JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Data Security and Privacy Protection for Cloud Storage: A Survey

Mr. Dasari Vikas Babu*[1], Mrs. P. Pavitra*[2]

[1]MCA Student, Department of Master of Computer Applications,
Vignan's Institute of Information Technology (A), Beside VSEZ, Duvvada, Vadlapudi Post,Gajuwaka, Visakhapatnam-530049.

[2]Assistant Professor, Department of Information Technology,
Vignan's Institute of Information Technology (A), Beside VSEZ, Duvvada, Vadlapudi Post,
Gajuwaka, Visakhapatnam-530049.

Abstract

Newtrends such as the Internet of Things (IoT), the smart city, the digital transformation of companies and the global digital economy are at the forefront. With data storage and management, the cloud storage system is becoming an indispensable part of the new era. Today, authorities, companies and individual users are actively transferring their data to the cloud. Such a large amount of knowledge can create great wealth. However, this increases potential risks such as unauthorized access, data leakage, disclosure of sensitive information and privacy. Although there have been some studies on data security and privacy protection, there is no systematic research on this topic in cloud storage. In this paper, we provide a comprehensive review of the security and privacy literature and first provide an overview of cloud storage, including defining application classification and architecture. Second, we provide a detailed analysis of data security and privacy protection challenges and cloud storage requirements. Third, data encryption techniques and protection methods are discussed. Finally, we discuss data security research topics in cloud storage.

1. INTRODUCTION

Information is considered the most important asset of an organization because it defines the uniqueness of each company. It is the most important foundation of knowledge, information and ultimately the wisdom of right decisions and actions. It can help cure diseases, increase business income, make a building more efficient or be responsible for achieving goals and improving performance. In addition, data storage, analysis and sharing are key services that every organization needs to improve performance. However, due to the explosion of data, companies are under enormous pressure to store big data on-premises. Finding information has also become more difficult due to limited resources. Most of the companies have switched to cloud computing for these services because of its many benefits such as on-demand service, scalability, reliability, flexibility, scalable services, disaster recovery, accessibility and more. Cloud computing is a paradigm that enables massive memory space and massive computing power at low cost. It enables users to receive targeted services from multiple platforms regardless of location and time, providing a wide range of conveniences for cloud users. By moving the local data management system to cloud storage and using cloud-based services, users can save costs and improve the productivity of project management and collaboration. As a result, individuals and organizations are increasingly moving to the cloud for many of their services. With the ever-expanding expansion of cloud technology, it is not difficult to imagine that almost all companies will move to the cloud in the near future. Despite the many features offered by cloud computing, it faces a number of obstacles that can hinder its rapid growth if not properly addressed. Consider a real-world application where a company allows its employees or departments to store and share data through the cloud. By using the cloud, the company can completely free itself from the burden of local maintenance and data storage. At the same time, it is also immune to various security threats, which is the biggest concern of cloud users. First, outsourcing data to cloud servers means that the data is under the control of the users, which makes users uncomfortable because the outsourced data may contain sensitive and valuable information. Second, information sharing often takes place in a hostile and open environment, and the cloud server has proven to be a target for attacks. In the worst case, the cloud server can expose users' data for illegal profit. In addition, information must be shared among various stakeholders such as business partners, employees, customers, etc. inside or outside the organization to improve business operations. However, the recipient may misuse this information and intentionally or unintentionally disclose it to an unauthorized third party.

2.LITERATURE SURVEY

[1] Kao et al. introduced a user-centric key management system called Cloud to protect the cloud. In the cloud, user data is encrypted indirectly with RSA using users' public keys. Users' private keys are stored on users' mobile devices, not on users' computers or servers. In addition, two-dimensional (2D) barcode images are used to represent users' private keys, which are later used to decrypt users' sensitive information.

[2] Al-Haj et al. provided two crypto-based algorithms to ensure data confidentiality, integrity and authenticity. They implemented an encryption function using a hash code and symmetric keys to protect the data. Integrity and authenticity are ensured by an elliptic curve digital signature algorithm. In addition, the standard galois counter mode of advanced encryption is used together with the Whirlpool hash function to support authenticity and confidentiality.

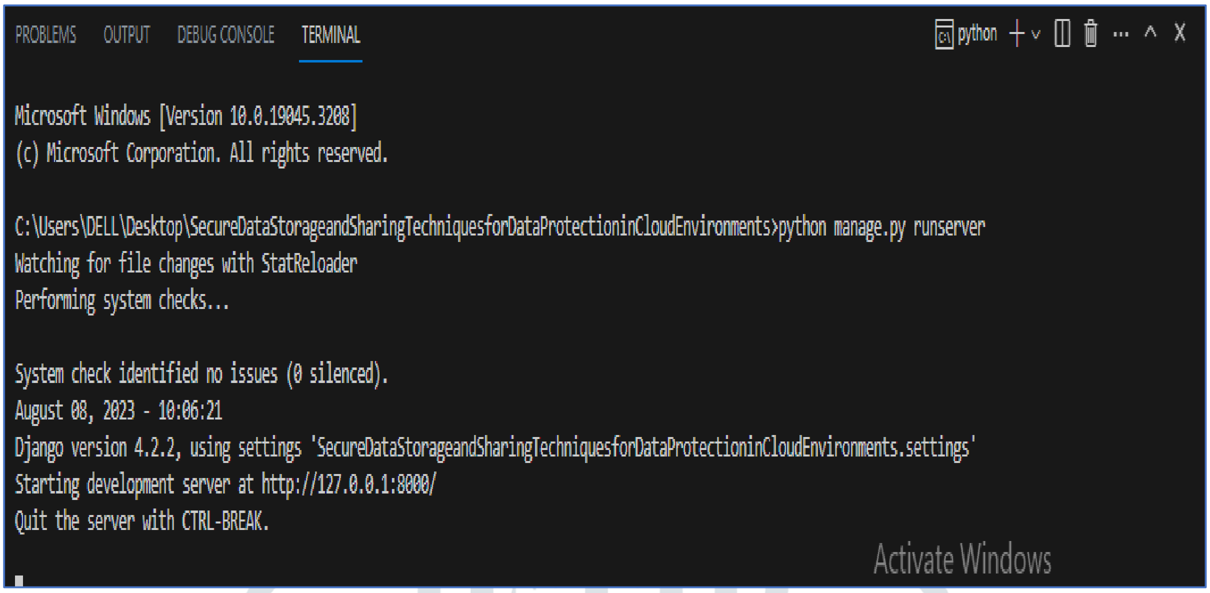
3.EXISTING SYSTEM

Data protection is a primary concern in the field of data security and cloud computing. Many solutions have been developed for this challenge. At the same time, there is no comprehensive analysis among the existing solutions, and it is necessary to study, classify and analyze the existing important work to find out the suitability of these solutions to the requirements.

4. PROPOSED SYSTEM

A number of clou data protection models have been researched and developed for many applications. Data protection is usually achieved through leak prevention and leak detection, and this article focuses on achieving effective protection by preventing leaks and identifying the malicious entity responsible for the leak as described. The main approaches to prevent data leakage are adaptive cryptography and access control mechanisms.

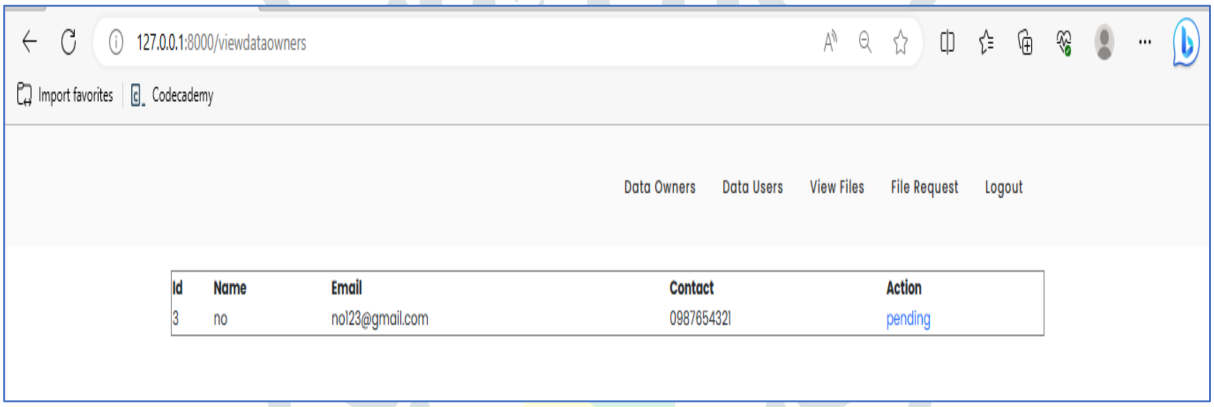
5.EXPERIMENTAL RESULTS



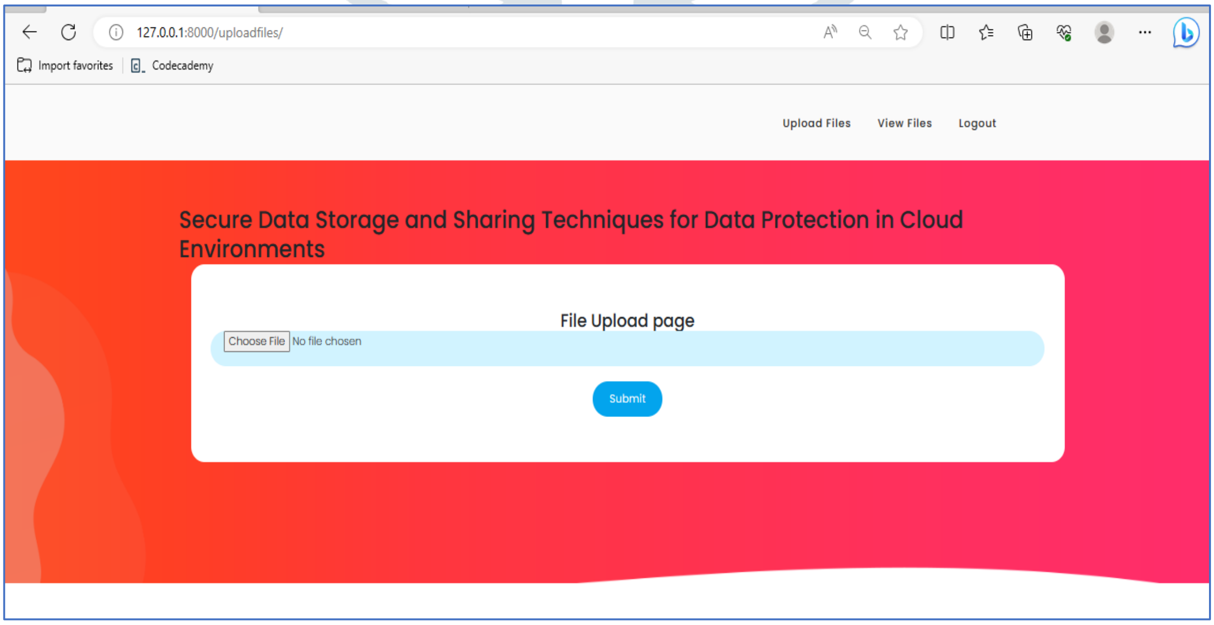
```
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL\Desktop\SecureDataStorageandSharingTechniquesforDataProtectioninCloudEnvironments>python manage.py runserver
Watching for file changes with StatReloader
Performing system checks...

System check identified no issues (0 silenced).
August 08, 2023 - 10:06:21
Django version 4.2.2, using settings 'SecureDataStorageandSharingTechniquesforDataProtectioninCloudEnvironments.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```



Id	Name	Email	Contact	Action
3	no	no123@gmail.com	0987654321	pending



Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments

File Upload page

6.CONCLUSION

Data protection is a complex task in the field of cloud services and data security. Many works are interpreted to mitigate this challenge. However, a comprehensive overview of current solutions is not enough. This article provided a comprehensive analysis and explored key operational technologies and related solutions to securely share data in a cloud environment for data protection purposes. Important and sufficient information necessary to find the core of the method is highlighted, as well as the research gaps and future directions of each discussed solution. In addition, a comprehensive analysis and comparison is made between the mentioned technologies. The importance of each technique is analyzed according to the context.

7. REFERENCES

[1] Mohammad Ausaf Anwar, DurgaprasadGangodkar, "Design and Implementation of Mobile Phones based Attendance Marking System", Department of Computer Science Engineering, Graphic Era University, Dehradun, Uttarakhand, India, 2015.

[2] Jun Lio, "Attendance Management System using a Mobile Device and a Web Application", Department of Socio-informatics, Faculty of Letters Chuo University 742-1 Higashinakano, Hachioji-shi, Tokyo 192-0393, Japan, 2016.

[3] Mahesh G, Jayahari KR, Kamal Bijlani, "A Smart Phone Integrated Smart Classroom", Amrita e-Learning Research Lab (AERL) Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham, Amrita University, India, 2016.

[4] Ekta Chhatar, Heeral Chauhan, Shubham Gokhale, Sompurna Mukherjee, Prof. Nikhil Jha, "Survey on Student Attendance Management System", S.B. Jain Institute of Technology, Management and Research, Nagpur, 2016.