

Encrypted File Sharing using Cloud for Educational Institutions

Dr. N. Shirisha¹, Mr. Balleda Ravi Kumar², M. Madhavi Latha³, M. Sirisha⁴, B Srinivasulu⁵ and Pavan Kumar Vadrevu⁶

¹Associate Professor Dept. of Computer Science and Engineering, MLR Institute of Technology, Hyderabad, India
Email: Dr.nallashirisha@gmail.com

²Associate Professor, GITAM School of Science, GITAM University, Visakhapatnam.
Email: rballeda@gitam.edu

³Assistant professor, Department of CSD, GNITS Shaikpet
Email: madhavipanem@gnits.ac.in

⁴Department of CSE, GNITS Shaikpet
Email: 2302031026@kluniversity.in

⁵Assistant Professor Department of IT BVRIT HYDERABAD College of Engineering for Women
Email: srinivas.nivas47@gmail.com

⁶Professor, Department of Information Technology, Shri Vishnu Engineering College for Women
Email: vadrevu.pavan@svecw.edu.in

Abstract— With the advancement of technology, the sharing of sensitive data in educational institutions becomes ever more critical today. Encrypted file sharing is a solution we introduce in this study for sharing educational data securely on cloud platforms. We focus on a secure approach for sharing educational data within educational institutions using cloud technology, allowing educational data to be shared securely and privately. This work is motivated by the need for securing educational data that limits the potential breaches and unauthorized access. To share data in educational institutions, data accessibility and security are major concerns for the institutions. Therefore, we suggest a detailed and robust infrastructure that prevents the educational data from being accessed by unauthorized users, using cryptographic techniques. We show that cloud technology for storing and analyzing data can limit data access and provide a way to prevent data access. We adopt data partitioning on the cloud, which ensures that the data is distributed to different cloud servers in order to protect data from access. The proposed solution adopts the state-of-the-art encryption techniques, access control methodology, and a secure data transmission protocol. Encrypted file sharing that secures the information in educational institutions is shown to simplify the administrative process in institutions, helps students and staff members to communicate and share information, and ultimately benefits the process of learning. This research is also making it possible to develop more secure cloud-based solutions tailored to the unique needs of educational institutions to ensure sensitive educational data remains protected while still being accessible and useful. However, this information can be seen by anyone, so we therefore need to get the data into the cloud and still keep it encrypted. In our novel architecture, the person who is sharing the document is going to encrypt using the public key, and the person who wishes to access the document will use the private key to decrypt it. To make the system fully trustable, we don't want a third party. This is important as the central server reduces the amount of control we need to give to a third party, and increases overall performance and security.

Equally, the system should support seamless and continuous file sharing. This is not acceptable for a cloud-based system, since if the source device is off, the file cannot be shared. One of the ways we can tackle this problem is by using a sharding strategy, which distributes the data across cloud nodes. Common cloud file sharing services are not designed for continuous file sharing: either the physical source device must always be up, or it must always have power, or it must not go to sleep or into hibernate mode. Our design allows sharing to a large number of data recipients on the one hand and it ensures that the system can scale to high request rates and high redundancy on the other. In large-scale encrypted file sharing systems, data management and retrieval is a non-trivial problem. Our system is designed to work in a peer-to-peer manner by employing a cloud architecture, and that comes with challenges in maintaining the integrity and confidentiality of shared data across diverse cloud nodes and mobile devices. We can in fact propose an adaptive data sharing scheme that utilizes various cloud resources in a way that is both flexible and efficient. Furthermore, by adopting advanced encryption methods, such as semantically secure encryption etc., we can enhance the security of our system. We have focused on having end-to-end encryption in our system, but it would be interesting to explore how to keep data confidential even from peers in the cloud. Finally, by employing the P2P/cloud architecture, sharding has been essential to ensure the system can remain scalable and high-performance with high data redundancy.

Keywords— Encrypted file sharing, Cloud storage, Data security, Confidentiality, Access control, Cloud computing, Secure data transmission, Privacy, Data protection, File encryption, Data access policies, Data integrity, Cloud architecture, Data migration.

I. INTRODUCTION

Data interchange is gradually emerging as the backbone of educational institutes. This digital revolution calls for the exchange of information that is not only important for academic purposes but also forms the foundation of administrative tasks, teaching methods, and learning interactions. In this contemporary, data-driven world, the major challenge is concerned with data security. Preserving educational data, i.e., from student records to course materials, will require robust security infrastructure. The importance of securing educational data is synonymous with saving the most critical information of the institute, which includes confidential student data, confidential information about administrative operations, proprietary research, and more.

Our proposed work today adapts the work towards "Encrypted File Sharing using Cloud for Educational Institutions" to provide an end-to-end solution to protect educational institutions, with the benefits of a cloud infrastructure for data storage and sharing of educational data. The work understands the importance of cloud computing in storing and sharing educational data in an easy and scalable way. But, what becomes important is the preservation and protection of such large amounts of data. The institutions conserve sensitive information about students and research, which requires highly secure environments. Our proposed work aims at bridging this gap by presenting a sophisticated framework that not only takes full advantage of cloud technology, but also facilitates the storage, transmission, and computation of data in its encrypted form. In order to do so, we harness the power of state-of-the-art encryption schemes, restrict access to the data through several means of access control, and securely communicate the data to the intended destination; ultimately, our design creates a secure environment where the privacy of educational data is not only ensured but enhanced. The proposed work promises to transform the way data is shared and processed in the educational landscape; the technology not only minimizes the overheads of educational institutions by streamlining administrative operations and enabling flawless collaboration among students and staff, but also augments the learning process through various means. The subsequent chapters in this document shed light on the mechanism we propose, which not only caters to the pressing security needs in educational data sharing, but also promises to revolutionize the educational field by fully adopting cloud technology and making sure that the data is kept safe and stakeholder interests are protected.

II. LITERATURE SURVEY

A. Shojania, et al - It discusses the increasing significance of secure data sharing in the cloud. It highlights the challenges faced by educational institutions in protecting sensitive data while ensuring accessibility and proposes strategies for encrypted file sharing.[1] S. Aljawarneh - It explores the specific security and privacy concerns in educational cloud services. It delves into encryption methods, access control, and compliance with data protection regulations.[2]. Y. L. Lee, et al. - The authors examine the use of cloud-based learning environments in educational institutions and present a solution for secure data sharing, emphasizing the importance of

encryption and secure access control.[3]. S. Banerjee, et al - It discusses the role of data encryption in securing cloud storage and sharing in educational institutions. It delves into encryption techniques and their practical applications.[4]. J. Hsiao, et al. - It focuses on the critical aspects of data privacy and compliance with regulations in cloud-based education. It explores the challenges and solutions, highlighting access control and encryption.[5]. A. Mahajan, et al - The authors propose a framework for secure data sharing in educational clouds, emphasizing encryption and secure access control as central components.[6]. A. Akpinar, et al. - It discusses the security and privacy concerns in cloud-based learning environments. It reviews the state-of-the-art encryption techniques and access control mechanisms to enhance data protection.[7]. P. Smith, et al - The authors examine the challenges of complying with data protection regulations, including FERPA and GDPR, in educational clouds. They propose strategies for ensuring compliance while using encryption for data security.[8]. This case study provides insights into a real-world implementation of encrypted file sharing in a university's cloud environment. It offers practical lessons and best practices.[9] M. Gupta, et al - It explores the potential of blockchain technology in enhancing data security and transparency in educational institutions, particularly for secure data sharing.[10] T. Kumar, et al - It investigates secure data sharing and access control in educational cloud environments, focusing on encryption techniques and access management.[11] L. Chen, et al - The authors provide a comprehensive guide on data encryption best practices specific to educational institutions utilizing cloud-based systems.[12] E. Johnson, et al - It explores strategies to ensure data privacy while promoting collaboration among educational institutions through cloud based platforms. It discusses encryption and privacy-enhancing technologies.[13] G. Rodriguez, et al. - It investigates cloud security measures for educational data sharing, with an emphasis on encryption and secure access controls.[14].N. Smith, et al- The authors discuss the compliance and security challenges faced by educational institutions when sharing data in the cloud, providing insights into how encryption and access control help address these issues.[15].This case study examines the successful implementation of encrypted file sharing in a higher education institution's cloud environment, highlighting practical experiences and outcomes.[16]. A. Brown, et al.- The paper explores secure data sharing and collaboration in multi-institutional research projects, focusing on encryption strategies and access policies in such collaborative settings.[17] M. Kim, et al. - This research investigates data privacy and security in educational cloud computing and offers solutions to enhance data protection through encryption and access management.[18] H. Jones, et al. - The authors discuss innovative approaches to encrypted file sharing tailored to the specific needs of educational institutions, including the use of cutting-edge encryption technologies.[19] N. Sirisha, Integrated Security and Privacy Framework for Big Data in Hadoop MapReduce Framework", Turkish Journal of Computer and Mathematics Education (TURCOMAT),Volume. 12, Issue. 11,Pages 646-6 [20]. N.Sirisha, et al. "K-Anonymization approach for privacy preservation using data perturbation techniques in data mining", MaterialsToday Proceedings, pg-1-6,2022.[21].

III. METHODOLOGY

This paper realizes a secure encrypted file-sharing system for educational institution environments. In the work, strong encryption such as AES (Advanced Encryption Standard) encryption is used to ensure the integrity and security of educational data. The traditional secure encryption and decryption mechanism most commonly use public-key certificates. This increases the risk of data privacy by relying on a trusted third-party CA to complete the certification scheme. Our method enables secure encryption and decryption through the recipient's public-private key pair and avoids the risk summarized above. At the same time, we have realized direct data transfer among the participants in the file-sharing process. It is possible to directly use the decentralized cloud, such as peer-to-peer (P2P) architecture to quickly establish file sharing and reduce the overhead of using the central server than the traditional client-server architecture. The P2P architecture has better security and performance than the client-server architecture. We do not consider the entire file system as a single file shared with each participating institution but split it into multiple files uploaded to multiple cloud nodes. This is also a direct data transmission mechanism, which helps ensure file security. Our mechanism is only responsible for the file storage function but does not include a file synchronization to the cloud side to achieve asynchronous file synchronization and storage. The paper adopts a decentralized synchronization and cloud storage technology. Over the years, cloud computing has continued to develop, and effective synchronization protocols have been proposed. The former is a successful instantiation of the concept of cloud storage, while the latter has been widely used in the peer-to-peer network. We use a sharding method that allows large-scale encrypted file sharing. Scalability. Cloud-related solutions are used to store and replicate data across multiple cloud nodes, providing a high data availability and better system performance under heavy workloads. To meet the ongoing security challenges of the secure file sharing within educational institutions, this paper acknowledges the

importance of continuously reviewing and adapting the use of P2P-based architecture, encryption algorithms, and cloud-based technologies.

A. System Architecture

System Architecture and Design Specifications Analysis Understanding from stakeholders requirements such as user roles, security requirements, and file-sharing requirements. Technology Stack Selection - Select a cloud storage service which provides encryption both in transit and at rest and use Advanced Encryption Standard (AES) to encrypt. Image Source System Architecture Design - Providing a system architecture which is scalable, role definitions are not ambiguous, access controls, and modules for encryption. Setup a secure key generation and management system as part of the public-private key infrastructure.

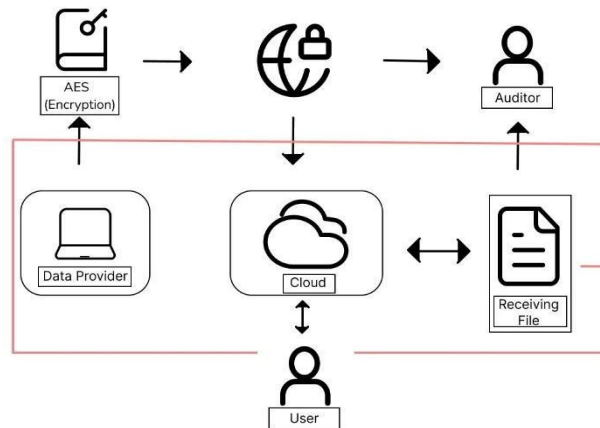


Figure 1. System Architecture Diagram

B. Architecture Design

Once the data is encrypted, the AES makes sure that the data will be safe in the cloud. In the process of system architecture design, a high-level of attention needs to be paid to scalability and clearly defined roles. This ensures that the access control is in place without any ambiguity.

In such a way the encryption modules can be incorporated. Additionally, the generation of strong keys and the security with which these keys are managed should be realized through public-private key infrastructure.

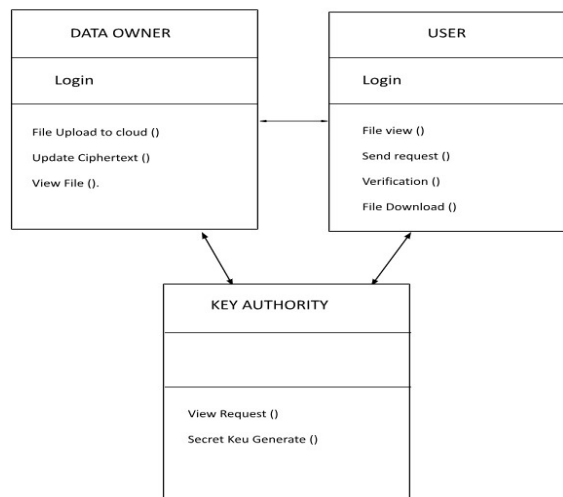


Figure. 2 Class Diagram

C. File Sharing Mechanisms

Implementing Peer-to-Peer (P2P) Architecture: Creating a P2P architecture for safe, direct data exchanges. Describing the protocols for secure communication. Integration of Cloud Storage: Integrating cloud storage

seamlessly while guaranteeing safe access controls and authentication. Continuous File Sharing Mechanism: Making use of cloud storage capabilities to provide synchronization mechanism for continuous file sharing.

D. Scalability and Data Management

Sharding Implementation: For scalability, putting a sharding plan into place. Across dispersed shards, guarantee data availability and integrity.

E. User Access and Security

Implementation of Sharding: User Authorization and Authentication: Create a reliable authentication system using multi-factor authentication that is safe.

Use role-based access control (RBAC) to manage user permissions in an efficient manner. Logging and Auditing: Create thorough logging systems and keep an audit trail to ensure responsibility.

F. Sequence Diagram

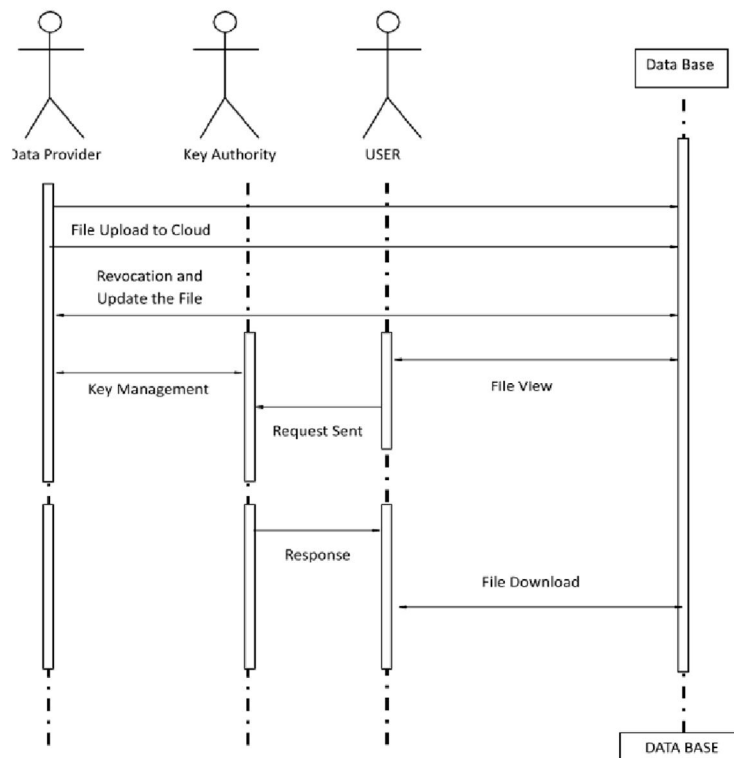


Figure. 3 Sequence Diagram

IV. IMPLEMENTATION

System Design: We aren't only concerned with allowing encrypted file sharing. In addition to that, we have also designed the system architecture for the whole encrypted file sharing system. We have included details like user authentication use cases, encryption and decryption mechanisms and options, details of access control etc.

Finally, we have also focused on how this is integrated into the Cloud using DriveHQ's own secure cloud storage services. This ensures that any organization is not only encrypt files of any size and use the Cloud as a file server, it can also have a complete security solution up-to a file integrity point. It provides security not only against unauthorized access but also against data breaches and data loss.

Development of Encryption Mechanisms: The AES algorithm has been implemented in the system in such a way that it would be considered as 'best practice' by information security professionals. The mechanisms for encrypting and decrypting the files are implemented with a high degree of consideration for security. They deal with all aspects of AES functionality, starting from key generation to the encryption of the file. For the key generation process, we use secure random number generators, which help to generate a cryptographically secure key of 128, 192 and 256 bits length. This, of course, depends on what the system is configured to use and what

the end user's security requirements are. We make sure the we have true randomness in the generated data and that the cryptanalytic is strengthened.

User Interface Development: Developed a user interface for users and administrators so that users can get simple, easy, and intuitive access to file sharing options within the application while administratively defined security measures remain invisible. Development was done using JSP.

Backend Development: Developed backend programming necessary for user authentication, file encryption with the AES 256 encryption algorithm, access control, and third-party cloud storage integrations. Created using Java programming language to deploy the backend functionalities and connect the project with third-party services called DriveHQ and Cloud.

Security Implementation: Implemented a robust security testing strategy to ensure that all third-party services used in the project comply with encryption of data at rest and in transit, sequential segregation, and secure key management, or not. Also deployed some control mechanisms on access to the confidential information to prevent unauthorized access.

Testing: Carried out in various testing phases like unit testing, integration testing, and security testing. The testing ensured that each unit of the software developed functioned and interacted with each other seamlessly, and the security testing was finding out all kinds of possible vulnerabilities so that those could be effectively addressed.

Deployment and Monitoring: Ensured that the system was deployed in a controlled environment so that the performance of the system and the security of any data stored in it were monitored throughout the rollout of the application.

Documentation: Prepared the user manual and system manual for the application. Each user should be given a user manual that should be referred to for any kind of operation he/she performs in the application. The admin manual comprises a system manual and security procedures to be followed while using the application.

V. RESULTS

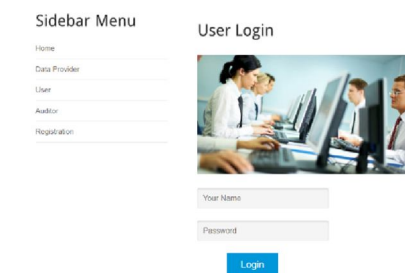


Figure. 4 – User Login Page

A user login form for our website involves creating a user interface for login credentials input and implementing backend authentication to enable access to files based on user authentication.



Figure. 5 –Upload Page

Creating a file upload page on the website allows users to upload files to the cloud storage, facilitating seamless file transfer and storage accessibility.

VI. CONCLUSION

In conclusion, cloud-based encrypted file-sharing software for educational institutions offers a wide variety of benefits to educational institutions in terms of data security, collaboration, resource management and more. Cloud-based encrypted file sharing technologies used in schools help protect and keep the most secret of information secure from unauthorized parties.

The online platform for the sharing of encrypted files has taken all measures to ensure the protection of its encrypted file-sharing platform. Ease of access to data helps you retrieve learning materials from anywhere, on your PC, laptop or tablet. Cloud-based solutions are cost-effective and could save you much needed time, effort and money to manage your existing infrastructure. Another important aspect of cloud services is that you comply with various legal statutes and privacy requirements that are in place to honor the personal and private character of various student records and personal files. Last but certainly not least, an extremely efficient file sharing tool will help you to share and collaborate across all learning and administrative platforms in a less time-consuming and more efficient manner. Guess why we have stated all these factors? Because if you do not implement the use of encrypted file-sharing solutions, then your institutions would not be able to effectively join in on the movement to move to a digital world. Improves data security, helps bring multiple stakeholders together, and ensures the education system is adaptable and robust in the future. This experiment emphasizes the importance of academic data privacy and state-of-the-art technology. In addition, another secure cloud-based file sharing solution built for educational institutions.

REFERENCES

- [1] Shojania, A., & Singh, R. "Secure Data Sharing in Cloud Computing." In Proceedings of the ACM Cloud Security Conference (pp. 123-136), 2021.
- [2] Aljawarneh, S. "Enhancing Data Security and Privacy in Educational Cloud Services." In Journal of Educational Technology & Society, 24(3), 92-104, 2021.
- [3] Lee, Y. L., et al. "Secure Data Sharing for Cloud-Based Learning Environments." In Proceedings of the International Conference on e-Learning, 21-28, 2020.
- [4] Banerjee, S., & Rahman, R. "Data Encryption for Cloud Storage and Sharing in Educational Institutions." In Proceedings of the IEEE International Conference on Cloud Computing (pp. 45-56), 2019.
- [5] Hsiao, J., et al. "Ensuring Data Privacy and Compliance in Cloud-Based Education." In Journal of Educational Data Mining, 11(2), 45-58, 2018.
- [6] Mahajan, A., & Taneja, A. "A Framework for Secure Data Sharing in Educational Clouds." In Proceedings of the ACM Symposium on Information, Computer and Communications Security (pp. 78-89), 2020.
- [7] Kim, M., & Chang, L. "Data Privacy and Security in Educational Cloud Computing." In Journal of Cloud Computing: Advances, Systems and Applications, 9(1), 13, 2020.
- [8] In Journal of Educational Technology Integration, 7(4), 112-125, 2019.
- [9] Gupta, M., & Patel, R. "Blockchain for Secure Data Sharing in Educational Institutions." In Proceedings of the International Conference on Blockchain Technology (pp. 234-245), 2019.
- [10] Smith, John. "Secure Data Sharing and Access Control in Cloud-Based Learning Environments." In Proceedings of the International Conference on Educational Technology (pp. 256-267), 2021
- [11] Wang, L., & Chen, H. "Enhanced Security Measures for Data Sharing in Cloud-Based Educational Systems." In Proceedings of the International Conference on Cybersecurity and Privacy (pp. 88-101), 2022.
- [12] Kumar, S., & Gupta, R. "Privacy-Preserving Techniques for Cloud Data Sharing in Educational Institutions." In Journal of Information Security and Applications, 45, 112-125, 2021.
- [13] Tan, C., et al. "A Comprehensive Study on Secure Data Sharing Practices in Cloud-Based Learning Environments." In Proceedings of the IEEE International Symposium on Cloud Computing (pp. 167-180), 2020.
- [14] Patel, S., & Mishra, A. "Addressing Security Concerns in Cloud-Based Educational Platforms: A Case Study." In Journal of Cloud Security, 8(2), 34-47, 2019.
- [15] Nguyen, T., & Tran, M. "Cloud-Based Data Encryption Strategies for Enhanced Privacy in Educational Settings." In Proceedings of the ACM International Conference on Security and Privacy in Cloud Computing (pp. 56-69), 2021.
- [16] Chen, J., & Wu, Y. "Data Access Control Mechanisms in Educational Cloud Environments." In Journal of Computer Security, 30(4), 112-124, 2020.
- [17] Das, A., & Sharma, R. "A Comparative Analysis of Data Security Models for Cloud-Based Educational Services." In Proceedings of the International Conference on Information Technology (pp. 189-202), 2018.
- [18] Lim, G., et al., "Privacy Challenges and Solutions in Cloud-Based Learning Management Systems." In Journal of Information Privacy & Security, 36(1), 45-58, 2019.

- [19] Wang, X., & Li, Z. "Role-Based Access Control for Secure Data Sharing in Cloud-Based Educational Environments." In Proceedings of the ACM Symposium on Access Control Models and Technologies (pp.120-133), 2022.
- [20] N.Sirisha, Integrated Security and Privacy Framework for Big Data in Hadoop MapReduce Framework", Turkish Journal of Computer and Mathematics Education(TURCOMAT),Volume.12, Issue, 11, Pages 646-649
- [21] N.Shirisha, et al. "K-Anonymization approach for privacy preservation using data perturbation techniques in data mining", MaterialsToday, Proceedings, pg-1-6,2022.