EEEP Deputado Roberto Mesquita

Desenvolvimento de Sistemas

Francisca Marta Gomes da Silva

Criptografia na proteção de dados sensíveis : análise comparativa de métodos de criptografia em ambientes corporativos.

General Sampaio -CE 2024

Introdução

1.análise comparativa:

A criptografia é a ciência de codificar informações de modo que apenas os indivíduos autorizados possam acessá-las. Ela utiliza algoritmos matemáticos para transformar dados legíveis em formatos ininteligíveis, protegendo assim a confidencialidade dos dados. Existem dois principais tipos de criptografia: a criptografia simétrica e a criptografia assimétrica.

A criptografia simétrica utiliza a mesma chave para cifrar e decifrar dados. Os algoritmos simétricos são geralmente rápidos e eficientes, mas a principal desvantagem é a necessidade de compartilhar a chave secreta entre as partes envolvidas. Exemplos de algoritmos simétricos incluem o Advanced Encryption Standard (AES) e o Data Encryption Standard (DES).

Em contraste, a criptografia assimétrica, também conhecida como criptografia de chave pública, utiliza um par de chaves: uma pública e uma privada. A chave pública é

utilizada para cifrar os dados, enquanto a chave privada é utilizada para decifrá-los. Embora os algoritmos assimétricos sejam mais lentos do que os simétricos, eles oferecem vantagens significativas em termos de gerenciamento de chaves e segurança. O RSA (Rivest-Shamir-Adleman) é um exemplo proeminente de criptografia assimétrica.

2. Métodos de Criptografia em Ambientes Corporativos

2.1 Criptografia Simétrica: Advanced Encryption Standard (AES)

O AES é amplamente adotado em ambientes corporativos devido à sua eficiência e robustez. Este algoritmo utiliza chaves de 128, 192 ou 256 bits, proporcionando diferentes níveis de segurança. O AES é conhecido por sua resistência a ataques e sua capacidade de operar de maneira eficiente em grandes volumes de dados. No entanto, a principal desvantagem é a necessidade de uma gestão cuidadosa das chaves, pois a segurança do sistema depende da proteção adequada da chave secreta.

2.2 Criptografia Assimétrica: RSA

O RSA é um dos algoritmos de criptografia assimétrica mais conhecidos e utilizados. Ele é amplamente empregado para a troca segura de chaves e para autenticação digital. O RSA utiliza pares de chaves de diferentes tamanhos, geralmente variando de 512 a 4096 bits. Embora o RSA ofereça um alto nível de segurança e facilite a gestão de chaves, sua velocidade de criptografia é mais baixa em comparação com os algoritmos simétricos, o que pode ser uma limitação em sistemas que requerem alta performance.

2.3 Criptografia Híbrida

A criptografia híbrida combina os benefícios da criptografia simétrica e assimétrica, utilizando ambos os métodos para otimizar a segurança e a eficiência. Em uma implementação híbrida típica, a criptografia assimétrica é utilizada para trocar uma chave simétrica de sessão, que por sua vez é empregada para cifrar os dados. Esta

abordagem oferece a segurança adicional da criptografia assimétrica enquanto mantém a eficiência da criptografia simétrica para a transmissão de dados.

3. Análise Comparativa:

É um método de pesquisa, coleta e análise de informações que envolve a comparação de dois ou mais processos, documentos, conjuntos de dados ou outros objetos para obter razões válidas na explicação de diferenças ou semelhança.

3.1 Eficiência e Desempenho

A criptografia simétrica, especialmente o AES, é conhecida por sua alta eficiência e capacidade de lidar com grandes volumes de dados sem comprometer significativamente o desempenho do sistema. Em contraste, a criptografia assimétrica, como o RSA, pode apresentar uma sobrecarga de processamento devido ao seu

algoritmo mais complexo, tornando-a menos eficiente para operações de criptografia em larga escala.

3.2 Segurança:

Em termos de segurança, a criptografia assimétrica oferece vantagens significativas, especialmente na gestão de chaves. O RSA, por exemplo, permite a troca segura de chaves sem a necessidade de um canal seguro pré-existente, um aspecto crucial em muitos cenários corporativos. Por outro lado, a criptografia simétrica, como o AES, é altamente segura quando utilizada com chaves de tamanho adequado e gerenciada corretamente. No entanto, a segurança do sistema é tão forte quanto a proteção da chave secreta.

3.3 Implementação e Complexidade:

A implementação da criptografia simétrica tende a ser mais simples e menos complexa em comparação com a criptografia assimétrica. No entanto, a gestão de chaves é um fator crítico para a criptografia simétrica, exigindo procedimentos rigorosos para evitar comprometer a segurança. A criptografia assimétrica, enquanto mais complexa, oferece um gerenciamento de chaves mais simplificado e robusto.

Conclusão:

A escolha do método de criptografia adequado em ambientes corporativos depende de diversos fatores, incluindo a eficiência desejada, o nível de segurança necessário e a complexidade da implementação. A criptografia simétrica, com algoritmos como o AES, oferece uma solução eficiente e robusta para a proteção de dados sensíveis, enquanto a criptografia assimétrica, exemplificada pelo RSA, é crucial para a segurança na troca de chaves e na autenticação. A criptografia híbrida, por sua vez, proporciona um equilíbrio entre segurança e desempenho, aproveitando o melhor dos dois mundos. Em última análise, a escolha do método de criptografia deve ser orientada pelas necessidades específicas da organização e pelo contexto em que os dados estão sendo protegidos.