CENTRO UNIVERSITÁRIO DO PARÁ – CESUPA
ESCOLA DE NEGÓCIOS, TECNOLOGIA E INOVAÇÃO – ARGO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

GABRIEL DE OLIVEIRA SANTOS
ISAAC PONTE ANGELIM
RICARDO LARRAT MOTA DE ALENCAR
SAMOEL VIEIRA LOPES JUNIOR

UMA ANÁLISE COMPARATIVA EM RELAÇÃO À CRIPTOGRAFIA NOS BANCOS DE DADOS ORACLE E MYSQL

BELÉM-PA
2023

GABRIEL DE OLIVEIRA SANTOS
ISAAC PONTE ANGELIM
RICARDO LARRAT MOTA DE ALENCAR
SAMOEL VIEIRA LOPES JUNIOR

UMA ANÁLISE COMPARATIVA EM RELAÇÃO À CRIPTOGRAFIA NOS BANCOS DE DADOS ORACLE E MYSQL

Trabalho de Conclusão de Curso apresentado à Escola de Negócios, Tecnologia e Inovação do Centro Universitário do Estado do Pará como requisito obrigatório para a obtenção do título de Bacharel em Ciência da Computação na modalidade ARTIGO.

Orientador: Prof. Eudes Danilo da Silva Mendonça

BELÉM-PA
2023

GABRIEL DE OLIVEIRA SANTOS
ISAAC PONTE ANGELIM
RICARDO LARRAT MOTA DE ALENCAR
SAMOEL VIEIRA LOPES JUNIOR

UMA ANÁLISE COMPARATIVA EM RELAÇÃO À CRIPTOGRAFIA NOS BANCOS DE DADOS ORACLE E MYSQL

Trabalho de Conclusão de Curso apresentado à Escola de Negócios, Tecnologia e Inovação do Centro Universitário do Estado do Pará como requisito obrigatório para a obtenção do título de Bacharel em Ciência da Computação na modalidade ARTIGO.

Data da aprovação: 07 / 12 / 2023

Nota final aluno(a) I: 8.5

Nota final aluno(a) II: 8.5

Nota final aluno(a) III: 8.5

Nota final aluno(a) IV: 8.5

Banca examinadora

Documento assinado digitalmente
gov.br
EUDES DANILO DA SILVA MENDONCA
Data: 18/12/2023 08:46:21-0300
Verifique em https://validar.iti.gov.br

_____
Prof(a) Esp. Eudes Danilo da Silva Mendonça
Orientador(a) e Presidente da banca

Documento assinado digitalmente
gov.br
ISAAC SOUZA ELGRABLY
Data: 15/12/2023 21:11:14-0300
Verifique em https://validar.iti.gov.br

_____
Prof(a) Dr. Isaac Souza Elgrably
Examinador(a) interno(a)

Documento assinado digitalmente
gov.br
VITOR HUGO FREITAS GOMES
Data: 18/12/2023 08:23:02-0300
Verifique em https://validar.iti.gov.br

_____
Prof(a) Dr. Vitor Hugo Freitas Gomes
Examinador(a) interno(a)

Dados Internacionais de Catalogação-na-publicação (CIP)
Biblioteca do CESUPA, Belém – PA

Santos, Gabriel de Oliveira.

Uma análise comparativa em relação à criptografia nos bancos de dados Oracle e MySQL / Gabriel de Oliveira Santos, Isaac Ponte Angelim, Ricardo Larrat Mota de Alencar, Samoel Vieira Lopes Junior; orientador Eudes Danilo da Silva Mendonça. — 2023.

Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Centro Universitário do Estado do Pará, Belém, 2023.

1. Criptografia de dados (Computação). 2. Banco de dados – Segurança. 3. Oracle (Programa de computador). 4. MySQL (Programa de computador). I. Angelim, Isaac Ponte. II. Alencar, Ricardo Larrat Mota de. III. Lopes Junior, Samoel Vieira. IV. Mendonça, Eudes Danilo da Silva, orient. V. Título.

CDD 23ª ed. 005.8

RESUMO

Em um mundo cada vez mais digital e interconectado, a segurança dos dados torna-se imperativa. No contexto empresarial, vazamentos e exposições de informações sensíveis representam ameaças significativas aos bancos de dados das empresas. A criptografia nos bancos de dados surge como uma proteção essencial, garantindo confidencialidade e integridade, elementos cruciais para prevenir potenciais danos e assegurar a confiança no armazenamento e gestão de dados. Este estudo realiza uma revisão bibliográfica sobre a criptografia, destacando sua importância histórica e objetivos, como confidencialidade e integridade da informação. Explora a evolução da criptografia, introduzindo os Sistemas de Gerenciamento de Banco de Dados Oracle e MySQL, ressaltando os recursos de segurança de ambos. Durante a jornada de pesquisa, foram encontradas diferentes técnicas de criptografias e ferramentas de segurança. Reforça-se a importância da criptografia na proteção de dados sensíveis. O estudo contribui para a compreensão das práticas de segurança em Oracle e MySQL, sendo valioso para profissionais de segurança da informação.

Palavras-chave: Criptografia; Banco de Dados; Oracle; MySQL; Segurança da Informação.

ABSTRACT

In an increasingly digital and interconnected world, data security becomes imperative. In the business context, leaks and exposures of sensitive information pose significant threats to company databases. Encryption in databases emerges as an essential protection, ensuring confidentiality and integrity, crucial elements to prevent potential harm and ensure trust in data storage and management. This study conducts a literature review on encryption, highlighting its historical significance and objectives, such as information confidentiality and integrity. It explores the evolution of encryption, introducing Oracle and MySQL Database Management Systems, emphasizing the security features of both. During the research journey, different encryption techniques and security tools were found. The importance of encryption in protecting sensitive data is emphasized. The study contributes to understanding security practices in Oracle and MySQL, proving valuable for information security professionals.

Keywords: Cryptography; Database; Oracle; MySQL; Information Security.

LISTA DE SIGLAS

AES	*Advanced Encryption Standard*
MD5	*Message Digest Algorithm 5*
MySQL	*My Structured Query Language*
RDBMS	*Relational Database Management System*
SGBD	Sistemas Gerenciadores de Banco de Dados
SSE-C	*Server-Side Encryption with Customer-Provided Keys*
SHA	*Secure Hash Algorithm*

SUMÁRIO

1 CONTEXTUALIZAÇÃO

1.1 Revisão Bibliográfica

1.1.1 Criptografia

Com o avanço da tecnologia e o desenvolvimento dos meios de comunicação ao longo do tempo, a tarefa de proteger informações escritas tornou-se progressivamente mais complexa. Sempre que há a necessidade de manter uma informação em segurança, paralelamente há interesse de terceiros em descobri-la. Esse jogo de busca e ocultação tem sido uma constante na história ao longo dos anos (Fiarresga, 2010).

A criptografia é uma técnica usada para proteger as informações em um conjunto de dados, de modo que um estranho/terceira parte não possa ler esses dados, a fim de proteger suas informações (Alves; Mateus-Coelho; Cruz-Cunha, 2021).

Ao longo dos milênios, a criptografia, uma técnica antiga que remonta à escrita dos egípcios conhecida como hieróglifo, tem desempenhado um papel fundamental na proteção de informações. Esse método, utilizado e aprimorado durante há aproximadamente quatro mil anos, evidencia-se como uma ferramenta essencial para salvaguardar dados sensíveis. Uma aplicação notável desse recurso remonta à Roma antiga, onde os planos de guerra eram submetidos à criptografia antes de serem enviados aos campos de batalha. Isso garantia que, se as mensagens fossem interceptadas por inimigos, elas permaneceriam ilegíveis e, portanto, não poderiam ser utilizadas de forma adversa (Ordonez; Pereira; Chiaramonte, 2005).

Até a década de 1970, todas as cifras eram de natureza simétrica, implicando o uso de uma única chave tanto para criptografar quanto para descriptografar uma mensagem, frequentemente com aplicações políticas e militares. Somente há algumas décadas, que a cifra de chave assimétrica começou a ser adotada, introduzindo um sistema com duas chaves distintas: uma chave pública, empregada para criptografar a mensagem, e uma chave privada, utilizada para descriptografá-la.

Com a proliferação do uso de computadores pela população em geral, a criptografia assume um papel fundamental em nossa vida cotidiana. Exemplos disso incluem o código de acesso de um caixa eletrônico e a assinatura digital em um cartão de identificação cidadã, apenas para citar alguns dos muitos casos possíveis.

A criptografia desempenha um papel crucial na segurança da informação, visando alcançar diversos objetivos. Conforme destacado por Fiarresga (2010), os principais objetivos da criptografia incluem:

a) Confidencialidade: Garantir que o conteúdo da informação permaneça secreto, acessível apenas às partes autorizadas.
b) Integridade da informação: Assegurar que a informação não seja alterada, de forma intencional ou acidental, por partes não autorizadas.
c) Autenticação da informação: Facilitar a identificação de pessoas ou processos envolvidos na comunicação.
d) Não repúdio: Prevenir que qualquer das partes envolvidas na comunicação negue sua participação ou o recebimento de informações.

Esses objetivos fornecem uma estrutura essencial para compreender o papel da criptografia na segurança da informação e sua aplicação em diversas áreas, incluindo transações financeiras, comunicações governamentais, entre outras.

No mercado atual, encontramos uma variedade de Sistemas Gerenciadores de Banco de Dados (SGBD), alguns dos quais exigem pagamento de licença, enquanto outros são de código aberto e podem ser adquiridos gratuitamente (Martins; Lima, 2016). Esses SGBDs oferecem uma ampla gama de recursos de segurança, e é observável que os SGBDs com recursos mais abrangentes geralmente estão associados a custos comerciais mais elevados.

1.1.2 Banco de Dados Oracle

O banco de dados Oracle disponibiliza uma variedade de conjuntos de ferramentas para aprimorar a segurança dos dados armazenados. Isso inclui soluções como o *Oracle Advanced Security*, *Oracle Key Vault* e *Oracle Data Masking and Subsetting*, entre outros. Além das diversas funcionalidades de

segurança, também abrange aspectos como alta disponibilidade, criptografia de dados, replicação e outros (Martins; Lima, 2016).

Esses conjuntos de ferramentas são projetados para oferecer suporte a recursos como a criptografia de dados transparente, gerenciamento de chaves de criptografia, autenticação multifator, controle de usuários com privilégios, classificação e descoberta de dados, monitoramento de atividades de banco de dados, auditoria e geração de relatórios consolidados, bem como o mascaramento de dados (Almeida *et al.*, 2019).

1.1.3 Banco de Dados MySQL

O MySQL é um SGBD relacional crucial na gestão de dados, organizando e manipulando informações para armazenamento, ordenação, consulta e recuperação eficientes. Desenvolvido para lidar com acesso concorrente, permite que vários usuários trabalhem simultaneamente. Com um sistema de acesso robusto, garante que apenas usuários autorizados possam modificar e acessar dados, contribuindo para a integridade e segurança do sistema (Leite; Bonomo, 2016).

Também amplamente conhecido como um banco de dados *open source* proeminente no mercado, o MySQL ganhou popularidade devido a uma série de características que o tornam uma escolha atraente para diversas aplicações. Sua reputação é fundamentada em sua velocidade, simplicidade e facilidade de configuração. Evoluindo ao longo do tempo, incorporou recursos avançados (Azevedo; Castro; Serrão, 2011). Ademais, é altamente portátil, podendo ser executado em várias plataformas, como sistemas operacionais Unix, OS X e Windows.

O MySQL também oferece recursos avançados de segurança, incluindo um sistema de senhas e privilégios flexível e seguro, além de suportar uma variedade de protocolos de conexão, permitindo que os clientes se conectem ao banco de dados de diferentes maneiras (Leite; Bonomo, 2016).

1.2 Problema da Pesquisa

A criptografia é uma técnica fundamental para proteger dados dos usuários em diversas situações, desde transações bancárias até informações confidenciais de empresas e governos. Em um mundo cada vez mais conectado e com um crescente volume de informações sendo compartilhadas, é essencial analisar como a criptografia pode ser aplicada para prevenir e mitigar riscos de vazamentos e exposições de dados.

No cenário da gestão de banco de dados, a criptografia desempenha um papel igualmente importante. Bancos de dados abrigam informações de natureza pessoal, governamental e empresarial, tornando-se alvos suscetíveis a ataques que comprometem a integridade, segurança, confiabilidade e privacidade dos dados. É incontestável a necessidade de investigar a eficácia da criptografia nesse contexto, a fim de proteger adequadamente os dados armazenados.

Dentre os principais bancos de dados atualmente utilizados, estão os bancos de dados Oracle e MySQL, que detêm as primeiras posições no ranking de SGBDs mais populares (DB-Engines, 2023). A forma como estes bancos aplicam a criptografia pode afetar a forma por meio da qual eles garantem a segurança dos dados manipulados.

1.3 Justificativa

À medida que a internet e o armazenamento de dados online continuam a crescer, o uso eficaz da criptografia torna-se crucial para evitar problemas como vazamento e exposição de informações confidenciais. Em grandes empresas, esse tipo de problema pode resultar em prejuízos consideráveis, como a perda de informações privadas importantes, a diminuição da confiabilidade e a perda de clientes e investimentos.

Nesse contexto, este trabalho tem como objetivo analisar dois bancos de dados, Oracle e MySQL, mostrando como a criptografia pode ser eficaz na proteção de dados sensíveis. A pesquisa examinará diferentes técnicas e soluções disponíveis, evidenciando a necessidade de sua aplicação correta em diferentes setores, como empresas e governos, visando minimizar os riscos de violações de privacidade e segurança.

1.4 Objetivos

1.4.1 Objetivo geral

Investigar como a criptografia pode contribuir para evitar vazamentos e exposição de dados sensíveis, causando problemas extremamente graves, analisando a sua aplicação nos bancos de dados Oracle e MySQL.

1.4.2 Objetivos específicos

a) Levantar as técnicas de criptografia disponíveis, para entender como elas podem ser aplicadas na proteção de dados sensíveis na Oracle e MySQL.
b) Analisar as diferentes técnicas de criptografia disponíveis nos bancos de dados Oracle e MySQL e suas características.
c) Comparar as técnicas de criptografia apresentadas pela Oracle e MySQL.

1.5 Estrutura do Trabalho

A estrutura deste trabalho consiste em um primeiro capítulo, que introduz a temática da criptografia nos bancos de dados Oracle e MySQL, fornecendo um referencial teórico, apresentando o problema de pesquisa e a justificativa que orientaram este estudo, além de detalhar seus objetivos. Em seguida, no segundo capítulo, será apresentada uma revisão bibliográfica que abordará o cenário atual da criptografia em bancos de dados Oracle e MySQL, explorando suas principais aplicações e recursos relacionados à segurança de dados. Em suma, os capítulos desta pesquisa incluem a metodologia, os resultados, a discussão e, finalmente, a conclusão.

2 UMA ANÁLISE COMPARATIVA EM RELAÇÃO À CRIPTOGRAFIA NOS BANCOS DE DADOS DA ORACLE E MYSQL

2.1 Introdução

Um SGBD é um sistema computadorizado de manutenção de registros, podendo ser considerado como um ‘’armário eletrônico’’ cheio de arquivos; em outras palavras, é um repositório para uma coleção de dados computadorizados (Date, 2004). A segurança dos dados manipulados por esses sistemas é fundamental para prevenir e mitigar vazamentos e exposições de dados, bem como garantir a proteção contra ataques, garantindo integridade, segurança, confiabilidade e privacidade dos dados (Santos, 2018). Uma importante ferramenta para a segurança de base de dados é a criptografia.

A criptografia é uma técnica que garante a proteção de dados de modo que pessoas sem autorização não possam acessá-las (Alves; Mateus-Coelho; Cruz-Cunha, 2021). Ela funciona em um processo de pegar uma mensagem em texto puro e uma chave gerada aleatoriamente e fazer operações matemáticas com as duas até que tudo que sobra é uma versão cifrada da mensagem embaralhada. Descriptografar é pegar o texto cifrado e a chave correta e fazer mais operações matemáticas até que o texto puro é recuperado (em Massa, 2013). Suas aplicações evoluíram consideravelmente, e hoje é quase impossível imaginar nossa vida sem a segurança que ela proporciona (Medeiros *et al*., 2023). Logo, observa-se como a criptografia é crucial para gestão de bancos de dados, mantendo os dados em segurança, protegendo a base de dados de vazamentos e exposições.

A segurança da informação tornou-se uma preocupação primordial. Bancos de dados desempenham um papel vital na armazenagem e recuperação de informações críticas, abrangendo desde dados pessoais até registros empresariais e governamentais. No entanto, esse ambiente também é propenso a ameaças, ataques cibernéticos e vazamentos de dados (Alves, 2022). Dentre os principais bancos de dados na atualidade estão o Oracle e o MySQL, amplamente utilizados em diferentes setores. A Oracle destaca-se por sua forte ênfase em segurança, oferecendo uma ampla variedade de recursos em suas funcionalidades e sendo compatível com diversas plataformas. Além disso, sua performance de alta

disponibilidade é notável, garantindo suporte a falhas de processamento para evitar interrupções. O MySQL é um sistema de gerenciamento de banco de dados (SGBD) abrangente, veloz e bem estruturado, incorporando todas as características encontradas em principais bancos de dados pagos. Embora inicialmente concebido para aplicações de pequeno a médio porte, atualmente demonstra vantagens ao suportar eficientemente aplicações de grande escala. Suas características atendem às exigências de grandes bancos de dados, sendo reconhecido por entidades como um SGBD de código aberto capaz de competir de forma equiparável com sistemas similares, como o Oracle (Morandi; Paixão, 2021).

Uma análise aprofundada revela que algumas lacunas de conhecimento persistem, como a compreensão abrangente das vulnerabilidades específicas desses sistemas, a avaliação de suas implementações criptográficas e a identificação das melhores práticas para mitigar riscos. Além disso, a adaptação e implementação adequada de técnicas de criptografia em diferentes setores e contextos podem ser áreas de incerteza (Cremer *et al*, 2022).

Este trabalho busca analisar e comparar o uso da criptografia nos bancos de dados Oracle e MySQL. Além disso, a pesquisa objetiva avaliar a hipótese de que a adoção de métodos criptográficos mais adequados pode reduzir significativamente a incidência de vazamentos de dados sensíveis. Este estudo pretende contribuir para a discussão sobre a importância da proteção de dados sensíveis, aprimorando a utilização da criptografia como ferramenta de proteção e acompanhando a evolução e eficácia da criptografia nesse cenário.

2.2 Metodologia

Este artigo consiste em uma análise comparativa baseada em uma pesquisa exploratória, por meio de investigação em acervos online, repositórios acadêmicos e documentações, com foco em materiais relacionados às temáticas de criptografia e banco de dados.

A busca foi realizada em bases de dados eletrônicas, como Google Scholar, Scielo e ScienceDirect. Para a seleção dos estudos, foram empregados quatro critérios: (1) correspondência à temática do trabalho; (2) termos de busca, tais como: “Criptografia”, “Criptografia em banco de dados”, “A importância da criptografia”,

“Banco de dados Oracle”, “Banco de dados MySQL” e “Segurança no banco de dados”; (3) ano de publicação; e o (4) idioma do texto, onde foram revisados textos em inglês e português. Esses critérios são apresentados no Quadro 1.

Quadro 1 – Dados da Pesquisa

Critérios	**Valores**
Temática do Trabalho	Como está o cenário atual acerca da segurança dos dois principais bancos de dados?
Termos de busca	Criptografia, Banco de Dados Oracle, Banco de Dados MySQL, A importância da Criptografia, Criptografia em bancos de dados
Ano de publicação	De 2015 a setembro/2023
Idioma do texto	Português e Inglês

Fonte: Autoral (2023).

Em seguida, foi criado um banco com os materiais selecionados para ordenar a análise dos resultados. A revisão concentrou-se inicialmente em materiais que continham propostas relacionadas à “Criptografia” e “Criptografia nos Bancos de dados Oracle e MySQL”. A coleta de dados baseou-se nos resultados dos materiais e estudos selecionados, priorizando a temática do trabalho.

2.3 Resultados

Inicialmente, os termos de buscas utilizados foram “Criptografia no banco de dados Oracle” e “Criptografia no banco de dados MySQL”, tanto em português quanto em inglês. Dessa forma, foram obtidos cerca de 192.800 resultados na plataforma Google Scholar. No entanto, a maioria dos trabalhos resultantes na pesquisa, dentro da temática mencionada, tangenciou o tema ou tratava-se de uma aplicação específica. Tendo em vista que o objetivo não era abordar uma aplicação específica, recorreu-se à documentação oficial dos bancos de dados e utilizou-se

termos para filtrar os resultados. A partir destes filtros foram encontrados 2 trabalhos, conforme apresentado pelo Quadro 2.

Quadro 2 – Trabalhos encontrados

SGBD	**Trabalhos**
Oracle	Criptografando dados
MySQL	Introdução à criptografia no MySQL

Fonte: Autoral (2023).

2.3.1 Criptografia no Banco de dados Oracle (Oracle, 2023)

Oracle utiliza a *Advanced Encryption Standard* de 265 bits (AES-265) para criptografar e descriptografar todos os objetos em seu banco de dados. Cada objeto possui sua própria chave de criptografia, e essas chaves são armazenadas em *buckets*, com a chave mestra sendo gerenciada pela Oracle por padrão. Além disso, a Oracle permite que o cliente forneça suas próprias chaves de criptografia para criptografar e descriptografar os objetos de *uploads* e *downloads*.

As chaves dos clientes desempenham um papel fundamental na estratégia de criptografia de dados no *Oracle Cloud Infrastructure Object Storage*. Os clientes têm a flexibilidade de gerenciar suas próprias chaves de criptografia, permitindo-lhes uma camada adicional de controle e segurança sobre seus dados armazenados. Ao optar pela Criptografia do Servidor com Suas Próprias Chaves (SSE-C), os clientes podem fornecer suas próprias chaves AES-256 bits, utilizadas para criptografar e descriptografar objetos durante o *upload* e o *download*. Isso significa que os dados permanecem confidenciais e acessíveis apenas por aqueles que possuem a chave de criptografia correta.

É importante destacar que o serviço *Object Storage* não armazena as chaves de criptografia dos clientes, transferindo a responsabilidade de gerenciamento e rastreamento direto para eles. Essa abordagem garante que os clientes mantenham controle total sobre suas chaves, permitindo simultaneamente o uso dos benefícios da criptografia de dados em repouso, sem a preocupação de gerenciar todo o processo de criptografia. No entanto, é crucial que os clientes estejam cientes de que, caso percam suas chaves de criptografia, não poderão

recuperar os objetos criptografados. Isso ressalta a importância da gestão adequada das chaves para garantir a segurança contínua de seus dados.

2.3.2 Criptografia no Banco de dados MySQL (Devmedia, 2016)

O MySQL utiliza como criptografia o *Advanced Encryption Standard* (AES), *Message Digest Algorithm 5 (*MD5) e *Secure Hash Algorithm 1* (SHA-1).

O AES é utilizado para criptografar arquivos e discos, garantindo que os dados permaneçam seguros mesmo em caso de acesso não autorizado ao dispositivo físico. Além disso, é aplicado em transmissões de dados, especialmente na internet, onde o MySQL pode empregar o AES para proteger a confidencialidade das informações trocadas entre o cliente e servidor. Em ambientes móveis que utilizam o MySQL, o AES pode ser empregado para criptografar dados armazenados localmente.

A seu turno, o MD5 é utilizado para verificar a integridade de dados. Ao calcular o *hash* MD5 de um conjunto de informações, é possível comparar o *hash* resultante com um valor conhecido previamente para determinar se os dados foram alterados. Na transmissão de dados, essa verificação evita corrupção. O MySQL utiliza *hashes* MD5 na gestão de credenciais, garantindo armazenamento seguro de senhas, tornando-as ininteligíveis no banco de dados.

Por fim, o SHA-1 é utilizado para garantir a integridade de dados sensíveis, fornecendo um *hash* que pode ser verificado para detectar qualquer alteração não autorizada. Assim como o MD5, o SHA-1 também é empregado na comunicação para assegurar que os dados transmitidos não sejam adulterados durante o processo.

2.3.3 Análise comparativa ORACLE e MYSQL

Conforme o DB-*Engines Ranking*, observado na figura 1, hoje a Oracle e o MySQL destacam-se como os maiores e mais utilizados SGBDs. Diante de tal relevância, torna-se imperativo realizar uma análise comparativa, avaliando a eficácia da criptografia como medida de proteção de dados nesses SGBDs. Ressalta-se que a escolha da criptografia mais adequada depende das

necessidades específicas de cada aplicação, e a implementação correta dessas soluções é fundamental para garantir a segurança dos dados armazenados.

Figura 1 – Ranking de SGBDs atualizado em novembro de 2023

416 systems in ranking, November 2023

Rank			DBMS	Database Model	Score		
Nov 2023	Oct 2023	Nov 2022			Nov 2023	Oct 2023	Nov 2022
1.	1.	1.	Oracle	Relational, Multi-model	1277.03	+15.61	+35.34
2.	2.	2.	MySQL	Relational, Multi-model	1115.24	-18.07	-90.30
3.	3.	3.	Microsoft SQL Server	Relational, Multi-model	911.42	+14.54	-1.09
4.	4.	4.	PostgreSQL	Relational, Multi-model	636.86	-1.96	+13.70
5.	5.	5.	MongoDB	Document, Multi-model	428.55	-2.87	-49.35
6.	6.	6.	Redis	Key-value, Multi-model	160.02	-2.95	-22.03
7.	7.	7.	Elasticsearch	Search engine, Multi-model	139.62	+2.48	-10.70
8.	8.	8.	IBM Db2	Relational, Multi-model	136.00	+1.13	-13.56
9.	9.	↑ 10.	SQLite	Relational	124.58	-0.56	-10.05
10.	10.	↓ 9.	Microsoft Access	Relational	124.49	+0.18	-10.53

Fonte: DB-Engines (2023).

Ao comparar as criptografias utilizadas pelo Oracle e MySQL, observa-se que ambas as soluções oferecem diferentes níveis de segurança e flexibilidade. O Oracle disponibiliza a possibilidade de utilização da AES-265 para criptografar e descriptografar objetos, enquanto o MySQL utiliza três algoritmos diferentes: AES, MD5 e SHA-1. Cada um desses algoritmos é aplicado em diferentes cenários, como criptografia de arquivos e discos, verificação de integridade de dados e proteção de senhas de usuários.

Quadro 2 – Comparação entre criptografias

CRIPTOGRAFIA	Vantagens	Desvantagens
AES	- É considerado um dos algoritmos de criptografia mais seguros; - É amplamente utilizado e suportado por muitos sistemas; - Permite a criptografia e descriptografia de dados.	- Pode ser mais lento do que outros algoritmos menos seguros; - Requer uma chave de criptografia forte e segura para garantir a segurança dos dados.
SHA-1	- É rápido e fácil de implementar - É amplamente utilizado e suportado por muitos sistemas; - Fornece um *hash* que	- Pode ser vulnerável a ataques de colisão; - É considerado menos seguro em comparação a outros algoritmos mais recentes;

	pode ser verificado para detectar qualquer alteração não autorizada.	
MD5	- É rápido e fácil de implementar; - É amplamente utilizado e suportado por muitos sistemas; - É unidirecional, ou seja, não pode ser revertido a fim de recuperar o valor original.	- Pode ser vulnerável a ataques de colisão. - É considerado menos seguro em comparação a outros algoritmos mais recentes;

Fonte: Autoral (2023).

2.4 Discussão

O estudo abordou a criptografia em bancos de dados Oracle e MySQL, iniciando com uma extensa pesquisa. No Banco de Dados Oracle, a *Advanced Encryption Standard* de 265 bits (AES-265) é utilizada, garantindo a criptografia e descriptografia de objetos, com a opção de os clientes gerenciarem suas próprias chaves AES-256 bits. No MySQL, três algoritmos - AES, MD5 e SHA-1 - são empregados para diferentes finalidades, como criptografia de arquivos, verificação de integridade de dados e proteção de senhas. A comparação entre os sistemas revela que ambos oferecem diferentes níveis de segurança e flexibilidade.

Diante do exposto, percebeu-se a importância de proteger os bancos de dados que armazenam essas informações e, nesse sentido, a utilização da criptografia emerge como uma estratégia eficaz para preservar a integridade e confidencialidade de dados durante o armazenamento ou transferência. Em caso de acesso indevido a informações, a criptografia, realizada por meio de algoritmos específicos, impõe dificuldades significativas ao intruso, uma vez que obscurece a informação ao substituir caracteres por outros, ocultando, assim, o real significado das palavras (Martins; Candido Junior, 2014).

A segurança dos bancos de dados é uma preocupação crucial para empresas e governos, pois a perda ou vazamento de informações pode ter consequências graves. Nesse sentido, tanto o Oracle quanto o MySQL oferecem soluções de segurança, incluindo criptografia e gerenciamento de chaves, controles de acesso, máscara de dados flexível, monitoramento abrangente de atividades e

recursos de auditoria. No entanto, existem algumas diferenças entre os dois bancos de dados em relação à segurança.

O *Oracle Database* é reconhecido por sua robustez em segurança, principalmente quando administrado de forma eficaz. Ele desempenha um papel importante na redução do risco de violação de dados e simplifica a conformidade regulatória, proporcionando soluções de segurança que abrangem criptografia e gerenciamento de chaves, controles de acesso, máscara de dados flexível, monitoramento abrangente de atividades e recursos de auditoria. Além disso, o Oracle oferece o *Oracle Advanced Security*, que inclui criptografia de dados em repouso e em movimento, autenticação forte, gerenciamento de chaves, máscara de dados e auditoria (Oracle Help Center, 2023).

Por outro lado, o MySQL é um sistema de gerenciamento de banco de dados relacional de código aberto (*Relational Database Management System* – RDBMS) que utiliza tabelas, restrições, gatilhos, funções, procedimentos armazenados e visualizações como principais componentes de trabalho. O MySQL utiliza três técnicas de criptografia: AES (*Advanced Encryption Standard*), MD5 (*Message Digest Algorithm 5*) e SHA-1 (*Secure Hash Algorithm 1*) (Devmedia, 2016).

O AES desempenha um papel essencial na criptografia, sendo empregado para proteger arquivos e discos, garantindo a segurança dos dados mesmo em situações de acesso não autorizado ao dispositivo físico. Além disso, é aplicado em transmissões de dados, especialmente na internet, onde o MySQL pode empregar o AES para preservar a confidencialidade das informações trocadas entre o cliente e servidor. Em ambientes móveis que fazem uso do MySQL, o AES também é empregado para criptografar dados armazenados localmente.

Por sua vez, o MD5 assume o papel de verificar a integridade de dados, calculando o *hash* MD5 de um conjunto de informações. Esse *hash* é comparado a um valor conhecido para verificar se os dados foram alterados. Na transmissão de dados, o MD5 é usado para garantir a integridade, evitando corrupção. No gerenciamento de credenciais no MySQL, o MD5 é empregado para proteger senhas, proporcionando um armazenamento seguro e tornando as senhas ininteligíveis no banco de dados.

Já o SHA-1 é utilizado para garantir a integridade de dados sensíveis, fornecendo um *hash* que pode ser verificado para detectar qualquer alteração não

autorizada. Assim como o MD5, o SHA-1 também é utilizado na comunicação para assegurar que os dados transmitidos não sejam adulterados durante o processo (MySQL, 2023).

Em resumo, ambos os bancos de dados oferecem soluções de segurança para criptografia e gerenciamento de chaves, controles de acesso, máscara de dados flexível, monitoramento abrangente de atividades e recursos sofisticados de auditoria.

No entanto, o Oracle oferece recursos adicionais, como o *Oracle Advanced Security*, que inclui criptografia de dados em repouso e em movimento, autenticação forte, gerenciamento de chaves, máscara de dados e auditoria. Já o MySQL utiliza três técnicas de criptografia: AES, MD5 e SHA-1, aplicadas em diferentes situações, como criptografar arquivos e discos, verificar a integridade de dados e garantir a integridade de dados sensíveis.

3 CONSIDERAÇÕES FINAIS

O presente trabalho propôs uma análise comparativa entre a criptografia nos bancos de dados Oracle e MySQL, destacando a importância dessa técnica na proteção de dados sensíveis em um cenário cada vez mais conectado e propenso a ameaças cibernéticas. Ao longo deste estudo, foram explorados conceitos fundamentais de criptografia, revisando aspectos específicos dos bancos de dados Oracle e MySQL, bem como apresentadas as técnicas de criptografia adotadas por cada um.

Este estudo contribuiu para a compreensão das práticas de segurança adotadas por dois dos principais bancos de dados do mercado. A escolha entre Oracle e MySQL dependerá das necessidades específicas de cada organização, considerando fatores como controle de chaves, flexibilidade e requisitos de segurança. Entre as principais dificuldades enfrentadas durante este estudo, destaca-se a dificuldade em encontrar informações específicas sobre determinadas técnicas de criptografia.

Em um ambiente digital cada vez mais interconectado, a proteção de dados sensíveis emerge como uma prioridade incontestável. A análise comparativa entre a criptografia nos bancos de dados Oracle e MySQL proporciona *insights* valiosos para profissionais de segurança da informação, desenvolvedores e gestores de TI, fornecendo orientações essenciais para a tomada de decisões informadas e assegurando a integridade e confidencialidade dos dados em ambientes empresariais e governamentais.

Este trabalho não apenas destacou a importância da criptografia nos bancos de dados Oracle e MySQL, mas também incentivou uma reflexão contínua sobre as melhores práticas de segurança em um mundo digital em constante evolução.

REFERÊNCIAS

ALVES, Dafne. **Ataques cibernéticos ao Brasil**: levantamento sistemático dos últimos dez anos (2010–2020). 2022. 86 f. Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais) – Departamento de Economia e Relações Internacionais, Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2022.

ALVES, Filipe; MATEUS-COELHO, Nuno; CRUZ-CUNHA, Manuela. Encryption file system framework-proof of concept. **Procedia Computer Science**, Amsterdam, v. 181, p. 1237-1246, 2021. DOI: https://doi.org/10.1016/j.procs.2021.01.322.

ALMEIDA, Ana Carolina Brito de *et al*. LGPD em ambientes de bancos de dados nas organizações. *In*: FRANÇA, Thiago Cruz; NOGUEIRA, José Luiz Thomaselli; ANTUNES, João Francisco (coord.). **Minicursos da VI Escola Regional de Sistemas de Informação**: 06 a 09 de novembro de 2019. Rio de Janeiro: SBC, 2019. p. 68-108. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/39/166/336-1?inline=1. Acesso em: 20 set. 2023.

AZEVEDO, Arthur Henrique Ataíde de; CASTRO, Edkarla Andrade de; SERRÃO, Paulo Roberto de Lima. **Segurança em banco de dados**. 2011. [85 slides]. Disponível em: https://pt.slideshare.net/artinfo/segurana-em-banco-de-dados. Acesso em: 20 set. 2023.

DATE, Chris. **Introdução a sistemas de banco de dados**. Tradução de Daniel Vieira. 8. ed. Corpus, Rio de Janeiro, 2004.

DB-ENGINES. **DB-Engines Ranking**. California, 2023. Disponível em: https://db-engines.com/en/ranking. Acesso em: 2 nov. 2023.

DEVMEDIA. **Introdução à criptografia no MySQL.** Rio de Janeiro, [2023]. Disponível em: https://www.devmedia.com.br/introducao-a-criptografia-no-mysql/37179. Acesso em: 8 nov. 2023.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e matemática**. 2010. 161 f. Dissertação (Mestrado em Matemática para Professores) – Departamento de Matemática, Faculdade de Ciências, Universidade de Lisboa, Lisboa, 201.

LEITE, Hermano Portella; BONOMO, Igor da Silva. **Análise comparativa de projeto e administração de banco de dados entre os SGBDs Cassandra e MySQL**. 2016. 61 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília, Brasília, DF, 2016.

MARTINS, André Luiz; LIMA, Edgar Ferreira. **Segurança em banco de dados: teste de quebra de senha por força bruta no banco de dados Oracle 11G**. 2016. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Banco de Dados) – Faculdade de Tecnologia FATEC Bauru, Bauru, 2016.

MARTINS, Fábio Crepaldi; CANDIDO JUNIOR, Eli. Segurança em banco de dados: conceitos e aplicações. **ETIC-Encontro de Iniciação Científica**, São Paulo, v. 10, n. 10, p. 1-13, 2014. Disponível em: https://docs.oracle.com/pt-br/iaas/Content/Object/Tasks/encryption.htm. Acesso em: 19 set. 2023.

MEDEIROS, Willa da Silva *et al*. O uso da criptografia como ferramenta motivacional nas aulas de probabilidade no ensino médio. **Observatório de la Economía Latinoamericana**, [*s. l.*], v. 21, n. 9, p. 10619-10639, 2023. DOI: https://doi.org/10.55905/oelv21n9-009.

MYSQL. Encryption and compression functions. *In*: ORACLE. **MySQL 8.0 reference manual**: including MySQL NDB Cluster 8.0. Austin, 2023. p. 2416-2425. Disponível em: https://dev.mysql.com/doc/refman/8.0/en/encryption-functions.html. Acesso em: 20 set. 2023.

ORACLE HELP CENTER. **Criptografando dados**. Austin, [2023]. Disponível em: https://docs.oracle.com/pt-br/iaas/Content/Object/Tasks/encryption.htm. Acesso em: 19 set. 2023.

ORDONEZ, Edward David Moreno; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em software e hardware**. São Paulo: Novatec, 2005.