Secure File Transfer using Deffie Hellman & 3DES

Ankit Srivastava (212IS003)

Department of Computer Science and Engineering
National Institute of Technology Karnataka
Surathkal, Mangaluru, India

Abstract. The safe transmission of data between client and server utilising the Diffie-Hellman key exchange and the 3DES algorithm. To begin, the sender and recipient exchange the key for the encrypted file using the Diffie-Hellman key exchange. As soon as the recipient receives the file, they decrypt it so that it may be read by the receiver. In this project, the application integrated the Diffie-Hellman Key Exchange with the 3DES algorithm to create a secure data transmission panel. This programme was the first to employ Diffie-Hellman Key Exchange to exchange shared secret keys.

Keywords: Encryption, Decryption, 3DES, Diffie-Hellman Key Exchange

1 Introduction

With the rising number of assaults and threats in today's world, data protection has become one of the most important requirements. Information is a precious asset that each firm creates, acquires, stores, and transfers. Safeguarding this from internal or external corruption and unauthorised access shields a firm from monetary loss, reputation damage, deterioration of consumer confidence, and image degradation. The relevance of information security stems from the fact that it safeguards our sensitive information, permits the safe functioning of applications deployed on the company's information technology system, and allows the business to function. It is advantageous in the sphere of business. As technology advances, so, too, do crime rates. As a result, information security must be used to secure your data. Algorithms used in modern cryptography include symmetric key, asymmetric key, hash function, and key exchange algorithms. To some extent, different cryptographic algorithms meet different security criteria. Nevertheless, cryptographic approaches must be used to offer a strong layer of security that assures the safe and secure transmission of messages to their intended recipients. Symmetric encryption techniques, for example, must employ a key exchange protocol to generate a more secure session key between two parties. Although hybrid cryptographic systems meet stringent security requirements, their performance might suffer as execution times lengthen.

1.1 Problem Description

In today's world, data is one of the most precious assets for both users and enterprises. Data breaches can be extremely damaging and can bring us to our knees both financially and psychologically. If data is sent in an unencrypted format, it is quite likely that it can be sniffed. This can provide an attacker over not just important information, as well as the information of server - side, allowing him to capture a transaction. Furthermore, non-secure communication can be tampered in by an intruder. In the upcoming section, we have come up with some secure way out to tackle such problems.

1.2 Motivation

Data breaches are a fairly regular issue that arises on a daily basis. Data leaking causes tremendous destruction, depending on the sort of data involved. Such repercussions include database destruction or corruption, the leakage of secret information, industrial espionage, and regulatory obligations to disclose and perhaps repay people impacted. The main motivation is to build a secure pipeline for data transmission so that attackers doesn't get easy access in this data flow penal. [1] In this paper, we have tried to integrate Diffie-Helman Key Exchange with triple Decryption to make a secure channel of data flow.

1.3 Scope

Data security entails implementing particular controls, standard rules, and processes to safeguard data from a wide range of threats such as unauthorised access, accidental loss, and destruction. Poor data privacy may expose a corporation to a variety of risks, including costly penalties and lawsuits, economic loss, and reputation harm. The loss or illegal exposure of sensitive data may be extremely expensive to a company. As technology improves, organisations become increasingly vulnerable to attack, necessitating the need for data security to protect information from attackers and provide a highly isolated channel for data flow. As a result, the data security sector is one of the most broad and trending topics to work on.

1.4 Objective

The ultimate purpose of network security is to secure data from dangers such as accidental or intentional data loss, destruction, or abuse. These attacks jeopardise the communication over network which causes integrity and access loss. In this paper, we are dealing with two major algorithm to secure the communication panel of data flow. Using Deffie-Helman Key Exchange, we allow two people conversing via a public channel to establish a shared secret without transmitting it over the Internet. Along with 3DES, which runs DES algorithm thrice using three separate keys, making it more difficult for the attackers to gain the unauthorized access.

1.5 Organization of the Report

The remainder of this work is structured as follows: Section 2 provides a detailed literature review of prior work in this topic. Section 3 identifies and provides the most significant aspect of this work, which includes several algorithm to deal with such attacks with detailed description of Deffie-Helman Key Exchange and triple decryption algorithm. Section 4 outlines all of the experimental results, which are then followed by the Conclusion and Reference.

2 Related Work

Data breaches may be incredibly costly, both economically and socially. If we continue to send data in an unencrypted manner, the odds of it being hacked are pretty significant. To solve this issue, several researchers have worked hard to devise solutions that make it more difficult for attackers to break security barriers. Some focused on cloud data security, while others attempted to design methods to deal with cryptographic issues. In this part, certain well-known works are analysed in depth.

At IEEE Transactions on Information Theory, Nov 1976, W. Diffie,Department of Electrical Engineering, University of Stanford, Stanford, CA, USA and M. Hellman from Department of Electrical Engineering, University of Stanford, Stanford, CA, USA proposed first view of Deffie-Helman Key Exchange. [1] It was developed in 1976 by Whitfield Diffie and Martin Hellman as the first viable mechanism for creating a shared secret across an unsecured communications channel. They examined two types of recent advances in cryptography that have resulted in the need for new forms of cryptographic systems that reduce the requirement for safe key distribution methods while providing the equivalent of a written signature. This study provides solutions to the difficulties that are currently unsolved.

At 2013 International Conference on Communication Systems and Network Technologies, Mr. Prashant Rewagad, HOD, Dept of Computer Science & Engineering and Ms.Yogita Pawar, M.E Student, Dept of Computer Science & Engineering,G.H.Raisoni Institute of Engg and Management Affiliated to North Maharashtra University Jalgaon, India, proposed different methodology to safeguard the secrecy of data saved in the cloud. [2] They proposed an integration of digital signature and Diffie Hellman key exchange with the (AES) Advanced Encryption Standard encryption method. They thought that even if the key in transit is hacked, the facility given by Diffie Hellman key exchange renders it meaningless, because the key in transit is useless without the user's private key, which is restricted to the genuine user. This suggested three-way technique makes it difficult for hackers to breach the security system, therefore safeguarding cloud resources.

In 2013, at International Journal of Computer Applications, Gurpreet Singh,a M.Tech Research Scholar and Supriya, a Assistant Professor, Department of Computer Science and Engineering Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India reviewed a study of all encryption algorithms (RSA, DES, 3DES and AES) for Information Security. [3] This paper was a general study and comparison among different encryption algorithm in tabular form. They presented an overview of existing efforts on encryption schemes. All of the strategies are beneficial for real-time encryption, but each is unique in its own way, which may be acceptable for different applications and has its own set of advantages and disadvantages. According to their investigation and review of the literature, they discovered that the AES algorithm is the most efficient in terms of speed, time, throughput, and avalanche impact.

During International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015, Mrs.Mamatha and Mr.Pradeep Kanchan, Department of CSE, NMAMIT, NITTE, proposed a hybrid cryptographic algorithm to enhance the security of cloud data. [4] This study combines the concepts of AES and 3DES to create a hybrid model that is used for uploading data to the cloud server by encrypting it and retrieving data from the cloud server by decrypting it.

At 2018 6th International Conference on Cyber and IT Service Management (CITSM), Yusfrizal Yusfrizal, Abdul Meizar, Helmi Kurniawan, Fhery Agustin proposed an article on cryptographic application for data security by using the Diffie-Hellman key exchange and the AES algorithm. [5] They developed security solutions for protecting cloud data from malevolent users, which the Diffie Hellman key exchange algorithm overlooked. They also handle access control issues by employing a good authentication technique based on two factors.

During INTERNATIONAL JOURNAL OF INFORMATION AND COMPUTING SCIENCE, Celeste Murnal,a PG Student and K.Pramilarani, a Senior Assistant professor, Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, India proposed a paper titled "Secure Text Transfer". [6] Their paper presents a secure file storage cloud system based on encryption and Diffie-Hellman. The approach encrypts the file stored in the cloud and uses Diffie-Hellman to authenticate the user in order to decrypt the needed file. According to the technique, the basic implementation of the provided methodology that may be improved and adjusted based on the needs of the user. It added a second layer of protection to files saved in the cloud by employing encryption and the Diffie Hellman Algorithm.

3 The Proposed Approach for

4 Experimental Results and Analysis

5 Conclusion

References

1. W. Diffie,M. Hellman "New directions in cryptography" in Proceedings of the IEEE Transactions on Information Theory (Volume: 22, Issue: 6, Nov 1976)

2. Prashant Rewagad, Yogita Pawar "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing".Communication Systems and Network Technologies (CSNT), 2013. DOI:10.1109/CSNT.2013.97
3. Gurpreet Singh, Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," in Proceedings of the International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.
4. Mrs.Mamatha, Mr.Pradeep Kanchan, "Use of Digital Signature with Diffie Hellman Key Exchange and Hybrid Cryptographic algorithm to Enhance Data Security in Cloud Computing" in Proceedings of the International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015, ISSN 2250-3153.
5. Yusfrizal Yusfrizal, Abdul Meizar, Helmi Kurniawan, Fhery Agustin "Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption" in 2018 6th International Conference on Cyber and IT Service Management (CITSM),DOI: 10.1109/CITSM.2018.8674278.
6. Celeste Murnal, K.Pramilarani "Secure Text Transfer" in 2019 INTERNATIONAL JOURNAL OF INFORMATION AND COMPUTING SCIENCE. ISSN NO: 0972-1347.