www.ijarp.com ISSN 2456-9992 Page: 01-07

International Journal Advanced Research Publications

Review Article

Volume: 02
Issue: 05

SECURE FILE SHARING USING DIFFIE–HELLMAN BASED KEY EXCHANGE IN A ZERO TRUST MODEL

[*1]Shadab Khan,[1]Shivesh Tandon, [2]Dr. Mohammad Suaib

[1]Research Scholar, Department of Computer Science Engineering, Integral University, Lucknow.

[2]Assosciate Professor, Department of Computer Science Engineering, Integral University, Lucknow.

Article Received: 24 March 2026, Article Revised: 14 April 2026, Published on: 04 May 2026

***Corresponding Author: Shadab Khan**

Research Scholar, Department of Computer Science Engineering, Integral University, Lucknow.

DOI: https://doi-doi.org/101555/ijrpa.8282

ABSTRACT

Secure file sharing has become a critical requirement in today's digital world, where sensitive information is constantly transmitted across networks that may not be fully secure. Traditional security approaches, which rely on perimeter-based protection, are increasingly ineffective due to the rise of sophisticated cyber threats and the growing adoption of cloud-based systems. This paper proposes a secure file-sharing framework that integrates the Diffie–Hellman key exchange mechanism within a Zero Trust architecture. The Diffie–Hellman method allows two communicating parties to generate a shared secret key over an insecure channel, which can then be used for encrypting files. Meanwhile, the Zero Trust model ensures that every access request is verified, authenticated, and continuously monitored. By combining these two approaches, the proposed system enhances confidentiality, integrity, and access control. The study further evaluates system performance, highlighting improvements in security while maintaining acceptable computational efficiency.

INTRODUCTION

The increasing dependence on digital communication and data sharing has made secure file transfer a fundamental aspect of modern information systems. Organizations and individuals frequently exchange sensitive data, including financial records, healthcare information, and intellectual property, over public or semi-secure networks. However, this widespread

connectivity also exposes data to various risks such as unauthorized access, interception, and data manipulation. Traditional security models typically assume that users within a network can be trusted, focusing primarily on protecting the network perimeter. This assumption is no longer valid in an era where threats can originate from both external attackers and internal users.

The Zero Trust model addresses this limitation by adopting a strict "never trust, always verify" approach. It requires continuous authentication and authorization of users and devices regardless of their location. At the same time, secure key exchange remains a cornerstone of protecting data during transmission. The Diffie–Hellman algorithm offers a reliable method for establishing a shared encryption key without prior communication between parties. This paper explores how integrating Diffie–Hellman key exchange with Zero Trust principles can create a more secure and resilient file-sharing system.

Literature Review

Over the years, numerous studies have examined secure communication and cryptographic protocols for protecting data transmission. Diffie–Hellman is widely recognized as one of the earliest and most influential key exchange algorithms, enabling secure communication over insecure channels. It is based on the mathematical difficulty of solving discrete logarithm problems, which makes it computationally infeasible for attackers to derive the shared key.

In addition, researchers have explored hybrid cryptographic systems that combine Diffie–Hellman with symmetric encryption algorithms such as AES to improve performance and security. These systems benefit from the efficiency of symmetric encryption while maintaining the security of asymmetric key exchange. Meanwhile, the concept of Zero Trust has gained significant attention in recent years as organizations shift towards cloud computing and remote work environments. Studies highlight the effectiveness of Zero Trust in reducing insider threats and preventing unauthorized access by enforcing strict identity verification and continuous monitoring.

Despite these advancements, there remains a gap in integrating Diffie–Hellman key exchange directly into a Zero Trust-based file-sharing framework. Existing solutions often treat key exchange and access control as separate components, leading to potential vulnerabilities. This research aims to bridge that gap by proposing a unified approach.

Problem Statement

Current file-sharing systems face several challenges that compromise their security and efficiency. One of the primary issues is the reliance on static trust assumptions, where users within a network are granted implicit trust. This approach makes systems vulnerable to insider attacks and unauthorized access. Additionally, many systems lack robust mechanisms for secure key exchange, increasing the risk of interception during data transmission. Man-in-the-middle attacks remain a significant threat, especially when authentication is weak or absent. Furthermore, the absence of continuous monitoring and dynamic access control limits the ability to detect and respond to suspicious activities in real time. These challenges highlight the need for a more comprehensive and integrated security framework.

Objectives of the Study

The main objective of this research is to design and implement a secure file-sharing system that combines Diffie–Hellman key exchange with Zero Trust principles. Specifically, the study aims to enhance data confidentiality by ensuring secure key generation, improve access control through continuous authentication, and evaluate the overall performance of the proposed system. Another important objective is to analyze the system's resistance to common cyber threats, including man-in-the-middle attacks and unauthorized access.

Mathematical Foundation of Diffie–Hellman

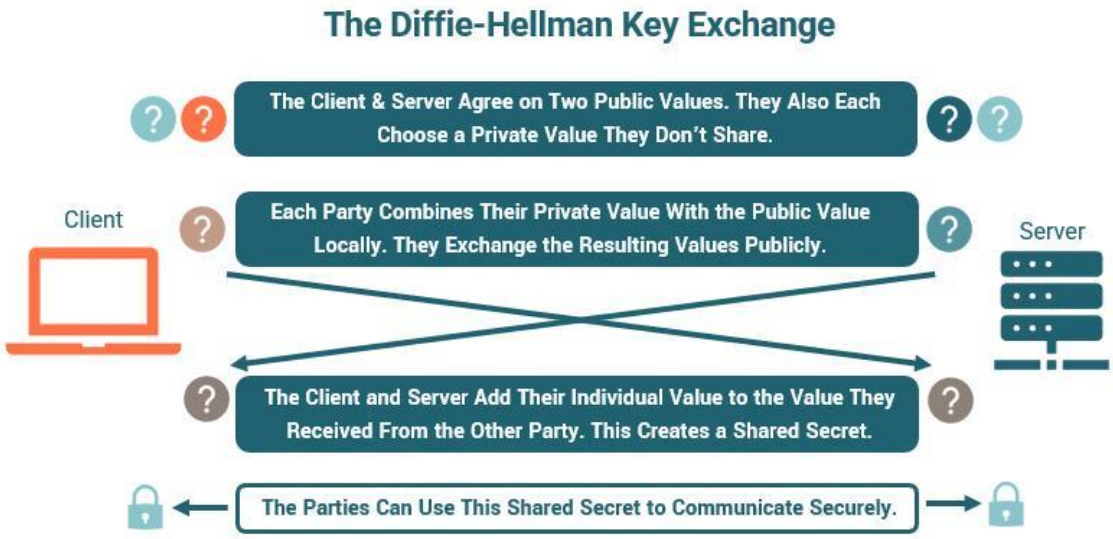
K=gabmod pK = g^{ab} \mod pK=gabmodp

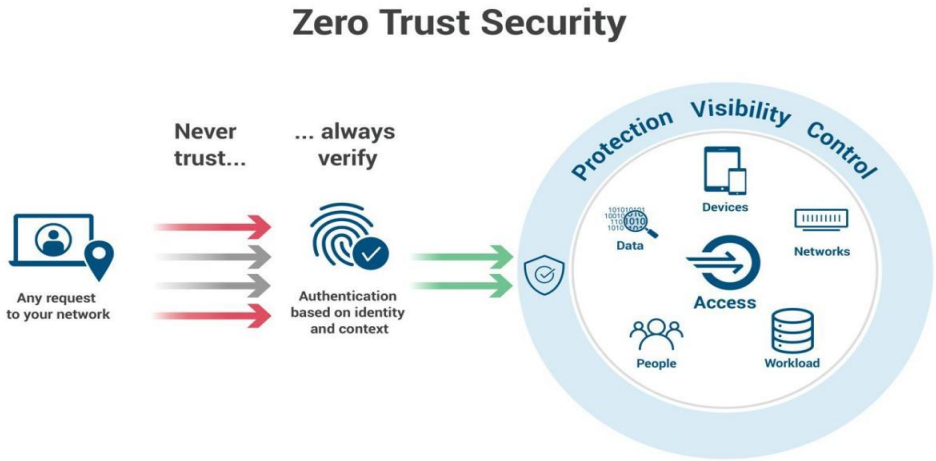
The Diffie–Hellman key exchange algorithm operates on modular arithmetic and relies on the use of a large prime number and a generator. Each party selects a private key and computes a corresponding public key, which is shared with the other party. Using these values, both parties independently calculate the same shared secret key. The security of this method is based on the computational difficulty of deriving the private key from the public key, making it highly resistant to brute-force attacks.

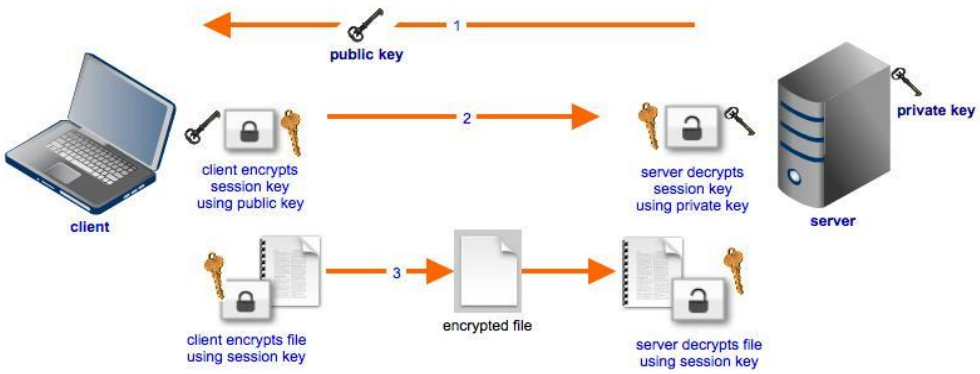
Proposed System Architecture

The proposed system consists of several interconnected components designed to ensure secure file sharing. The user authentication module verifies the identity of users through mechanisms such as multi-factor authentication. The key exchange module implements the Diffie–Hellman algorithm to generate a shared secret key. The encryption and decryption engine uses this key to secure files before transmission. Additionally, the access control engine enforces Zero Trust policies by continuously validating user permissions. Finally, a

monitoring and logging system tracks all activities, enabling real-time detection of anomalies and potential threats.







Working Mechanism

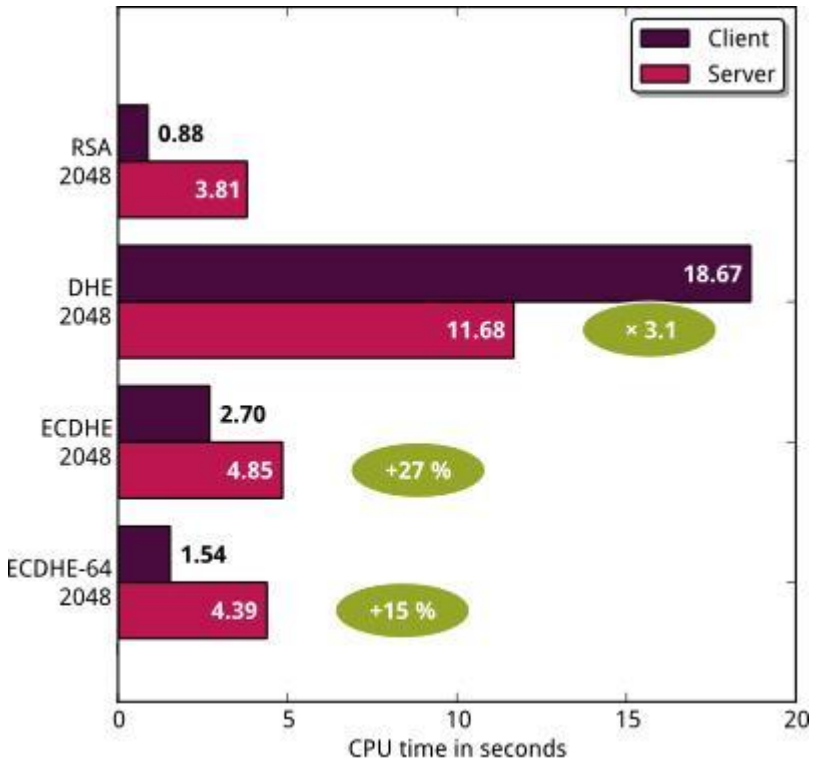
The operation of the proposed system begins with user authentication, where the identity of the user is verified using multiple factors. Once authenticated, the system initiates the Diffie–Hellman key exchange process to establish a shared secret key between the sender and receiver. This key is then used to encrypt the file using a symmetric encryption algorithm. The encrypted file is transmitted over the network, ensuring that even if intercepted, it cannot be deciphered without the key. Upon receiving the file, the recipient decrypts it using the same shared key. Throughout this process, the Zero Trust model continuously monitors and validates all actions, ensuring that only authorized users can access the data.

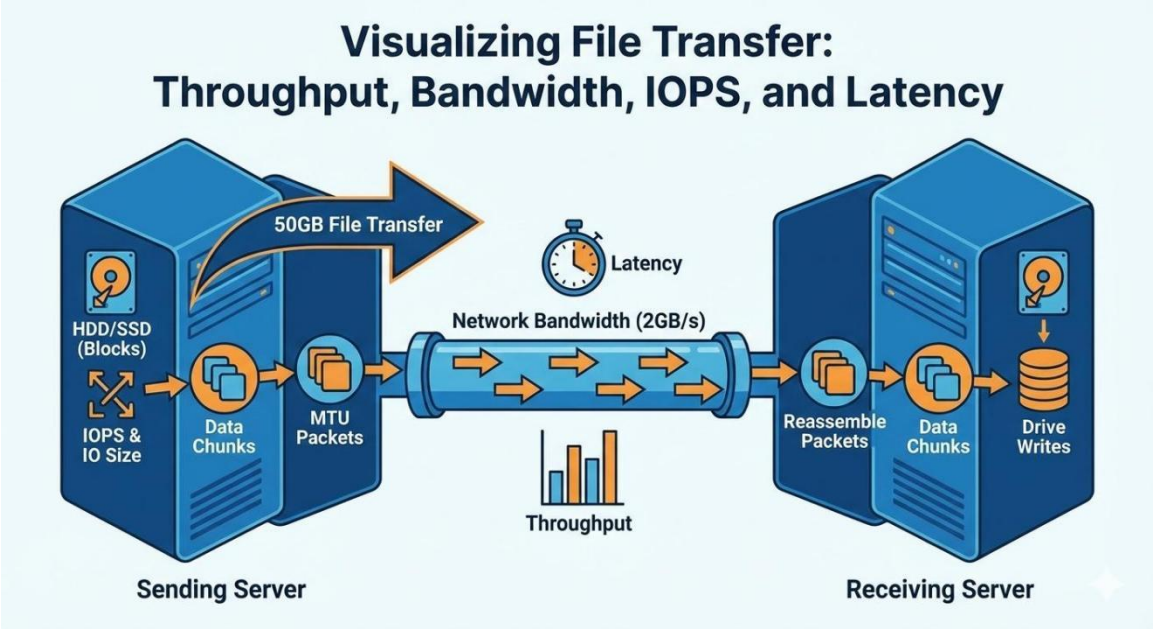
Performance Evaluation

To assess the effectiveness of the proposed system, a comparative analysis was conducted between traditional security models and the proposed Zero Trust-based approach. The results indicate that while the proposed system introduces a slight increase in computational overhead due to continuous authentication and key exchange, it significantly enhances security. The system demonstrates improved resistance to attacks, better access control, and stronger encryption capabilities.

Parameter	Traditional Model	Proposed Model
Security Level	Moderate	High
Key Exchange Time	Lower	Slightly Higher
Encryption Strength	Medium	Strong
Attack Resistance	Low	High
Access Control	Static	Dynamic

Graphical Analysis





The graphical representation of the results shows a clear improvement in security metrics, including resistance to attacks and data protection levels. Although there is a minor increase in processing time, the trade-off is justified by the substantial gains in security.

Security Analysis

The integration of Diffie–Hellman and Zero Trust provides several security advantages. It enables secure key exchange without requiring prior communication, ensures confidentiality

through strong encryption, and supports forward secrecy, meaning that even if a key is compromised, past communications remain secure. However, Diffie–Hellman alone does not provide authentication, which makes it vulnerable to man-in-the-middle attacks. This limitation is effectively addressed by the Zero Trust model, which enforces continuous verification and eliminates implicit trust.

Applications of the Proposed System

The proposed secure file-sharing system has wide-ranging applications across various sectors. In cloud computing, it can protect sensitive data stored and shared across distributed environments. In the banking sector, it ensures the secure transfer of financial information. Healthcare systems can use this approach to safeguard patient records, while government and military organizations can benefit from enhanced data security for confidential communications.

FUTURE SCOPE

Future research can focus on integrating advanced technologies such as blockchain to further enhance security and transparency. The development of quantum-resistant cryptographic algorithms is another promising area, given the potential impact of quantum computing on existing encryption methods. Additionally, incorporating artificial intelligence for real-time threat detection can further strengthen the system's ability to identify and respond to cyber threats.

CONCLUSION

This research highlights the importance of combining cryptographic techniques with modern security architectures to address emerging cybersecurity challenges. By integrating Diffie–Hellman key exchange with a Zero Trust model, the proposed system provides a comprehensive solution for secure file sharing. The approach enhances confidentiality, integrity, and access control while maintaining scalability and efficiency. Although there is a slight increase in computational overhead, the overall benefits in terms of security far outweigh the costs. The findings of this study suggest that the proposed model is well-suited for modern digital environments, where secure and reliable data sharing is essential.