**TRABALHO DE COMPUTAÇÃO EM**

**NUVEM – 2º TRIMESTRE**

****

**Alunos: Kauã Rosa de Souza & Taylor Santolin Borges Laignier**

**Série: 3° IPI 01**

**Criptografia na Nuvem: A Blindagem Digital na Era da Conectividade Constante**

1. **O Que É e Por Que a Criptografia na Nuvem É Tão Importante?**

A criptografia funciona como um escudo, transformando informações claras em códigos indecifráveis. Apenas quem possui a chave correta consegue reverter o processo e acessar o conteúdo original. Imagine que seus dados estão guardados em um cofre digital, acessível somente com a combinação exata.

Em ambientes de nuvem, onde seus arquivos ficam em servidores remotos, acessíveis pela internet, a criptografia é vital. Ela protege informações confidenciais, como dados pessoais, financeiros e empresariais, impedindo o acesso por pessoas não autorizadas, mesmo que os servidores sejam invadidos. Sem ela, uma invasão poderia revelar dados cruciais, comprometendo a privacidade e segurança das informações.

2. **Quais São os Tipos de Criptografia Mais Utilizados?**

Existem diferentes formas de aplicar a criptografia na nuvem, variando conforme o tipo de dado, a estrutura do sistema e o nível de segurança desejado. Veja os principais:

**Criptografia Simétrica**

- Como Funciona: Utiliza uma única chave tanto para codificar quanto para decodificar os dados.

- Pontos Fortes: Rápida e eficaz, ideal para grandes volumes de informação.

- Pontos Fracos: A chave precisa ser distribuída de forma segura, o que pode ser complicado.

- Onde Usar na Nuvem: Proteção de arquivos, backups e dados armazenados.

**Criptografia Assimétrica**

- Como Funciona: Usa um par de chaves, uma pública (para codificar) e uma privada (para decodificar).

- Pontos Fortes: Facilita a troca segura de dados entre diferentes partes.

- Pontos Fracos: Mais lenta em comparação com a criptografia simétrica.

- Onde Usar na Nuvem: Autenticação de usuários, troca segura de informações entre servidores e clientes.

**Criptografia de Ponta a Ponta (End-to-End)**

- Como Funciona: Os dados são criptografados no dispositivo de quem envia e só são descriptografados no dispositivo de quem recebe.

- Pontos Fortes: Nem mesmo o provedor da nuvem consegue acessar os dados.

- Pontos Fracos: Pode limitar algumas funcionalidades, como a busca por informações.

- Onde Usar na Nuvem: Comunicação segura entre usuários, como em aplicativos de mensagens.

3. **Quais São os Desafios da Criptografia na Nuvem?**

Apesar de ser essencial, a implementação da criptografia na nuvem apresenta alguns desafios:

- Gerenciamento de Chaves: É complexo manter as chaves seguras e acessíveis apenas para quem tem permissão, principalmente em ambientes com muitos usuários.

- Desempenho: A criptografia pode diminuir a velocidade de acesso e processamento dos dados, especialmente em sistemas que exigem alta performance.

- Compatibilidade: Nem todos os serviços de nuvem oferecem suporte aos mesmos padrões de criptografia, dificultando a integração entre plataformas.

- Conformidade Legal: É preciso garantir que os métodos de criptografia sigam as leis e regulamentações, como a LGPD no Brasil e o GDPR na Europa.

4. **Caso Prático**: Protegendo Dados Médicos com Criptografia na Nuvem

Qual É o Problema?

Um consultório médico tomou a decisão de transferir seus registros de saúde digitais para um ambiente de nuvem. Contudo, os dados dos pacientes — abrangendo diagnósticos, análises e histórico clínico — demandam o máximo cuidado. A maior apreensão era assegurar que tais informações não fossem vistas por pessoas não autorizadas, nem mesmo pela empresa de nuvem.

**Sugestão Implementada**

O consultório optou por um modelo de criptografia de ponta a ponta, juntamente com criptografia simétrica para guardar os arquivos localmente. Cada registro é codificado no aparelho do médico e só pode ser visto por quem tem permissão e a chave correta. Além disso, criaram um sistema de controle de chaves com base em hardware (HSM), que guarda as chaves em aparelhos físicos seguros.

**Vantagens Aguardadas**

- Maior segurança: Os dados ficam protegidos mesmo se o servidor for invadido.

- Privacidade assegurada: Nem a empresa de nuvem consegue ver os registros.

- Adequação legal: A solução cumpre as normas da LGPD, protegendo os dados dos pacientes.

**Implantação e Aspectos Práticos**

A implantação precisou de instrução da equipe médica e adaptações nos acessos. Um dos desafios foi a união com softwares de outros, que não permitiam criptografia de ponta a ponta. A solução foi criar APIs seguras que deixassem os sistemas se comunicarem sem que a criptografia fosse afetada.

Foi preciso também criar regras para recuperar a chave, caso um médico perdesse o acesso. Isso foi resolvido com um sistema de autenticações diversas e cópia de segurança das chaves.