IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204006 |

Self-Destructing Data System for User Data Privacy in Cloud

[1]Dr.P.Manikandaprabhu, [2]K.Agilesh

Assistant Professor, PG& Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore , Tamil Nadu India

UG Student, PG& Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore , Tamil Nadu India

ABSTRACT: Personal data stored in the Cloud may contain account numbers, passwords, notes, and other important information that could be used and misused by a miscreant, a competitor, or a court of law. These data are cached, copied, and archived by Cloud Service Providers (CSPs), often without users' authorization and control. Self-destructing data mainly aims at protecting the user data's privacy. The "Self-Destructing Data System for User Data Privacy in Cloud" paper introduces an innovative approach to safeguarding user data privacy within cloud environments. Traditional cloud storage systems raise concerns about data retention and unauthorized access. In response, our project proposes a dynamic and secure data management system that automatically and irreversibly deletes user data after a predefined retention period. By integrating cryptographic techniques, secure algorithms, and cloud infrastructure, this system provides a robust solution for users seeking heightened control over their personal information in the cloud. This self-destruction feature is designed to be user-controlled, ensuring that individuals or organizations retain autonomy over their data. Users can trigger the self-destruction process through secure authentication methods, enabling them to respond promptly to security threats or concerns. The system employs advanced encryption techniques to protect data during normal operations, and the self-destruction mechanism acts as a fail-safe option in extreme scenarios. This paper aims to mitigate the impact of potential data breaches, unauthorized access, or other security incidents by offering users an effective and decisive response to protect their sensitive information. By integrating this self-destruction system into the cloud server architecture, the project seeks to enhance user confidence in cloud-based services, ultimately contributing to a more secure and privacy-aware computing environment. The "Self-Destruction System in a Cloud Server for Data Privacy" combines the strength of AES cryptography, specifically the Rijndael algorithm, with a self-destruct mechanism to fortify the security of sensitive data stored in the cloud. This innovative approach aims to mitigate the risks associated with unauthorized access, providing a robust solution for safeguarding data privacy in cloud computing environments.

KEYWORDS: Privacy, AES, Authentication methods, cloud, security

I. INTRODUCTION

In the era of digital ubiquity, cloud storage has become the lifeblood of our internet-driven world. While convenient and scalable, entrusting sensitive data to external servers raises critical concerns about privacy and security. Traditional deletion methods often leave recoverable traces, rendering data vulnerable to unauthorized access even after intentional removal. This abstract presents a novel solution: a self-destruction system embedded within a cloud server, specifically designed to safeguard data privacy.

The "Self-Destruction System in a Cloud Server for Data Privacy" project represents a pioneering initiative at the forefront of addressing the escalating concerns surrounding the confidentiality of data in cloud computing environments. In an era marked by the exponential growth of digital information and the increasing prevalence of cyber threats, the imperative to fortify data privacy measures has never been more critical. This project introduces a cutting-edge solution in the form of a self-destruction mechanism embedded within cloud server infrastructures. The central aim is to furnish an additional layer of security by empowering users to remotely trigger the destruction of their stored data in response to unauthorized access or potential security breaches.

At its core, this self-destruction feature offers users unprecedented control, ensuring that individuals and organizations retain autonomy over their sensitive data. Activation of the self-destruction mechanism is contingent upon secure authentication protocols, allowing users to promptly respond to security threats or apprehensions. Employing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204006 |

advanced encryption techniques during routine operations, the self-destruction system serves as a fail-safe option, augmenting the overall resilience of data protection measures.

This paper seeks to assuage the impact of potential data breaches and unauthorized access by providing users with a robust and decisive tool to safeguard their confidential information. By seamlessly integrating the self-destruction system into the architecture of cloud servers, the project not only bolsters user confidence in cloud-based services but also contributes significantly to cultivating a more secure and privacy-conscious computing environment. Through its innovative approach, this project represents a pivotal stride toward enhancing the integrity and privacy of data stored in cloud infrastructures.

II. RELATED WORKS

Cloud computing, commonly called as 'cloud' has been a buzz word of today's IT industries. But there is no complete understanding of this word and the exact benefits achieved by implementing this technology. But this 5th generation of computing is gaining momentum in many companies as big IT corporate such as IBM, Amazon ,Microsoft are pushing this new technique in great pace, which has started around in early 1990's. According to the National Institute of Standards and Technology (NIST) cloud computing is defined as a model for enabling ubiquitous network access to a shared pool of configurable computing resources. The main technology that paved the way for this methodology is the INTERNET, without which sharing of resources, accessing data from remote location, globalisation of information is impossible.

Commonly, cloud computing is pay-per-use worldview to empower fitting on-request arrange access to a mutual pool of configurable registering assets for example systems, servers, applications, and so forth., that can be quickly provisioned and discharged with the ideal administration exertion or specialist co-op interface. Numerous associations can remodel to cloud computing for social event its solicitations as customers and friends can utilize applications with no framework and access their private archives at any PC with Internet get to [1]. For the most part, distributed computing includes three distinct administrations, for example, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Every equipment framework segments are virtualized into virtual elements. Virtualization implies a procedure that encourages execution of various Operating Systems (OSs) together on one Physical Machine (PM). These OSs are detached from one another and from the center physical framework utilizing a Virtual Machine (VM) [2].Cloud computing has numerous difficulties at expanding the quantity of clients since the interest of assets assignment and usage are expanded quickly. Accordingly, Load Balancing (LB) between assets is the most significant test [3]. For the most part, LB is the way toward doling out and reassigning the remaining burden among every accessible asset that amplifies the throughput, asset utilization and vitality sparing while at the same time diminishing the expense and reaction time. Astounding LB systems may give the Service Level Agreement (SLA) and customer experience. In this way, the development of powerful calculations and procedures for LB is a primary part of distributed computing frameworks. Various explores have been done in the zone of LB and assignment planning for cloud frameworks [4-5].

In the modern decades, worldwide presentation is transforming into a novel hypothesis at field of processing called osmotic figuring following the compound osmotic conduct hypothesis. Osmotic processing is basically used to accomplish adjusted organization in profoundly dispersed frameworks. In cloud computing frameworks, assimilation figuring is created to give adjusted VMs that are moved in the cloud frameworks [6-7]. In LB frameworks, however a few bio-enlivened calculations like Ant Colony Optimization (ACO), and so on., may check their effectiveness, the greater part of them need accomplishing better results in all qualities. Accordingly, a crossover meta-heuristics technique was proposed by joining the osmotic trademark and bio-roused LB calculations [8]. The osmotic trademark was utilized to empower a programmed arrangement of VMs that are relocated by means of cloud frameworks. Likewise, the constraints of traditional bio-motivated calculations were settled by hybridizing the Artificial Bee Colony (ABC) and ACO in the cloud computing.

Cloud computing is a relatively new business model for outsourced services. However, the technology behind cloud computing is not entirely new. Virtualization, data outsourcing, and remote computation have been developed over the last 20 years, and cloud computing provides a streamlined way of provisioning and delivering such services to customers. In this regard, cloud computing has often been criticized as representing just a new trend, rather than an innovative computing technology. As such, it is often best described as a business paradigm or computing model rather than any specific technology. A cloud consumer adopting a cloud-based solution needs to follow these steps:

1. Describe the service or application for which a cloud-based solution may be leveraged

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204006 |

2. Identify all functional capabilities that must be implemented for this service
3. Identify the security and privacy requirements and the security controls needed to secure the service or application.

The trust relation between cloud customers (CCs) and cloud service providers (CSPs) has to be established before CCs move their information systems to the cloud. This requires an in-depth understanding of associated risks. Moreover, regulations related to data protection, financial reporting, etc. involve certain requirements that should be complied with when outsourcing business processes to third parties, like CSPs. User authentication and authorization among cloud actors is a critical element of cloud architecture. Without knowing who is logging into the cloud-based information system, and who is accessing what data, cloud actors are not able to protect the data housed by a cloud ecosystem. Understanding who the users are, what data they are trying to access, where the data are stored, and how are users trying to get to these data—these are critical pieces of information that help cloud consumers determine an appropriate cloud architecture and deployment model.

III. PROPOSED WORK

The service models are nothing but the type of services provided by the cloud providers. Based on the needs of the business concerns the services are provided in three types

1 .Infrastructure as a Service

This service shortly called as IaaS provides all the resources that are needed to setup the business infrastructure. It includes various components such as networking, storage, servers, operating systems, virtual machines (VM's). IaaS cloud providers supply these resources on-demand from their large pools of equipment. Eg: AmazonElasticCloud (EC2), Rack space.

2. Platform as a Service

The next level up from IaaS is PaaS where the cloud providers not only take care of the components provided by IaaS but also manages the platform – level components and methods like middleware (IIS, Tomcat, JBoss .) and runtime(.Net framework ,java runtime) will be pre-installed. The customer can just focus on developing and managing application and data related to it. Eg: GoogleAppEngine, Windows Azure Platfrom.

3. Software as a Service

The most common service is the SaaS where all the business activities are run in cloud and all portions are managed by the cloud providers itself>They take care of everything from the application to networking. The firms need not pay for license but use the software's as service whenever needed and pays the vendors accordingly. Eg: Gmail, Google Docs, Office 365 All these applications provide a storage place for our files in the network thus enabling ubiquitous access of resources. Files include documents, images, videos etc.

The proposed system for the "Self-Destruction System in a Cloud Server for Data Privacy" project envisions a cutting-edge solution that significantly enhances data privacy and security in cloud computing environments. The core functionality allows users to register and log in securely, providing them access to a range of features. The File Upload module facilitates seamless uploading of various file types to the cloud server while ensuring the implementation of robust security measures. The distinctive Self-Destruction Process empowers users with the ability to remotely initiate the secure deletion of their uploaded files, offering an additional layer of protection against unauthorized access. Moreover, the View Overall Updated Files feature provides users with a comprehensive overview of their uploaded files, enhancing their ability to manage and monitor their data effectively.

IV. RESULTS AND DISCUSSION

The Registration module facilitates the on boarding of new users into the system. Users are prompted to provide necessary information such as a unique username, a secure password, and a valid email address. This step ensures the creation of individual user accounts within the platform.The Login module enables registered users to securely access the system. Users enter their credentials, including the username and password, and undergo a secure authentication process. Successful login grants users access to their personalized accounts, ensuring data security. The File Upload module empowers users to transfer files to the cloud server seamlessly. Users can select and upload files of various formats, and

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204006 |

the system employs security measures to protect the integrity and privacy of the uploaded data. This critical module allows users to take control of the security of their uploaded files. Through a secure and authenticated process, users can initiate the self-destruction of their files, providing an added layer of data privacy and security in case of unauthorized access or other security concerns. The Cloud Admin module serves as the administrative interface for overseeing user activities. Admins have the capability to manage user accounts, reviewing details of registered users and ensuring adherence to security protocols. Furthermore, administrators can oversee and manage the files uploaded by users, ensuring system-wide compliance and security. This module acts as a centralized hub for effective oversight and management of the entire system

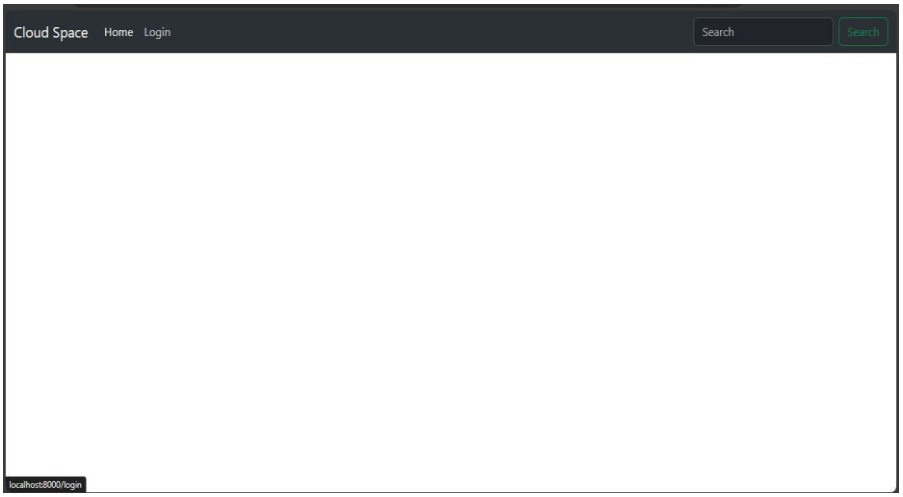

Fig-1 User Interface

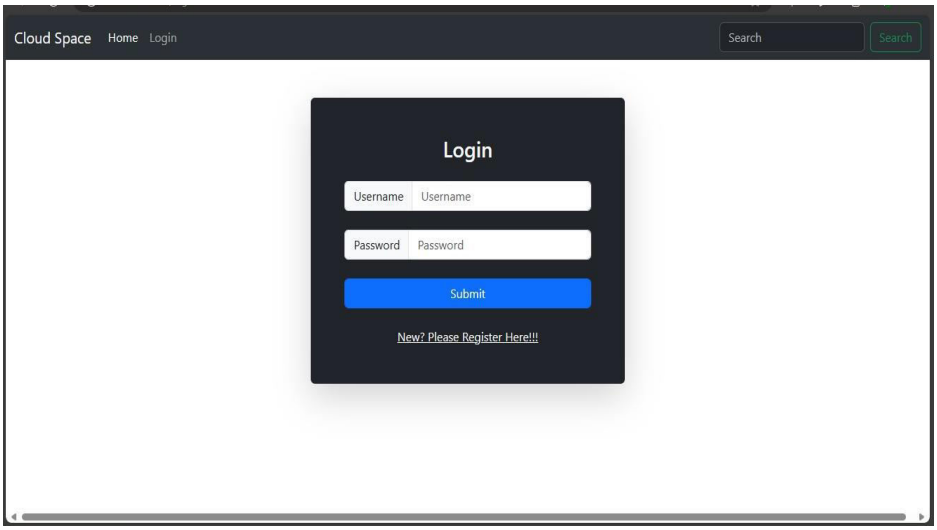

Fig-2 login Interface

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204006 |

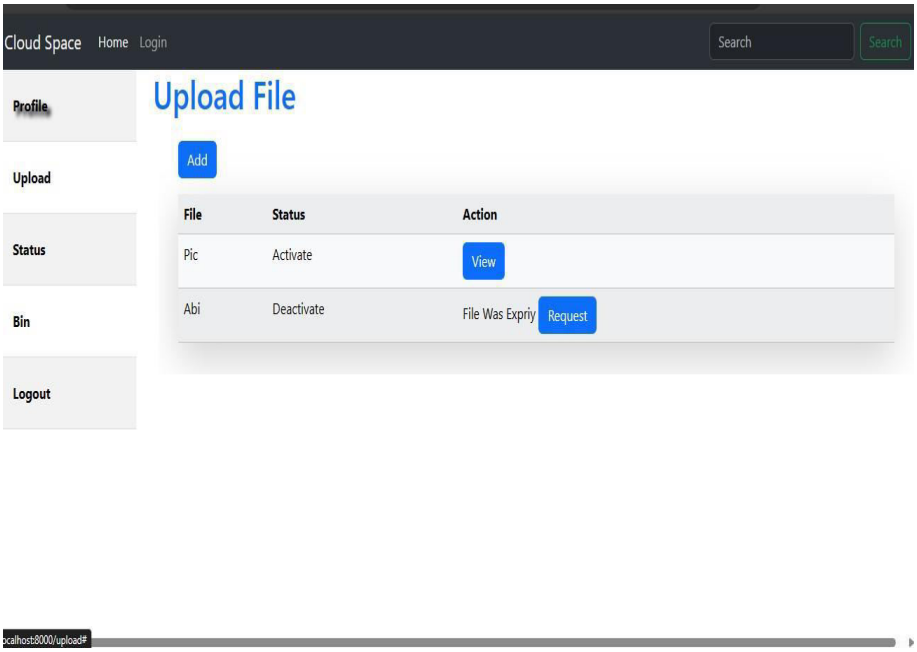

Fig-3 Results

V. CONCLUSION

In conclusion, this system introduces a novel approach by leveraging the essential properties of the active storage framework based on the T10OSD standard. The feasibility of this approach is demonstrated through SeDas, a proof-of-concept prototype utilizing object-based storage techniques. SeDas facilitates the irreversible self-destruction of sensitive information, such as account numbers, passwords, and notes, without requiring any action from the user. Our comprehensive measurement and experimental security analysis provide valuable insights into the practicality and effectiveness of our approach.

REFERENCES

1. Lutz, M. (2013). Learning Python, 5th *Edition* (5 edition). Beijing: O'Reilly Media.
2. Tibbits, S., van der Harten, A., & Baer, S. (2011). Rhino *Python* Primer (3rd ed.).
3. Downey, A. B. (2015). "Think Python: How to Think Like a Computer Scientist (2edition)". Sebastopol, CA: O'Reilly Media.
4. Greg Wilson. "Data crunching: solve everyday problems using Java, Python and more. The pragmatic programmers", Pragmatic Bookshelf, Raleigh.
5. Guido van Rossum and Fred L. Drake, Jr. "The Python Tutorial — An Introduction to Python". Network Theory Ltd., Bristol,
6. Michael Dawson. "Python programming for the absolute beginner". Premier Press Inc., Boston, MA, USA, 2003.
7. Harvey M. Deitel, Paul Deitel, Jonathan Liperi, and Ben Wiedermann"Python How To Program". P T R Prentice-Hall, Englewood Cliffs.
8. Brad Dayley. "Python phrasebook: essential code and commands. Developer's library". SAMS Publishing, Indianapolis,
9. Liza Daly. "Next-generation web frameworks in Python". O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol.
10. Mike Dawson. "Python programming for the absolute beginner". Thomson Course Technology, Boston,
11. Peter Norton, Alex Samuel, David Aitel, Eric Foster-Johnson, Leonard Richardson, Jason Diamond, Aleatha Parker, Michael Roberts, "Begining Python", 2005.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details