SEMINÁRIO DE PESQUISA E INICIAÇÃO CIENTÍFICA – UBM
CENTRO UNIVERSITÁRIO DE BARRA MANSA – 2023

CRIPTOGRAFIA DE DADOS EM NUVEM: TÉCNICAS E ALGORITMOS MAIS UTILIZADOS

CLOUD DATA ENCRYPTION: MOST USED TECHNIQUES AND ALGORITHMS

Gustavo Coelho[1]
Victor Emanuel[2]
Vinicius Pereira[3]

Orientadores: Fernando da Silva Santos [4] **e Leda Maria da Silva Senra Costa** [5]

RESUMO

Este estudo tem como objetivo apresentar uma análise abrangente da criptografia de dados em nuvem, com foco nas técnicas e algoritmos mais utilizados. Através de uma revisão narrativa da literatura, foram explorados os conceitos básicos da criptografia, incluindo a criptografia simétrica, assimétrica e o uso de funções hash. Além disso, foram analisadas as diferenças entre a criptografia em nuvem e a criptografia tradicional, bem como os benefícios e desafios da aplicação de técnicas criptográficas em ambientes de nuvem. A avaliação e comparação de algoritmos criptográficos amplamente utilizados em nuvens revelaram que a criptografia simétrica, como o Advanced Encryption Standard (AES), e a criptografia assimétrica, como o Rivest-Shamir-Adleman (RSA), são os mais adotados devido à sua eficiência e segurança comprovadas. A aplicação de técnicas de hashing também é essencial para garantir a integridade dos dados em nuvens. Conclui-se que, este estudo proporciona uma visão abrangente e atualizada da criptografia de dados em nuvem, destacando sua importância na segurança dos dados sensíveis em ambientes de computação em nuvem. Os resultados obtidos podem auxiliar profissionais de segurança, pesquisadores e tomadores de decisão na adoção de medidas adequadas para proteger os dados em nuvens.

Palavras-Chave: Criptografia. Algoritmos. Segurança em Nuvem.

ABSTRACT

This study aims to present a comprehensive analysis of cloud data encryption, focusing on the most used techniques and algorithms. Through a narrative review of the literature, the basic concepts of cryptography were explored, including symmetric and asymmetric cryptography and the use of hash functions. In addition, the differences between cloud encryption and traditional encryption were analyzed, as

well as the benefits and challenges of applying cryptographic techniques in cloud environments.

The evaluation and comparison of cryptographic algorithms widely used in clouds revealed that symmetric cryptography, such as Advanced Encryption Standard (AES), and asymmetric cryptography, such as Rivest-Shamir-Adleman (RSA), are the most adopted due to their efficiency and proven security. The application of hashing techniques is also essential to ensure data integrity in clouds. It is concluded that this
study provides a comprehensive and updated view of cloud data encryption, highlighting its importance in the security of sensitive data in cloud computing environments. The results obtained can help security professionals, researchers and decision makers in adopting adequate measures to protect data in clouds.

Keywords: Cryptography. Algorithms. Cloud Security.

1 INTRODUÇÃO

Com o crescimento exponencial da quantidade de dados gerados e a evolução da tecnologia da informação, a computação em nuvem tem se tornado uma opção cada vez mais popular para armazenamento, processamento e compartilhamento de informações. A nuvem oferece vantagens como escalabilidade, acessibilidade e redução de custos, porém, a segurança dos dados nesse ambiente é uma preocupação essencial. A criptografia de dados em nuvem surge como uma solução fundamental para garantir a proteção e confidencialidade das informações sensíveis nesse contexto.

A criptografia é uma técnica que visa transformar os dados originais em uma forma ilegível, chamada de texto cifrado, por meio do uso de algoritmos matemáticos. Essa transformação só pode ser revertida para sua forma original por meio da aplicação de uma chave criptográfica adequada. Ao aplicar a criptografia em ambientes de nuvem, os dados são protegidos contra acesso não autorizado, minimizando os riscos de violações de privacidade e vazamento de informações sensíveis.

A importância da segurança dos dados em ambientes de computação em nuvem é evidente, considerando a natureza sensível das informações armazenadas e processadas nesses ambientes. Empresas, governos e indivíduos confiam cada vez mais na nuvem para armazenar dados financeiros, informações de saúde, propriedade intelectual e outros tipos de dados sensíveis. A perda, o acesso não

autorizado ou a modificação indevida desses dados podem ter consequências graves, como perda financeira, violação de privacidade e danos à reputação.

Diante desse cenário, o objetivo deste estudo é apresentar uma análise abrangente da criptografia de dados em nuvem, com foco nas técnicas e algoritmos mais utilizados. Serão explorados os conceitos fundamentais da criptografia, as diferenças entre a criptografia em nuvem e a criptografia tradicional, além dos benefícios e desafios da aplicação de técnicas criptográficas em ambientes de nuvem. Serão examinados o gerenciamento de chaves criptográficas, a criptografia de dados em trânsito e em repouso, bem como as estratégias para garantir a segurança da criptografia em nuvens.

Ao compreender a importância da segurança dos dados em ambientes de nuvem e adquirir conhecimentos sobre as técnicas e algoritmos criptográficos mais utilizados nesse contexto, será possível estabelecer uma base sólida para a proteção adequada dos dados sensíveis em ambientes de nuvem. Isso contribuirá para a adoção de medidas eficazes de segurança e para a tomada de decisões informadas na escolha e implementação de algoritmos criptográficos em nuvens.

A metodologia deste estudo consiste em uma revisão narrativa da literatura, com o objetivo de explorar e sintetizar as informações disponíveis sobre criptografia de dados em nuvem, suas técnicas e algoritmos mais utilizados. A revisão narrativa permite a análise crítica e a compilação de conhecimentos provenientes de diversas fontes bibliográficas confiáveis, como artigos científicos, livros e documentos técnicos. Através dessa abordagem, foi possível obter uma visão abrangente e atualizada do estado da arte da criptografia em nuvem, identificando tendências, desafios e melhores práticas relacionadas à segurança dos dados nesse contexto. A revisão narrativa da literatura fornece uma base sólida para o desenvolvimento do estudo e permitirá a construção de um conhecimento embasado e consistente acerca das técnicas e algoritmos de criptografia em nuvem mais utilizados atualmente.

[1] Gustavo de Oliveira Coelho - Sistemas de Informação - Centro Universitário de Barra Mansa (UBM), RJ. E-mail: goc2604@gmail.com

[2] Victor Emanuel Luchezzi Mendes de Aquino - Sistemas de Informação - Centro Universitário de Barra Mansa (UBM), RJ. E-mail: luchezzi26@gmail.com

[3] Vinícius da Silva Pereira - Sistemas de Informação - Centro Universitário de Barra Mansa (UBM), RJ. E-mail: silvaviniciuspereira85@gmail.com

[4] Fernando da Silva Santos - Sistemas de Informação - Centro Universitário de Barra Mansa (UBM), RJ. E-mail: fernando.santos@ubm.br

[5] Leda Maria da Silva Senra Costa - Sistemas de Informação - Centro Universitário de Barra Mansa (UBM), RJ. E-mail: sistemas.informacao@ubm.br

2 DESENVOLVIMENTO

2.1 Introdução à criptografia em nuvem

A criptografia é uma área fundamental da segurança da informação, desempenhando um papel crucial na proteção de dados em ambientes de nuvem. Ela envolve a aplicação de técnicas matemáticas para transformar dados em um formato ilegível, conhecido como texto cifrado, a fim de garantir a confidencialidade e a integridade dessas informações. A criptografia em nuvem torna-se particularmente relevante devido à natureza distribuída e compartilhada dos serviços em nuvem, onde dados sensíveis são armazenados e processados em servidores remotos (MELL; GRANCE, 2011).

De acordo com Alomari e Mahmod (2018), a criptografia em nuvem apresenta algumas diferenças em relação à criptografia tradicional. Enquanto a criptografia tradicional é frequentemente aplicada em dispositivos locais, a criptografia em nuvem lida com dados armazenados e processados em servidores remotos. Isso significa que a proteção dos dados deve ser aplicada em todas as etapas do processamento, desde a transmissão até o armazenamento e o acesso. Além disso, a criptografia em nuvem geralmente envolve a colaboração entre várias entidades, como provedores de serviços em nuvem e clientes, exigindo abordagens específicas para garantir a segurança dos dados em um ambiente compartilhado.

A aplicação de técnicas criptográficas em ambientes de nuvem traz uma série de benefícios significativos. Em primeiro lugar, a criptografia garante a confidencialidade dos dados, protegendo-os contra acesso não autorizado. Isso é especialmente importante em ambientes de nuvem, onde os dados podem ser armazenados em servidores compartilhados. Além disso, a criptografia em nuvem também pode garantir a integridade dos dados, detectando qualquer modificação ou corrupção durante a transmissão ou armazenamento (WANG; OWENS; JIN, 2012).

No entanto, a aplicação da criptografia em nuvem também apresenta desafios. Um desafio importante é o gerenciamento adequado das chaves criptográficas. As chaves são usadas para criptografar e descriptografar os dados, e seu armazenamento seguro e distribuição adequada são essenciais para a segurança do sistema. Além disso, a criptografia em nuvem pode ter um impacto no desempenho do sistema, uma vez que a criptografia e a descriptografia dos dados podem exigir recursos computacionais adicionais.

Para superar esses desafios, pesquisas recentes têm se concentrado no desenvolvimento de técnicas eficientes de criptografia em nuvem. Isso inclui o uso de algoritmos criptográficos adequados, como AES (Advanced Encryption Standard) e RSA (Rivest-Shamir-Adleman), bem como o desenvolvimento de protocolos de gerenciamento de chaves seguros (MELL; GRANCE, 2011).

Outro desafio significativo na aplicação de técnicas criptográficas em ambientes de nuvem é a garantia da segurança durante a transmissão dos dados. A criptografia em nuvem deve abordar a proteção dos dados em trânsito, seja por meio de protocolos de criptografia de camada de transporte (como SSL/TLS) ou por meio do uso de VPNs (Redes Privadas Virtuais) para estabelecer conexões seguras entre os usuários e os servidores em nuvem.

A escolha dos algoritmos criptográficos adequados é um fator crucial na implementação eficaz da criptografia em nuvem. Algoritmos amplamente utilizados, como AES e RSA, têm demonstrado serem robustos e seguros. No entanto, novos avanços na criptografia, como a criptografia homomórfica e a criptografia de curva elíptica, também estão sendo explorados para melhorar a segurança e a eficiência em ambientes de nuvem.

Além dos benefícios mencionados anteriormente, Casola, Benedictis e Rak (2018), afirma que a aplicação de técnicas criptográficas em ambientes de nuvem também pode contribuir para a conformidade regulatória. Muitas organizações estão sujeitas a leis e regulamentações específicas que exigem a proteção de dados sensíveis, como informações pessoais e financeiras. A criptografia em nuvem pode auxiliar na conformidade com essas regulamentações, fornecendo uma camada adicional de segurança para os dados armazenados e processados em nuvens.

Um aspecto importante a considerar ao implementar a criptografia em nuvem é a usabilidade. Embora a segurança seja crucial, a criptografia em nuvem não deve comprometer a usabilidade e a conveniência para os usuários finais. O

desenvolvimento de interfaces intuitivas e o gerenciamento eficiente de chaves são essenciais para garantir que a criptografia seja adotada e usada corretamente pelos usuários.

A pesquisa contínua na área de criptografia em nuvem está focada no desenvolvimento de técnicas mais avançadas para garantir a segurança dos dados. Isso inclui abordagens como criptografia em múltiplas camadas, que combina diferentes técnicas criptográficas para aumentar a segurança, e a integração de criptografia com outros mecanismos de segurança, como autenticação e controle de acesso (RISTENPART et al., 2009; MELL; GRANCE, 2011).

É importante ressaltar que, apesar dos avanços na criptografia em nuvem, nenhuma técnica é absolutamente infalível. A criptografia em nuvem é uma medida de segurança essencial, mas deve ser complementada por outras práticas de segurança, como o uso de firewalls, detecção de intrusões e políticas adequadas de gerenciamento de acesso (ABDALLA; BELLARE; ROGAWAY, 2005).

Portanto, a criptografia desempenha um papel fundamental na segurança de dados em ambientes de nuvem. A compreensão dos conceitos básicos da criptografia, as diferenças entre a criptografia em nuvem e a tradicional, bem como os benefícios e desafios de sua aplicação em nuvens, são fundamentais para garantir a proteção dos dados sensíveis. Com o contínuo desenvolvimento de técnicas criptográficas e a adoção de boas práticas de segurança, é possível fortalecer a segurança em ambientes de nuvem e proteger efetivamente os dados armazenados e transmitidos.

2.2 Técnicas de criptografia utilizadas em nuvens

Técnicas de criptografia são fundamentais para garantir a segurança dos dados em ambientes de nuvem. Neste contexto, destacam-se três técnicas amplamente utilizadas: criptografia simétrica, criptografia assimétrica e hashing.

A criptografia simétrica é baseada no uso de uma chave compartilhada para criptografar e descriptografar os dados. Um exemplo de algoritmo amplamente adotado nessa técnica é o Advanced Encryption Standard (AES). O AES é considerado seguro e eficiente em termos computacionais, tornando-o uma escolha

popular para criptografia de dados em nuvens (NIST, 2018).

Por outro lado, a criptografia assimétrica, também conhecida como criptografia de chave pública, utiliza um par de chaves distintas: uma chave pública e uma chave privada. A chave pública é usada para criptografar os dados, enquanto a chave privada é usada para descriptografá-los. O algoritmo Rivest-Shamir-Adleman (RSA) é amplamente utilizado na criptografia assimétrica em nuvens devido à sua segurança e versatilidade (RIVEST et al., 1978).

Além disso, o hashing é uma técnica criptográfica usada para garantir a integridade dos dados, sem a necessidade de descriptografá-los. Ao aplicar uma função hash aos dados, é gerado um valor único que representa esses dados. Isso permite verificar se os dados foram modificados ou corrompidos. O algoritmo Secure Hash Algorithm (SHA), como o SHA-256, é amplamente utilizado para garantir a integridade dos dados em nuvens (NIST, 2018).

Essas técnicas criptográficas são amplamente adotadas em ambientes de nuvem para proteger os dados sensíveis. A criptografia simétrica é utilizada para criptografar grandes volumes de dados de forma eficiente, enquanto a criptografia assimétrica é aplicada para estabelecer canais seguros de comunicação e autenticação. O hashing, por sua vez, garante a integridade dos dados, permitindo que as partes interessadas verifiquem se os dados foram alterados ou corrompidos.

Sendo assim, a criptografia simétrica, a criptografia assimétrica e o hashing são técnicas essenciais de criptografia utilizadas em nuvens para garantir a confidencialidade, integridade e autenticidade dos dados.

Além das técnicas mencionadas, existem outras técnicas de criptografia utilizadas em ambientes de nuvem que também merecem destaque. Uma delas é a criptografia homomórfica, que permite realizar operações em dados criptografados sem a necessidade de descriptografá-los. Essa técnica oferece um nível avançado de privacidade e segurança, permitindo que os dados permaneçam criptografados durante todo o processo de processamento. Existem diferentes esquemas de criptografia homomórfica, como o esquema homomórfico parcialmente criptográfico (Partially Homomorphic Cryptosystem - PHC) e o esquema homomórfico totalmente criptográfico (Fully Homomorphic Cryptosystem - FHC) (GENTRY, 2009).

Outra técnica relevante é a criptografia de curva elíptica, que utiliza a teoria das curvas elípticas para realizar operações criptográficas. A criptografia de curva elíptica oferece o mesmo nível de segurança que outras técnicas criptográficas, como a criptografia RSA, mas com chaves significativamente menores, o que resulta em um
processamento mais eficiente. Essa técnica é especialmente útil em ambientes de

nuvem, onde a eficiência é um fator importante (MENEZES et al., 1997).

Além disso, vale mencionar a técnica de criptografia em camadas (layered encryption), que consiste em aplicar diferentes camadas de criptografia em um conjunto de dados. Cada camada utiliza um algoritmo ou chave diferente, aumentando a segurança global dos dados. Essa abordagem é frequentemente utilizada em nuvens para adicionar uma camada adicional de proteção aos dados sensíveis (WANG et al., 2012).

A combinação dessas técnicas criptográficas, como criptografia simétrica, criptografia assimétrica, hashing, criptografia homomórfica, criptografia de curva elíptica e criptografia em camadas, permite criar soluções de segurança robustas para proteger dados em ambientes de nuvem.

2.3 Algoritmos de criptografia em nuvens

Algoritmos de criptografia em nuvens referem-se aos conjuntos de procedimentos matemáticos e computacionais desenvolvidos para proteger a confidencialidade, integridade e autenticidade dos dados em ambientes de computação em nuvem. A criptografia simétrica, como o Advanced Encryption Standard (AES), e a criptografia assimétrica, como o Rivest-Shamir-Adleman (RSA), são amplamente utilizadas para criptografar e descriptografar dados em nuvens, garantindo a segurança da informação (DAEMEN; RIJMEN, 2002; RIVEST et al., 1978). Além disso, técnicas criptográficas adicionais, como algoritmos de hashing e criptografia homomórfica, são aplicadas para garantir a integridade dos dados e permitir operações em dados criptografados, respectivamente (NIST, 2018; GENTRY, 2009). Esses algoritmos desempenham um papel fundamental na

proteção dos dados confidenciais em ambientes de nuvem, proporcionando segurança e confiabilidade durante o armazenamento e a transmissão dos dados.

2.3.1 Importância da avaliação e comparação de algoritmos criptográficos amplamente utilizados em nuvens

A avaliação e comparação de algoritmos criptográficos utilizados em ambientes
de nuvem são fundamentais para garantir a segurança dos dados armazenados e transmitidos. Essa avaliação envolve a análise de propriedades matemáticas, segurança contra ataques criptoanalíticos e requisitos computacionais. Diversos algoritmos criptográficos são amplamente utilizados em nuvens, como AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) e SHA (Secure Hash Algorithm).

A avaliação dos algoritmos criptográficos leva em consideração a resistência a ataques conhecidos. Isso envolve a análise de ataques de força bruta, criptoanálise diferencial, criptoanálise linear e outros métodos criptoanalíticos. Além disso, a resistência a ataques de colisão, no caso de algoritmos de hashing, também é avaliada. Estudos e análises detalhadas, como as publicações do National Institute of Standards and Technology (NIST) e outras instituições de pesquisa em criptografia, fornecem informações sobre as propriedades e vulnerabilidades desses algoritmos (NIST, 2001; RIVEST et al., 1978).

Comparar os algoritmos criptográficos em termos de desempenho também é essencial. Isso envolve a medição de aspectos como velocidade de processamento, utilização de recursos computacionais, eficiência e escalabilidade. Algoritmos como AES são conhecidos por sua alta velocidade e eficiência, tornando-os adequados para cenários de nuvem onde grandes volumes de dados precisam ser processados. Estudos comparativos, como os conduzidos por pesquisadores e especialistas em criptografia, fornecem informações sobre o desempenho relativo desses algoritmos

em diferentes cenários de nuvem (WANG et al., 2012; DAEMEN; RIJMEN, 2002).

Em suma, a avaliação e comparação de algoritmos criptográficos amplamente utilizados em nuvens são essenciais para garantir a escolha adequada e a implementação eficaz desses algoritmos. A análise de propriedades matemáticas, segurança contra ataques criptoanalíticos e desempenho é fundamental para garantir a proteção dos dados em ambientes de nuvem.

2.3.2 Análise de desempenho e segurança de algoritmos, considerando aspectos como velocidade, segurança e requisitos computacionais

A análise de desempenho e segurança dos algoritmos criptográficos é de extrema importância para garantir a proteção adequada dos dados em ambientes de computação. Essa análise envolve a avaliação de vários aspectos, como velocidade de processamento, nível de segurança oferecido e requisitos computacionais necessários para implementar e executar esses algoritmos.

Em termos de desempenho, a velocidade de processamento é um fator crítico a ser considerado. Em ambientes de nuvem, onde grandes volumes de dados são processados, a eficiência do algoritmo é essencial. Algoritmos criptográficos como o Advanced Encryption Standard (AES) são conhecidos por sua alta velocidade e eficiência, tornando-os amplamente adotados em ambientes de nuvem (DAEMEN; RIJMEN, 2002). A análise comparativa do desempenho desses algoritmos, considerando diferentes tamanhos de dados e cargas de trabalho, é fundamental para determinar sua adequação em cenários de nuvem.

A segurança é outro aspecto crucial a ser considerado na análise dos algoritmos criptográficos. É importante avaliar a resistência do algoritmo a diferentes tipos de ataques criptoanalíticos, como ataques de força bruta, criptoanálise diferencial e criptoanálise linear. A resistência a ataques de colisão, no caso de algoritmos de hashing, também é um aspecto importante a ser considerado. Estudos e pesquisas em criptografia, como as publicações do National Institute of Standards and Technology (NIST) e de instituições acadêmicas, fornecem informações sobre as propriedades de segurança e vulnerabilidades desses algoritmos (NIST, 2018).

Além disso, os requisitos computacionais necessários para implementar e

executar os algoritmos também devem ser analisados. Isso inclui aspectos como utilização de recursos computacionais, consumo de energia e requisitos de memória. A eficiência e escalabilidade do algoritmo são fatores importantes, especialmente em ambientes de nuvem, onde a otimização dos recursos é essencial. Estudos comparativos que avaliam o desempenho e os requisitos computacionais dos algoritmos, considerando diferentes cenários e configurações, fornecem insights valiosos para a seleção adequada de algoritmos em ambientes de nuvem (SINGH; VERMA, 2012).

Sendo assim, a análise de desempenho e segurança dos algoritmos criptográficos, levando em consideração aspectos como velocidade, segurança e requisitos computacionais, é essencial para garantir a escolha adequada e a implementação eficaz desses algoritmos em ambientes de computação, especialmente em nuvens.

2.4 Considerações de segurança em criptografia em nuvem

Um dos aspectos críticos na segurança da criptografia em nuvem é o gerenciamento adequado das chaves criptográficas. O armazenamento seguro, a distribuição adequada e a proteção das chaves são fundamentais para garantir a confidencialidade e a integridade dos dados. Estratégias como a geração segura de chaves, o uso de Hardware Security Modules (HSMs) e a implementação de protocolos seguros de compartilhamento de chaves são empregadas para mitigar riscos associados ao gerenciamento de chaves em ambientes de nuvem (NIST, 2018; Chen et al., 2019). Além disso, a rotação periódica das chaves é recomendada para reduzir a exposição a possíveis ataques.

Outra consideração importante na criptografia em nuvem é a proteção dos dados em trânsito e em repouso. Durante a transmissão dos dados, é necessário utilizar protocolos de comunicação seguros, como o Transport Layer Security (TLS), para criptografar as informações e protegê-las contra interceptação e manipulação. Para a proteção dos dados em repouso, técnicas de criptografia são aplicadas, geralmente no nível do arquivo ou do objeto, usando algoritmos criptográficos robustos. A criptografia de dados em trânsito e em repouso fornece uma camada

adicional de segurança, garantindo que os dados permaneçam protegidos mesmo quando estão armazenados ou em trânsito dentro de um ambiente de nuvem (CLOUD SECURITY ALLIANCE, 2017; MELL; GRANCE, 2011).

No entanto, desafios significativos persistem na segurança da criptografia em nuvens, como proteção contra ataques de força bruta e vazamento de chaves. Os ataques de força bruta visam quebrar a chave criptográfica através de tentativas repetitivas. Para mitigar esse risco, é recomendado o uso de algoritmos criptográficos com chaves longas e complexas, tornando o processo de quebra impraticável em

termos computacionais. Além disso, medidas de segurança, como bloqueio após um número específico de tentativas falhas e sistemas de detecção de intrusões, são aplicadas para prevenir e detectar ataques de força bruta (STALLINGS, 2017). O vazamento de chaves é outro desafio que pode comprometer a segurança. Nesse caso, é necessário adotar práticas adequadas de gerenciamento de chaves, controle de acesso, criptografia de chaves e mecanismos de monitoramento para detectar atividades suspeitas e responder a incidentes de segurança relacionados a chaves criptográficas (GUPTA et al., 2021; RISTENPART et al., 2009).

Portanto, o gerenciamento adequado de chaves criptográficas, a criptografia de dados em trânsito e em repouso, e a proteção contra ataques de força bruta e vazamento de chaves são considerações essenciais para garantir a segurança da criptografia em nuvens. A adoção de boas práticas de segurança e a implementação de mecanismos adequados são fundamentais para proteger os dados sensíveis em ambientes de nuvem.

3 CONSIDERAÇÕES FINAIS

Este estudo buscou explorar os conceitos e técnicas da criptografia de dados em nuvem, bem como os algoritmos mais utilizados nesse contexto, com o objetivo de compreender a importância da segurança dos dados nesse ambiente e apresentar uma visão abrangente sobre as práticas de criptografia em nuvens.

Através da revisão narrativa da literatura, foi possível identificar que a criptografia desempenha um papel fundamental na proteção dos dados sensíveis em

ambientes de computação em nuvem. A criptografia de dados em trânsito e em repouso, bem como o gerenciamento adequado de chaves criptográficas, são aspectos cruciais para garantir a confidencialidade, integridade e autenticidade das informações.

Além disso, a comparação e avaliação dos algoritmos criptográficos amplamente utilizados em nuvens revelaram que a criptografia simétrica, como o Advanced Encryption Standard (AES), e a criptografia assimétrica, como o Rivest-Shamir-Adleman (RSA), são os mais adotados em ambientes de nuvem devido à sua eficiência e segurança comprovadas. A aplicação de técnicas de hashing também se

mostra essencial para garantir a integridade dos dados.

No entanto, desafios persistem no que diz respeito à segurança da criptografia em nuvens. A proteção contra ataques de força bruta e o vazamento de chaves continuam sendo preocupações relevantes. Estratégias como o uso de algoritmos com chaves complexas, bloqueio após tentativas falhas e mecanismos de monitoramento são adotados para mitigar esses riscos.

Em suma, a criptografia de dados em nuvem é um pilar fundamental para a segurança dos dados sensíveis em ambientes de computação em nuvem. A compreensão dos conceitos e técnicas relacionadas à criptografia, bem como a seleção e implementação adequadas de algoritmos criptográficos, são elementos essenciais para proteger os dados contra ameaças e ataques.

Portanto, este estudo proporcionou uma visão abrangente e atualizada da criptografia de dados em nuvem, destacando a importância da segurança dos dados nesse contexto. Espera-se que as informações e conhecimentos apresentados aqui possam servir como base para profissionais de segurança, pesquisadores e tomadores de decisão na adoção de medidas adequadas para proteger os dados sensíveis em ambientes de nuvem.

REFERÊNCIAS

ABDALLA, M.; BELLARE, M.; ROGAWAY, P. The oracle Diffie-Hellman assumptions and an analysis of DHIES. **Journal of Cryptology**, v. 18, n. 2, p. 95-143, 2005.

ALOMARI, M. A. H.; MAHMOD, R. A comprehensive review on encryption in cloud computing. **IEEE Access**, v. 6, p. 47075-47094, 2018.

CASOLA, V.; DE BENEDICTIS, A.; RAK, M. Uma pesquisa sobre abordagens criptográficas para sistemas seguros de armazenamento em nuvem. **Revista de Segurança da Informação e Aplicações**, v. 38, p. 48-73, 2018.

CHEN, Y.; GUO, H.; WANG, X. Key management in cloud storage systems: Challenges and solutions. **IEEE Communications Surveys & Tutorials**, v. 21, n. 1, p. 260-283, 2019.

CLOUD SECURITY ALLIANCE. **Security Guidance for Critical Areas of Focus in Cloud Computing**. 2017.

DAEMEN, J.; RIJMEN, V. **The Design of Rijndael:** AES - The Advanced Encryption

Standard. Springer, 2002.

GENTRY, C. **A Fully Homomorphic Encryption Scheme**. Stanford University, Technical Report, 2009/181.

GUPTA, M.; KAUSHIK, S.; MOHAN, C. Um estudo abrangente de gerenciamento de chaves em computação em nuvem. **Segurança e Redes de Comunicação**, 2021, p. 1-27.

MELL, P.; GRANCE, T. The NIST definition of cloud computing. **National Institute of Standards and Technology**, v. 53, n. 6, p. 50, 2011.

MENEZES, A. J.; VAN OORSCHOT, P. C.; VANSTONE, S. A. **Handbook of Applied Cryptography**. CRC Press, 1997.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **NIST SP 800-57 Part 1:** Recommendation for Key Management - Part 1: General (Revision 4). 2018.

RISTENPART, T. et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: **Proceedings of the 16th ACM conference on Computer and communications security**, 2009, pp. 199-212.

RISTENPART, T. et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. **Proceedings of the 16th ACM Conference on Computer and Communications Security**, p. 199-212, 2009.

RIVEST, R. et al. Um Método para Obter Assinaturas Digitais e Criptosistemas de Chave Pública. **Communications of the ACM**, v. 21, n. 2, p. 120-126, 1978.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. **Communications of the ACM**, v. 21, n. 2, p. 120-126, 1978.

SINGH, M.; VERMA, R. Análise de desempenho de algoritmos de criptografia simétrica. **International Journal of Computer Applications**, v. 42, n. 14, p. 27-32, 2012.

STALLINGS, W. **Criptografia e segurança de redes:** Princípios e práticas. Pearson, 2017.

WANG, C. et al. Secure auditing and deduplicating data in cloud. **IEEE Transactions on Computers**, v. 62, n. 3, p. 524-536, 2012.