Priyank Patel

ITWP 2600

Two main techniques for protecting data are private-key encryption which often known as symmetric encryption and public-key encryption which often known as asymmetric encryption. Private-key encryption uses the same key for decryption and encryption. This calls for the same secret key for both the sender and the receiver, which has to be safely swapped before to use. Though securely exchanging the secret is the main difficulty, this approach is quick and efficient, especially for huge data volumes. Often used to encrypt data during storage or transmission the Advanced Encryption Standard (AES) is an example of private-key encryption. Conversely, public-key encryption employs two keys: a public key to encrypt data and a private key to decode it. While the private key stays secret, the public key may be shared freely. This approach improves security by removing the need to share hidden keys. On the other hand, it is slower computationally than private-key encryption. RSA, often used for secure email communications and digital signatures, is one form of public-key encryption; it also helps to protect connections over the internet (e.g., SSL/TLS).

In the framework of cloud computing for an online sales system, firewall problems could result from the need to control and protect traffic across several cloud environments. Ensuring correct configuration of firewall rules to prevent illegal access and the difficulty of keeping consistent security policies across different cloud platforms are among challenges. The perimeter expansion issue arises from the fact that conventional firewalls are meant for static network perimeters whereas cloud computing stretches this perimeter to distant servers, hence complicating the consistent security management across several sites.

Source:

https://www.geeksforgeeks.org/difference-between-private-key-and-public-key/

https://www.1kosmos.com/authentication/private-key/