



VIII Congresso Científico
Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

IMPLEMENTAÇÃO DE UM BACKEND SEGURO E OTIMIZADO PARA SISTEMAS DE TELEMEDICINA

Área temática: Tecnologia e Saúde

*Arthur Magalhães Ribeiro, Osmarindo Ferreira de Borba Neto, Felipe Ramos Ribeiro,
Walter Rodrigues de Andrade*

DOI: 10.47224/revistamaster.v10i20.789

Resumo

O avanço das tecnologias digitais permitiu a consolidação da telemedicina como uma ferramenta essencial para ampliar o acesso à saúde em contextos diversos, especialmente em regiões com baixa cobertura médica. A adoção de soluções remotas para consultas, diagnósticos e monitoramento exige, no entanto, a implementação de sistemas robustos de backend que assegurem a integridade, confidencialidade e disponibilidade dos dados dos pacientes. Este trabalho apresenta o desenvolvimento e a implementação de um backend seguro e otimizado para uma aplicação de telemedicina, com foco em segurança da informação e eficiência no desempenho. O sistema foi desenvolvido utilizando a linguagem JavaScript com Node.js e o framework Express, organizando a arquitetura de forma modular. O banco de dados escolhido foi o MongoDB, e o controle de acesso foi implementado por meio de autenticação JWT (JSON Web Token) e criptografia de senhas com bcrypt. Foram definidos esquemas específicos para usuários e pacientes, e as rotas da API REST foram protegidas com middlewares que verificam os tokens de autenticação. A revisão da literatura evidenciou os principais desafios de segurança enfrentados por sistemas de telemedicina, incluindo a proteção dos dados em trânsito e em repouso (MOTTA et al., 2001), conformidade com legislações como LGPD e HIPAA, além de práticas recomendadas como controle de acesso baseado em atributos (ABAC) e autenticação via OAuth 2.0. Os testes realizados com o Postman simularam cenários de registro, login e operações sobre os dados de pacientes, demonstrando que as medidas implementadas garantem a segurança e o controle de acesso esperado (QUEIROZ et al., 2021). O backend se mostrou funcional ao registrar novos usuários com senhas criptografadas, permitir login e emissão de tokens válidos, cadastrar pacientes e listar seus dados apenas para usuários autenticados. Os resultados confirmam a viabilidade da proposta e



VIII Congresso Científico Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

apontam que a combinação de boas práticas de segurança com uma estrutura modular e escalável oferece um caminho eficaz para a construção de sistemas de telemedicina confiáveis. O estudo conclui que, além da aplicação prática bem-sucedida, o projeto fornece uma base para melhorias futuras, como controle de acesso baseado em papéis (RBAC), criptografia de dados em repouso, registro de acessos sensíveis e integração de soluções com blockchain para rastreabilidade e integridade dos dados médicos (SANTOS et al., 2023). A pesquisa demonstra que, mesmo utilizando tecnologias de código aberto, é possível atingir altos níveis de segurança e desempenho, contribuindo para o desenvolvimento de soluções em saúde digital que atendam às demandas crescentes por serviços remotos, transparentes e seguros.

Palavras-chave: Telemedicina; Backend; Segurança da Informação; API REST; JWT.

Abstract: The advancement of digital technologies has enabled the consolidation of telemedicine as an essential tool to expand access to healthcare, especially in underserved areas. However, the success of such systems depends directly on the robustness and security of the backend infrastructure that supports these applications. This study presents the development and implementation of a secure and optimized backend for a telemedicine application, focusing on data protection and system performance. The backend was built using Node.js with the Express framework, and the database used was MongoDB. The architecture followed a modular design pattern, with user and patient data schemas, secure route definitions, and token-based authentication using JWT. Passwords were hashed using bcrypt. A literature review highlighted key security challenges such as data protection in transit and at rest, and compliance with LGPD and HIPAA. Best practices such as ABAC, OAuth 2.0, and end-to-end encryption were also discussed. Functional tests using Postman confirmed the successful implementation of all core features, including user registration, login, patient creation, and restricted access to sensitive data. The results show the feasibility of building a secure backend using open-source technologies and suggest future improvements such as RBAC, encrypted data storage, audit trails, and the adoption of blockchain for immutable medical records. The solution contributes to the growing need for trustworthy and efficient digital health systems.

Keywords: Telemedicine; Backend; Information Security; REST API; JWT.

Afiliações:

[1] Graduando em Análise e Desenvolvimento de Sistemas; Centro Universitário IMEPAC Araguari; arthur.ribeiro@aluno.imepac.edu.br

[2] Graduando em Análise e Desenvolvimento de Sistemas; Centro Universitário IMEPAC Araguari; osmarindo.neto@aluno.imepac.edu.br

[3] Graduando em Análise e Desenvolvimento de Sistemas; Centro Universitário IMEPAC Araguari; felipe.ribeiro@aluno.imepac.edu.br

1 INTRODUÇÃO



VIII Congresso Científico Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

A telemedicina representa uma revolução na forma como os serviços de saúde são prestados, permitindo a realização de consultas, diagnósticos e monitoramento remoto. Essa transformação tecnológica se mostrou especialmente relevante durante e após a pandemia de COVID-19, quando o distanciamento social exigiu soluções inovadoras para manter a assistência médica. No entanto, a adoção dessas tecnologias exige atenção especial à segurança da informação, principalmente devido à sensibilidade dos dados envolvidos. A literatura aponta desafios importantes como o controle de acesso, proteção dos dados em trânsito e em repouso, e conformidade com legislações como a LGPD e a HIPAA. Este trabalho se propõe a apresentar o desenvolvimento e a implementação de um backend seguro e otimizado, aplicável a sistemas de telemedicina, com foco na proteção dos dados dos pacientes e no desempenho eficiente da aplicação.

2 METODOLOGIA

O backend foi desenvolvido utilizando a linguagem JavaScript com Node.js e o framework Express, aplicando o padrão arquitetural REST. O banco de dados utilizado foi o MongoDB, devido à sua flexibilidade na manipulação de documentos em formato JSON. A arquitetura foi dividida em módulos (Models, Routes, Controllers e Middlewares), facilitando a manutenção e escalabilidade do sistema. A autenticação foi implementada por meio de JWT (JSON Web Token) e as senhas foram armazenadas com criptografia via bcrypt. Os testes de funcionalidade foram realizados com a ferramenta Postman, simulando operações de registro, login, cadastro e listagem de pacientes.

3 RESULTADOS E DISCUSSÃO

O sistema backend demonstrou funcionamento pleno das funcionalidades propostas. O registro de novos usuários foi executado com sucesso, e as senhas foram devidamente criptografadas.



VIII Congresso Científico Internacional IMEPAC

Inteligência Artificial:
Desafios e Oportunidades.

O login permitiu a emissão de tokens JWT válidos, que foram utilizados na autenticação das rotas protegidas. A criação e a listagem de pacientes foram testadas com usuários autenticados, confirmando o correto funcionamento das restrições de acesso. As práticas de segurança aplicadas, como a separação de responsabilidades e uso de middlewares, reforçaram a proteção das informações. A estrutura modular adotada favorece a expansão futura do sistema com novas funcionalidades. Em conformidade com a literatura, a aplicação seguiu recomendações modernas como o uso de autenticação forte, criptografia e arquitetura segura. Os resultados indicam que é possível construir soluções de backend seguras e eficientes com ferramentas de código aberto.

4 CONSIDERAÇÕES FINAIS

O desenvolvimento do backend para aplicação de telemedicina atendeu aos objetivos propostos, implementando mecanismos de segurança como autenticação por token, criptografia de senhas e proteção de rotas. Os testes comprovaram o funcionamento correto das funcionalidades e a segurança no tratamento das informações sensíveis. A arquitetura adotada se mostrou eficiente, permitindo manutenção e escalabilidade. Como perspectivas futuras, propõe-se a adoção de controle de acesso baseado em papéis (RBAC), criptografia dos dados em repouso, logging de acessos sensíveis e integração com blockchain para garantir a imutabilidade dos registros médicos.

5 REFERÊNCIAS

MOTTA, G. H.; FURUIE, S. S.; NARDON, F. B.; GUTIERREZ, M. A.; YAMAGUTI, M. Autorização e Controle de Acesso para o Prontuário Eletrônico do Paciente em Ambientes Abertos e Distribuídos: Uma Proposta de Modelo e Arquitetura. *Anais do I Workshop em Segurança de Sistemas Computacionais (WSeg 2001)*, Florianópolis, p. 92-97, 2001. Disponível em: <<https://sol.sbc.org.br/index.php/sbseg/article/view/21291>>. Acesso em: 11 maio 2025.

QUEIROZ, Carlos Felipe; CONCEIÇÃO, Lucas Maués Calandrine; BARRETO, Marcos Vinicius Casais. Estudo dos aspectos para a disponibilização de dados locais na nuvem: estudo de caso NetDoctor. *RECIMA21 - Revista Científica Multidisciplinar*, [S. l.], v. 2, n. 3, p. 45-50, 2021. Disponível em: <<https://recima21.com.br/index.php/recima21/article/view/474>>. Acesso em: 11 maio 2025.



**VIII Congresso Científico
Internacional IMEPAC**

Inteligência Artificial:
Desafios e Oportunidades.

SANTOS, Yago de R. dos; REIS, L. H. A.; BARBOSA, G. N. N.; OLIVEIRA, N.; MENDES, A. C.; VALLE, R.; MEDEIROS, D. S. V.; MATTOS, D. M. F. SmartMed: uma ferramenta de controle de acesso a dados de saúde baseado em contratos inteligentes. In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS – SBSEG ESTENDIDO, 23., 2023, Porto Alegre. *Anais Estendidos do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais – SBSEG Estendido 2023*. Porto Alegre: SBC, 2023. p. 65–72. Disponível em: https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/27274. Acesso em: 11 maio 2025.