IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024

DOI: 10.17148/IARJSET.2024.11814

IMAGE FRAGMENTATION & CLOUD CONTROL TO AVOID UNAUTHORISED ACCESS

Abhishek K S[1], Dr. H R Divakar[2]

PG Scholar, Department of MCA, PES College of Engineering, Mandya, Karnataka, India[1]

Associate Professor, Department of MCA, PES College of Engineering, Mandya, Karnataka, India[2]

Abstract: The project's primary objective is to bolster the security of files stored in public cloud environments by implementing additional security measures. The focus is on developing an application that introduces an extra layer of protection to cloud storage, safeguarding files from potential attacks. Concerns arise from the delegation of data to third-party administrative control in cloud computing, which exposes data to security threats from other users and nodes within the cloud. The proposed solution revolves around the division of a file into fragments, which are then strategically distributed across various cloud storage spaces. This fragmentation and distribution strategy augments security, creating a formidable challenge for attackers attempting to access meaningful information, even if they compromise a specific cloud node. The methodology emphasizes the replication of fragmented data across multiple cloud nodes, ensuring a heightened level of security for stored files.

Significantly, the method adopts a progressive recovery mechanism, surpassing conventional crypto techniques in terms of rate-distortion. This innovative approach significantly enhances the efficiency and effectiveness of recovering hidden information from encrypted images. In summary, the project addresses security concerns in public cloud storage through file fragmentation, distribution, and the application of an advanced crypto technique for reversible data hiding in encrypted images.

Keywords: File Fragmentation, Cloud Security, Cloud Storage.

I. INTRODUCTION

Cloud computing has revolutionized data storage, offering unprecedented flexibility and scalability, but it also introduces significant security challenges, particularly concerning the relinquishment of control to third-party administrators. To address these risks, this paper proposes a comprehensive approach to bolstering the security of files stored in public cloud environments. The project focuses on developing an application that introduces an additional layer of protection by strategically fragmenting files and distributing them across various cloud storage spaces. This strategy complicates efforts by attackers to access meaningful information, even if a specific cloud node is compromised, thereby enhancing the overall security of the stored data.

The primary objective of this project is to create an innovative application that safeguards files from potential cyber threats and attacks. Central to this approach is the strategic division of files into fragments, which are then distributed across multiple cloud storage spaces. This technique employs a progressive recovery mechanism and involves three key parties: the content owner, the data-hider, and the recipient. By integrating file fragmentation, distribution, and advanced cryptographic techniques for reversible data hiding in encrypted images, the project provides a robust solution to security concerns in public cloud storage. This methodology ensures a heightened level of security for stored files, protecting them against unauthorized access and potential cyber threats. Overall, this paper contributes to enhancing the security capabilities of cloud storage systems, paving the way for more secure and resilient data storage solutions in the cloud computing era.

II. LITERATURE SURVEY

“A Secured Distributed and Data Fragmentation Model & Cloud Storage” by Kuamal, Shenling Liu, Dong Chen, Yujiao Chen [1]. In this paper robust defence against network threats, efficient recovery after attacks, and secure third-party access to sensitive information stored in the cloud. The proposed model aims to enhance the security, confidentiality, and reliability of data stored in the cloud by leveraging distributed storage and data fragmentation techniques.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024
DOI: 10.17148/IARJSET.2024.11814

Rather than relying solely on a single storage provider, it distributes encrypted data fragments across multiple cloud storage spaces, thereby mitigating the risks associated with centralized storage and single points of failure. This paper presents the conceptual framework, detailing its architecture, encryption algorithms, data fragmentation strategies, and access control mechanisms. DDFM (Distributed and Data Fragmentation Model) - addresses cloud storage security challenges through a layer-to-layer protection strategy, Data Fragmentation (Granular Computing) - implementing these algorithms in a distributed and fragmented architecture. By fragmenting data into smaller segments and distributing them across disparate cloud nodes, it not only enhances security but also improves data reliability through redundancy and fault tolerance.

"A Method for Text Data Fragmentation to Provide Security in Cloud Computing" by Archana M, Mallikarjun Shastry P M [2]. In the realm of cloud computing, ensuring the security of text data stored in cloud environments is a critical concern due to the potential risks of unauthorized access and data breaches. The proposed approach addresses the challenge of safeguarding text data by fragmenting it into smaller, discrete units and distributing these fragments across distributed cloud storage nodes. The method begins by segmenting the text data into smaller fragments using advanced cryptographic techniques to ensure data confidentiality and integrity. These fragments are then strategically distributed across multiple cloud storage nodes, utilizing encryption and access control mechanisms to protect against unauthorized access and data breaches. Calculating lower and higher range values from the random number, fragments are obtained, and block size or fragment size is determined. This ensures data division into secure fragments, offering an innovative security solution. The efficacy of the proposed text data fragmentation method is demonstrated in terms of security, efficiency, and scalability. Comparative analyses with existing approaches highlight the superior security benefits and resource optimization achieved by the proposed method. Overall, this paper presents a comprehensive solution to enhance the security of text data in cloud computing environments through innovative data fragmentation techniques.

III. PROBLEM STATEMENT

The convenience of public cloud environments for data storage and access is overshadowed by significant security risks, as data control is handed over to third-party administrators, making it vulnerable to various cyber threats. Traditional security measures are often insufficient, leaving data exposed to breaches and unauthorized access, and the centralized nature of cloud storage further heightens these risks by making single points of failure more critical. To address these issues, the proposed solution involves enhancing cloud storage security by fragmenting files and distributing these fragments across multiple cloud nodes, thus providing an additional layer of protection against potential attacks.

IV. OBJECTIVE

The primary objective is to address concerns related to the outsourcing of data to third-party administrative control in cloud computing, which can expose data to security threats from other users and nodes within the cloud. The aim of the project is to enhance the security of files stored in public cloud environments by developing an application that implements additional security measures.

V. METHODOLOGY

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely used across the globe to secure data. Developed by Vincent Rijmen and Joan Daemen, AES was selected by the National Institute of Standards and Technology (NIST) in 2001 as the standard for encrypting electronic data. It operates on a block size of 128 bits, with key sizes of 128, 192, or 256 bits, making it highly versatile and secure. The algorithm uses a series of substitution-permutation network (SPN) transformations, including multiple rounds of substitution, permutation, mixing, and key addition, to transform the plaintext into cipher text. AES is extensively employed in numerous applications, including file encryption, secure communications, and financial transactions. Its widespread adoption and rigorous security make AES a cornerstone of modern cryptography.

VI. PROPOSED SOLUTION

The proposed system enhances cloud data security by dividing files into fragments based on user-defined criteria, ensuring individual fragments lack meaningful information. This strategy prevents substantial details of the original file from being revealed if a fragment is compromised. Additionally, the locations of these fragments are concealed, so even if an attacker compromises one node, they remain unaware of the other fragments' locations. Advanced cryptographic techniques are employed during the division and replication process to secure the fragments, adding another protection layer. The careful placement of nodes increases security, making it difficult for attackers to reconstruct the complete file structure.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024
DOI: 10.17148/IARJSET.2024.11814

By implementing these measures, the proposed system offers optimal security for user files in the cloud through fragmentation, encrypted storage, strategic node selection, and controlled replication.

The application has 3 main modules namely

- Application Manager (admin)
- College
- Student

VII. SOFTWARE IMPLEMENTATION

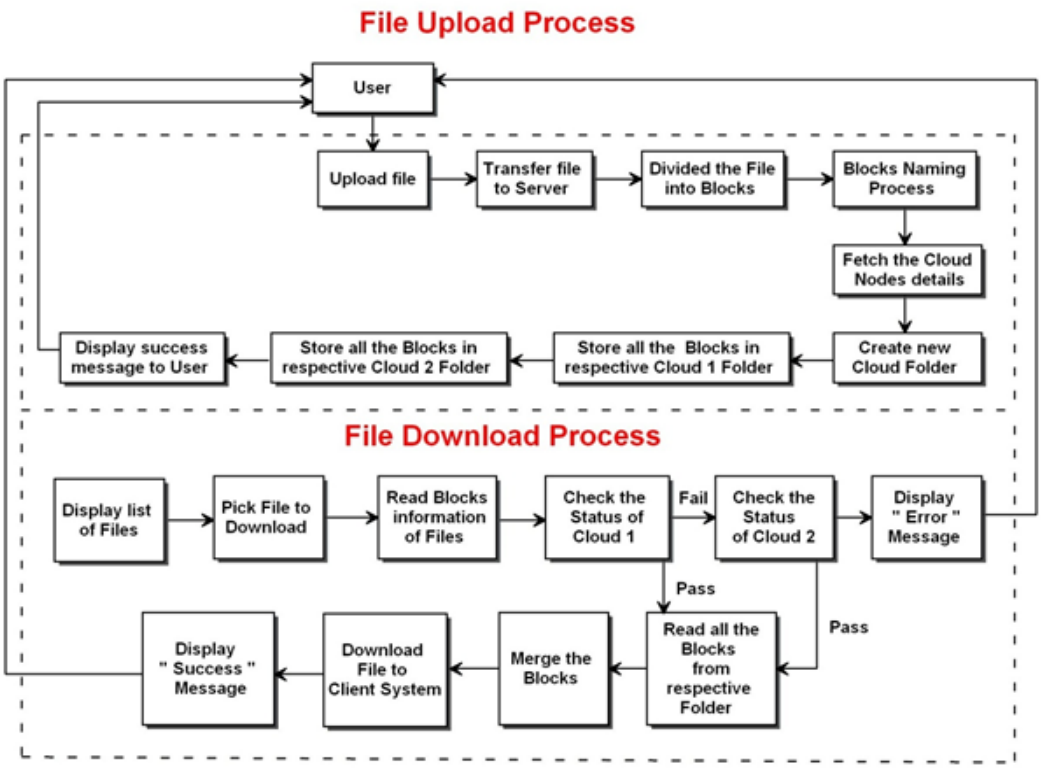

Fig 1: SYSTEM ARCHITECTURE

The "File Upload Process," starts with user uploading a file. That file gets sent over to the server. What's is that the server takes this file and splits it into several blocks. Each block is given a name, & info about the cloud nodes is gathered. These blocks are safely stored in two different AWS S3 buckets (fragment1 & fragment2). Once everything is uploaded, the user gets a message saying file uploaded successfully

Next is the "File Download Process." It starts by showing the user a list of files. The user picks one to download. The system checks the block info for that selected file, looking at the status of the first fragment. The system just checks the second fragment next. Then it reads all the blocks from the right AWS S3 buckets and puts them together as one file. This final file gets downloaded to the user's system, & they'll see another success message. But if both fragment have trouble, an error message pops up.

In short, this entire process shows a smart way to share file storage across various cloud locations. This helps make sure there's data redundancy and reliability. By keeping file blocks in different fragment, the system becomes better at handling faults. The status checks during downloading ensure that users get their complete file.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024

DOI: 10.17148/IARJSET.2024.11814

FORMS OF THE APPLICATION

Fig 2: LOGIN WINDOW

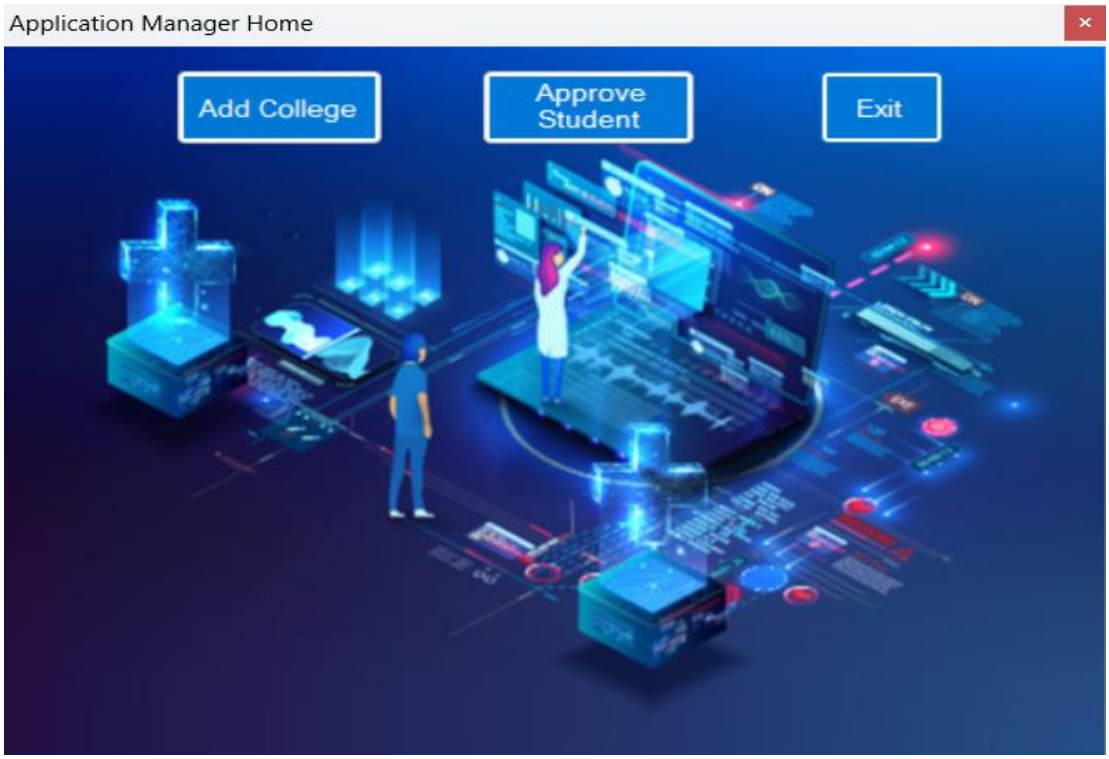

FIG 2: APPLICATION MANAGER HOME WINDOW

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024

DOI: 10.17148/IARJSET.2024.11814

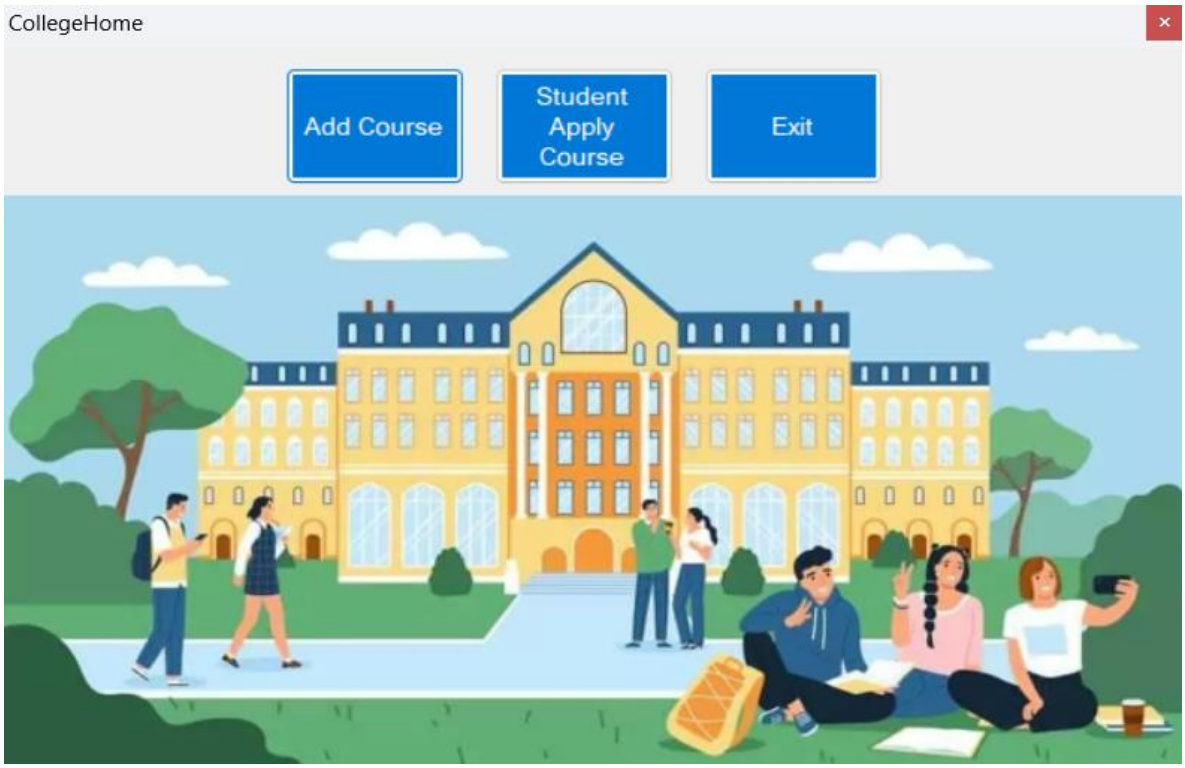

FIG 3: COLLEGE HOME WINDOW

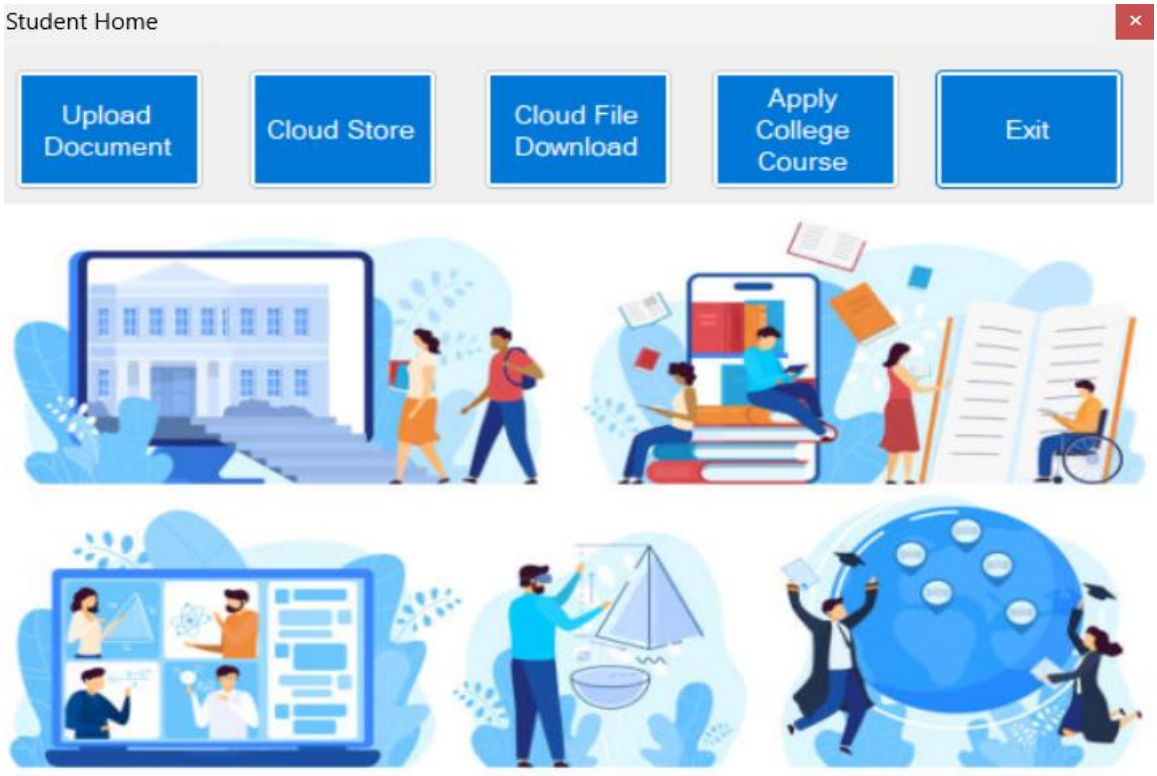

FIG 4: STUDENT HOME WINDOW

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024

DOI: 10.17148/IARJSET.2024.11814

VIII. CONCLUSION AND FUTURE SCOPE

This system gives a special solution invoking security in AWS cloud storages. Our proposed architecture involves AWS cloud storage system, the user files are split into fragments, encrypted using encryption algorithm and stored data in cloud storages namely AWS S3. The study results show encryption algorithm as secured and requires less processing time. This system deals with the enhancement of security to cloud servers by implementation detection and prevention techniques against cyber-attacks. Safety of the data is enhanced in this system. Hence this architecture provides complete secure access/storage of data across AWS clouds.

In future:

- We can add more number of clouds and also keep a backup copy of each of the parts.
- Student can apply for Study purpose (Higher Education) & respective college/organization can view the verified student certificates.
- Student can apply for Job & respective companies can view the student certificates.

REFERENCES

[1]. Amjad and Alsiri Hani, “Improving Database Security in Cloud Computing by Fragmentation of Data”, vol 21, 98-101, 2020.
[2]. P D Patni1, Dr. S N Kakarwal, “Security Enhancement of Data in Cloud using Fragmentation and Replication”, vol 8. 61-64, 2020.
[3]. L M Nithya and P Anu Priya, “Data Fragmentation and Duplication in Cloud for Secure Performance”, vol 4, 33-37, 2021.
[4]. S Abdul Saleem and N Ramya, “File Fragmentation to Improve Security in Cloud Using Graph Topology Grid Algorithm: A Survey”, vol 91, 324-328, 2021.
[5]. Mrs. K Rajani, Y Sreeja, T Tejaswini, B Manasa, “Optimal Performance of Security by Fragmentation and Replication of Data in Cloud”, vol 45, 898-902, 2022.
[6]. Mrs. K Rajani, Y Sreeja, T Tejaswini, B Manasa, “Optimal Performance of Security by Fragmentation and Replication of Data in Cloud”, vol 1, 1-5, 2022.
[7]. S Srinidhi, Supriya B M, T M Mohan Kumar, Vaishnavi V, Prof. Pruthvi P R, “Data Fragmentation in Cloud for Enhanced Confidential Computing: A Comprehensive Review”, vol 7, 77-81, 2022.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License