IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Cloud Based Secure File Transfer System

M.K.Hadap
Assistant Professor
YCCE,Nagpur
manishhadap@yahoo.co.in

Rutuja Vaidya
Information Technology
YCCE,Nagpur
rutujavaidya@gmail.com

Shruti Meshram
Information Technology
YCCE,Nagpur
shrutimeshram50@gmail.com

Rupal Akarte
Information Technology
YCCE,Nagpur
rupalakarte646@gmail.com

Piyush Dolhare
Information Technology
YCCE,Nagpur
Piyushdolhare7112000@gmail.com

***Abstract*— Cloud computing has become increasingly popular in recent years, providing organizations with benefits such as scalability, flexibility, and cost-effectiveness. However, this trend has also brought with it a higher risk of cyber-attacks and data breaches. To address these challenges, we propose a comprehensive approach to enhancing data security in private cloud environments using encryption, checksum, file corruption detection, and prevention of external code execution.**

The proposed approach ensures data confidentiality and integrity using encryption, which protects data by encoding it before storing it in the cloud environment. The system also employs checksum to verify the integrity of data blocks and includes a sophisticated mechanism to detect corrupted files and prevent their access by isolating them from the rest of the system. Moreover, the approach employs a range of security measures to prevent external code execution, reducing the risk of cyber-attacks and data breaches. The system also blocks IP addresses to prevent unauthorized access to the private cloud environment.

The proposed approach provides a complete solution for ensuring data security and integrity in private cloud environments, which is essential for organizations that rely on cloud computing for their operations. By implementing this approach, organizations can improve their data security and minimize the risk of cyber-attacks and data breaches. The proposed approach can be easily integrated into existing private cloud environments, providing an efficient and cost-effective solution to enhance data security.

Keywords—Cloud, Data Security, Encryption

I. INTRODUCTION

Data security in private cloud computing is the practice of protecting sensitive data and ensuring that it is not compromised, lost, or stolen. Private cloud environments are dedicated to a single organization and offer greater control and customization options than public cloud environments. However, they also require organizations to take responsibility for implementing robust security measures to protect their data.

- Data security in private cloud environments involves several key components, including:
- Access controls: Organizations must implement access controls to prevent unauthorized access to sensitive data. Access controls can include strong passwords, two-factor authentication, and role-based access controls.
- Encryption: Encryption is a critical security measure for protecting data in transit and at rest. Data should be encrypted before storing it in the cloud environment, and encryption keys should be kept secure to prevent unauthorized access.
- Data backup and recovery: Organizations must implement data backup and recovery plans to ensure that data can be restored in the event of data loss or corruption.
- Malware protection: Organizations must implement malware protection measures, such as antivirus software and firewalls, to prevent malware from infecting the system and stealing sensitive data.
- Continuous monitoring: Organizations must continuously monitor the system for any vulnerabilities or threats and take appropriate measures to address them.
- Overall, data security in private cloud environments requires a comprehensive approach that includes access controls, encryption, data backup and recovery, malware protection, and continuous monitoring. Organizations must implement these security measures and continuously review and update them to ensure the smooth and secure functioning of their cloud-based operations.

As organizations increasingly adopt private cloud computing for their data storage and computing needs, the importance of data security in these environments cannot be overstated. Private cloud computing offers many advantages over public cloud computing, including greater control and customization options, improved scalability, and cost-effectiveness. However, private clouds are not immune to security risks, and organizations must implement robust security measures to protect their data from unauthorized access, data breaches, and cyber-attacks.

Data security in private cloud environments involves a wide range of measures and technologies, including access controls, encryption, data backup and recovery, malware protection, and continuous monitoring. These security measures must be implemented and continuously reviewed and updated to ensure the smooth and secure functioning of cloud-based operations.

One of the main challenges in data security in private cloud environments is ensuring that sensitive data is not compromised, lost, or stolen. Private cloud environments are often accessed through a wide range of devices and networks, making it difficult to control access to sensitive data. Additionally, private clouds can be targeted by malicious actors seeking to steal sensitive data or disrupt cloud-based operations.

To address these challenges, organizations must take a holistic approach to data security in private cloud environments. This includes implementing access controls to prevent unauthorized access to sensitive data, encrypting data to protect it from unauthorized access, implementing data backup and recovery plans to ensure data can be restored in the event of data loss or corruption, using malware protection measures to prevent malware from infecting the system and stealing sensitive data, and continuously monitoring the system for any vulnerabilities or threats.

Overall, data security in private cloud environments is a critical concern for organizations, and requires a comprehensive approach that includes robust security measures, continuous monitoring, and ongoing review and updating of security policies and procedures.

II. LITERATURE REVIEW

1] Sajid Habib Gill, Mirza Abdur Razzaq, Muneer Ahmad , Fahad M. Almansour , Ikram Ul Haq, NZ Jhanjhi, Malik Zaib Alam and Mehedi Masud," **Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study".** In this case study they categorized the security and privacy aspects of the cloud, concentrating on a case study set in a smart campus scenario. They discussed security issues such as data privacy, access control, and data availability. The lack of security measures and ease of access in the cloud can result in the compromise of data without the victim's knowledge. Security issues in cloud applications must be recognized, and safety measures taken in communication networks. Hence, it is emphasized to deploy the efficient security and privacy measures to ensure data integrity, privacy, and reliability. However, cloud service providers are not providing enough security to satisfy users. Additionally, blockchain improves security problems in cloud computing. They highlight cloud security concerns/challenges and their behavior/nature with suggested solutions that will benefit other researchers.

2] P. Shanmugapriya, K.S.V. Srinivas, Rampam Pavan Kumar**," Secure Data Transfer Based On Cloud Computing".** In this proposed system we can safely store data on the cloud by encrypting and decrypting it. On the cloud, we can also safely share data. The transmitter encrypts data with a public key, which is then decrypted by the receiver with a private key. As a result, even if a hacker obtains the data, he will be unable to decode it until he obtains the private key, ensuring that data on the cloud is secure.

The proposed method opposes encrypting the file with any conventional encryption technology and then utilizing Diffie Hellman for user authentication. As a result, the files can be safely saved in the public domain without the risk of being accessed by unauthorized individuals.

3] Shreya Sambhaji Ranadive, Harshada Sanjay Sawant, Jayesh Ekanath Pinjarkar," **Secure File Storage on Cloud Computing Using Cryptographic Algorithm**",The main aim of the system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography. Data security is achieved by using AES and ECC Algorithms. Users are most concerned about data security, so virtualization security and data security are the main problem of the cloud computing security. They concern here data security with Elliptic curve cryptography to provide confidentiality and authentication of data between clouds. The input text file is transformed into encrypted form using AES encryption but the key is generated through ECC (Elliptic curve cryptography). Client will use that key to decrypt the text file which is uploaded to the server in encrypted form to get the original text file. At last analysis of AES encryption with ECC is done based on different parameters like storage requirement, encryption time, decryption time, effect and correlation. Obtained results illustrate that the impact of this hybrid approach is significant and better than other algorithms.

4] Niteen Kale, Abraar Khan, Swapnil Sawant, Atharva Shrotre , S. M. Bhadkumbhe," **Secure File Transfer on Cloud with Encryption",** In this system, the user can store the file safely in online Cloud storage as these files are going to be stored in encrypted form within the cloud and only the authorized user has access to their files using by encrypting the file using AES 128-bit encryption.

IV.EXSISTING SYSTEM

As organizations increasingly adopt private cloud computing for their data storage and computing needs, the importance of data security in these environments cannot be overstated. Private cloud computing offers many advantages over public cloud computing, including greater control and customization options, improved scalability, and cost-effectiveness. However, private clouds are not immune to security risks, and organizations must implement robust security measures to protect their data from unauthorized access, data breaches, and cyber-attacks.

Data security in private cloud environments involves a wide range of measures and technologies, including access controls, encryption, data backup and recovery, malware protection, and continuous monitoring. These security measures must be implemented and continuously reviewed and updated to ensure the smooth and secure functioning of cloud-based operations.

One of the main challenges in data security in private cloud environments is ensuring that sensitive data is not compromised, lost, or stolen. Private cloud environments are often accessed through a wide range of devices and networks, making it difficult to control access to sensitive data. Additionally, private clouds can be targeted by malicious actors seeking to steal sensitive data or disrupt cloud-based operations.

To address these challenges, organizations must take a holistic approach to data security in private cloud environments. This includes implementing access controls to prevent unauthorized access to sensitive data, encrypting data to protect it from unauthorized access, implementing data backup and recovery plans to ensure data can be restored in the event of data loss or corruption, using malware protection measures to prevent malware from infecting the system and stealing sensitive data, and continuously monitoring the system for any vulnerabilities or threats.

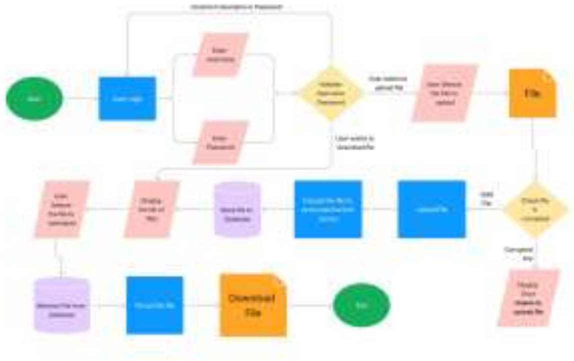
V. PROPOSED METHODOLOGY

Cloud computing has become increasingly popular in recent years, providing organizations with benefits such as scalability, flexibility, and cost-effectiveness. However, this trend has also brought with it a higher risk of cyber-attacks and data breaches. To address these challenges, we propose a comprehensive approach to enhancing data security in private cloud environments using encryption, checksum, file corruption detection, and prevention of external code execution.

The proposed approach ensures data confidentiality and integrity using encryption, which protects data by encoding it before storing it in the cloud environment. The system also employs checksum to verify the integrity of data blocks and includes a sophisticated mechanism to detect corrupted files and prevent their access by isolating them from the rest of the system. Moreover, the approach employs a range of security measures to prevent external code execution, reducing the risk of cyber-attacks and data breaches. The system also blocks IP addresses to prevent unauthorized access to the private cloud environment.

The proposed approach provides a complete solution for ensuring data security and integrity in private cloud environments, which is essential for organizations that rely on cloud computing for their operations. By implementing this approach, organizations can improve their data security and minimize the risk of cyber-attacks and data breaches.

The proposed approach can be easily integrated into existing private cloud environments, providing an efficient and cost-effective solution to enhance data security.



Workflow Diagram

VI. RESULTS AND DISCUSSION

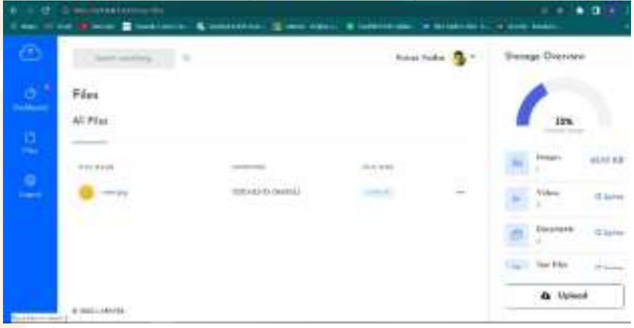
The project focused on enhancing data security over the private cloud by testing various conditions and implementing several security measures such as encryption, external code execution, file corruption, checksum, and block IP.

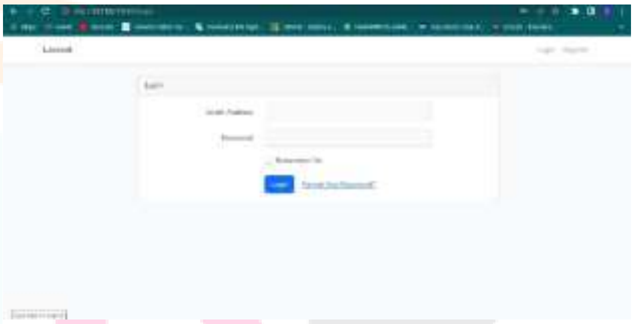
The project resulted in a significant improvement in data security over the private cloud environment. By encrypting sensitive data, the project ensured that only authorized personnel could access the data, preventing data breaches and unauthorized access.

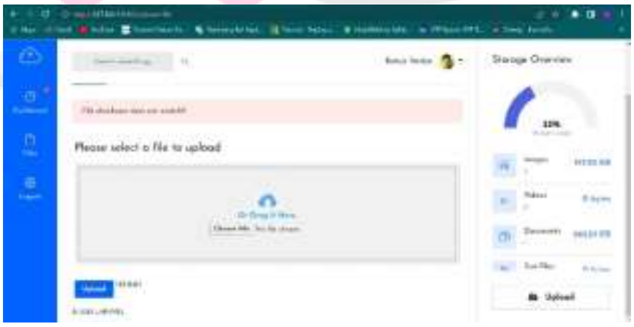
The external code execution feature ensured that only trusted code could run on the system, preventing malicious code from compromising the system. File corruption detection and correction ensured that data integrity was maintained even in the event of file corruption, further enhancing data security.

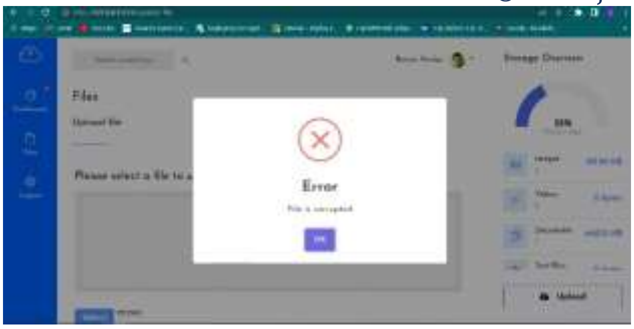
Checksum validation helped to detect any data tampering, ensuring that the data was not modified without authorization. Finally, blocking IP addresses that showed suspicious activity helped to prevent unauthorized access and data breaches.

Overall, the project was successful in enhancing data security over private cloud environments. By implementing a range of security measures, the project ensured that data was protected from unauthorized access, tampering, and breaches, making the private cloud a more secure environment for storing and processing sensitive data.





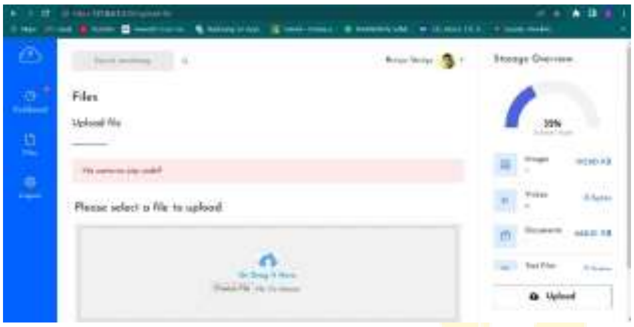




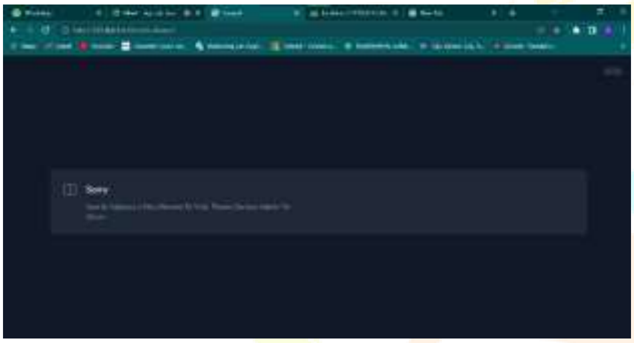
Please select a file to u

Error

File is corrupted



Please select a file to upload



Sorry

VII. FUTURE SCOPE

The future scope of the secure file transfer project over the cloud with the integration of multi-factor authentication and blockchain technology is significant.

Multi-factor authentication provides an additional layer of security by requiring users to provide two or more forms of identification before accessing the system. This could include something the user knows, like a password, something they have, like a smart card or token, or something they are, like a biometric scan. By implementing multi-factor authentication, the project could greatly enhance the security of the file transfer system, making it more difficult for attackers to gain unauthorized access.

Another potential improvement is the integration of blockchain technology. The use of blockchain technology would provide a secure and transparent way of tracking file transfers. By creating an immutable record of all file transfers on the blockchain, the project could ensure that all transactions are transparent and tamper-proof. This would enable users to track the movement of their files and ensure that they reach their intended destination securely.

The integration of these technologies would significantly improve the security and functionality of the secure file transfer project over the cloud. By incorporating multi-factor authentication and blockchain technology, the project would provide a more robust solution for secure file transfer, ensuring that data remains confidential, secure, and tamper-proof.

VIII. CONCLUSION

The secure file transfer project over the cloud is a robust and reliable solution for ensuring that files are transferred safely and securely. By incorporating various security measures such as AES CBC 128-bit encryption, prevention of external code execution, blocking unauthorized IP addresses, checksums, and detection of corrupted files, the project provides a comprehensive approach to file transfer security. The encryption of files ensures that sensitive data remains confidential, while the prevention of external code execution prevents the injection of malicious code. Blocking unauthorized IP addresses adds an additional layer of security, while the checksum feature verifies the integrity of the files being transferred. Detection of corrupted files ensures that only clean and secure files are transferred. Overall, the project provides a highly secure solution for file transfer over the cloud, and its various security measures ensure that users can transfer files with complete confidence in their security.

IX. REFERENCES

1] Sajid Habib Gill, Mirza Abdur Razzaq , Muneer Ahmad , Fahad M. Almansour , Ikram Ul Haq, NZ Jhanjhi, Malik Zaib Alam and Mehedi Masud,"Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study", IASC, 2022, vol.31.

2] P. SHANMUGAPRIYA, K.S.V. SRINIVAS, RAMPAM PAVAN KUMAR," SECURE DATA TRANSFER BASED ON CLOUD COMPUTING", International Research Journal of Engineering and Technology (IRJET), Mar 2022.

3] Shreya Sambhaji Ranadive, Harshada Sanjay Sawant, Jayesh Ekanath Pinjarkar," Secure File Storage on Cloud Computing Using Cryptographic Algorithm", International Journal for Research in Applied Science & Engineering Technology (IJRASET), 4, April 2022.

4] Niteen Kale, Abraar Khan, Swapnil Sawant, Atharva Shrotre , S. M. Bhadkumbhe," Secure File Transfer on Cloud with Encryption", International Journal of Recent Advances in Multidisciplinary Topics (IJRAMT), 4, April 2021.

5] Madhumala RB, Sujan Chhetri, Akshatha KC, Hitesh Jain," International Journal of Computer Science and Mobile Computing", 5, May 2021.

6] Nagesh Rajendra Salunke, Pratik Mahaling Jangam , Pratiksha Ramdas Biradar , Suchita Sangram Jaybhaye , Prof. Savitri Patil," Files Storage & Sharing Platform Using Cloud", International Journal for Research in Applied Science & Engineering Technology (IJRASET) ,11, Nov 2021.

7] Y. Kiran Kumar, R. Mahammad Shafi," An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem", International Journal of Electrical and Computer Engineering (IJECE), February,2020.

8] K. Jaspin; Shirley Selvan; S Sahana; G Thanmai," Efficient and Secure File Transfer in Cloud Through

Double Encryption Using AES and RSA Algorithm", IEEE, 07 March 2021.

9] Manoj V. Bramhe & Dr. Milind V. Sarode & Dr. Meenakshi S. Arya," Design and Implementation of Secure File Storage using Distributed Cloud Mechanism", IJRAR-International Journal of Research and Analytical Reviews, JAN– MARCH 2019.

10] Gift Chisoni and Dr. Glorindal Selvam," The Design and Implementation of a Secure File Storage on the Cloud using Hybrid Cryptography", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), April 2023.