

JEFERSON CARVALHO AUGUSTO

Segurança em banco de dados nosql:

FALHAS E BRECHAS OBSERVADAS

São Gonçalo

2020

JEFERSON CARVALHO AUGUSTO

Segurança em banco de dados nosql:

FALHAS E BRECHAS OBSERVADAS

Trabalho de conclusão de curso apresentado à (Anhanguera), como requisito parcial para a obtenção de título de graduado em bacharel para Ciência da Computação.

Orientador: (Ver o nome do Tutor)

São Gonçalo

2020

JEFERSON CARVALHO AUGUSTO

Segurança em banco de dados nosql:

FALHAS E BRECHAS OBSERVADAS

Trabalho de conclusão de curso apresentado à (Anhanguera), como requisito parcial para a obtenção de título de graduado em bacharel para Ciência da Computação.

**BANCA EXAMINADORA**

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

São Gomçalo, dia XX de XXXX de 2020

Primeiramente, graças a mim pude realizar esse trabalho, também tenho muito a agradecer aos meus familiares, especialmente a minha amada esposa que sempre esteve ao meu lado me apoiando em tudo, essa conquista não seria possível sem a sua dedicação e seus esforços de estar sempre comigo. O meu mais sincero muito obrigado.

AUGUSTO, Jeferson Carvalho. **Segurança em banco de dados**: falhas e brechas observadas. 2020. Número total de folhas 17. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Anhanguera, São Gonçalo, 2020.

RESUMO

A ser desenvolvido nas próximas entregas

AUGUSTO, Jeferson Carvalho. **Segurança em banco de dados**: falhas e brechas observadas. 2020. Número total de folhas 17. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Anhanguera, São Gonçalo, 2020.

ABSTRACT

Deve ser feita a tradução do resumo para a língua estrangeira.

***Key-words*:** Word 1; Word 2; Word 3; Word 4; Word 5.

LISTA DE TABELAS

**Tabela 1** – Estatística de utilização dos bancos de dados (adaptado) 11

**LISTA DE ABREVIATURAS E SIGLAS**

SQL Structured Query Language (Linguagem de consulta estruturada)

DOS Denial Of Service (Negação de serviço)

NoSQL Not Only Structured Query Language (Não apenas linguagem de consulta estruturada)

TCP Transmission Control Protocol (Protocolo de Controle de Transmissão)

HTTP HyperText Transfer Protocol (Protocolo de Transferência de Hipertexto)

**SUMÁRIO**

[1. INTRODUÇÃO 10](#_Toc531940670)

[2. ANÁLISE DE USO DOS BANCOS DE DADOS nOsql 11](#_Toc531940671)

[3. FALHAS E BRECHAS 12](#_Toc531940672)

* + 1. BANCO DE DADOS MONGODB.......................................................13
    2. BANCO DE DADOS CASSANDRA....................................................14

# 

# INTRODUÇÃO

Pode-se considerar banco de dados como sendo qualquer recipiente, seja físico (anotações e pais organizados em um arquivo) ou lógico (um programa de computador) que possa comportar dados. Com o avanço da computação os programas desenvolvidos para o gerenciamento de banco de dados tornaram-se ferramentas indispensáveis para lidarmos com dados digitais, bancos de dados hoje em dia são necessidade essenciais.

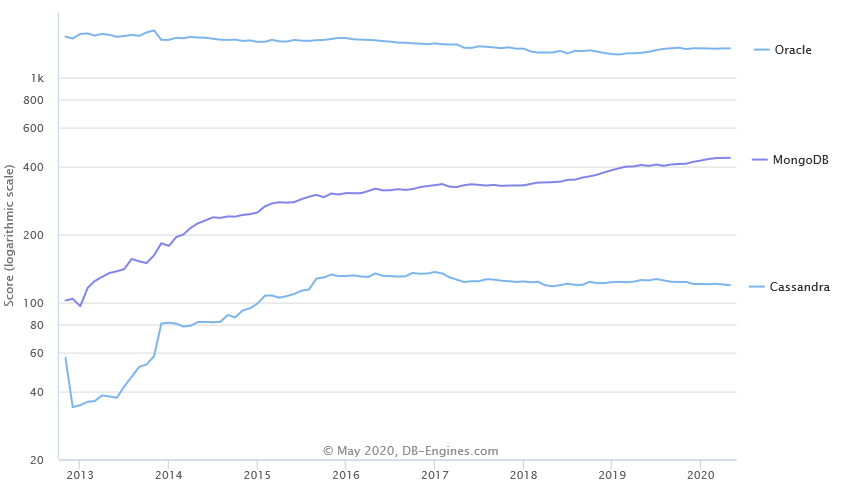
Atualmente toda população é dependente de sistemas de banco de dados, seja ao fazer uma lista de compras para o supermercado ou ouvindo músicas através da internet. Em quase todas as áreas (seja ela voltada a negócios, saúde, engenharia, entre outras) onde utilizamos computadores , faz-se necessário o uso de banco de dados. Banco de dados na sua forma mais genérica são estruturas lógicas relacionadas ou não que permite armazenar, consultar e distribuir dados, seu armazenamento é feito de forma estruturada a fim de facilitar o acesso autorizado.

Todas as organizações lidam com objetos de valor como: formulas de produtos únicos no mercado, fotos e vídeos pessoais, senhas de acesso, documentos de usuários ou cliente, entre outros tipos de dados. Todos esses dados são armazenados em algum tipo de banco de dados, seja ele um arquivo em formato de papel ou um software eletrônico com auxilio de um computador. Por lidar com dados críticos, é preciso garantir que ninguém sem autorização tenha acesso às informações contidas nele.

Foi abordado com maior ênfase os bancos de dados Not Only Structured Query Language (NoSQL), devido ao seu grande crescimento nos últimos anos, especialmente a partir do ano 2000, quando foi necessário um novo paradigma para lidar com a grande quantidade de dados que estava sendo gerada. Essa nova tecnologia surgiu como uma necessidade e não houve tempo suficiente de amadurecer para que pudessem mapear todas as falhas antes de ir para produção, sendo assim, temos problemas como falta de criptografia e fraca autenticação do cliente e do usuário.

# análise dE uso dos bancos de dados NOSQL

Com a rápida evolução da informática e a interligação dos computadores com o auxilio da internet foi necessário surgir um meio para gerir os dados (Preecha & Tawatchai, 2014). Tendo em vista esse pensamento as ferramentas para armazenamento de dados das principais empresas do ramo de NoSQL sofrem atualizações periodicamente para garantir um serviço de qualidade aumentando assim o número de usuários que aderem a esse tipo de serviço.



Fonte <https://db-engines.com/en/ranking_trend(acessado> em 01/05/2020)

Tabela 1-Estatistica de utilização dos bancos de dados (adaptado)

Através da figura acima se pode comparar a utilização dos bancos de dados NoSQL em função dos anos e analisando a figura podemos comprovar o que foi analisado por Cardoso, o paradigma NoSQL vem ganhando ênfase como a nova opção que está em crescimento focando no problema e não na padronização (Cardoso, 2014,p. 1).No gráfico temos banco de dados relacional Oracle que segundo Anderson já possui 43 anos de mercado (Anderson, 2007) que foi adicionado a fim de comparar a distancia entre o serviço que de fato será analisado nessa pesquisa (Banco de dados não relacionais). Foi analisado um período de 2013 até 2020, onde podemos notar o crescente avanço da utilização dos bancos de dados NoSQL. Especialmente o serviço MongoDB teve um grande crescimento nos últimos anos. Até o momento da elaboração dessa atividade (maio 2020) o serviço Oracle possui 1.345.441 pontos, o serviço MongoDB possui 438.994 pontos e o serviço Cassandra possui 119.156. Essa estatística score significa a quantidade de pontos que o determinado banco de dados alcançou com um uma série de avaliações, são elas: A quantidade de vezes que foi citado o nome desse determinado banco de dados em algum site, interesse pelo programa, frequência que houve discussões técnicas para o sistema, quantidade de empregos oferecidos fazendo menção ao sistema, número de vezes em que nas redes profissionais é citado o nome do sistema e a relevância que possui em comentários das redes sociais.

O banco de dados NoSQL que possui o maior Score até o momento é o MongoDb surgiu em 2009 é um banco de dados orientado a documento, sua posição atual é justificada por possui código aberto, alta performance durante execução, não possui transações nem Joins(união entre duas tabelas), possui um resultado simples para a aplicação que estiver consumindo seus recursos, possui índices de consultas dinâmicas e é muito bem documentado para auxiliar os desenvolvedores.

Em 2008 surgiu o Cassandra que hoje é o segundo Banco de dados NoSQL mais usado até o momento. Inicialmente desenvolvido pela empresa Facebook e hoje em dia mantido pela empresa Apache. Suas principais características são o modelo de dados facilmente alterado (é flexível a mudanças), possui uma grande vantagem em relação à escalabilidade, tanto horizontal quanto vertical e possui claro esquema de tabelas definido mesmo operando em ambiente NoSQL.

1. **FALHAS E BRECHAS**

Um dos maiores problemas relacionado à segurança é a privacidade (Rajan, Fujitsu Sreeranga;, 2012), ou seja, um usuário ou invasor possuindo acesso a determinado recurso que não deveriam.

Como é possível notar, todo sistema NoSQL permite ser escalável de forma vertical onde é agregado ao servidor mais componentes (memória, processador, disco rígido, etc.) ou horizontal onde o sistema do servidor é replicado em outros equipamentos e funcionarão de forma paralela ou distribuída. No entanto, garantir a segurança em um sistema que possui uma arquitetura de distribuição é um desafio maior se comparado à segurança de apenas um equipamento (Ebrahim & Nematbakhsh, 2015).

* 1. BANCO DE DADOS MONGODB

Segundo Lior et al o principais sistemas de banco de dados NoSQL dessa pesquisa MongoDB possuem três grandes problemas, a falta de suporte a criptografia, o sistema de autenticação do cliente com servidor é simples o que gera uma segurança fraca e também possui vulnerabilidade que facilita dois tipos de ataques conhecidos, a injeção de SQL (consistem na inserção de comandos SQL por parte de um invasor para manipular o banco de dados) e o ataque denial of servisse (DOS) (onde um invasor sobrecarrega o servidor para que não seja possível fornecer o serviço para os usuários) (Lior, Nurit, Yaron, Ehud, & Jenny, 2011),

Ainda sobre o autenticação no MongoDB, anos mais tarde Precha et al analisou os três modos de funcionamento possíveis e a forma como os dados são salvos em disco concluiu que o MongoDB não possui suporte a autenticação em modo compartilhamento, para o caso de operar como autônomo ou conjunto de réplicas possui uma autenticação utilizando um arquivo pré-compartilhado criptografado com o algoritmo MD5, no entanto os invasores com esse arquivo em mãos podem quebrar o código e obter a chave para autenticação ao banco de dados e quanto a disposição dos dados foi observado que eles são salvos em arquivo sem criptografia (Preecha & Tawatchai, 2014), ou seja, simplesmente um texto, esse tipo de funcionamento acaba gerando condições para que um invasor possuindo acesso ao sistema de arquivos obtenha informações contidas no banco. Ainda em 2014, nessa mesma pesquisa foi observado que nos dois modos de transmissão de mensagens (wire-level através da porta TCP 27017 e HTTP através da porta TCP 28017) entre cliente e servidor não existe criptografia nos dados, permitindo que um invasor possa interpretar as mensagens após intercepta-las.

Em 2017 Hossain e Haddad fizeram uma nova análise profunda sobre a segurança dos bancos de dados MongoDB e constatou-se que ainda existiam falhas relacionadas a criptografia (visto que os dados nunca são criptografados por padrão), autenticação(ainda sem suporte para autenticar com modo compartilhado e também não solicita autenticação para acesso a interface de monitoramento do sistema e clientes conectados), transferência dos dados entre os nós da rede de servidores(por não possuir configurações pré definidas de SSL são necessárias etapas adicionais para poder garantir uma comunicação segura do tráfego de dados) (Hossain & Haddad, 2017).

1. * 1. BANCO DE DADOS CASSANDRA

Lior et al também fez uma análise em cima do banco de dados Cassandra e constatou problemas em comum com o MongoDB. Não existe de suporte pré-definido para a criptografia dos dados armazenados, sistema básico de autenticação entre os nós da rede e também vulnerabilidades para ataques de DOS (Lior, Nurit, Yaron, Ehud, & Jenny, 2011).

Anos mais tarde Preecha e Tawatchai reanalisaram os aspectos visto por Lior et al e concluíram que não houve grandes mudanças nas falhas de segurança. Ainda não tinha nenhuma criptografia nos dados armazenados gerando ameaça à confidencialidade, tanto com o nó do cliente quanto o nó interno do servidor (Preecha & Tawatchai, 2014).

Em 2017 foi feita nova análise no banco de dados e identificado os mesmos problemas com relação à criptografia dos dados, autenticação (desativada por padrão), autorização (todos os usuários tem permissão de administrador por padrão) e auditoria (somente está disponível na versão Cassandra Interprise) (Hossain & Haddad, 2017).