XXI Escola Regional de Redes de Computadores / VIII Workshop de Segurança (ERRC). DOI: 10.5753/errc.2024.4580

Artigo Completo/Full Paper

Criptografando dados em um sistema de monitoramento de sinais vitais

Encrypting Data in a Vital Signs Monitoring System

Leonardo de Paula • leodepaula315@gmail.com
Centro de Robótica e Ciência de Dados (iTEC)

Jeferson Pereira Feijó • jeferson.sdi@gmail.com
Centro de Robótica e Ciência de Dados (iTEC)

Debora Bertaco • deb.bertaco@gmail.com
Universidade Federal do Rio Grande (FURG)
Centro de Robótica e Ciência de Dados (iTEC)

Eduardo da Rosa Asevedo • dudupel18@gmail.com
Centro de Robótica e Ciência de Dados (iTEC)

Emily Marques Salum • emilymarquessalum@gmail.com
Centro de Robótica e Ciência de Dados (iTEC)

Luiz Oscar Homann de Topin • ltopin@gmail.com
Centro de Robótica e Ciência de Dados (iTEC)

Luciano Maciel Ribeiro • luciano@furg.br
Universidade Federal do Rio Grande (FURG)
Centro de Robótica e Ciência de Dados (iTEC)

Giancarlo Lucca • giancarlo.lucca@ucpel.edu.br
Universidade Católica de Pelotas (UCPel)

Bruno L. Dalmazo • dalmazo@furg.br
Universidade Federal do Rio Grande (FURG)
Centro de Robótica e Ciência de Dados (iTEC)

resumo. Este artigo apresenta uma arquitetura de segurança para sistemas de monitoramento remoto de sinais vitais baseados em IoT, utilizando o algoritmo simétrico AES para criptografia de dados. A solução visa garantir a proteção dos dados durante a coleta, transmissão e armazenamento, atendendo às restrições de dispositivos com recursos computacionais limitados. A arquitetura proposta prioriza a eficiência energética e a privacidade dos dados dos pacientes, em conformidade com normativas brasileiras como a Lei Geral de Proteção de Dados (LGPD), oferecendo uma abordagem escalável e segura para o monitoramento remoto de saúde.

abstract. This article presents a security architecture for IoT-based remote vital signs monitoring systems, utilizing the AES symmetric algorithm for data encryption. The solution aims to ensure data protection during collection, transmission, and storage, addressing the constraints of devices with limited computational resources. The proposed architecture prioritizes energy efficiency and patient data privacy, in compliance with Brazilian regulations such as the General Data Protection Law (LGPD), offering a scalable and secure approach for remote health monitoring.

palavras-chave: Criptografia de dados • Proteção de Dados • Sinais Vitais • Segurança em IoT de Saúde
keywords: Data Encryption • Data Protection • Vital Signs • IoT Healthcare Security

1 Introdução

A segurança da informação é um requisito essencial em sistemas que lidam com dados sensíveis, sobretudo em aplicações na área da saúde. Com o avanço dos dispositivos de Internet das Coisas (IoT) voltados ao monitoramento remoto de sinais vitais, práticas de homecare e monitoramento à distância têm se tornado componentes fundamentais na assistência médica moderna. O acompanhamento remoto permite que pacientes com condições crônicas ou em reabilitação possam ser monitorados continuamente fora do ambiente hospitalar, proporcionando maior comodidade e qualidade de vida. Esse monitoramento remoto não apenas melhora o acesso aos cuidados, mas também auxilia na identificação precoce de anomalias, promovendo intervenções rápidas e reduzindo a necessidade de internações prolongadas [1].

A coleta, transmissão e armazenamento de dados de

saúde em tempo real apresentam desafios significativos no que tange à privacidade e à segurança da informação. Informações como frequência cardíaca, temperatura e pressão arterial, quando compartilhadas entre dispositivos e armazenadas em servidores, tornam-se vulneráveis a acessos não autorizados, manipulações e interceptações. Assim, soluções robustas de segurança tornam-se imprescindíveis para proteger essas informações contra violações e garantir a confidencialidade e a integridade dos dados dos pacientes [2].

Este trabalho propõe uma arquitetura criptográfica para sistemas de monitoramento remoto de sinais vitais, buscando assegurar a proteção dos dados durante todo o processo de comunicação entre os dispositivos de IoT. A proposta utiliza criptografia simétrica, devido à sua eficiência e menor demanda por recursos computacionais, tornando-a adequada para dispositivos que frequentemente operam com restrições de processamento e energia. Dentre os métodos disponíveis, propomos a utilização de um conhecido e estabelecido algoritmo, o Advanced Encryption Standard (AES). Essa abordagem é destacada como uma opção confiável para a proteção dos dados, equilibrando segurança e desempenho [3, 4].

O artigo está organizado da seguinte maneira: a Seção 2 aborda a fundamentação teórica sobre criptografia e segurança de dados; a Seção 3 discute trabalhos relacionados à proteção de dados em monitoramento remoto; a Seção 4 detalha a proposta de arquitetura de criptografia para sistemas de monitoramento remoto de sinais vitais; e, finalmente, a Seção 5 apresenta as conclusões e recomendações para direções futuras.

2 Fundamentação Teórica

2.1 Criptografia de Dados

A criptografia de dados é uma técnica fundamental para a proteção de informações sensíveis, consistindo na transformação de dados legíveis, chamados de texto plano, em um formato cifrado que só pode ser acessado por aqueles que possuem a chave apropriada. Essa transformação garante a confidencialidade e a integridade dos dados, impedindo que informações críticas sejam interceptadas ou manipuladas durante a transmissão e o armazenamento [2]. No contexto da saúde, onde dispositivos de monitoramento remoto capturam sinais vitais de pacientes, a criptografia oferece uma camada essencial de proteção que assegura a privacidade dos dados e o cumprimento de normativas de proteção de dados [5].

Existem dois tipos principais de criptografia: simétrica e assimétrica. Na criptografia simétrica, a mesma chave é usada tanto para cifrar quanto para decifrar os dados, o que torna esse método mais rápido e adequado para sistemas de IoT com recursos limitados [6]. Por outro lado, a criptografia assimétrica utiliza pares de chaves (uma pública e uma privada), oferecendo uma camada adicional de segurança. No entanto, sua demanda computacional é mais elevada, o que pode limitar sua aplicação em dispositivos com restrições de processamento e energia [7].

Para sistemas de monitoramento remoto de saúde, o algoritmo AES é amplamente reconhecido como uma solução robusta de criptografia simétrica. Estabelecido como padrão pelo Instituto Nacional de Padrões e Tecnologia (NIST), o AES utiliza uma estrutura de blocos e oferece chaves de 128, 192 e 256 bits, proporcionando um equilíbrio eficaz entre segurança e eficiência computacional [3]. Este algoritmo é particularmente adequado para aplicações em IoT devido ao seu baixo consumo de energia e alta velocidade de operação, essenciais para dispositivos médicos que monitoram sinais vitais de forma contínua.

2.2 Segurança e Privacidade em Sistemas de Monitoramento de Saúde

Sistemas de monitoramento remoto de saúde capturam dados sensíveis dos pacientes em tempo real, proporcionando uma visão contínua do seu estado de saúde. Essas informações são frequentemente transmitidas para servidores remotos, onde podem ser analisadas por profissionais de saúde ou disponibilizadas para acompanhamento de familiares. Embora essa tecnologia traga avanços significativos para o cuidado ao paciente, ela também representa um desafio em termos de segurança da informação. A transmissão e o armazenamento de dados de saúde envolvem o risco de exposição a ataques cibernéticos, tornando a criptografia e a proteção da privacidade componentes críticos desses sistemas [1].

A proteção de dados de saúde exige que medidas de segurança sejam implementadas em todas as etapas do fluxo de dados: desde a coleta no dispositivo até a transmissão para o servidor e o armazenamento final. Além disso, regulamentações de privacidade, como a Lei Geral de Proteção de Dados (LGPD) e o General Data Protection Regulation (GDPR), estabelecem diretrizes rigorosas para o tratamento de dados pessoais e exigem que sistemas de monitoramento adotem padrões de segurança que protejam a privacidade dos pacientes [8].

3 Trabalhos Relacionados

A segurança de dados em sistemas de monitoramento remoto de saúde tem sido objeto de pesquisas crescen-

tes, em resposta à demanda por proteção da privacidade em ambientes médicos e à crescente utilização de dispositivos IoT. Diversos estudos destacam a aplicação de criptografia como medida essencial para proteger informações sensíveis e assegurar que apenas usuários autorizados possam acessar esses dados. Nesta seção, são discutidos alguns dos principais trabalhos relacionados à criptografia e à segurança em sistemas de monitoramento de sinais vitais, com ênfase nas soluções utilizadas para garantir a privacidade dos dados.

Um estudo de Amir Alkodri *et al.* [9] explorou o uso de criptografia simétrica para proteger dados médicos transmitidos entre dispositivos IoT e servidores de armazenamento. Nesse trabalho, os autores destacam que algoritmos simétricos, como o AES, são particularmente adequados para dispositivos de monitoramento remoto, devido à sua alta eficiência e baixo consumo de energia. A proposta foi aplicada a um sistema de monitoramento de pacientes com doenças crônicas, onde os sinais vitais eram coletados e transmitidos de maneira contínua. Esse estudo enfatiza a viabilidade de algoritmos de criptografia simétrica para aplicações médicas, especialmente em dispositivos que necessitam de uma operação contínua e confiável.

Outro estudo relevante, de Sutradhar *et al.* [10], propôs o uso de blockchain como uma solução de segurança complementar para monitoramento remoto. Os dados dos pacientes foram protegidos por criptografia e armazenados em uma rede blockchain, garantindo a integridade e a imutabilidade das informações. Embora essa abordagem forneça uma camada adicional de segurança, o uso do blockchain em dispositivos IoT exige maior capacidade de processamento e energia, o que pode não ser viável para dispositivos de monitoramento com recursos limitados. Esse trabalho destaca os desafios que soluções computacionalmente intensivas apresentam para o monitoramento de saúde.

Estudos mais recentes também exploram o uso de criptografia leve para reduzir o impacto de segurança em dispositivos com baixo poder computacional. Radhakrishnan; Jadon; Honnavalli [11] propuseram uma variante leve do AES, conhecida como LAES, projetada para atender a dispositivos de IoT que requerem alta eficiência energética e baixo consumo de memória. Em sistemas de monitoramento remoto, o LAES apresentou um bom desempenho na proteção de dados sensíveis, oferecendo uma alternativa interessante para dispositivos que demandam uma operação energética eficiente. No entanto, as implementações leves de criptografia devem ser cuidadosamente avaliadas quanto à sua robustez, uma vez que simplificações no algoritmo podem impactar a segurança.

A partir dessas análises, observa-se que a criptografia simétrica é amplamente considerada uma solução eficaz e eficiente para sistemas de monitoramento remoto de sinais vitais, sendo comumente utilizada em dispositivos de IoT devido ao seu equilíbrio entre segurança e desempenho. Contudo, os estudos indicam a importância de adaptar algoritmos de segurança às restrições dos dispositivos, considerando não apenas a proteção dos dados, mas também a necessidade de eficiência energética e baixa complexidade computacional.

A arquitetura proposta neste trabalho difere das abordagens discutidas nos trabalhos relacionados ao adotar uma solução específica para sistemas de monitoramento remoto que operam em dispositivos de IoT com limitações de processamento e energia.

4 Uma proposta de criptografia para sistemas de monitoramento de sinais vitais

A arquitetura proposta tem como objetivo garantir a segurança dos dados de saúde coletados e transmitidos, proporcionando proteção ao longo de todo o fluxo de dados, desde a coleta inicial dos sinais vitais até o armazenamento final. Para isso, são descritos quatro componentes principais que formam o sistema de segurança, ilustrados na Figura 1.

4.1 Sistema de Monitoramento de Sinais Vitais

A primeira etapa do sistema envolve a coleta dos sinais vitais do paciente. Realizada por dispositivos de monitoramento não invasivos que capturam dados como frequência cardíaca, temperatura, etc.

Para garantir a confidencialidade desde a origem, o algoritmo AES é implementado diretamente nesses dispositivos, que realizam a cifragem dos dados assim que são coletados. A aplicação do AES em dispositivos de IoT se justifica por sua eficiência e segurança, sendo uma criptografia simétrica capaz de operar em dispositivos com recursos limitados, mantendo a integridade dos dados e minimizando a possibilidade de interceptação não autorizada [3].

É importante destacar que inicialmente, para troca de chaves, optamos por utilizar abordagem Massey-Omura [12] que é um esquema de criptografia de chave pública baseado no conceito de exponenciação modular. Ele foi desenvolvido para permitir a troca de mensagens seguras sem que o remetente e o destinatário precisem compartilhar previamente uma chave secreta, sendo uma forma de criptografia assimétrica.

Os dispositivos que podem ser utilizados para essa coleta incluem oxímetros de pulso, monitores de temperatura, dispositivos de eletrocardiograma (ECG) e

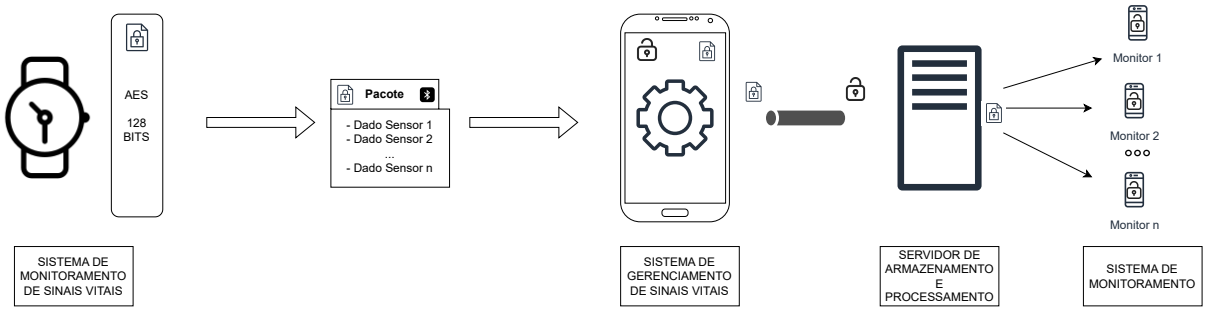

Figura 1. Uma visão geral da proposta de criptografia do sistema.

smartwatches que oferecem monitoramento de sinais vitais. Além desses, equipamentos como monitores de pressão arterial e pulseiras fitness também são comuns na prática clínica e no monitoramento pessoal de saúde. Cabe destacar que o emprego de sensores em seres humanos exige dispositivos certificados pela Agência Nacional de Vigilância Sanitária (ANVISA).

O algoritmo AES, descrito no Algoritmo 1, pode ser implementado em qualquer linguagem de programação, desde que a linguagem permita manipulação de bits e operações matemáticas como XOR, multiplicação em campos finitos (Galois Fields), entre outras. O que significa que os dados criptografados em uma linguagem podem ser corretamente descriptografados em outra, desde que os mesmos parâmetros criptográficos sejam seguidos. Isso se deve ao fato de que AES é um padrão amplamente reconhecido e implementado de maneira consistente em diferentes plataformas. Tanto a chave de criptografia, o modo de operação (como CBC ou GCM), quanto o vetor de inicialização (IV) são elementos essenciais para garantir que a criptografia e a descriptografia funcionem de forma interoperável, independentemente da linguagem. Assim, o que garante a integridade dos dados criptografados é a correta implementação dos algoritmos, e não a linguagem.

4.2 Sistema de Gerenciamento dos Dados Recebidos

Após a coleta e cifragem, os dados de saúde criptografados são transmitidos ao sistema de gerenciamento, que atua como um intermediário responsável por organizar e classificar os dados antes de seu armazenamento. O sistema de gerenciamento verifica a integridade e a autenticidade das informações, utilizando algoritmos de hashing, como o SHA-256, para identificar qualquer alteração nos dados durante a transmissão. Esse gerenciamento dos dados recebidos assegura que apenas informações válidas e não comprometidas avancem para as próximas fases do processo, protegendo o fluxo de dados e evitando a propagação de possíveis anomalias.

Algorithm 1 Função para criptografar a mensagem

```
1: function ENCRYPT_MESSAGE(message, encrypted_message, key, iv)
2: end function

3: procedure MAIN
4:     int sock;
5:     struct sockaddr_in server_addr;
6:     unsigned char *key = ”0123456789abcdef”;
7:     unsigned char iv[AES_BLOCK_SIZE] = {0};
8:     unsigned char message[] = ”Esta é uma mensagem secreta”;
9:     unsigned char encrypted_message[128];
                                ▷ Criptografar a mensagem
10:    ENCRYPT_MESSAGE(message, encrypted_message, key, iv);
           ▷ Converter a mensagem criptografada para Base64
11:    char *base64_encrypted_message = base64_encode(encrypted_message, strlen((char *)encrypted_message));
12: end procedure
```

A implementação do AES em dispositivos de IoT não apenas assegura a proteção dos dados durante a coleta, mas também minimiza a possibilidade de interceptação não autorizada. Ao cifrar os dados assim que são coletados, os dispositivos garantem que informações sensíveis, como os sinais vitais dos pacientes, permaneçam protegidas durante a transmissão para servidores ou sistemas de análise.

O Algoritmo 2, é implementado na linguagem Python e implementa uma classe chamada `NotificationHandler`, projetada para lidar com notificações criptografadas utilizando o algoritmo AES no modo CBC (Cipher Block Chaining). A classe armazena notificações, gerencia a chave de criptografia (AES key) e descriptografa mensagens recebidas.

Algorithm 2 Função para descriptografar a mensagem

Input: aes_iv = bytes([0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0])
Class: NotificationHandler

Procedure init(aes_iv)

1. Initialize an empty list *notifications*
2. Set *aes_key* to *None*
3. Set *aes_iv* to the input value *aes_iv*
4. Set *first_message_received* to *False*

Method handle(sender, data)

1. **If** *first_message_received* is *False*:
   a. Call *set_key(data)*
   b. Set *first_message_received* to *True*
   c. Print "Key set to: ", *aes_key.hex()*
2. **Else**:
   a. Call *uncypher(data)* and store result in *message*
   b. Append *message* to *notifications*
   c. Print "Encrypted notification from sender (Handle: ", *sender.handle*, "): ", *data*
   d. Print "Decrypted notification from sender (Handle: ", *sender.handle*, "): ", *message*
3. **Exception Handling**:
   Print "Notification from sender (Handle: ", *sender.handle*, "): Error: ", *e*

Method set_key(data)

1. Convert *data* to *aes_key* using *bytes.fromhex(data.decode('utf-8'))*
2. Print "Received key: ", *aes_key.hex()*

Method uncypher(data)

1. Decode *data* from base64 into *encrypted_message_bytes*
2. Initialize AES cipher in CBC mode using *aes_key* and *aes_iv*
3. Decrypt *encrypted_message_bytes* and unpad the result into *decrypted_message_bytes*
4. Return the UTF-8 decoded *decrypted_message_bytes*

4.3 Sistema de Armazenamento e Processamento

No sistema de armazenamento, os dados criptografados são mantidos em um banco de dados seguro, garantindo que o acesso aos dados brutos seja restrito. A descriptografia ocorre apenas quando é realizada uma solicitação autenticada e validada por um profissional autorizado, que possui as credenciais necessárias para visualizar os dados sensíveis. Para reforçar a segurança, recomenda-se o uso de políticas de controle de acesso baseadas em múltiplos fatores, exigindo, por exemplo, uma autenticação adicional antes de liberar os dados. Além disso, a integridade dos dados armazenados é periodicamente verificada, assegurando que não houve modificações não autorizadas durante o armazenamento [2].

A criptografia neste processo utilizando AES funciona de maneira bastante eficiente e segura. Inicialmente, os pacotes de dados são formados pelos dados coletados de diferentes sensores. Cada pacote pode conter informações diversas, como "Dado Sensor 1", "Dado Sensor 2" até "Dado Sensor n", representando um conjunto de informações contínuas geradas pelos dispositivos de monitoramento.

Quando esses pacotes de dados chegam ao servidor de armazenamento, eles passam por um processo de criptografia utilizando o algoritmo AES com uma chave de 128 bits. O AES opera em blocos de dados, ou seja, ele divide o conteúdo dos pacotes em blocos de tamanho fixo, geralmente 128 bits, e então aplica a chave de criptografia para embaralhar os dados de forma que apenas quem possui a chave correta possa decifrá-los.

A segurança fornecida por essa técnica de criptografia é essencial. Mesmo que os pacotes de dados sejam interceptados durante a transmissão ou acessados de forma não autorizada, a utilização do AES garante que os dados permanecem protegidos. Isso ocorre porque, sem a chave correta, é praticamente impossível decifrar ou acessar o conteúdo dos dados criptografados.

4.4 Sistema de Monitoramento

Por fim, o sistema de monitoramento é responsável por avaliar continuamente os sinais vitais do paciente em tempo real, alertando profissionais de saúde e familiares em caso de anomalias detectadas. Como os dados transmitidos e armazenados permanecem cifrados até a visualização final, a arquitetura proposta assegura que qualquer comunicação entre o sistema de monitoramento e os dispositivos de coleta respeite o fluxo de segurança estabelecido.

Após o processamento dos sinais vitais no servidor, os dados são criptografados e enviados simultaneamente para múltiplos dispositivos de monitoramento,

como celulares, tablets ou computadores de profissionais de saúde. Esse processo utiliza AES 128 bits, garantindo que cada dispositivo só possa acessar as informações com a chave criptográfica correta. Adicionalmente, a comunicação entre o servidor e os dispositivos pode considerar os protocolos já estabelecidos pelos serviços de nuvem, como, por exemplo, a Amazon AWS que utiliza o SSL/TLS, No contexto da AWS, o TLS pode ser aplicado de várias maneiras para proteger a comunicação.

Esse sistema mantém a privacidade do paciente enquanto permite uma análise ágil e contínua dos sinais vitais, possibilitando a resposta imediata a qualquer situação crítica, conforme as normativas de proteção de dados, como a LGPD e GDPR. Com isso, além de garantir a segurança e a privacidade, ele oferece confiabilidade e eficiência no monitoramento de saúde em tempo real [5].

5 Conclusão

A segurança e a privacidade dos dados são elementos essenciais em sistemas de monitoramento remoto de saúde, especialmente com o crescimento do uso de dispositivos de IoT para coleta e transmissão de informações sensíveis. Neste trabalho, foi proposta uma arquitetura de criptografia para o sistema um sistema de monitoramento de sinais vitais, para proteger os dados dos pacientes em todas as etapas do fluxo de comunicação, desde a coleta inicial até o armazenamento final.

A proposta utiliza o algoritmo de criptografia simétrica AES. A estrutura modular do sistema, organizada em etapas de coleta de sinais, gerenciamento de dados, armazenamento seguro e monitoramento, garante a confidencialidade e integridade dos dados ao longo de todo o processo. Esse modelo também permite a implementação de controle de acesso e autenticação multifator, garantindo que apenas usuários autorizados acessem informações sensíveis, conforme regulamentações nacionais.

Para trabalhos futuros será possível a implementação total do sistema proposto considerando diferentes dispositivos criados e considerar a utilização de algoritmos assimétricos ou algoritmos estado-da-arte. Isso permitirá uma avaliação e validação da proposta.

Declarações complementares

Financiamento

Os autores gostariam de agradecer a Fundação de amparo à pesquisa do estado do Rio Grande do Sul - FAPERGRS (24/2551-0001396-2, 23/2551-0000773-8), Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq com FAPERGS/CNPq (23/2551-0000126-8).

Outras informações relevantes

Este trabalho fez uso de ferramentas de IA generativa na revisão de escrita do artigo.

Referências

1 Rajpoot, N. K. *et al. The Future of Healthcare: A Machine Learning Revolution*. v. 1. 2023. P. 1–6. DOI: 10.1109/ICAIIHI57871.2023.10489320.

2 Stallings, W. *Cryptography and Network Security: Principles and Practice*. Pearson, 2018.

3 Daemen, J.; Rijmen, V. *The Design of Rijndael: AES–The Advanced Encryption Standard*. Springer Science & Business Media, 2002.

4 Dalmazo, B. L.; Vilela, J. P.; Curado, M. Performance analysis of network traffic predictors in the cloud. *Journal of Network and Systems Management*, Springer, v. 25, p. 290–320, 2017.

5 Lucena, R. A Lei Geral de Proteção de Dados e sua Aplicação em Tecnologias de Saúde. *Revista Brasileira de Direito Digital*, v. 4, p. 22–35, 2022.

6 Menezes, A. J.; Vanstone, S. A.; Oorschot, P. C. *Handbook of Applied Cryptography*. CRC Press, 1996.

7 Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*. Chapman e Hall/CRC, 2014.

8 Moerel, L. The long arm of EU data protection law: Does the data protection directive apply to processing of personal data of EU citizens by websites worldwide? *International Data Privacy Law*, Oxford University Press, v. 3, n. 4, p. 221–235, 2014.

9 Amir Alkodri, A. *et al.* Use of the Advanced Encryption Standard Algorithm for Encryption Short Message Service on Real Count Applications, p. 1–6, 2020. DOI: 10.1109/CITSM50537.2020.9268868.

10 Sutradhar, S. *et al.* A blockchain privacy-conserving framework for secure medical data transmission in the internet of medical things. *Decision Analytics Journal*, v. 10, p. 100419, 2024. ISSN 2772-6622. DOI: https://doi.org/10.1016/j.dajour.2024.100419. Disponível em: https://www.sciencedirect.com/science/article/pii/S2772662224000237.

11 Radhakrishnan, I.; Jadon, S.; Honnavalli, P. B. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. *Sensors*, v. 24, n. 12, 2024. ISSN 1424-8220. DOI: 10.3390/s24124008. Disponível em: https://www.mdpi.com/1424-8220/24/12/4008.

12 Merlanti, D.; Mazzini, G. Massey Omura multiple users key distribution. *In*: IEEE. SOFTCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks. 2011. P. 1–5.