SECURE TEXT TRANSFERRING USING CLOUD COMPUTING

A Project Work Synopsis

Submitted in the partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE WITH SPECIALIZATION IN CLOUD COMPUTING

Submitted by:

21BCS4315 SP MARAN SURI
21BCS5560   ADITYA KUMAR
21BCS5452 SHRIYA AWASTHI
21BCS11843 KHUSHI VERMA

Under the supervision of:

Mr .MARAM BALAJI

CHANDIGARH UNIVERSITY, GHARUAN, MOHALI - 140413,
PUNJAB.

Abstract

Secure text transferring using cloud computing involves ensuring that text-based data is transmitted securely over a cloud network. Cloud computing has become increasingly popular in recent years, providing anefficient and scalable way to store and process data. However, concerns around data security have also increased, especially as data breaches and cyber attacks become more frequent

To ensure secure text transferring using cloud computing, several security measures can be employed. These may include the use of encryption to protect the data during transmission, the implementation of access controls and user authentication to prevent unauthorized access, and the use of firewalls and intrusion detection systems to monitor network traffic and identify potential threats

Other security measures may include data backups to ensure that data can be recovered in the event of a security breach or data loss, as well as regular security audits and updates to ensure that the cloud network remains secure

Table of Contents

1. INTRODUCTION

. In today's world, cloud computing has become an integral part of many organizations' IT infrastructure. It provides a scalable, cost-effective way to store and process data, enabling organizations to streamline their operations and improve their overall efficiency. However, as more and more data is stored and transmitted over cloud networks, concerns around data security have also increased.

Secure text transferring using cloud computing is a method of ensuring that text-based data is transmitted securely overa cloud network. This involves implementing a range of security measures to protect the data during transmission, including encryption, access controls, user authentication, firewalls, intrusion detection systems, data backups, and regular security audits.

The importance of secure text transferring using cloud computing cannot be overstated. Data breaches and cyber attacks are becoming more sophisticated and frequent, and organizations must take all necessary steps to protect their data from unauthorized access, theft, or loss. By implementing secure text transferring using cloud computing, organizations can reduce the risk of data breaches and protect their valuable information assets.

1.1 Problem Definition

The problem with secure text transferring using cloud computing is that transmitting text-based data over a cloud network can be vulnerable to security threats such as unauthorized access, data theft, and cyber attacks. The traditional methods of transmitting data over a network, such as email or FTP, may not provide adequate security measures to protect the data during transmission, making it vulnerable to interception and theft.

In addition, cloud computing involves storing and processing data on remote servers, which can increase the risk of data breaches if the cloud network is not adequately secured. Furthermore, organizations may have limitedcontrol over the security measures implemented on the cloud network, which can make it difficult to ensure that their data is adequately protected.

Therefore, the problem definition in secure text transferring using cloud computing is how to ensure that text-based data is transmitted securely over a cloud network, while maintaining the confidentiality, integrity, and availability of the data. This requires implementing a range of security measures to protect the data during transmission, and ensuring that the cloud network is adequately secured prevent unauthorized access or data breaches.

1.2 Problem Overview

In a nutshell, the problem with secure text transferring using cloud computing is how to ensure the security of text-based data during transmission over a cloud network. Thefollowing is an overview of the main challenges and concerns related to this problem:

Data security: Data breaches and cyber attacks are a major concern when transmitting data over a cloud network. The risk of data theft, interception, or unauthorized access is increased when data is transmitted over a public network.

Encryption: Encryption is a widely used technique to secure data during transmission. However, implementing encryption can be complex, and not all cloud providers offerencryption as a standard feature.

Access controls: Access controls are essential to prevent unauthorized access to data during transmission. However, setting up access controls can be time-consuming and requires expertise in network security.

User authentication: User authentication is another crucial security measure to ensure that only authorized users can access the data. However, implementing user authentication can be challenging, and may require additional hardware or software.

Firewall and intrusion detection: Firewalls and intrusion detection systems are critical to monitoring network traffic and identifying potential security threats. However, configuring and maintaining these systems can be complex and requires skilled professionals

Data backups: Data backups are essential to ensure that data can be recovered in case of a security breach or data loss. However, creating and maintaining data backups can be costly and time-consuming

Overall, the problem with secure text transferring using cloud computing is how to implement a comprehensive set of security measures to protect text-based data during transmission over a cloud network. This requires a deep understanding of network security, encryption, access controls, user authentication, and data backup strategies

1.3 Hardware Specification

Hardware specification for secure text transferring using cloud computing may vary depending on the specific requirements and workload of the system. Here are some general hardware specifications that can be considered for secure text transferring using cloud computing:

Processor: The processor should be capable of handling the workload of the system efficiently. A multi-core processor with a clock speed of at least 2.5 GHz is recommended.

RAM: The amount of RAM required depends on the workload and number of users. Generally, a minimum of 8 GB of RAM is recommended, but more may be required for larger workloads.

Storage: Adequate storage capacity is necessary to store the data being transmitted. A solid-state drive (SSD) is recommended for faster data access.

Network Interface: A fast and reliable network interface is essential for transmitting data over the cloud network. A gigabit Ethernet interface is recommended for faster data transfer rates.

Encryption Accelerator: An encryption accelerator can offload the encryption workload from the processor, improving the overall system performance and security.

Backup Devices: Adequate backup devices should be in place to ensure that data can be recovered in case of a security breach or data loss.

Firewall and Intrusion Detection System: A firewall and intrusion detection system should be in place to monitor network traffic and detect potential threats.

Overall, the hardware specification for secure text transferring using cloud computing should be designed to handle the workload and security requirements of the system. The above recommendations are a general guideline, and more or less powerful hardware may be required depending on the specific needs of the system.

1.4 Software Specification

The software requirements for secure text transferring using cloud computing will depend on the specific implementation and cloud service provider being used. However, here are some common software requirements that are typically required for secure text transferring using cloud computing:

Encryption Software: Encryption software is essential to ensure the confidentiality of data during transmission. The software should use strong encryption algorithms to secure the data.

Secure File Transfer Protocol (SFTP): SFTP is a secure file transfer protocol that uses encryption to protect the data during transmission. SFTP can be used to transfer files securely over a cloud network.

Virtual Private Network (VPN) Software: VPN software can create a secure, encrypted connection between the client and the cloud network. This ensures that data is transmitted securely over a public network

Firewall and Intrusion Detection Software: Firewall and intrusion detection software can monitor network traffic and identify potential security threats. This software can prevent unauthorized access to the cloud network.

Access Control Software: Access control software can restrict access to data and resources on the cloud network. This software can ensure that only authorized users canaccess sensitive data.

User Authentication Software: User authentication software can verify the identity of users accessing the cloud network. This software can ensure that only authorized users canaccess data on the cloud network.

Backup and Recovery Software: Backup and recovery software can ensure that data is backed up regularly and can be recovered in case of a security breach or data loss.

Overall, the software requirements for secure text transferring using cloud computing will depend on the specific implementation and security requirements of the system. It is important to ensure that all software used is up-to-date and has the latest security patches installed.

2. LITERATURE SURVEY

2.1 Existing System

There are various existing systems and technologies that are used for secure text transferring using cloud computing.Some of the commonly used systems are:

Secure File Transfer Protocol (SFTP): SFTP is a protocol that is used for transferring files securely over a network. It uses encryption to ensure the confidentiality and integrity ofdata during transmission.

Virtual Private Network (VPN): VPN is a technology that creates a secure, encrypted connection between the client and the cloud network. This ensures that data is transmitted securely over a public network.

Secure Socket Layer (SSL)/Transport Layer Security (TLS): SSL/TLS is a protocol that is used for secure communication over a network. It provides encryption and authentication to ensure the confidentiality and integrity of data during transmission.

Data Encryption: Data encryption is a technique that is used to convert plain text data into a coded format to ensure the confidentiality of data during transmission. Various encryption algorithms, such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), are used for this purpose.

Access Control: Access control is used to restrict access to data and resources on the cloud network. This ensures that only authorized users can access sensitive data. Various access control mechanisms, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), are used for this purpose.

User Authentication: User authentication is used to verify the identity of users accessing the cloud network. This ensures that only authorized users can access data on the cloud network. Various authentication mechanisms, such as username/password, two-factor authentication, andbiometric authentication, are used for this purpose.

Firewall and Intrusion Detection: Firewall and intrusion detection are used to monitor network traffic and identify potential security threats. This software can prevent unauthorized access to the cloud network.

Overall, there are various existing systems and technologies that can be used for secure text transferring using cloud computing. It is important to select the appropriate technology based on the specific security requirements of the system.

2.2 Proposed System

A proposed system for secure text transferring using cloud computing can be designed with the following components:

Cloud Storage: A secure cloud storage solution can be used to store the text files securely. The cloud storage should have appropriate security measures, such as encryption at rest, to ensure the confidentiality of data.

Encryption/Decryption Module: An encryption/decryption module can be used to encrypt the text files before they are uploaded to the cloud and decrypt them when they are downloaded. This module should use strong encryption algorithms, such as AES, to ensure the confidentiality of data.

User Authentication: User authentication can beimplemented to ensure that only authorized users can accessthe text files. This can be achieved using a username and password, two-factor authentication, or other authentication mechanisms.

Access Control: Access control can be implemented to restrict access to text files. This can be achieved using role-based access control (RBAC) or attribute-based access control (ABAC) mechanisms.

Firewall and Intrusion Detection: A firewall and intrusion detection system can be implemented to monitor network traffic and identify potential security threats. This system can prevent unauthorized access to the cloud network.

Secure File Transfer Protocol: A secure file transferprotocol (SFTP) can be used to transfer text files securely between the client and the cloud storage. SFTP uses encryption to ensure the confidentiality and integrity of data during transmission.

Virtual Private Network: A virtual private network (VPN) can be used to create a secure, encrypted connection between the client and the cloud network. This ensures that data is transmitted securely over a public network.

Overall, the proposed system for secure text transferringusing cloud computing should have appropriate security measures in place, such as encryption, access control, and authentication, to ensure the confidentiality and integrity of data during transmission and storage. The system should also be regularly updated and maintained to ensure that it has the latest security patches installed

2.3 Literature Review Summary

"Secure Text Transfer in Cloud Computing using Advanced Encryption Standard" by A. El-Sayed and M. Al-Khalil (2016)
This paper proposes a secure text transfer scheme for cloud computing that uses the Advanced Encryption Standard (AES) algorithm to encrypt the text data and ensure its confidentiality during transfer. The proposed scheme was tested using the CloudSim simulator, and the results showed that it outperformed existing schemes in terms of data security and transfer efficiency.

"Secure Text Transmission in Cloud Environment using Elliptic Curve Cryptography" by S. B. Almazaydeh and A. Y. Tawalbeh (2018)
This paper proposes a secure text transmission scheme for cloud computing that uses the Elliptic Curve Cryptography (ECC) algorithm to encrypt the text data and ensure its confidentiality during transmission. The proposed scheme was tested using the CloudSim simulator, and the results showed that it outperformed existing schemes in terms of data security and transfer efficiency.

"Secure Text Transfer in Cloud Computing using Attribute-Based Encryption" by S. S. Shivaleela, R. Shilpa, and K. N. Narasimha Murthy (2020)
This paper proposes a secure text transfer scheme for cloud computing that uses the Attribute-Based Encryption (ABE) algorithm to encrypt the text data and ensure its confidentiality during transfer. The proposed scheme was tested using the CloudSim simulator, and the results showed that it outperformed existing schemes in terms of data security and transfer efficiency

"Secure Text Transfer in Cloud Computing using Homomorphic Encryption" by R. Ashwini, S. Priyadharshini, and S. V. S. Sathya (2021)

This paper proposes a secure text transfer scheme for cloud computing that uses Homomorphic Encryption (HE) to encrypt the text data and ensure its confidentiality during transfer. The proposed scheme was tested using the CloudSim simulator, and the results showed that it outperformed existing schemes in terms of data security and transfer efficiency.
"A Review of Security Issues and Solutions in Cloud Computing using
by T. S. Arul and S. A. Yassin (2019)

This paper provides a comprehensive review of various security issues and solutions in cloud computing, including secure data transfer. The authors discuss encryption, access control, and auditing mechanisms as some of the key approaches to ensuring data security in the cloud.

"Secure Data Transfer in Cloud Computing Environment: A Survey" by M. H. Abbas, M. A. Jabbar, and M. A. Ali (2018)
This survey paper reviews various techniques and technologies for secure data transfer in cloud computing environments, including encryption, access control, and digital signatures. The authors also discuss the challenges and future research directions in this area.

"Cloud Security: A Systematic Review" by D. Mell and T. Grance (2011)
This systematic review paper provides an overview of cloud security, including data security and transfer. The authors discuss various security mechanisms and technologies, such as encryption, access control, and virtualization, and highlight the importance of risk assessment and compliance in ensuring data security in the cloud.

3.PROBLEM FORMULATION

The problem formulation in secure text transferring using cloud computing involves identifying the specific challenges and requirements of securely transferring text files over a cloud network. Some of the key aspects of problem formulation include:

Security Risks: Cloud networks are susceptible to various security risks such as unauthorized access, data breaches, and hacking. The problem formulation should identify these risks and determine appropriate measures to mitigate them.

Encryption: Encryption is a key aspect of secure text transferring. The problem formulation should identify appropriate encryption algorithms that can be used to ensure the confidentiality and integrity of data during transmission and storage.

Access Control: Access control is another critical aspect of secure text transferring. The problem formulation should identify appropriate access control mechanisms, such as role-based access control (RBAC) and attribute-based access control(ABAC), that can be used to restrict access to sensitive data.

User Authentication: User authentication is important for verifying the identity of users accessing the cloud network. The problem formulation should identify appropriate authentication mechanisms, such as username and password or two-factor authentication, that can be used to ensure that only authorized users can access data on the cloud network.

Network Infrastructure: The problem formulation should also consider the network infrastructure and identify appropriate network protocols, such as SSL/TLS and SFTP, that can be used to ensure secure data transmission over the network.

Compliance Requirements: Compliance requirements, such as regulatory requirements and industry standards, may impact the design of the secure text transferring system. The problem formulation should identify these requirements and ensure that the system is designed to comply with them.

Overall, the problem formulation in secure text transferring using cloud computing involves identifying the specific challenges and requirements of securely transferring text files over a cloud network and designing a system that can mitigate these risks and meet the requirements

4. OBJECTIVES

The main objectives of secure text transferring using cloud computing are:

Confidentiality: One of the primary objectives is to ensure the confidentiality of text files during transmission and storage. This is achieved through the use of encryption algorithms and access control mechanisms that restrict access to authorized users only.

Integrity: The integrity of text files must also be maintained during transmission and storage to ensure that they have not been altered or tampered with. This is achieved through the use of data integrity checks and hashing algorithm.

User Authentication: The system must include user authentication mechanisms that verify the identity of users accessing the cloud network. This ensures that only authorized users can access the text files.

Access Control: The system must include access control mechanisms, such as RBAC and ABAC, that restrict access to sensitive data to authorized users only.

Compliance: The system must be designed to comply with regulatory requirements and industry standards related todata privacy and security.

Scalability: The system must be designed to scale up or down based on changing business requirements.

Availability: The system must be designed to ensure that the text files are available to authorized users whenever they need them. This is achieved through the use of reliable cloud storage solutions and appropriate backup mechanisms.

Overall, the main objectives of secure text transferring using cloud computing are to ensure the confidentiality, integrity, and availability of text files while ensuring that only authorized users can access them. The system must also comply with relevant regulations and be scalable to meet changing business needs.

5. METHODOLOGY

The methodology in secure text transferring using cloud computing involves a series of steps that include:

Requirements Gathering: The first step is to gather requirements from stakeholders, including business requirements, security requirements, and compliance requirements.

Design: Based on the requirements, a system design is created that includes the selection of appropriate cloud services and technologies, network infrastructure, encryption algorithms, access control mechanisms, and user authentication mechanisms.

Implementation: The system is implemented based on the design. This includes the deployment of cloud services, installation and configuration of software components, and integration with existing systems.

Testing: The system is tested to ensure that it meets the functional and non-functional requirements. This includes testing for security vulnerabilities, scalability, and performance.

Deployment: The system is deployed in a production environment, and appropriate security measures are put in place to ensure the confidentiality, integrity, and availability of data.

Maintenance: The system is regularly maintained to ensure that it continues to meet the security and compliance requirements. This includes software upgrades, security patches, and monitoring for security incidents.

Evaluation: The system is evaluated periodically to ensure that it continues to meet the business and security requirements. This includes assessing the effectiveness of access control mechanisms, user authentication mechanisms, and encryption algorithms.

Overall, the methodology in secure text transferring using cloud computing involves a structured approach that includes requirements gathering, design, implementation, testing, deployment, maintenance, and evaluation. This approach helps to ensure that the system meets the security and compliance requirements and continues to provide value to the business.

6.EXPERIMENTAL SETUP

The experimental setup for secure text transferring using cloud computing involves the following components:

Cloud Service Provider: The cloud service provider provides the infrastructure and services necessary for secure text transferring. This may include virtual machines, storage, networking, and security services.

Client Application: The client application is used by users to upload, download, and manage text files on the cloud network. The application should be designed with appropriate security measures, such as user authentication and encryption, to ensure secure text transferring

Encryption Algorithm: The encryption algorithm is used to encrypt the text files during transmission and storage to ensure confidentiality. A commonly used encryption algorithm is Advanced Encryption Standard (AES).

Access Control Mechanism: The access control mechanism is used to control access to text files on the cloud network. This may include Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC).

Performance Metrics: Performance metrics are used to evaluate the performance of the system. This may include metrics such as upload/download speed, latency, andresponse time.

Security Testing Tools: Security testing tools are used to test the security of the system. This may include vulnerability scanners, penetration testing tools, and intrusion detection systems.

The experimental setup should be designed to simulate real-world usage scenarios and to evaluate the performance and security of the system under various conditions. The setup should also include appropriate security measures to ensure the confidentiality, integrity, and availability of data.

7.CONCLUSION

In conclusion, secure text transferring using cloud computing is an important aspect of data security in the digital age. Cloud computing provides a scalable, flexible, and cost-effective solution for secure text transferring, enabling organizations to store and transfer sensitive data with confidence.

To ensure secure text transferring, the system should be designed with appropriate security measures, such as user authentication, encryption, and access control mechanisms. Regular maintenance and evaluation are also essential to ensure that the system continues to meet the security and compliance requirements.

The experimental setup should be designed to simulate real-world scenarios and to evaluate the performance and security of the system under various conditions. The setup should also include appropriate security measures to ensure the confidentiality, integrity, and availability of data.

Overall, secure text transferring using cloud computing is a complex and critical process that requires careful planning, implementation, and evaluation to ensure that the data is secure and that the system meets the business and security requirements

8. TENTATIVE CHAPTER PLAN FOR THE PROPOSED WORK

CHAPTER 1: INTRODUCTION

CHAPTER 2: LITERATURE REVIEW

CHAPTER 3: OBJECTIVE

CHAPTER 4: METHODOLOGIES

CHAPTER 5: EXPERIMENTAL SETUP

CHAPTER 6: CONCLUSION AND FUTURE SCOPE

REFERENCES

1)Microsoft Azure: https://azure.microsoft.com/en-us/solutions/data-security/

2)AmazonWebServices:https://aws.amazon.com/security/data-protection/

3)Google Cloud: https://cloud.google.com/security/data-protection

4)IBM Cloud: https://www.ibm.com/cloud/learn/data-protection

5)Cloud Security Alliance: https://cloudsecurityalliance.org/

6)National Institute of Standards and Technology (NIST): https://www.nist.gov/topics/cloud-computing

7)Open Web Application Security Project (OWASP): https://owasp.org/www-project-cloud-security