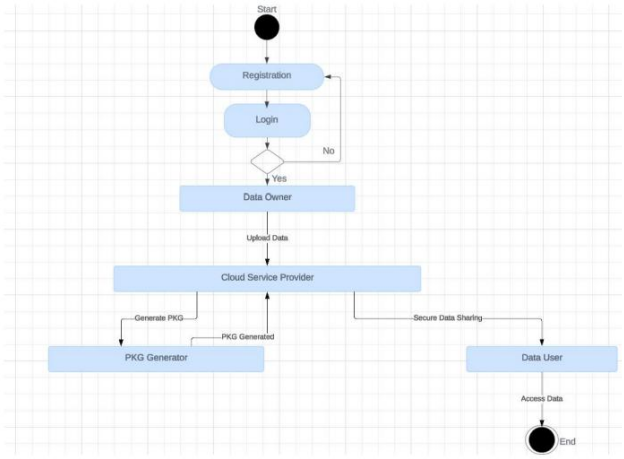

Figure 3.3 Activity Diagram

The Activity Diagram provides a visual representation of the work flow and control flow with in the WebCloud system. It illustrates the sequence of activities, decisions, and parallel flows involved in completing a specific task or use case. Activities such as user registration, log in authentication, data encryption, storage, and retrieval are depicted along with decision points and branching conditions. The Activity Diagram aids in understanding the system's behavior and logic during execution.

8. OUTPUT SCREENS

Figure 4.1 Cloud Main Page

The output screen represents the login page interface to login with their respected credentials

ISSN: 2366-1313

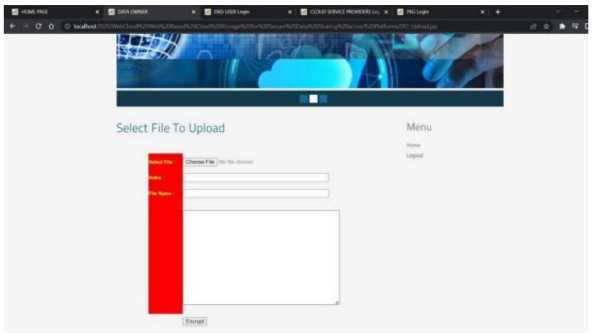

Figure 4.2 Represents Upload Files to Cloud

The output screen shows how the user upload the file

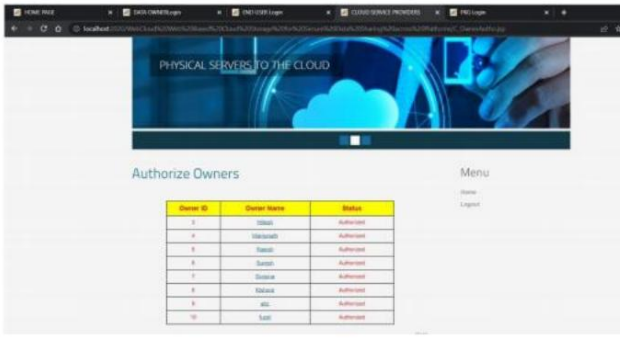

Figure 4.3 Represents Authorize Data Owners

The output screen shows the Authorize Data Owners

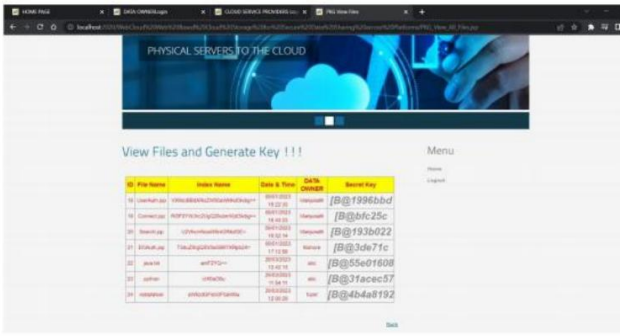

Figure 4.4 Represents Generating Key for Encryption

The output screen shows all the Files and their Generated Keys

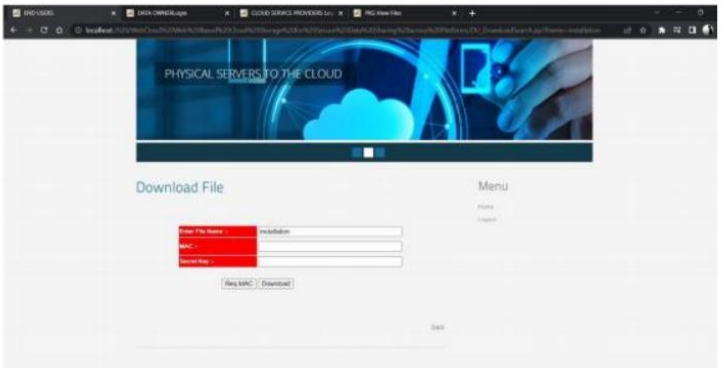

Figure 4.5 Request Mac Key

The above output screen shows the Interface to Download a File

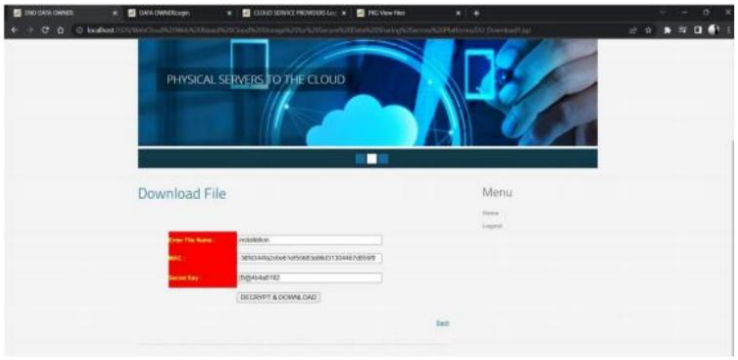

Figure 4.6 Decrypt and Download

The above output screen shows a Decrypt and Download for the user to download the File

ISSN: 2366-1313

5. CONCLUSION

In conclusion, we introduce WebCloud, a novel approach to the pressing problem of safe and intuitive client-side encryption in public cloud storage settings over the internet. WebCloud ensures end-to-end data security and privacy by utilizing contemporary web technologies to allow users to conduct cryptographic operations from within their browsers. We have shown the usefulness and efficacy of Web Cloud via thorough security study and deployment based on our own Cloud platform. Our solution keeps excellent performance and usability across several web browsers and devices, while also offering strong encryption for sensitive data. Moreover, the experimental assessment carried out on WebCloud demonstrates its effectiveness and dependability in practical situations. The outcomes validate the feasibility of our methodology and its capacity to tackle the security issues that are intrinsic to cloud storage setups. Additionally, WebCloud's design presents a novel CP-AB-KEM scheme that is applicable and versatile even outside of its primary use case. This extra functionality highlights the adaptability and creativity built into the WebCloud solution, creating opportunities for wider applications and improvements in cryptographic systems. All things considered, WebCloud is a big advancement in improving data security and privacy in the context of cloud storage. WebCloud has the potential to completely transform data protection in the digital age by enabling users to easily and confidently secure their data thanks to its practicality, security, and adaptability.

6.FUTURE ENHANCEMENTS

In future iterations, we plan to implement a number of improvements in next versions to further improve the WebCloud platform's functionality and usability. Improving the system's performance and scalability to handle more users and heavier workloads is one possible improvement path. This can entail employing cloud-native technologies, streamlining backend infrastructure, and putting in place caching techniques to speed up data retrieval. Furthermore, adding support for multi-factor authentication and broadening the spectrum of supported encryption techniques could improve user flexibility and security. To further improve the platform's resilience and dependability, integration with cutting-edge technologies like blockchain for improved data integrity and decentralized storage options could be investigated. Additionally, adding features

like file versioning and collaborative editing capabilities, as well as improving the user interface and experience through intuitive design changes, could improve user satisfaction and encourage adoption. All things considered, the goal of these next improvements is to further advance WebCloud's position as an all-encompassing and important solution for safe data sharing and storing across a variety of platforms and user scenarios.

7. 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 darkweb,"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-one-automakers/

[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/

ISSN: 2366-1313

[10] W. Ma, J. Campbell, D. Tran, and D. Kleeman, “Password entropy and password quality,”inFourth International Conference on Network and System Security, NSS 2010, Melbourne, Victoria.