Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

Building Intelligent Systems on a Foundation of Secure Data Exchange

Anil Kumar Soni
Lead Site Reliability Engineer
CSAA Insurance Group
Glendale, AZ, USA

***Abstract*— In the rapidly evolving Information Technology (IT) landscape, Secure File Transfer (SFT) has emerged as a critical tool for safeguarding data security and confidentiality. With the increasing prevalence of data breaches and cyber threats, organizations recognize the need to protect sensitive information during transmission to preserve its integrity and privacy. SFT is pivotal in enabling accurate and secure data handling, particularly in Artificial Intelligence (AI) projects that rely on timely, reliable, and safe data transfers for optimal performance. Beyond ensuring compliance and accountability through audit trails, this article delves into the fundamentals of SFT, explores its application in AI-driven IT businesses, and examines prominent security methods like Pretty Good Privacy (PGP) encryption. Additionally, it highlights key players in the SFT industry and their contributions to advancing secure digital exchanges.**

***Keywords*— Information Technology, Artificial Intelligence, Data Security, PGP Encryption/Decryption, Secure File Transfer, Managed File Transfer**

I. INTRODUCTION

Secure file transfer (SFT) has become one of the most crucial technologies in the modern Information technology (IT) landscape for ensuring data security and confidentiality. SFT has been increasingly part of the IT infrastructure, with data breaches and cyber threats well on their way to becoming more prevalent. If an enterprise must preserve the confidentiality and integrity of data, it is essential to protect sensitive information during transmission. SFT is a hot topic today, especially when decisions are being made based on data, and even more so for AI projects, which rely on such data to be transferred, stored, and processed safely and accurately. This helps keep track of data for audit trial purposes to ensure accountability and support compliance.

What is Secure File Transfer (SFT)?
Secure file transfer is the process of transferring or moving files from one place to another, keeping in view the data's availability, confidentiality, and integrity. SFT provides security protocols and data encryption against unauthorized access, modification, or data loss while in motion or at rest. SFT derives its security from encryption and secure protocols, which protect data from interception and tampering.

The reasons IT organizations use SFT include:

Data Exchange: Sharing sensitive information between departments or with outside partners.

Backup and Recovery: Secure transfer of backup files to off-site locations.

Software Updates: Providing security-related fixes and updates without compromising on security.

Compliance: The data transfer technique must follow the industry's rules and regulations.

What is Secure About Secure File Transfer (SFT)?
SFT derives its security from encryption and secure protocols. Data becomes unreadable to everybody, lacking a valid decryption (private) key. Secure protocols ensure that tampering and interception will not happen, as the data will travel via a secure, encrypted channel.

Key Components for Secure File Transfer:
Data Encryption refers to the encryption of data in transit or at rest, which renders it unreadable without the correct key for conversion.

Checksums and Hashing: The mechanism used for the integrity of the data, which creates some value in the form of a Checksum or hash from the original data. This is to be compared with the received data value.

Digital Signatures: A digital signature is a method of authenticating a transaction using cryptographic techniques that verify the sender's identity and make tampering with data impossible.

Secure Protocols: There are protocols like SSH, Secure Shell, SFTP, Secure File Transfer Protocol, and HTTPS that establish a secure connection and, hence, securely transfer data.

Some of the security protocols used in secure file transfer include:

Secure Sockets Layer (SSL)/Transport Layer Security (TLS): Ensures that data is encrypted during transmission over the internet.

Secure Shell (SSH): Provides a secure channel to exchange data over insecure networks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

File Transfer Protocol Secure (FTPS): an extension of FTP with added support for the encryption offered through SSL/TLS.

Secure File Transfer Protocol (SFTP): This protocol uses SSH to encrypt the commands and the transferred data.

PGP Encryption Method:

Pretty Good Privacy, PGP, is an encryption program that provides cryptographic privacy and authentication for data communication [2]. With PGP, no one can decrypt your file except the person you present it to, provided you encrypt it with that person's public key. Here is how it works:

Key Generation: PGP generates a pair of keys, which are a public key and a private key. The public key is given to others, but the private key remains secret.

Encryption: The sender encrypts the file using the recipient's public key. This ensures that only the recipient with the corresponding private key can decrypt and access the file.

Decryption: Decrypt the received file using the recipient's private key.

The Importance of Secure File Transfer:

Data Integrity: SFT ensures the accuracy and reliability of data by preventing data alteration in the transfer process. This is critical, for example, in the case of financial transactions, where SFT can avoid errors and fraud that could lead to severe financial loss.

Confidentiality: The secure transfer method makes accessing the data hard for unauthorized processes and maintains data privacy and regulatory adherence. For example, to meet the Health Insurance Portability and Accountability Act (HIPAA) guidelines and protect the patient's information, healthcare organizations must protect patient records when they are in transit.

Availability: Reliable SFT mechanisms enable businesses to run smoothly and make sound decisions since data is easily accessible when needed. For example, efficient and timely transmission of transaction data in the e-commerce sector enables efficient order processing and fulfillment, increasing client happiness.

Compliance and Regulatory Requirements: Certain rules govern data protection in several organizations. Using SFT, organizations can thus prevent legal consequences if they adhere to such laws. For instance, the General Data Protection Regulation (GDPR) is a European Union (EU) law that restricts organizations from handling personal data unsecured, including when transferring it.

Data Security Considerations for Companies - When it comes to data security, companies should be vigilant about:

Access Controls: Implementing access controls that ensure only authorized personnel can access data.

Data Encryption: It protects data both in transit and at rest from unauthorized access by encrypting it.

Regular Audits: Conduct regular security audits to find and patch vulnerabilities.

Employee Training: Educating employees on best practices for data security and the importance of following security protocols.

Secure File Transfer and AI - Artificial intelligence systems rely on substantial datasets for model training and the generation of insights. Secure File Transfer contributes to this system through the following aspects:

Data Quality: Secured, high-quality data is crucial for accurate decision-making and AI predictions. For example, if the historical data used for training AI models in predictive analytics is accurate, projections will also be more precise, leading to wiser business decisions. Accurate AI predictions depend heavily on the quality of secured input data.

Enabling Data Integration: SFT allows multiple data sources to integrate safely into one AI model dataset. This could be the case in the automotive industry, where safely incorporating the data from various sensors and systems may lead to significant enhancements in AI algorithms used for self-driving cars.

Compliance Support: SFT allows organizations to avoid fines and reputational damage due to violations of data protection regulations. For example, in the financial services industry, handling client data via secure file transfer helps ensure that regulations such as PCI DSS compliance are followed. PCI DSS is a compliance specification typically required for any organization that handles payments [1].

Improving Collaboration: In most AI development cases, collaboration among teams or outside partners is imperative. SFT makes this collaboration possible while ensuring safety and efficiency in data exchange. For example, crucial data sets can be shared safely between academic institutes working on AI projects, thus promoting collaborative innovation without compromising data security.

Case Studies:

Health Sector: SFT supports AI-driven diagnosis and treatment plans while ensuring that patient information is protected across transfers by providers. A hospital could, for instance, employ SFT to send MRI pictures safely to a specialist for analysis.

Financial Services: SFT is deployed by financial organizations to securely transfer transaction information to AI models to detect fraud, which makes financial processes smoother. An example would be a bank using SFT to send all customer transaction information into an AI system to detect suspicious activity.

Insurance Industry: Insurance companies use SFT to encrypt private customer data in transmission. For example, SFT securely transmits policy or claims data to a third-party processor while keeping all data confidential and compliant with the required regulations, such as the Payment Card Industry Data Security Standard (PCI DSS). Doing so ensures that the data breach does not occur and that the customers' trust remains intact.

SFT can be integrated into Open Telemetry-based observability methods, particularly in hybrid environments where telemetry data (logs, metrics, traces) may need to be securely exported to centralized systems for analysis. In cases where direct streaming is not feasible, due to network restrictions, regulatory requirements, or batch processing constraints, SFT

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

ensures encrypted, protocol-compliant delivery of observability data. This approach supports data integrity and compliance, especially in regulated industries. Incorporating Open Telemetry can enhance observability and trustworthiness in the observability framework [3].
Market Leaders in Secure File Transfer Solutions - Some of the market leaders in this domain include:

Axway SecureTransport: This provides an end-to-end secure file transfer solution across multiple platforms.

GoAnywhere MFT: This is also an all-inclusive managed file transfer solution that includes a secured manner of integration with systems, employees, customers, and trading partners.

AWS Transfer Family: The AWS service provides fully managed support for SFTP, FTPS, and FTP, thus allowing secure file transfers in and out of AWS storage services like Amazon S3 and Amazon EFS.

MOVEit: Progress secure file transfer software, supporting all major protocols, including FTP(S) and SFTP, providing the necessary automation services and analytics for efficient data exchange.

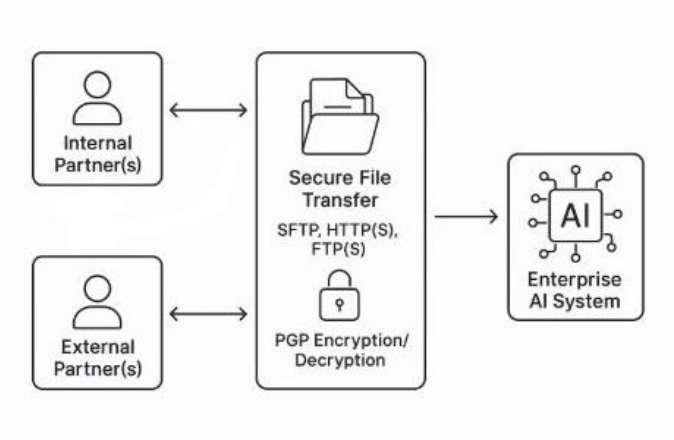
IBM Aspera: Fully featured high-speed file transfer solutions for secure and reliable data exchange.

Signiant: Securely and efficiently perform high-speed file transfer in media and entertainment.

Figure 1 shows the connectivity among Internal Partner(s), External Partner(s), and the Enterprise AI System.

A. Figures and Tables

Fig. 1. Example of a figure caption. (SFT – AI Integration)



ACKNOWLEDGMENT

A secure transfer of files allows organizations to safeguard their data when in transit. Encryption, imposition of secure protocols, and use of best practices will help organizations protect sensitive information from cyberattacks and ensure regulatory compliance. With these ever-evolving digital environments, stronger demands arise for strong and secure file transfers. File transfer security is vital for any successful AI project in IT. The SFT will support AI considerably by ensuring integrity, confidentiality, and data availability for effective development and deployment. As more industries embrace AI and need secure file transfers to increase their success, more case studies in supply chain and logistics, research, media, and retail may be helpful. This could also mean that organizations that can implement file transfer security would allow their companies to harness all the potential of AI as the key driver for innovation and competitive advantage.

REFERENCES

[1] S. M. Kerner, “Will PCI DSS 3.2 Make Payments More Secure?” EWeek, p. 1, 2016.
[2] R. McCollum, “A pretty good paper about Pretty Good Privacy,” unpublished, 1995.
[3] A. Soni, “Enhancing Site Reliability Engineering (SRE) observability: A comprehensive approach,” Scholars Journal of Engineering and Technology, 2025. [Online]. Available: https://www.saspublishers.com/article/21485/