Secure Communication: An Overview

por Mayko Silva

The Two Pillars of Secure Communication

Security is vital in communications between cloud systems and between cloud and on-premise systems. This protection operates on two essential fronts that work together to create a comprehensive security approach.

On one hand, trust is required in the security on the user side, and on the other hand, you must ensure that data on the communication path cannot be read or manipulated by third parties.

User-Side Trust

Ensuring that users accessing your systems are properly authenticated and using secure devices and connections.

Data Protection in Transit

Implementing measures to prevent data interception or tampering while information travels between systems.

Complete Security Model

Both elements must work together - like trusting both the sender and the secure packaging when shipping valuable items.

Understanding the Security Requirements

Trust on the user side means verifying that users accessing your systems are who they claim to be and that they're connecting through secure devices and connections. This forms the foundation of your security architecture.

Data protection in transit ensures that information traveling between systems remains confidential and intact, preventing unauthorized access or manipulation by third parties.

1

Authentication

Verify the identity of users and systems attempting to access your resources through strong authentication methods.

2

Secure Connections

Ensure that all connections use encrypted protocols to protect data as it moves between endpoints.

3

Data Integrity

Implement measures to detect any tampering or modification of data during transmission.

4

Continuous Monitoring

Regularly audit and monitor communication channels to identify and address potential security threats.

The Evolution of Secure Communication

Especially in the consumer sector, secure communication was rarely the focus of attention in the past. This lack of priority stemmed primarily from the additional costs providers faced and the specialized knowledge required for implementation.

A significant shift occurred when Google began giving preferential treatment in its search results to secure websites. This policy change prompted a widespread rethinking among service providers, making secure communication a standard practice rather than an optional feature.

1

Cost Barriers

Historically, secure communication implementation was considered too expensive for many consumer-facing services.

2

Knowledge Gap

The technical expertise required for proper security implementation created adoption challenges for many organizations.

3

Search Engine Incentives

Google's decision to favor HTTPS websites in search rankings created a powerful business incentive for widespread adoption.

4

Industry Standard

Secure communication has now become the expected norm across both consumer and business applications.

Business Applications and Security Protocols

In business applications, secure communication is essential and has not been debatable for decades. When securing communications, several concepts like Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Hypertext Transfer Protocol Secure (HTTPS) are often mentioned but frequently confused or misinterpreted.

These protocols are based on symmetric and asymmetric encryption methods, which provide the foundation for secure data transmission across networks.

SSL/TLS

Cryptographic protocols designed to provide secure communication over a computer network, with TLS being the successor to SSL.

HTTPS

An extension of HTTP that uses SSL/TLS for encryption and authentication, securing website connections and protecting sensitive information.

Encryption Methods

Symmetric encryption uses one key for both encryption and decryption, while asymmetric encryption uses public and private key pairs.