SECURE TEXT TRANSFERRING USING CLOUD COMPUTING

S.P Maran Suri
Chandigarh University
Mohali, India
21BCS4315@cuchd.in

Aditya Kumar
Chandigarh University
Mohali, India
21BCS5560@cuchd.in

Khushi Verma
Chandigarh University
Mohali, India
21BCS11843@cuchd.in

Shriya Awasthi
Chandigarh University
Mohali, India
21BCS5452@cuchd.in

Abstract—Advent of Cloud Computing has been a phenomenal phase in the history of computer science. It provided capabilities to solve many problems that were earlier deemed impossible to be computed by a machine. It removed the pressure from those responsible for manufacturing better machines to keep up with the increasing complexity of the problems that the machines are intended to solve. Cloud Computing provided platform for better utilization of the resource spread across the world. Being a nascent field, it is crowded with many different problems that the engineers and scientist are working assiduously to eliminate. One of the main drawbacks with cloud is security. So, this project proposes a mechanism for secure file storage cloud using encryption and Diffie-Hellman. The algorithm involves encrypting the file stored on the cloud and using Diffie-Hellman for authenticating the user to decrypt the required file.

Keywords— Encryption, Decryption, AES, Public Key, Private Key

I. INTRODUCTION

Cloud security is one of the main concerns in the cloud computing domain. Storing personal and sensitive information on a third-party storage medium poses serious risks of data theft and data misuse by any person with malicious intent. The threat is so humongous that it has dissuaded governments and many other big organizations from migrating their operations on a cloud platform. The traditional methods of securing files and information are superfluous in the scenario of cloud. Extensive research and study is undergoing in this field to make cloud more secure and reliable. Among this behemoth instances of research, some of the methods that stand out include AES encryption and Diffie Hellman Key Exchange. The latter method is so powerful that it may take millions of years for even the most powerful computers of current times to crack the code and reads the file. Our approach proposes a method that involves encrypting the file using any standard encryption technique and using Diffie Hellman for user authentication. In this way the files can be ultimately save lives. This research paper aims to contribute to the ongoing discussion on blood bank management systems. saved in a public domain securely without the threat of being used by any unauthorized person.

II. DIFFIE-HELLMAN KEY EXCHANGE

Diffie–Hellman key exchange (DH) is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols named after Whitfield Diffie and Martin Hellman. [1] DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography. In public key cryptosystem, enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring more than 10100 instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. This was the main ideology behind Diffie-Hellman Key Exchange Protocol. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver can decipher it. As such, a public key cryptosystem is a multiple access cipher. A private conversation can therefore be held between any two individuals regardless of whether they have ever communicated before. Each one sends messages to the other enciphered in the receiver's public enciphering key and deciphers the messages he receives using his own secret deciphering key.

A.Background of the study:

With the increasing popularity and adoption of cloud computing, there has been a growing concern about the security of data transfer in the cloud environment. The cloud platform provides a scalable and cost-effective solution for storing and sharing data, but it also introduces new security challenges due to the nature of its architecture. One of the most critical issues is ensuring secure text transfer between two parties over an unsecured network .To address this issue, cryptographic techniques have been widely used to secure data transfer in the cloud environment. The Diffie-Hellman key exchange algorithm is one of the most popular cryptographic techniques used for secure key exchange between two parties. The algorithm enables two parties to establish a shared secret key over an insecure network without any prior knowledge of each other's secret key. Previous studies have proposed various cryptographic techniques for secure text transfer in the cloud environment. However, these techniques have limitations such as high computation time, communication overhead, and key management issues. Therefore, there is a need to develop an efficient and secure mechanism for text transfer in the cloud environment .In this study, we propose a secure text transfer mechanism using the Diffie-Hellman key exchange algorithm in the cloud environment. The proposed mechanism ensures secure communication between two parties over an unsecured network, providing an effective solution for secure text transfer in the cloud. We also evaluate the performance of the proposed mechanism and compare it with other existing cryptographic techniques. The results show that our proposed mechanism provides an efficient and secure solution for text transfer in the cloud environment.

II OBJECTIVE(S),SCOPE ,LIMITATIONS AND LITERATURE STUDIES

A. Objective(s)

The main objective of this study is to propose a secure text transfer mechanism using the Diffie-Hellman key exchange algorithm in the cloud environment. The specific objectives are:

1. To implement the proposed mechanism in a cloud computing environment.
2. To evaluate the performance of the proposed mechanism in terms of computation time and communication overhead.
3. To compare the performance of the proposed mechanism with other existing cryptographic techniques for secure text transfer in the cloud environment.
4. To analyze the key management issues of the proposed mechanism and propose solutions for efficient key management in the cloud environment.
5. To demonstrate the effectiveness of the proposed mechanism through experimental results and show that it provides an efficient and secure solution for text transfer in the cloud environment.
6. To provide insights into the limitations of the proposed mechanism and identify future research directions for improving the security of text transfer in the cloud environment.

By achieving these objectives, we aim to contribute to the development of a secure and efficient mechanism for text transfer in the cloud environment, which can be beneficial for various cloud-based applications.

B. Problem Statement

The use of cloud computing for data storage and transfer has become increasingly popular in recent years. However, the security of data transfer in the cloud environment remains a critical issue. One of the most significant concerns is the secure transfer of text messages between two parties over an unsecured network. Various cryptographic techniques have been proposed to ensure secure text transfer in the cloud environment. However, these techniques have limitations such as high computation time, communication overhead, and key management issues. Therefore, there is a need for an efficient and secure mechanism for text transfer in the cloud environment. In this study, we propose a secure text transfer mechanism using the Diffie-Hellman key exchange algorithm in the cloud environment. The mechanism ensures secure communication between two parties over an unsecured network, providing an effective solution for secure text transfer in the cloud. The aim of this study is to evaluate the performance of the proposed mechanism and compare it with other existing cryptographic techniques. We will analyze the computation time, communication overhead, and key management issues of the proposed mechanism and compare it with other existing techniques. By doing so, we aim to provide an efficient and secure solution for text transfer in the cloud environment.

B. Scope

The scope of this study is focused on the development of a secure text transfer mechanism using the Diffie-Hellman key exchange algorithm in the cloud environment. The study will evaluate the performance of the proposed mechanism in terms of computation time, communication overhead, and key management issues. The study will also compare the proposed mechanism with other existing cryptographic techniques for secure text transfer in the cloud environment. The comparison will be based on the efficiency, security, and practicality of each technique. The study will be limited to the secure transfer of text messages between two parties in the cloud environment. It will not cover other types of data transfer or other cloud computing applications. The study will also not address the security issues related to cloud storage or other cloud computing services. The experimental evaluation of the proposed mechanism will be conducted on a cloud computing platform, specifically Amazon Web Services (AWS). The study will use a simulated environment for testing and evaluation purposes and will not involve real-world scenarios or sensitive data. Overall, the scope of this study is to provide an efficient and secure solution for text transfer in the cloud environment, which can be applied to various cloud-based applications

.

C Limitation

There are several limitations to the proposed mechanism for secure text transfer using the Diffie-Hellman key exchange algorithm in the cloud environment. Some of the limitations are:

1. Key management: The proposed mechanism uses the Diffie-Hellman key exchange algorithm for key generation, but it does not address the issue of key management. The secure and efficient management of keys is critical to ensure the security of text transfer in the cloud environment.
2. Limited scalability: The proposed mechanism may not be scalable enough to handle a large number of text transfer requests in a cloud environment. The computational and communication overheads may increase significantly as the number of users and data transfer requests increase.
3. Communication overhead: The proposed mechanism requires multiple rounds of communication between the two parties for key exchange and text transfer. This can lead to increased communication overhead, which may affect the efficiency of the mechanism.
4. Security limitations: The proposed mechanism may not be resistant to attacks such as man-in-the-middle attacks or replay attacks. Further research is needed to enhance the security of the mechanism and make it more robust against potential attacks.
5. Dependency on cloud service provider: The proposed mechanism relies on the cloud service provider's infrastructure and security measures. If the service provider's security is compromised, the security of the proposed mechanism may also be compromised.

Overall, these limitations highlight the need for further research and development to improve the efficiency and security of text transfer in the cloud environment.

D.Significance of the problem

The problem of secure text transfer in the cloud environment is significant because of the increasing use of cloud computing for data storage and transfer. With the growth of cloud computing, there is a corresponding increase in the amount of data transferred over unsecured networks. Therefore, ensuring the security of data transfer in the cloud environment has become a critical concern.

The proposed mechanism for secure text transfer using the Diffie-Hellman key exchange algorithm in the cloud environment is significant because it provides an efficient and secure solution for text transfer. The mechanism can be applied to various cloud-based applications, such as instant messaging, email, and social media.

The significance of the problem is further highlighted by the potential risks associated with unsecured text transfer in the cloud environment. These risks include data breaches, unauthorized access to sensitive information, and loss of data privacy. By providing a secure solution for text transfer in the cloud environment, the proposed mechanism can help mitigate these risks and enhance the overall security of cloud computing.

Overall, the significance of the problem lies in the need to ensure the security of data transfer in the cloud environment, which has become a critical concern in the context of increasing cloud adoption and the potential risks associated with unsecured data transfer. The proposed mechanism provides an efficient and secure solution for text transfer, which can help enhance the security of cloud-based applications and mitigate potential risks.

A. Literature Studies

Several research studies have been conducted on secure text transfer in the cloud environment using various cryptographic techniques. The following are some of the key studies related to the use of the Diffie-Hellman key exchange algorithm for secure text transfer in the cloud:

1. "An Improved Text Encryption and Decryption Mechanism Based on Cloud Computing and Diffie-Hellman Algorithm" by Liu et al. (2019): This study proposed an improved text encryption and decryption mechanism using the Diffie-Hellman key exchange algorithm in the cloud environment. The proposed mechanism was shown to be efficient and secure compared to other existing techniques.
2. "A Secure and Efficient Text Encryption Technique for Cloud Computing Environment" by Gupta et al. (2017): This study proposed a secure and efficient text encryption technique for cloud computing using the Diffie-Hellman key exchange algorithm. The proposed technique was evaluated using various performance metrics and was shown to be effective in ensuring the security of text transfer in the cloud environment.
3. "A Secure Text Messaging Protocol Based on Public Key Cryptography for Cloud Computing" by Wang et al. (2016): This study proposed a secure text messaging protocol based on public key cryptography for cloud computing. The protocol used the Diffie-Hellman key exchange algorithm for key generation and was shown to be secure against potential attacks such as man-in-the-middle attacks and replay attacks.
4. "A New Approach for Secure Text Messaging Using Cloud Computing" by Okeyode et al. (2015): This study proposed a new approach for secure text

messaging in the cloud environment using the Diffie-Hellman key exchange algorithm. The proposed approach was evaluated using various performance metrics and was shown to be effective in ensuring the security of text transfer in the cloud environment.

III. CONCLUSION

Secure text transfer in the cloud environment is a critical concern due to the increasing use of cloud computing for data storage and transfer. The proposed mechanism for secure text transfer using the Diffie-Hellman key exchange algorithm in the cloud environment provides an efficient and secure solution for text transfer.The mechanism can be applied to various cloud-based applications, such as instant messaging, email, and social media. The significance of the problem lies in the need to ensure the security of data transfer in the cloud environment, which has become a critical concern in the context of increasing cloud adoption and the potential risks associated with unsecured data transfer.

The literature review has shown that several research studies have been conducted on secure text transfer in the cloud environment using various cryptographic techniques, including the Diffie-Hellman key exchange algorithm. These studies demonstrate the effectiveness of the algorithm in ensuring the security of text transfer in the cloud environment and highlight the need for further research and development to improve the efficiency and security of text transfer in the cloud.

IV .References

1.Diffie, W.; Hellman, M. (1976). "New directions in cryptography" (PDF). IEEE Transactions on Information Theory. 22 (6):644–.654.doi:10.1109/TIT.1976.1055638. Archived (PDF) from the original on 2014-11-29

2.Wikipedia

3.Kuhlman, Dave. "A Python Book: Beginning Python, Advanced Python, and Python Exercises". Archived from the original on 23 June 2012.

4."About Python". Python Software Foundation. Retrieved 24 April 2012., second section "Fans of Python use the phrase "batteries included" to describe the standard library, which covers everything from asynchronous processing to zip files."

5.Tkinter Wiki

6.Flask Wiki

7.thrain GitHub repository