PÓS-GRADUAÇÃO EM ENGENHARIA DE DADOS

IEC PUC MINAS

Disciplina:

BANCOS DE DADOS NoSQL

Professor: Augusto Zadra

3.3 – Segurança em bancos NoSQL

INTRODUÇÃO

- Segurança efetivamente é um dos pontos de preocupação nos bancos de dados NoSQL.
- A maioria dos bancos de dados NoSQL não fornece recursos de segurança embutidos no próprio banco de dados e os desenvolvedores precisam programar os requisitos de segurança em seu código.
- Aí está um dos problemas desta nova geração de bancos de dados que se concentram primeiro em questões de escalabilidade horizontal e usam a camada de aplicativo para implementar recursos de segurança.

INTRODUÇÃO

- O problema deste modelo é a possibilidade de erros, tendo em vista que se a falta de segurança se torna um dos motivos principais da não adoção destes bancos em empresas que tem critérios mais rigorosos de segurança.
- Desta forma, recursos de segurança como autenticação, autorização e integridade, direcionam as escolhas para que os dados confidenciais sejam hospedados de forma mais segura no SGBD relacional.

INTRODUÇÃO

- Há muitas ameaças de segurança, como cross-site scripts, SQL Injections, root kits e a famosa engenharia social.
- Para as questões eletrônicas que dependem de codificação os bancos relacionais conseguem trabalhar melhor estas vulnerabilidades devido a seus aprimoramentos.
- Os bancos de dados NoSQL estão sempre sujeitos a ataques à segurança devido à natureza não estruturada dos dados e ao ambiente de computação distribuído

INTRODUÇÃO

- A distribuição dos nós permite a computação paralela que aumenta a superfície de ataque e resulta na implementação de procedimentos mais complexos de segurança.

- Além de ambiente distribuído, dados de uma variedade de nós movem-se de um nó para outro, o que leva ao compartilhamento de dados e aumenta o risco de roubo.

Bancos de dados NoSQL

Problemas de suporte a segurança

1. Suporte de criptografia insuficiente para os arquivos de dados
2. Autenticação fraca entre o cliente e os servidores
3. Controle de acesso granular
4. Autorização muito simples sem o suporte para RBAC (Role-based Access Control)
5. Vulnerabilidade à injeção de SQL
6. Validação / filtragem de entrada de ponto final
7. Armazenamento e comunicação de dados inseguros
8. Mineração e análise de dados preservando a privacidade

PUC Minas

Bancos de dados NoSQL

Problemas de suporte a segurança

- Aponta-se o perigo de confiar na segurança do perímetro, ou seja, do firewall, tendo em vista que Java Script ou JSON podem ser usados para ataca-los obtendo acesso não autorizado aos dados do banco de dados.
- Outra questão é que os sistemas não fornecem controles de acesso granulares necessários para separar funções e responsabilidades do usuário e esta vulnerabilidade a ataques é alta se a curva de aprendizado do invasor terminar e ele for capaz de identificar fraquezas ocultas do software.

PUC Minas

Bancos de dados NoSQL

Mitigando os problemas de segurança

- A metodologia de **relacionamento de atributos** é um método popular para impor segurança em bancos de dados NoSQL.
- Proteger as informações valiosas é o objetivo principal desta metodologia e o atributo com maior relevância considerado o elemento-chave da extração [chave do hash] de informação e recebe mais importância do que os demais atributos.

PUC Minas

Bancos de dados NoSQL

Mitigando os problemas de segurança

- Outro método de controle de acesso a dados adequado para bancos de dados NoSQL é a **criptografia baseada em atributos**.
- O método consiste em permitir aos proprietários de dados criptografar dados sob a política de acesso de forma que apenas os usuários que têm permissão para acessar os dados possam descriptografá-los.
- Lembram-se da topologia Edge /FOG ? Pois bem, uma das soluções de segurança que estão sendo adotadas é o deslocamento deste processamento para as pontas.

PUC Minas

Bancos de dados NoSQL

Mitigando os problemas de segurança

- Outro método de controle de acesso a dados adequado para bancos de dados NoSQL é a **criptografia baseada em atributos**.
- O método consiste em permitir aos proprietários de dados criptografar dados sob a política de acesso de forma que apenas os usuários que têm permissão para acessar os dados possam descriptografá-los.
- Lembram-se da topologia Edge /FOG ? Pois bem, uma das soluções de segurança que estão sendo adotadas é o deslocamento deste processamento para as pontas.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Cluster

- Um banco de dados distribuído controlado centralmente sincroniza periodicamente todos os dados e garante que as atualizações e exclusões realizadas nos dados sejam automaticamente refletidas nos dados armazenados em outro lugar.
- Nesta transição de dados é ideal que o aplicativo implemente o controle de acesso no nível de documento (ou coluna) para evitar acessos indevidos de usuários não autorizados viabilizando isto para o processo de replicação.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Cluster

- São vários nós distribuídos nos quais os bancos de dados NoSQL são executados aumentando a superfície de ataque e tornando o sistema complexo para proteger.
- A possibilidade de acesso não autorizado ao banco de dados aumenta devido a vários pontos de entrada.
- Esses pontos de entrada podem ser de um local remoto ou de um local *on-premise* do cliente através de algum dos seus clientes.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Cluster

- O ambiente distribuído é geralmente mais sujeito a riscos de segurança devido à falta de um sistema central de gerenciamento de segurança.
- Os bancos de dados Cassandra e Dynamo são vulneráveis a riscos de segurança em ambiente distribuído.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Autenticação

- Geralmente o mecanismo de autenticação em um banco de dados NoSQL é aplicado no nível do nó local, mas falha em todos os servidores de commodities (distribuídos em nuvem).
- Devido a isso, os bancos de dados NoSQL são expostos a ataques de força bruta, ataques de injeção e ataques de retransmissão, que levam ao vazamento de informações.
- As razões para esses ataques são o mecanismo de autenticação fraco destas soluções.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Autenticação

- Geralmente o mecanismo de autenticação em um banco de dados NoSQL é aplicado no nível do nó local.
- Devido a isso, os bancos de dados NoSQL são expostos a ataques de força bruta, ataques de injeção e ataques de retransmissão, que levam ao vazamento de informações.
- As razões para esses ataques são o mecanismo de autenticação fraco destas soluções mesmo utilizando-se Kerberos para autenticar os clientes e os nós de dados.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Integridade

- Proteger a integridade é um requisito de segurança para garantir a proteção dos dados contra modificações não autorizadas devido à inserção, exclusão ou atualização de dados no banco de dados.
- Como os bancos de dados NoSQL não têm um esquema, as permissões em uma tabela, coluna ou linha não podem ser segregadas.
- Portanto, manter a integridade transacional também é muito difícil em bancos de dados NoSQL.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Integridade

- Isso pode levar a várias cópias dos mesmos dados, o que torna difícil manter os dados consistentes, especialmente porque as alterações em várias tabelas não podem ser agrupadas em uma transação onde uma unidade lógica de inserção, atualização ou exclusão de operações é executada como um todo.
- Devido à complexidade de impor restrições de integridade aos bancos de dados NoSQL, não é recomendado que estes bancos de dados sejam usados para transações financeiras.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Autenticação de usuários

- Autenticação desempenha um papel muito importante em qualquer banco de dado e os bancos relacionais permitem autorização no nível da tabela.
- Os bancos de dados NoSQL não têm esquema e armazenam dados heterogêneos juntos.
- Portanto, é difícil implementar a autorização em uma tabela como um todo.
- O controle de acesso refinado não é implementado à característica *schemaless* dos bancos de dados NoSQL que permitem em sua maioria autorização em nível de família de colunas.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Dados em repouso e em movimento

- **Dados em repouso** significam dados que foram eliminados da memória e gravados no disco.
- Possuem duas categorias:
  - ✓ Comunicação cliente-nó
  - ✓ Comunicação entre nós
- A maioria dos bancos de dados NoSQL não emprega nenhuma técnica para proteger os dados em repouso.
- Apenas alguns fornecem mecanismos de criptografia para proteger os dados.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Dados em repouso e em movimento

- **Dados em movimento** significam dados que estão em comunicação ou sendo trocados durante uma comunicação.
- Os bancos de dados NoSQL populares oferecem os seguintes serviços de criptografia para proteção de dados.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Dados em repouso e em movimento

- Para **dados em repouso** o Cassandra usa a técnica TDE (Transparent Data Encryption).
- Já o MongoDB não fornece nenhum método para criptografar o arquivo de dados. Os arquivos de dados podem ser criptografados na camada do aplicativo antes de gravar os dados no banco de dados, o que requer forte segurança do sistema.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Dados em repouso e em movimento

- Para **dados em movimento** o Cassandra não criptografada a comunicação **cliente-nó** e ela é feita gerando certificados de servidor válidos na camada SSL.
- Já o MongoDB não oferece suporte à comunicação no modo cliente SSL sendo que, para criptografar os dados usando a comunicação de nó com o cliente SSL, o MongoDB precisa ser recompilado configurando a comunicação SSL.
- Na **comunicação entre nós** o Cassandra não oferece suporte para comunicação entre nós criptografados e o MongoDB não oferece suporte para comunicação entre nós.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Privacidade dos dados de usuário

- NoSQL armazena grande quantidade de informações confidenciais e manter a privacidade dessas informações é a principal preocupação de qualquer administrador de banco de dados.
- Os clientes acessam bancos de dados NoSQL por meio de vários nós e gerenciadores de recursos.
- Mesmo que haja um único local, os dados maliciosos se propagam para todo o sistema, pois não há gerenciamento de segurança central.

PUC Minas

Bancos de dados NoSQL

Riscos de segurança para bancos NoSQL

Privacidade dos dados de usuário

- A natureza distribuída do banco de dados também leva ao comprometimento da segurança.
- Os principais problemas de privacidade estão relacionados a:
  - Acesso não autorizado,
  - Bloqueio de fornecedor,
  - Exclusão de dados,
  - Backup,
  - Vulnerabilidades,
  - Falha de isolamento,
  - Monitoramento inadequado
  - Auditoria.

FINALIZANDO

- Percebemos que todas as soluções tem suas vantagens e desvantagens.
- Bancos de dados NoSQL são apropriados para diversos nichos porém a questão da segurança nos traz algumas restrições.
- Além disto, nós precisamos aprofundar nas questões de implementação de técnicas de programação nos aplicativos para que todas as questões de vazamento sejam tratadas.

PUC Minas

FINALIZANDO

- Espero que tenham aproveitado este curso e conto com sua colaboração para avaliação de fatores que podem melhorá-lo!

OBRIGADO!

E ATÉ A PRÓXIMA!

PUC Minas

REFERÊNCIAS BIBLIOGRÁFICAS

Ebrahim S., Mohammad A.N. Survey on security issues in big data and NoSQL. ACSIJ. 2015;4(4):68–73 No. 16.

Padhy R.P., Patra M.R. RDBMS to NoSQL: reviewing some next-generation non-relational databases. Int. J. Adv. Eng. Sci. Technol. 2011;11(2):45–52**.**

Hashem I.A.T., Yaqoob I., et al. The rise of big data on cloud computing: review and open research issues. Inf. Syst. 2015;47:98–115.

Ahmed J., Gulmeher R. NoSQL databases: new trend of databases, emerging reasons, classification and security issues. Int. J. Eng. Sci. Res. Technol. 2014;4(6):176–184.