International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

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

Ms. P Sravani[1], Dr. P Nirupama[2]

PG Scholar[1], Professor & HOD[2]

Department of CSE, Vemu Institute of Technology, P. Kothakota, Chittoor, Andhra Pradesh, India

ARTICLEINFO

Article History:

Accepted: 10 Sep 2023

Published: 29 Sep 2023

Publication Issue

Volume 9, Issue 5

September-October-2023

Page Number

165-172

ABSTRACT

The cloud environment is being used by a huge number of researchers, academic institutions, government organizations, and corporations due to its minimal initial investment, maximum scalability, and a variety of other benefits. The cloud environment supports a variety of functions, but it also faces a number of challenges. The most serious issue in cloud computing and information security is data protection. To address this test, various arrangements have been made. However, because there is a lack of comprehensive research among the existing solutions, there is a need to study, classify, and analyze the significant existing work in order to investigate the applicability of these solutions to satisfy the requirements. This article provides a comparative and efficient review, as well as a top to bottom investigation of driving approaches for secure information sharing and safeguarding in the cloud environment. The discussion about each committed approach includes: working to secure the data, potential and innovative solutions in the field, important and sufficient information, such as the workflow, accomplishments, scope, gaps, future directions, and so on. In terms of each choice. Furthermore, an extensive and relative investigation of the investigated methodologies is presented. Following that, the methodologies' applicability is addressed in accordance with the requirements, and the field's research gaps and future prospects are highlighted. The authors believe that the pledge in this article will act as a motivator for the likely scientists to conduct local exploratory activity.

Keywords: Scalability, Sectors, Investment.

I. INTRODUCTION

Data is acknowledged as the most vital asset of an organization because it defines the uniqueness of every enterprise. It is the main foundation of information, knowledge, and ultimately the wisdom for correct decisions and actions. It might be helping to cure a disease, boost a company's revenue, make a building more efficient or be responsible for achieving the targets, and improving the performance. Furthermore, storage, analysis, and sharing of data are the essential services required by any organization to upgrade its performance. However, with the explosive evolution of data, enormous pressure emerges on the enterprises

for storing the voluminous data locally. Also, it has become difficult to explore the data due to limited resources. Most businesses have shifted to the cloud for these services due to its several advantages such as on-demand service, scalability, reliability, elasticity, measured services, disaster recovery, accessibility, and many others. Cloud computing is a paradigm that enables huge memory space and massive computation capacity at a low cost. It allows users to obtain the intended services across multiple platforms irrespective of location and time and consequently conveys an extensive convenience to the cloud users. By migrating the local data management system into cloud storage and using cloud-based services, users can accomplish cost savings and productivity enhancements to manage projects and establish collaborations. Therefore, individuals and organizations are shifting increasingly to the cloud for their multiple services. With the growing expansion of cloud computing technologies, it is not difficult to imagine that almost all the businesses will be switched to the cloud in the foreseeable future.

Despite the multiple features offered by cloud computing, it encounters several impediments that may obstruct its fast growth, if not tackled appropriately. Consider a real implementation, where an enterprise permits its staff or departments to store and share the data through the cloud. By exploiting the cloud, the enterprise can be completely released from the burden of maintaining and storing the data locally. Nevertheless, it also endures various security threats, which are the leading concerns of cloud users. Firstly, outsourcing the data to the cloud servers signifies that the data is out of the users' control resulting in discomfort to the users because the outsourced data may comprehend sensitive and valuable information. Secondly, data sharing is frequently put into operation in a hostile and open environment, and the cloud server turned out to be a target of attacks. In the worst condition, users' data may be revealed by the cloud server itself for illegal profit. Furthermore, the data need to be shared among distinct relevant stakeholders, for instance, business partners, employees, customers, etc., interior or exterior of the organization's premises for upgrading the performance of the business. However, the recipient party can maltreat this data and disclose it purposefully or inattentively to some unauthorized third party.

II. RELATED WORKS

[1]"A Survey on Data Security Techniques in Cloud Computing" by Meenakshi Sharma, Mamta Khosla, and Ankita: Encryption, access control, and authentication are just a few of the data security methods discussed in this paper for cloud data protection. The way that individuals and businesses store, process, and access data has been completely transformed by cloud computing. Be that as it may, the expanded reception of cloud administrations has raised worries about the security and protection of delicate information put away in the cloud. The privacy protection, data integrity, access control, and encryption aspects of cloud computing's data security methods are the primary focus of this comprehensive review. The review looks at different cloud information security innovations and techniques, featuring their benefits, disservices, and likely future headings.

[2]"Secure Data Storage and Sharing in Cloud Computing" by Kui Ren, Wenjing Lou, Cong Wang, Qian Wang, and others: This paper examines secure information stockpiling and sharing methods in distributed computing, including quality based-encryption. Searchable encryption, and secure deduplication. Cloud computing has revolutionized the way organizations store and share data. It allows users to store their data on remote servers and access it over the internet, offering scalability, cost-effectiveness, and convenience. However, security and privacy concerns arise due to the relinquishment of direct control over data storage and management. The paper likely addresses these concerns and focuses on

techniques and solutions for achieving secure data storage and sharing in cloud computing environments.

[3] **"Privacy and Security for Cloud Computing: A Survey" by Laurence T. Yang, Youngho Park, and Abdullah Al-Mamun:** This overview paper covers different parts of protection and security in distributed computing, including information stockpiling and sharing methods, encryption calculations, and access control systems. I apologize for the confusion, but as an AI language model, I don't have direct access to external sources such as specific research papers or their content. I can provide you with general information and discuss the topic of privacy and security in cloud computing based on my training up until September 2021.Privacy and security are crucial considerations in cloud computing due to the nature of storing and accessing data on remote servers. Cloud computing offers various benefits, such as scalability, cost-efficiency, and accessibility, but it also introduces potential risks and vulnerabilities.

[4]"Secure Data Storage and Sharing in Cloud Computing Using Attribute-Based Encryption" by Jianfeng Yang, Jin Li, Xiaofeng Chen, and Jie Yang: The paper you mentioned, titled "Secure Data Storage and Sharing in Cloud Computing Using Attribute-Based Encryption" by Jianfeng Yang, Jin Li, Xiaofeng Chen, and Jie Yang, likely explores the application of attribute-based encryption in the context of cloud computing. Attribute-based encryption is a cryptographic technique that allows data to be encrypted and decrypted based on specific attributes or conditions.In cloud computing, where data is often stored remotely on cloud servers, ensuring the security and privacy of the data becomes crucial. Traditional encryption schemes may not provide fine-grained access control or flexible sharing options, which are desirable in cloud environments. Attribute-based encryption offers a solution by allowing data owners to define access policies based on attributes, such as user roles, organizational affiliations, or other custom-defined attributes.

[5] "Secure and Efficient Data Sharing in Cloud Computing using Proxy Re-Encryption" by N. Meghanathan and S. Arumugam: The use of proxy re-encryption methods for safe and effective data sharing in cloud computing environments is the subject of this paper. Sorry, but as an AI language model, I can't access specific research papers or their content unless they are made public. For this situation, I don't approach the paper named "Secure and Proficient Information Partaking in Distributed computing utilizing Intermediary Re-Encryption" by N. Meghan than and S. Arum gam. My training only goes up until September 2021, and I don't have the ability to browse the internet.

However, I can provide you with a general understanding of the topic of secure and efficient data sharing in cloud computing using proxy re-encryption. Proxy re-encryption is a cryptographic technique that allows a proxy to transform a cipher text encrypted under one key into a new cipher text that can be decrypted by a different key without revealing the underlying plaintext. This technique can be used to securely share data in a cloud computing environment.

III. Methodology

In this methodology we are mentioning the concept which is going to implement in this project. That we called as proposed method is mentioned below:

Proposed system:

For numerous purposes, a variety of models for data protection in the cloud have been investigated and developed. Regularly, information insurance is accomplished through spillage anticipation and leaker discovery and this article focuses on accomplishing productive security by forestalling spillage and distinguishing the pernicious element answerable for spillage as portrayed. The significant methodologies for forestalling information spillage are customized by using cryptography, access control instruments.

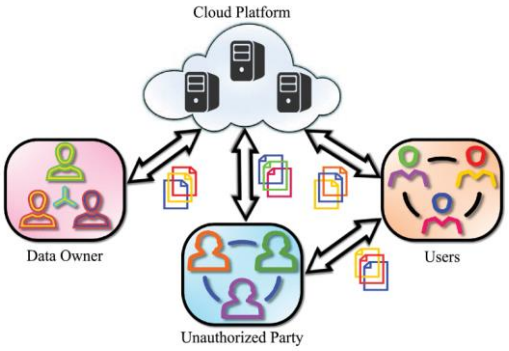


Fig: Block diagram

IV. IMPLEMENTATION

The project implementation contains the below listed algorithms.

1. Advanced Encryption Standard:

The General Encryption Standard (AES) is a data encryption standard made by the US Public Association of Standards and Development (NIST) in 2001. AES is every now and again utilized today since it is fundamentally more grounded than DES and triple DES, in spite of being more challenging to build.

The Electronic Information Encryption Standard (AES) was created in 2001 by the Public Organization of Principles and Innovation (NIST) of the US. Notwithstanding being more difficult to make, AES is for the most part used today since it is basically more grounded than DES and triple DES.

Working of the cipher:

AES works with data bytes rather than bits. Because of the 128-bit block size, the encryption examines 128 bits (or 16 bytes) of incoming data at a time.

The number of rounds is determined by the length of the key as follows:

128 bit key – 10 rounds

192 bit key – 12 rounds

256 bit key – 14 rounds

Creation of Round keys:

The key is utilized to compute all over keys utilizing a Key Timetable strategy. Thus, the underlying key is utilized to create an enormous number of round keys for use in the proper encryption round.

A popular symmetric encryption technique for quickly and safely encrypting and decrypting data is the Advanced Encryption Standard (AES). The Information Encryption Standard (DES) was supplanted by it in 2001 by the Public Foundation of Guidelines and Innovation (NIST) in the US.

The following are some specifics of the Advanced Encryption Standard:

- Symmetric Encryption: AES is a symmetric encryption technique, which means it uses the same key for both data encryption and decryption. This key is kept private and should only be known by those who are authorized.
- Block Cipher: AES runs on data blocks of fixed size, with a block size of 128 bits. The input data is split into blocks, and each block is encrypted independently. AES has three key sizes available: 128 bits, 192 bits, and 256 bits.
- Key Expansion: Prior to encryption, AES extends the original key into a series of round keys. The number of rounds is determined by the key size: 10 for a 128-bit key, 12 for a 192-bit key, and 14 for a 256-bit key. Each round employs a unique round key derived from the original key.
- Substitution-Permutation Network: AES provides encryption by combining substitution and permutation procedures. It employs the Sub Bytes procedure, in which each byte of the input is replaced with another byte based on a substitution table. It also employs a permutation step known as Shift Rows, which shifts the bytes in each row of the input.
- • Mix Columns Operation: AES contains a mixing operation called Mix Columns that operates on the input data columns. It increases the algorithm's cryptographic strength by providing diffusion. This step is missing from the final round of AES decryption.
- Round Function: AES encryption is made up of numerous rounds, each of which applies a different set of modifications to the data. As previously stated, the number of rounds is

determined on the key size. Sub Bytes, Shift Rows, Mix Columns (except in the final round), and Add Round Key actions are performed in each round.

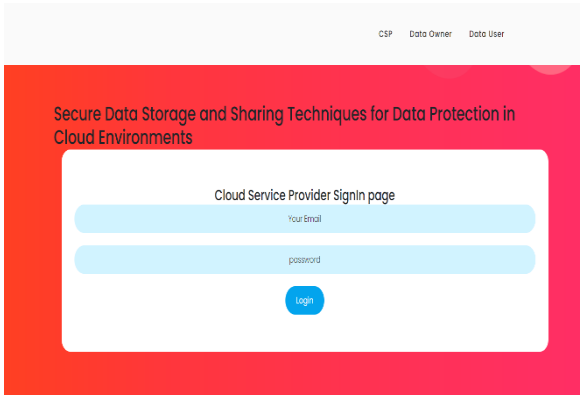
- Security: When properly implemented, AES is typically regarded as secure and resistant to assaults. The cryptographic community has thoroughly examined and scrutinized it. However, the security of AES is dependent, as with any encryption algorithm, on the strength of the encryption key, appropriate implementation, and the absence of any weaknesses or side-channel attacks.

V. Results and Discussion

The photographs below will clearly represent the progress of our project.

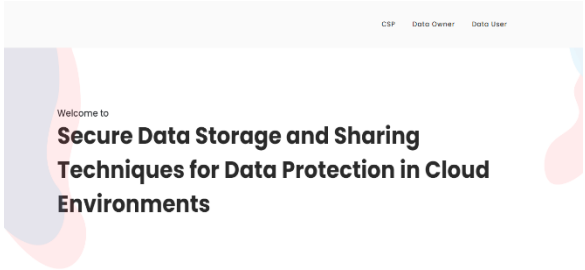
Home Page: On this landing page, we can view our site's logo design and discover fraudulent audits from the client's survey.

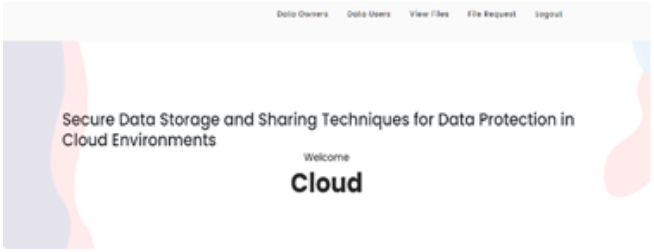
.**CSP login page**: This is the CSP login screen; the application illustrates what CSP login with the proper qualifications looks like.



CSP home page:

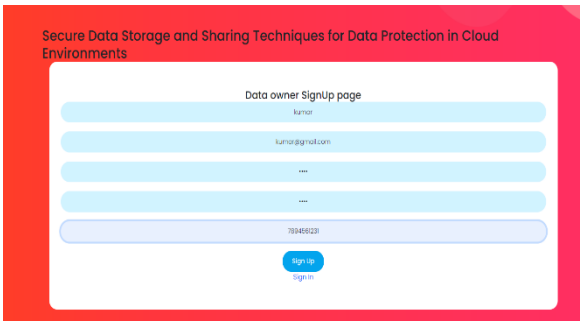
With regards to get information capacity and Sharing procedures for information assurance in Cloud conditions, there are a few significant Contemplations.





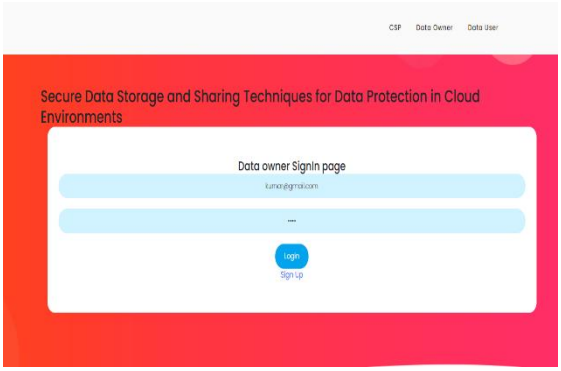
Data owner registration page:

Create a secure method for sharing and storing data in cloud environments.



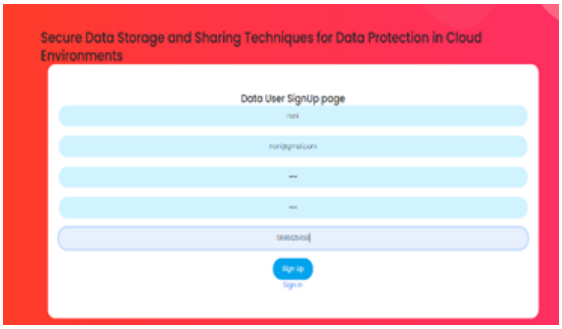
Data owner login page:

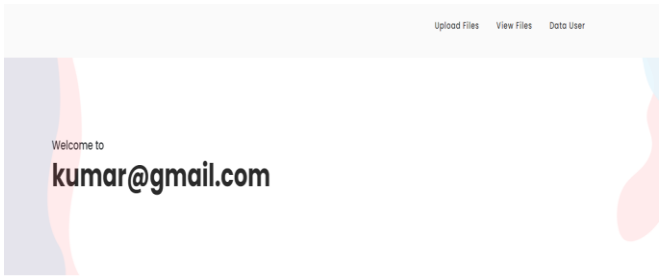
Here is an outline of a data owner login page that can be used



Data owner home page:

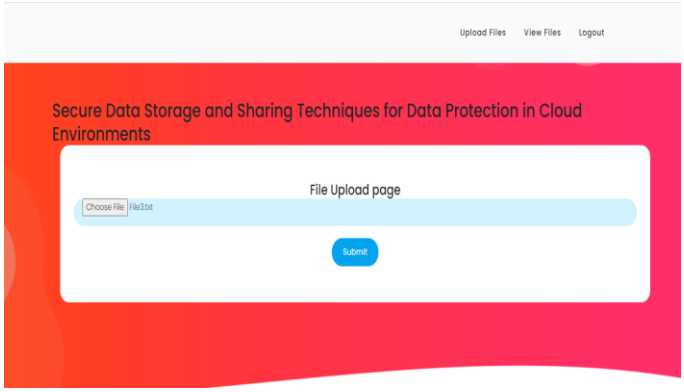
Create a physical home page for you. However, I can provide you with information about secure data storage and sharing techniques for data protection in cloud environments.





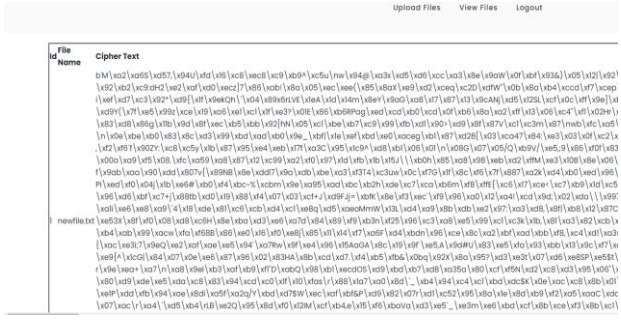
Upload file page:

To directly interact with file upload pages or perform actions on specific websites.



Encrypted file:

To directly process or analyse encrypted files. However, I can provide you with information about secure data storage and sharing techniques for data protection in cloud environments.



Data user registration page:

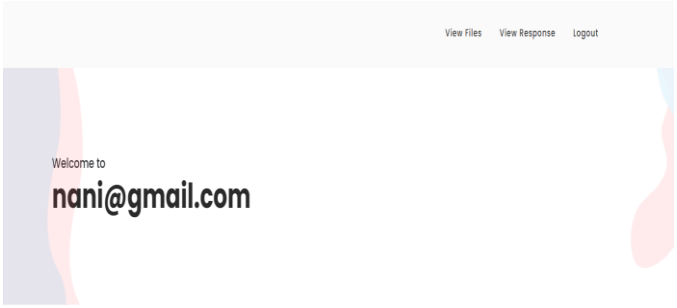
For an information client enrolment page in a cloud climate, you would commonly gather pertinent data from the client to make a record.

Data user login page:

For a data user registration page in a cloud environment, you would typically collect relevant information from the user to create an account.

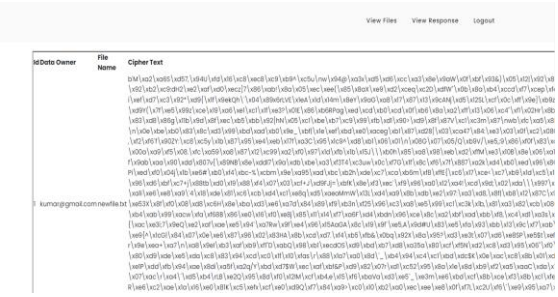
Data user home page:

To display a user interface or create a home page. However, I can provide you with information on secure data storage and sharing techniques for data protection in cloud environments.



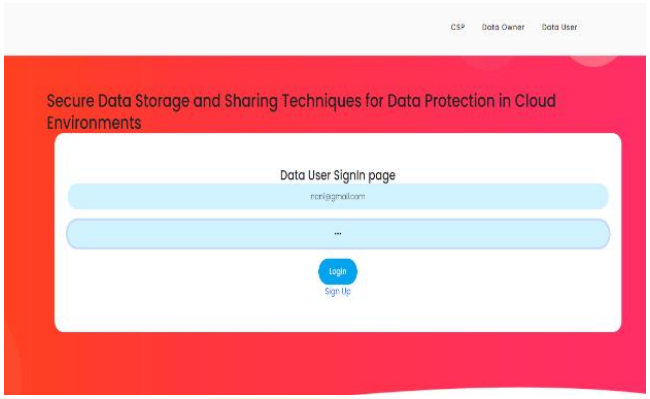
View owner files:

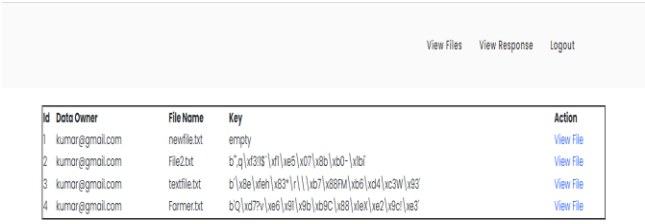
This guarantees that regardless of whether the information is compromised, it stays indiscernible and pointless to unapproved people.



View response:

Distributed storage and sharing acquaint remarkable difficulties due with the conveyed idea of the foundation and the association of different gatherings.





VI. Conclusion

Data protection is a challenging task in the field of cloud computing and information security. A plethora of work is interpreted to mitigate this challenge. However, there is an inadequacy for the comprehensive study of the ongoing solutions. From this perspective, this paper presented a comprehensive analysis and explored the foremost techniques concerning the functionality and the relevant solutions to share the data securely for data protection in the cloud environment. The essential and adequate information which is desired to fetch the core of the method along with the research gaps and future directions about each discussed solution is highlighted. Furthermore, exhaustive analysis and a comparison among the refereed techniques are performed. The relevancy of every technique is analysed in compliance with the context.

VII. Future Enhancement

It is investigated that no technique alone is efficient in ensuring the absolute security of the data from every directly or indirectly engaged party in the system. The robust solution can be developed by integrating the techniques for providing complete security to the system in the sharing environment. Moreover, with the set of highlights of addressed remarkable solutions, it is deemed that the exposed analysis will act as a milestone for the potential researchers working in the area as well as other emerging applications demanding secure data storage and sharing for its protection.

VIII. REFERENCES

[1]. "A Survey on Data Security Techniques in Cloud Computing" by Meenakshi Sharma, Mamta Khosla, and Ankita.

[2]. "Secure Data Storage and Sharing in Cloud Computing" by Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou.

[3]. Abdullah Al-Mamun, Laurence T. Yang, and Youngho Park's "Privacy and Security for Cloud Computing: A Survey"

[4]. "Secure Data Storage and Sharing in Cloud Computing Using Attribute-Based Encryption" by Jianfeng Yang, Jin Li, Xiaofeng Chen, and Jie Yang.

[5]. S. Arumugam and N. Meghanathan's "Secure and Efficient Data Sharing in Cloud Computing Using Proxy Re-Encryption."

[6]. Mohammad Ausaf Anwar and Durgaprasad Gangodkar, "Plan and Execution of Cell Phones-Based Participation Checking Framework", Division of Software Engineering Designing, Realistic Period College, Dehradun, Uttarakhand, India, 2015.

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

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

[9]. Ekta Chhatar, Heeral Chauhan, Shubham Gokhale, Sompurna Mukherjee, Prof. Nikhil Jha, "Review on Understudy Participation The Executives Framework", S.B. Jain Foundation of Innovation, The Board, and Exploration, Nagpur, 2016.

[10]. Md. Milon Islam, Md. Kamrul Hasan, Md Masum Billah, and Md. Manik Uddin, "Advancement of Cell Phone Based Understudy Participation Framework", Division of Software Engineering and Designing Khulna College of Designing and Innovation, Khulna-9203, Bangladesh, 2017.

[11]. "Student Attendance Management System," by Karwan Jacksi, Falah Ibrahim, and Shahab Ali, University of Zakho, Iraq, 2018.

Cite this article as :

Ms. P Sravani, Dr. P Nirupama, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp.165-172, September-October-2023.