PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Instituto de Ciências Exatas e de Informática

Data Security and Privacy Protection for Cloud Storage: A Survey

Diego Moreira Rocha
Luan Barbosa Rosa Carrieiros
22/09/2024
Leonardo Vilela Cardoso

Dados do Artigo

Título: Data Security and Privacy Protection for Cloud Storage: A Survey

Autores: Pan Yang, Naixue Xiong, Jingli Ren

Congresso/Periódico: IEEE Access (Special Section on Emerging Approaches to Cyber Security)

Ano de Publicação: 2020

O artigo [1] foi publicado em uma das maiores plataformas científicas, a IEEE Access, e pertence à seção especial de abordagens emergentes de cibersegurança, o que demonstra a relevância e atualidade do tema abordado.

Problema abordado

Com o crescimento do IoT e cidades inteligentes, a demanda por armazenamento em nuvem explodiu. Embora ofereça acessibilidade e escalabilidade, surgem desafios de segurança, como:

- Acesso não autorizado à dados sensíveis;
- Vazamento de dados, seja por falhas de segurança ou ataques;
- Risco de roubo de informações devido à hospedagem em servidores compartilhados;

Esses problemas são ainda mais críticos em áreas como saúde e finanças, onde a proteção dos dados é essencial.

Motivação

Com mais organizações migrando para a nuvem, os riscos de segurança aumentam. Estima-se que até 2025 haverá 41,6 bilhões de dispositivos IoT, gerando 79,4 zettabytes de dados, majoritariamente na nuvem. Abordagens tradicionais, como criptografia simples, já não são suficientes; novas técnicas, como criptografia homomórfica, são necessárias para lidar com essas ameaças.

Objetivo do Artigo

O artigo revisa técnicas de segurança para armazenamento em nuvem, abordando:

- **Criptografia**: simétrica e assimétrica para proteger o acesso a dados.
- **Controle de acesso**: métodos que garantem acesso seguro a informações autorizadas.
- **Segurança durante o processamento de dados**: criptografia homomórfica para processar dados sem expor sua privacidade.

Essas ferramentas são essenciais para mitigar os riscos de vazamentos e acessos não autorizados.

Conclusões

A criptografia é crucial, mas precisa ser mais eficiente. Métodos de controle de acesso, como ABE, oferecem proteção, mas exigem melhorias em escalabilidade. Futuras pesquisas devem explorar criptografia pós-quântica e privacidade em machine learning para ambientes em nuvem.

- Criptografia é essencial;
- Necessidade de melhorias na segurança do acesso;
- Tópicos para trabalhos futuros;

Trabalhos futuros

O artigo destaca que, embora já existam diversas abordagens para enfrentar os desafios de segurança na nuvem, ainda há um longo caminho a ser percorrido. Algumas das principais conclusões são: Entre os temas apontados para trabalhos futuros estão:

Criptografia pós-quântica: proteger contra a ameaça dos computadores quânticos.

Aprendizado de máquina preservador de privacidade: garantir a confidencialidade dos dados usados no treinamento.

Soluções de busca criptografada: aprimorar a eficiência e segurança em buscas sobre dados criptografados.

Perguntas da apresentação

Qual foi o critério de avaliação que os autores escolheram para selecionar os artigos escolhidos para essa pesquisa?
Os autores da pesquisa escolheram os artigos com base em tópicos relacionados à segurança de dados e privacidade no armazenamento em nuvem. Eles selecionaram as tecnologias de criptografia e os métodos de proteção que correspondiam aos requisitos de segurança do sistema de armazenamento na nuvem, como controle de acesso refinado, criptografia homomórfica, e controle de acesso baseado em atributos (ABE), entre outros.

Perguntas da apresentação

Motivação?
A motivação principal para o estudo está no fato de que, à medida que mais organizações migram para a nuvem, os riscos de segurança se tornam maiores. A nuvem passou a ser um componente essencial da economia digital, hospedando aplicações de cidades inteligentes, IoT, governos e até pequenas empresas.
Estatísticas do artigo mostram que até 2025, haverá cerca de 41,6 bilhões de dispositivos conectados à IoT, gerando 79,4 zettabytes de dados. Esses dados serão, em sua maioria, armazenados na nuvem, aumentando a pressão por soluções eficazes de segurança.
Outro ponto motivador é que as abordagens de segurança tradicionais, como a criptografia simples e o controle de acesso, não são mais suficientes para enfrentar as ameaças em grande escala que os sistemas de nuvem enfrentam atualmente. É necessário explorar novas técnicas, como criptografia homomórfica e controle de acesso baseado em atributos.

Referências I

[1] Pan Yang, Naixue Xiong e Jingli Ren. “Data Security and Privacy Protection for Cloud Storage: A Survey”. Em: *IEEE Access* 8 (2020), pp. 131723–131740. DOI: 10.1109/ACCESS.2020.3009876.

Muito obrigado!