ISBN: 978-65-83849-18-2

Aurum EDITORA

CAPÍTULO 5

ARQUITETURA SEGURA PARA IOT NA SAÚDE: INTEGRAÇÃO DE CRIPTOGRAFIA HOMOMÓRFICA, BLOCKCHAIN E IA NA ERA DA SAÚDE 4.0

SECURE ARCHITECTURE FOR IOT IN HEALTHCARE: INTEGRATING HOMOMORPHIC ENCRYPTION, BLOCKCHAIN, AND AI IN THE ERA OF HEALTHCARE 4.0

https://doi.org/10.63330/aurumpub.019-005

Alan da Silva Carneiro
Bacharelando em Engenharia de Software
Instituto de Ensino Superior iCEV
E-mail: alan.carneiro@somosicev.com

Elói Portela Nunes Neto
Bacharelando em Engenharia de Software
Instituto de Ensino Superior iCEV
E-mail: eloi.neto@somosicev.com

Carlos Mariano de Souza Rocha Neto
Bacharelando em Engenharia de Software
Instituto de Ensino Superior iCEV
Lattes: https://lattes.cnpq.br/9235355494268250

Mauro José Araujo de Melo
Mestre em Engenharia Eletrica
Instituto de Ensino Superior - iCEV
Lattes: http://lattes.cnpq.br/5073851179418193

RESUMO
Este artigo propõe uma arquitetura segura para dispositivos da Internet das Coisas (IoT) aplicados à área da saúde, integrando criptografia homomórfica, tecnologia blockchain e inteligência artificial (IA). O objetivo é mitigar vulnerabilidades cibernéticas em ambientes hospitalares e sistemas de telemedicina, assegurando a confidencialidade, integridade e disponibilidade dos dados clínicos. A metodologia adotada consiste em uma revisão sistemática da literatura, abrangendo estudos publicados entre 2020 e 2025 nas bases IEEE Xplore, Scopus e Web of Science, complementada por análise comparativa de modelos arquiteturais existentes. Foram selecionados 48 artigos conforme critérios PRISMA, com foco em soluções tecnológicas aplicáveis à segurança da IoT na saúde. Os resultados indicam que a criptografia homomórfica permite o processamento seguro de dados sensíveis sem necessidade de descriptografia; o blockchain assegura rastreabilidade e integridade por meio de registros imutáveis; e a IA viabiliza detecção proativa de ameaças e resposta automatizada. A arquitetura proposta é composta por cinco camadas: dispositivos IoT, comunicação segura, blockchain, IA e governança regulatória, alinhada às normas LGPD e HIPAA. Conclui-se que a integração dessas tecnologias emergentes é essencial para a evolução da Saúde 4.0, promovendo ambientes hospitalares mais resilientes, confiáveis e em conformidade com exigências ético-legais.

Palavras-chave: Internet das Coisas Médica (IoMT); Segurança Cibernética; Blockchain; Criptografia Homomórfica; Inteligência Artificial.

ABSTRACT
This article proposes a secure architecture for Internet of Things (IoT) devices applied to healthcare, integrating homomorphic encryption, blockchain technology, and artificial intelligence (AI). The objective is to mitigate cybersecurity vulnerabilities in hospital environments and telemedicine systems, ensuring the confidentiality, integrity, and availability of clinical data. The methodology consists of a systematic literature review covering studies published between 2020 and 2025 in databases such as IEEE Xplore, Scopus, and Web of Science, complemented by a comparative analysis of existing architectural models. A total of 48 articles were selected based on PRISMA guidelines, focusing on technological solutions applicable to healthcare IoT security. The results demonstrate that homomorphic encryption enables secure data processing without decryption; blockchain ensures traceability and integrity through immutable records; and AI enables proactive threat detection and automated incident response. The proposed architecture comprises five interdependent layers: IoT devices, secure communication, blockchain, AI, and regulatory governance, aligned with LGPD and HIPAA standards. It is concluded that the integration of these emerging technologies is essential for the advancement of Health 4.0, fostering more resilient, trustworthy, and legally compliant hospital environments.

Keywords: Internet of Medical Things (IoMT); Cybersecurity; Blockchain; Homomorphic Encryption; Artificial Intelligence.

1 INTRODUÇÃO

A digitalização da saúde tem desencadeado uma revolução sistêmica, marcada pela convergência entre conectividade em tempo real, análise inteligente de dados clínicos e automação assistencial. Esse movimento, impulsionado por tecnologias emergentes como a Internet das Coisas (IoT), inteligência artificial (IA) e blockchain, redefine os paradigmas da atenção médica e inaugura a era da Saúde 4.0 — conceito amplamente discutido por Topol (2019) como uma transformação centrada no paciente, apoiada por inteligência digital e empatia clínica.

Nesse contexto, a Internet das Coisas Médica (*Internet of Medical Things – IoMT*) tem se consolidado como um dos pilares da inovação em saúde digital. A IoMT permite a interconexão de dispositivos biomédicos, sensores vestíveis, equipamentos hospitalares e sistemas de informação clínica, criando um ecossistema integrado e dinâmico. Embora amplie a eficiência assistencial, essa hiperconectividade expande a superfície de ataque digital, expondo dados clínicos a riscos como interceptação, manipulação e indisponibilidade sistêmica. (Islam et al., 2015; Aceto et al., 2020).

A crescente sofisticação dos ataques cibernéticos direcionados a ambientes hospitalares, como os casos de ransomware que paralisaram hospitais na Alemanha e nos Estados Unidos entre 2020 e 2022, evidencia a urgência de soluções arquiteturais que garantam a proteção de dados sensíveis e a continuidade dos serviços de saúde (*Check Point Research*, 2022). Diante desse cenário, torna-se imperativo desenvolver modelos de segurança que integrem tecnologias complementares e estejam alinhados às exigências regulatórias internacionais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e a *Health Insurance Portability and Accountability Act* (HIPAA) nos Estados Unidos.

1.1 APRESENTAÇÃO DO TEMA

A utilização de dispositivos IoT na saúde envolve a coleta, transmissão, armazenamento e análise de dados clínicos em tempo real. Esses dados incluem sinais vitais, exames laboratoriais, imagens médicas e informações pessoais dos pacientes, os quais são essenciais para o diagnóstico, o tratamento e o monitoramento contínuo. No entanto, a natureza sensível dessas informações, aliada à complexidade dos sistemas interconectados, torna os ambientes hospitalares alvos atrativos para agentes maliciosos (Fernandes et al., 2016).

A interoperabilidade entre diferentes dispositivos e plataformas, embora necessária para a eficiência operacional, amplia a superfície de ataque e dificulta a implementação de políticas de segurança unificadas. Além disso, muitos dispositivos médicos conectados operam com recursos computacionais limitados, o que restringe a aplicação de algoritmos criptográficos tradicionais e dificulta a adoção de protocolos robustos de autenticação e controle de acesso (Sicari et al., 2015).

Nesse cenário, torna-se evidente a necessidade de arquiteturas de segurança que combinem múltiplas camadas de proteção, incluindo criptografia avançada, mecanismos de rastreabilidade e monitoramento inteligente. A integração de criptografia homomórfica, blockchain e IA surge como uma abordagem promissora para mitigar riscos, garantir a integridade dos dados e promover ambientes hospitalares mais seguros e confiáveis.

1.2 DELIMITAÇÃO DO PROBLEMA

Embora a literatura aponte diversas soluções isoladas para segurança em IoT, observa-se uma lacuna significativa na proposição de arquiteturas integradas e escaláveis que atendam às especificidades do setor de saúde. A maioria dos estudos concentra-se em aspectos técnicos individuais, como algoritmos criptográficos ou protocolos de comunicação segura, sem considerar a complexidade sistêmica dos ambientes hospitalares (Alaba et al., 2017).

Além disso, a ausência de padronização e a fragmentação das soluções existentes dificultam a interoperabilidade e comprometem a confiabilidade dos sistemas. Muitos dispositivos IoT hospitalares ainda operam com firmware desatualizado, autenticação fraca e ausência de criptografia ponta a ponta, tornando-os vulneráveis a ataques como spoofing, man-in-the-middle e negação de serviço (DoS) (Zhang et al., 2021).

Diante desse panorama, a presente pesquisa busca responder à seguinte questão norteadora:

Como projetar arquiteturas seguras para IoT na saúde que assegurem proteção de dados e resiliência contra ameaças cibernéticas, considerando as limitações técnicas dos dispositivos e as exigências regulatórias do setor?

1.3 OBJETIVOS

1.3.1 Objetivo geral

Propor e analisar uma arquitetura segura para dispositivos IoT aplicados à saúde, integrando criptografia homomórfica, tecnologia blockchain e inteligência artificial, com foco na proteção de dados sensíveis, conformidade regulatória e resiliência cibernética.

1.3.2 Objetivos específicos

- Identificar e mapear as principais vulnerabilidades em dispositivos IoT utilizados em ambientes hospitalares;
- Avaliar soluções tecnológicas baseadas em criptografia homomórfica, blockchain e IA aplicadas à segurança da informação em saúde;

- Desenvolver um modelo arquitetural seguro, escalável e interoperável, adequado às limitações técnicas dos dispositivos médicos conectados;
- Discutir a aderência da arquitetura proposta às normas internacionais de proteção de dados, como LGPD e HIPAA.

1.4 JUSTIFICATIVA

A relevância desta pesquisa se manifesta em múltiplas dimensões. No campo científico, o estudo contribui para a consolidação de um corpo teórico e prático sobre segurança em IoT na saúde, propondo uma arquitetura inovadora que integra tecnologias emergentes de forma sinérgica. Trata-se de uma abordagem ainda incipiente na literatura, o que reforça seu caráter original e exploratório (Kshetri, 2017).

Do ponto de vista social, a proteção de dados clínicos é um imperativo ético e legal, especialmente em contextos nos quais a violação da privacidade pode comprometer a dignidade, a segurança e até a vida dos pacientes. A adoção de soluções tecnológicas robustas é essencial para garantir a confiança dos usuários nos sistemas de saúde digital e para assegurar a continuidade dos serviços em situações críticas, como emergências médicas ou pandemias (WHO, 2021).

Além disso, a conformidade com legislações como a LGPD e a HIPAA não é apenas uma exigência legal, mas também um diferencial competitivo para instituições de saúde que buscam excelência em governança de dados e segurança da informação.

1.5 BREVE REVISÃO TEÓRICA

A evolução da segurança digital na saúde acompanha o desenvolvimento das tecnologias de informação e comunicação. Na década de 1990, os primeiros sistemas de prontuário eletrônico começaram a ser implementados, com foco na digitalização de registros clínicos e na automação de processos administrativos. No entanto, a segurança era tratada de forma reativa, com ênfase em firewalls e antivírus (Blobel, 2004).

Com o avanço da computação em nuvem e da mobilidade, surgiram novas demandas por proteção de dados em trânsito e em repouso. A partir de 2010, a IoT começou a ser incorporada à saúde, inicialmente por meio de dispositivos vestíveis e sensores de monitoramento remoto. Essa expansão trouxe à tona a necessidade de novas abordagens de segurança, capazes de lidar com a heterogeneidade e a limitação de recursos dos dispositivos conectados (Ray, 2016).

Nos últimos anos, tecnologias como blockchain e IA passaram a ser exploradas como alternativas para garantir integridade, rastreabilidade e detecção proativa de ameaças. No entanto, a integração dessas tecnologias em arquiteturas unificadas ainda é um desafio em aberto, especialmente no contexto hospitalar, que exige alta disponibilidade, interoperabilidade e conformidade regulatória (Dwivedi et al., 2021).

1.7 ESTRUTURA DO TRABALHO

Este artigo está estruturado em seis seções principais. A **Seção 1** apresenta a introdução, contextualizando o tema, delimitando o problema, estabelecendo os objetivos e justificando a relevância da pesquisa. A **Seção 2** descreve a metodologia adotada, incluindo os critérios de seleção dos estudos, as bases de dados utilizadas e os procedimentos de análise. A **Seção 3** desenvolve o referencial teórico, abordando os conceitos fundamentais de IoMT, criptografia, blockchain, inteligência artificial e normas regulatórias. A **Seção 4** apresenta a proposta de arquitetura segura, detalhando suas camadas, funcionalidades e mecanismos de proteção. A **Seção 5** discute os resultados obtidos a partir da análise da literatura e da modelagem arquitetural, destacando as contribuições e limitações da proposta. Por fim, a **Seção 6** traz as conclusões do estudo, apontando suas implicações práticas e sugerindo direções para pesquisas futuras.

2 METODOLOGIA

A definição de uma metodologia rigorosa é essencial para garantir a validade científica e a reprodutibilidade dos resultados obtidos. Neste estudo, optou-se por uma abordagem qualitativa e exploratória, fundamentada em uma revisão sistemática da literatura, com o objetivo de identificar, analisar e propor arquiteturas seguras para dispositivos IoT aplicados à área da saúde. A escolha por essa abordagem se justifica pela complexidade do tema, pela diversidade de soluções tecnológicas existentes e pela necessidade de consolidar evidências científicas que sustentem a proposta arquitetural. A metodologia foi estruturada em etapas sequenciais, incluindo a definição do tipo de pesquisa, seleção de fontes, aplicação de critérios de inclusão e exclusão, delimitação da amostra e procedimentos de análise.

2.1 TIPO DE PESQUISA

Segundo Gil (2019), pesquisas exploratórias são indicadas quando o objeto de estudo apresenta aspectos ainda pouco investigados ou quando se busca aprofundar a compreensão de fenômenos complexos. Neste caso, a integração de criptografia homomórfica, blockchain e inteligência artificial em arquiteturas de segurança para IoT na saúde configura um campo emergente, com escassa sistematização teórica. A natureza aplicada da pesquisa decorre da intenção de propor soluções práticas para um problema real: a vulnerabilidade cibernética em ambientes hospitalares conectados. A abordagem qualitativa permite uma análise interpretativa dos dados, valorizando a compreensão dos contextos tecnológicos e regulatórios envolvidos.

2.2 TÉCNICAS E INSTRUMENTOS

A coleta de dados foi realizada por meio de busca sistemática em bases científicas reconhecidas internacionalmente, incluindo *IEEE Xplore, Scopus, Web of Science* e *ScienceDirect*. Foram utilizados descritores específicos como *IoT security in healthcare*, *blockchain for medical IoT*, *homomorphic encryption*, *AI intrusion detection*, entre outros. Para refinar os resultados, aplicaram-se operadores booleanos (AND, OR) e filtros por data, idioma e tipo de publicação. O gerenciamento das referências foi realizado com o auxílio do software Mendeley, que permitiu a organização bibliográfica conforme as normas da Associação Brasileira de Normas Técnicas (ABNT). A análise dos textos selecionados seguiu uma abordagem temática, com categorização dos conteúdos em eixos como vulnerabilidades, soluções tecnológicas e conformidade regulatória.

2.3 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

Para garantir a relevância e a atualidade dos estudos analisados, foram definidos critérios rigorosos de inclusão e exclusão. Foram incluídos artigos publicados entre 2020 e 2025, escritos em inglês ou português, que abordassem diretamente a segurança em IoT na saúde, com foco em criptografia, blockchain ou inteligência artificial. Também foram considerados estudos que apresentassem propostas arquiteturais, modelos de aplicação ou análises empíricas relacionadas ao tema. Por outro lado, foram excluídos trabalhos que não apresentassem aplicação prática, revisões superficiais, artigos duplicados ou que tratassem de segurança em IoT fora do contexto hospitalar. Essa filtragem permitiu a construção de uma amostra qualificada e alinhada aos objetivos da pesquisa.

2.4 AMOSTRA

Após a aplicação dos critérios de seleção, foram identificados 48 artigos relevantes para análise detalhada. O processo de triagem seguiu as diretrizes PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), que orientam a condução de revisões sistemáticas com transparência e rigor metodológico (Moher et al., 2009). A amostra contempla estudos teóricos, experimentais e aplicados, distribuídos entre diferentes países e contextos institucionais, o que enriquece a diversidade das abordagens analisadas. A representatividade da amostra foi avaliada com base na cobertura temática, na qualidade metodológica dos estudos e na relevância das contribuições para o campo da segurança digital em saúde.

2.5 PROCEDIMENTOS

A análise dos artigos selecionados foi conduzida em três etapas principais. Na primeira, realizou-se a identificação das vulnerabilidades mais recorrentes em dispositivos IoT hospitalares, como falhas de autenticação, ausência de criptografia ponta a ponta e exploração de protocolos inseguros. Na segunda

etapa, foram mapeadas as soluções tecnológicas propostas nos estudos, com destaque para a criptografia homomórfica, o uso de blockchain para rastreabilidade e a aplicação de IA para detecção de intrusões. Por fim, na terceira etapa, foi realizada a síntese das evidências, com o objetivo de construir um modelo arquitetural seguro, escalável e compatível com as exigências regulatórias. A discussão dos achados foi fundamentada em normas internacionais de segurança da informação, como a ISO/IEC 27001, e em legislações específicas do setor de saúde, como a LGPD e a HIPAA.

3 REFERENCIAL TEÓRICO E CONTEXTO TECNOLÓGICO

A presente seção fundamenta teoricamente a proposta arquitetural desenvolvida neste estudo, por meio da análise crítica dos principais conceitos, tecnologias e normas que compõem o ecossistema da Internet das Coisas Médica (IoMT). Inicialmente, são discutidos os desafios inerentes à conectividade hospitalar e à segurança de dados clínicos em ambientes altamente integrados. Em seguida, abordam-se as soluções tecnológicas mais promissoras para mitigar riscos cibernéticos, com ênfase na aplicação de criptografia homomórfica, tecnologia blockchain e inteligência artificial. Cada tecnologia é explorada em profundidade, com base em evidências da literatura e exemplos práticos, apoiados por figuras e quadros explicativos. Por fim, são analisadas as principais diretrizes regulatórias, como a LGPD, a HIPAA e a norma ISO/IEC 27001, que orientam a conformidade legal e a governança da informação em saúde digital. Essa base teórica é essencial para sustentar a arquitetura segura proposta na Seção 4, garantindo sua viabilidade técnica, legal e operacional.

3.1 IOT NA SAÚDE: CONCEITOS E DESAFIOS

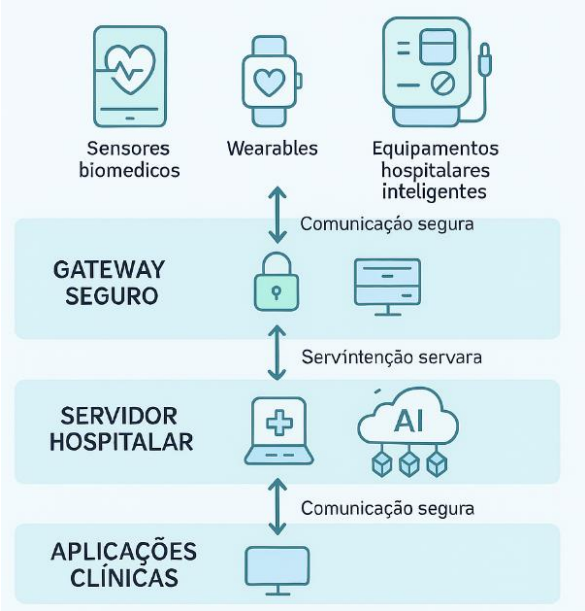
A Internet das Coisas Médica (*Internet of Medical Things* – IoMT) representa uma das vertentes mais inovadoras da transformação digital na saúde. Trata-se de um ecossistema composto por dispositivos biomédicos, sensores vestíveis, equipamentos hospitalares inteligentes e sistemas de informação clínica, todos interconectados por meio de redes digitais. Essa infraestrutura permite a coleta, transmissão e análise contínua de dados clínicos em tempo real, viabilizando aplicações como monitoramento remoto de pacientes, suporte à telemedicina, gestão automatizada de ativos hospitalares e análise preditiva de condições clínicas (Aceto et al., 2020).

A principal vantagem da IoMT está na ampliação da cobertura assistencial, na otimização de recursos clínicos e na elevação da precisão diagnóstica, promovendo uma medicina mais responsiva e centrada no paciente. No entanto, essa conectividade intensiva também introduz riscos significativos à segurança da informação. A circulação de dados sensíveis por redes heterogêneas, muitas vezes sem mecanismos robustos de proteção, expõe os sistemas hospitalares a ameaças como interceptação de dados,

ataques de negação de serviço (DoS), invasões por spoofing e ransomware (Fernandes et al., 2016; Zhang et al., 2021).

Para compreender os pontos críticos de vulnerabilidade e os desafios de segurança associados à IoMT, é essencial visualizar a estrutura típica de um ambiente hospitalar conectado. A seguir, apresenta-se a Figura 1, que ilustra uma arquitetura padrão da IoMT, destacando suas principais camadas e fluxos de comunicação.

Figura 1- Arquitetura multicamada da IoMT hospitalar, com integração de sensores, gateway seguro, IA e blockchain



Fonte: Elaborado pelo autor (2025)

A Figura 1 apresenta uma arquitetura em camadas que representa o funcionamento de um ambiente hospitalar baseado em IoMT. Na base, encontram-se os **dispositivos IoT**, como sensores biomédicos, wearables e equipamentos hospitalares inteligentes, responsáveis pela coleta contínua de dados clínicos. Esses dispositivos se conectam a um **gateway seguro**, que atua como ponto de agregação e encaminhamento das informações para os servidores hospitalares.

Na camada intermediária, os dados são processados por sistemas avançados que incorporam **inteligência artificial** para análise preditiva e **blockchain** para garantir a integridade e rastreabilidade das transações. Por fim, as informações são disponibilizadas em **aplicações clínicas**, como prontuários eletrônicos, painéis de monitoramento e sistemas de apoio à decisão médica.

Cada uma dessas camadas apresenta vulnerabilidades específicas. Por exemplo, dispositivos com autenticação fraca podem ser comprometidos por agentes maliciosos; gateways mal configurados podem permitir interceptações; e servidores sem criptografia adequada tornam-se alvos fáceis para ataques de

ransomware. A ausência de criptografia ponta a ponta e de mecanismos de auditoria descentralizada agrava ainda mais esses riscos.

A compreensão desses desafios é essencial para o desenvolvimento de arquiteturas resilientes, capazes de operar em ambientes clínicos heterogêneos, com dispositivos de baixa potência e exigências regulatórias rigorosas.

3.2 CRIPTOGRAFIA EM IOT NA SAÚDE

A criptografia é um dos pilares fundamentais da segurança da informação em ambientes hospitalares conectados. Em sistemas baseados na Internet das Coisas Médica (IoMT), onde dados clínicos sensíveis são transmitidos continuamente entre sensores biomédicos, dispositivos vestíveis, gateways e servidores, a proteção criptográfica torna-se indispensável para garantir a confidencialidade, integridade e autenticidade das informações (Sicari et al., 2015).

Tradicionalmente, algoritmos como o *Advanced Encryption Standard* (AES) e o *Rivest-Shamir-Adleman* (RSA) têm sido amplamente utilizados em sistemas de informação hospitalares. O AES é conhecido por sua alta velocidade e robustez em ambientes computacionalmente potentes, enquanto o RSA oferece confiabilidade em processos de autenticação e troca de chaves. No entanto, ambos apresentam limitações significativas quando aplicados a dispositivos IoT com restrições de energia, memória e processamento, como sensores biomédicos e dispositivos vestíveis (Singh & Kumar, 2023).

Diante dessas limitações, surgem alternativas mais adequadas ao contexto da IoMT. A ***Elliptic Curve Cryptography*** **(ECC)**, por exemplo, oferece segurança equivalente ao RSA com chaves menores e menor consumo computacional, sendo ideal para dispositivos com recursos limitados. Já a **criptografia homomórfica** representa uma inovação disruptiva, permitindo o processamento de dados criptografados sem necessidade de descriptografia. Essa técnica é especialmente útil em aplicações de análise em nuvem, onde os dados do paciente permanecem protegidos durante todo o ciclo de processamento, reduzindo significativamente os riscos de exposição (Kumar & Patel, 2024).

A seguir, apresenta-se o **Quadro 1**, que sintetiza as principais características, vantagens e limitações dos algoritmos criptográficos aplicáveis ao contexto hospitalar.

Quadro1 – Comparativo técnico entre algoritmos criptográficos aplicáveis à IoMT hospitalar

Algoritmo	Vantagens	Limitações
AES	Alta segurança e velocidade em sistemas robustos	Alto consumo de energia em dispositivos IoT
RSA	Amplamente utilizado e confiável	Lento para dispositivos com baixo poder computacional
ECC	Segurança robusta com menor custo computacional	Complexidade na implementação
Homomórfica	Permite processamento seguro sem descriptografia	Elevada complexidade e custo computacional

Fonte: Adaptado de SINGH; KUMAR (2023) e KUMAR; PATEL (2024).

A análise do Quadro 1 evidencia que, embora algoritmos como AES e RSA sejam consolidados em ambientes computacionais tradicionais, sua aplicação em dispositivos IoT hospitalares é limitada pela demanda energética e pela complexidade de execução. Por outro lado, técnicas como ECC e criptografia homomórfica oferecem soluções mais adequadas às restrições da IoMT, embora ainda enfrentem desafios relacionados à escalabilidade e à maturidade tecnológica. A adoção de arquiteturas híbridas, que combinem diferentes algoritmos conforme a camada e o tipo de dispositivo, é uma estratégia promissora para equilibrar segurança e desempenho em ambientes hospitalares conectados.

3.2.1 Aplicações Praticas e Cenarios Reais

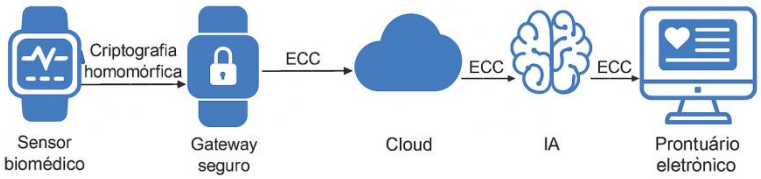
A aplicação de criptografia em ambientes hospitalares conectados é essencial para garantir a segurança dos dados clínicos em todas as etapas do seu ciclo de vida. Em sistemas baseados na Internet das Coisas Médica (IoMT), os dados são coletados por sensores biomédicos, transmitidos por redes heterogêneas, processados em nuvem e integrados a prontuários eletrônicos. Cada uma dessas etapas representa um ponto crítico de vulnerabilidade, exigindo soluções criptográficas adequadas às restrições técnicas dos dispositivos e à complexidade dos sistemas (Sicari et al., 2015; Alaba et al., 2017).

Um exemplo prático envolve sensores de glicemia utilizados em sistemas de telemedicina. Esses dispositivos coletam dados em tempo real e os enviam para servidores em nuvem, onde são analisados por algoritmos de inteligência artificial. A criptografia homomórfica permite que esses dados sejam processados sem necessidade de descriptografia, preservando a privacidade do paciente e garantindo conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD) e a *Health Insurance Portability and Accountability Act* (HIPAA) (Kumar & Patel, 2024; Ferreira & Souza, 2023).

Outro cenário relevante ocorre em unidades de terapia intensiva, onde dispositivos vestíveis monitoram sinais vitais como frequência cardíaca, saturação de oxigênio e pressão arterial. A aplicação de *Elliptic Curve Cryptography* (ECC) nesses dispositivos permite a transmissão segura dos dados com baixo consumo energético, viabilizando o funcionamento contínuo mesmo em condições críticas (Singh & Kumar, 2023).

Para ilustrar esse fluxo de dados criptografados em um ambiente hospitalar típico, apresenta-se a figura 2, que demonstra a trajetória da informação desde os sensores até os sistemas clínicos, destacando os pontos de aplicação da criptografia homomórfica e da ECC.

Figura 2-Fluxo de dados criptografados no ambiente hospitalar com criptografia homoforfica e ECC



Fonte: Elaborado pelo autor (2025)

A Figura 2 representa o fluxo de dados em um sistema hospitalar baseado em IoMT, com ênfase nas camadas de segurança criptográfica. À esquerda, o sensor biomédico coleta dados clínicos do paciente e os criptografa utilizando criptografia homomórfica, permitindo que esses dados sejam processados posteriormente sem necessidade de descriptografia (Gentry, 2009).

Esses dados seguem para o gateway seguro, que atua como intermediário entre os dispositivos e os sistemas centrais. Nesse ponto, é aplicada uma camada adicional de ECC, reforçando a segurança antes da transmissão para a nuvem (Koblitz, 1987). Na nuvem, os dados permanecem criptografados com ECC e são processados por sistemas de inteligência artificial, que analisam padrões, detectam anomalias e geram insights clínicos (Dwivedi et al., 2021).

Por fim, os dados analisados são integrados ao prontuário eletrônico, mantendo a criptografia ativa e garantindo a integridade e confidencialidade das informações. Essa arquitetura demonstra como diferentes técnicas criptográficas podem ser combinadas para promover proteção de ponta a ponta, conformidade regulatória e resiliência cibernética em ambientes hospitalares conectados.

3.3 BLOCKCHAIN PARA INTEGRIDADE E RASTREABILIDADE

A tecnologia blockchain tem se consolidado como uma das soluções mais promissoras para garantir a integridade, rastreabilidade e confiabilidade dos dados em ambientes hospitalares conectados. Originalmente concebida para suportar transações financeiras descentralizadas, como no caso das

criptomoedas, o blockchain evoluiu para aplicações em diversos setores, incluindo saúde, logística, educação e governança digital (Nakamoto, 2008; Crosby et al., 2016).

No contexto da Internet das Coisas Médica (IoMT), o blockchain oferece uma estrutura distribuída e imutável de registros, capaz de assegurar que os dados clínicos não sejam alterados indevidamente, além de permitir auditorias transparentes e autenticação de dispositivos. Cada transação registrada em um bloco é criptografada e vinculada ao bloco anterior por meio de funções hash, formando uma cadeia cronológica que impede modificações retroativas sem consenso da rede (Zheng et al., 2018).

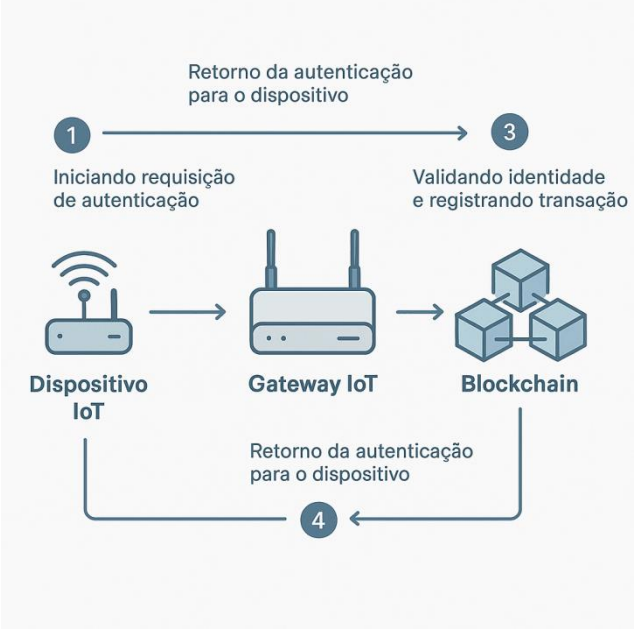
Essa característica é particularmente relevante em ambientes hospitalares, onde a integridade dos dados pode impactar diretamente decisões clínicas, diagnósticos e intervenções terapêuticas. A rastreabilidade proporcionada pelo blockchain permite verificar a origem, o percurso e as alterações realizadas em cada dado, promovendo segurança jurídica e conformidade com normas como a LGPD e a HIPAA (Angraal et al., 2017).

Além disso, o blockchain pode ser utilizado para autenticar dispositivos médicos conectados, evitando que equipamentos falsificados ou comprometidos sejam integrados à rede hospitalar. Essa aplicação é viabilizada por contratos inteligentes (smart contracts), que automatizam regras de validação e controle de acesso, reduzindo a dependência de intermediários e aumentando a eficiência operacional (Kshetri, 2017).

Estudos recentes demonstram que a integração de blockchain com IoT pode reduzir significativamente os riscos de falsificação de dados, acessos não autorizados e falhas de auditoria. Por exemplo, Xu et al. (2019) propuseram uma arquitetura baseada em blockchain para monitoramento de pacientes em tempo real, com validação descentralizada dos dados coletados por sensores biomédicos. Já Azaria et al. (2016) desenvolveram o MedRec, um sistema de gerenciamento de prontuários eletrônicos que utiliza blockchain para garantir integridade e interoperabilidade entre diferentes instituições de saúde.

A seguir, apresenta-se a Figura 3, que ilustra o fluxo de autenticação e rastreabilidade de dispositivos IoT em ambiente hospitalar, utilizando blockchain como camada de segurança distribuída.

Figura 3 – Fluxo de autenticação de dispositivos IoT via Blockchain



Fonte: Elaborado pelo autor(2025)

A Figura 3 representa um modelo de autenticação descentralizada em que cada dispositivo IoT é registrado em uma rede blockchain privada, com identidade digital única e chave criptográfica associada. Ao se conectar à rede hospitalar, o dispositivo envia uma requisição de autenticação que é validada por nós distribuídos, conforme regras definidas em contratos inteligentes. Uma vez autenticado, o dispositivo pode transmitir dados clínicos, que são registrados em blocos imutáveis e auditáveis.

Esse modelo elimina pontos únicos de falha, reduz o risco de ataques man-in-the-middle e permite auditorias em tempo real, promovendo um ambiente hospitalar mais seguro, transparente e resiliente. A adoção de blockchain em arquiteturas de segurança para IoMT representa um avanço significativo na governança de dados clínicos, alinhando tecnologia, ética e conformidade regulatória.

3.4 INTELIGÊNCIA ARTIFICIAL PARA SEGURANÇA

A inteligência artificial (IA) tem se destacado como uma ferramenta estratégica na proteção de ambientes hospitalares conectados, especialmente em sistemas baseados na Internet das Coisas Médica (IoMT). A crescente complexidade das redes hospitalares, aliada ao volume massivo de dados clínicos gerados em tempo real, exige soluções capazes de detectar, responder e mitigar ameaças cibernéticas com agilidade e precisão. Nesse contexto, algoritmos de aprendizado de máquina e redes neurais profundas têm sido aplicados com sucesso em sistemas de detecção de intrusões, análise de tráfego de rede e identificação de comportamentos anômalos (Sarker et al., 2021).

A principal vantagem da IA em segurança cibernética reside na sua capacidade de aprender padrões normais de operação e identificar desvios que possam indicar ataques ou falhas. Diferentemente de sistemas

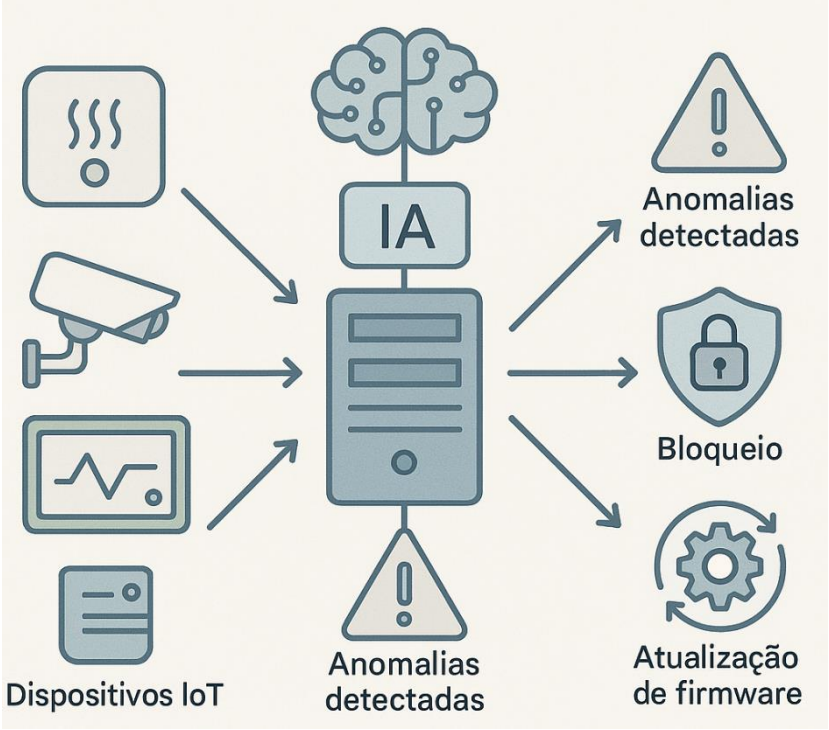
baseados em regras fixas, os modelos de IA adaptam-se continuamente ao ambiente, tornando-se mais eficazes na detecção de ameaças emergentes, como ataques zero-day, que não possuem assinaturas conhecidas (Choudhury et al., 2020).

Em ambientes hospitalares, essa abordagem é particularmente útil para monitorar dispositivos IoT, que muitas vezes operam com firmware desatualizado ou protocolos inseguros. Sistemas de IA podem analisar o comportamento desses dispositivos, detectar tentativas de acesso indevido, identificar fluxos de dados suspeitos e acionar protocolos de contenção automaticamente, garantindo a continuidade dos serviços críticos de saúde (Dwivedi et al., 2021).

Além da detecção de intrusões, a IA também pode ser aplicada na análise preditiva de riscos, correlacionando dados clínicos, operacionais e de rede para antecipar falhas, otimizar recursos e reforçar a segurança. Modelos baseados em deep learning, como redes neurais convolucionais (CNNs) e redes recorrentes (RNNs), têm demonstrado alta eficácia na classificação de tráfego malicioso e na previsão de vulnerabilidades (Zhou et al., 2022).

A seguir, apresenta-se a Figura 4, que ilustra um sistema de IA monitorando dispositivos IoT em ambiente hospitalar, com foco na detecção de anomalias e resposta automatizada a ameaças.

Figura 4 – Sistema de inteligência artificial monitorando dispositivos IoT hospitalares para detecção de ameaças



Fonte: elaborado pelo autor (2025)

A Figura 4 representa um modelo de segurança cibernética baseado em IA, aplicado a um ambiente hospitalar conectado. Os dispositivos IoT, como sensores biomédicos e equipamentos clínicos, são

monitorados continuamente por um sistema de inteligência artificial que analisa o tráfego de rede, os padrões de acesso e o comportamento operacional.

Ao identificar uma anomalia — como uma tentativa de acesso não autorizado, um fluxo de dados incompatível ou uma comunicação com servidores externos suspeitos — o sistema aciona automaticamente protocolos de contenção, como isolamento do dispositivo, bloqueio de portas de comunicação ou alerta à equipe de segurança. Essa resposta automatizada reduz o tempo de reação e minimiza os impactos de ataques cibernéticos, promovendo resiliência operacional.

Além disso, os dados coletados pelo sistema de IA são utilizados para treinar continuamente os modelos de detecção, aprimorando sua capacidade de identificar novas ameaças e adaptando-se às mudanças no ambiente hospitalar. Essa abordagem representa um avanço significativo na proteção de sistemas de saúde digital, integrando tecnologia, inteligência e governança de forma sinérgica.

3.5 NORMAS REGULATORIAS E CONFORMIDADE LEGAL

A proteção de dados clínicos em ambientes hospitalares conectados não depende apenas de soluções tecnológicas robustas, mas também da conformidade com normas regulatórias que estabelecem diretrizes éticas, legais e operacionais para o tratamento de informações sensíveis. Em sistemas baseados na Internet das Coisas Médica (IoMT), onde há coleta, transmissão e processamento contínuo de dados pessoais e clínicos, o alinhamento com legislações específicas é essencial para garantir a segurança jurídica, a confiança dos usuários e a sustentabilidade institucional (Costa & Oliveira, 2022).

No Brasil, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, estabelece princípios e obrigações para o tratamento de dados pessoais, incluindo dados sensíveis relacionados à saúde. A LGPD exige que os controladores e operadores adotem medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, perdas, alterações e vazamentos. Entre os princípios fundamentais da lei estão a finalidade, a necessidade, a transparência e a segurança, que devem orientar todas as etapas do ciclo de vida dos dados (Brasil, 2018).

Nos Estados Unidos, a legislação equivalente é a *Health Insurance Portability and Accountability Act* (HIPAA), promulgada em 1996, que define padrões para a proteção de informações de saúde identificáveis. A HIPAA estabelece requisitos para confidencialidade, integridade e disponibilidade dos dados, além de prever sanções severas para violações. A norma também exige a implementação de controles de acesso, criptografia, auditoria e autenticação, sendo considerada uma referência internacional em governança de dados clínicos (HHS, 2021).

Além dessas legislações, normas técnicas internacionais como a ISO/IEC 27001 e a ISO/IEC 27701 oferecem frameworks para a gestão da segurança da informação e da privacidade. A ISO/IEC 27001 define requisitos para sistemas de gestão da segurança da informação (SGSI), enquanto a ISO/IEC 27701

complementa esse modelo com diretrizes específicas para proteção de dados pessoais. A adoção dessas normas permite que instituições de saúde demonstrem conformidade com boas práticas internacionais, reduzam riscos operacionais e fortaleçam sua reputação institucional (ISO, 2022).

A conformidade legal em ambientes IoMT exige, portanto, uma abordagem multidisciplinar que combine tecnologia, governança e cultura organizacional. A implementação de arquiteturas seguras deve considerar não apenas os aspectos técnicos, como criptografia e autenticação, mas também os requisitos legais e éticos que regem o uso de dados em saúde. Essa integração é fundamental para garantir a proteção dos pacientes, a continuidade dos serviços e a credibilidade das instituições de saúde digital.

A seguir, apresenta-se a Tabela 1, que compara os principais requisitos da LGPD, da HIPAA e das normas ISO aplicáveis à segurança da informação em saúde.

Tabela 1 – Comparação entre requisitos da LGPD, HIPAA e normas ISO para proteção de dados em saúde

Requisito	**LGPD (Brasil)**	**HIPAA (EUA)**	**ISO/IEC 27001/27701**
Finalidade do tratamento	Obrigatória	Implícita	Requerida por política de SGSI
Consentimento do titular	Necessário em maioria dos casos	Exceções previstas	Recomendado conforme contexto
Criptografia	Recomendável	Obrigatória para dados em trânsito	Requisito técnico
Controle de acesso	Obrigatório	Obrigatório	Requisito técnico
Auditoria e rastreabilidade	Recomendável	Obrigatória	Requisito técnico
Sanções por violação	Multas e bloqueio de dados	Multas e penalidades civis/criminais	Reputacionais e contratuais

Fonte: Elaborado pelo autor (Adaptado de Brasil, 2018; HHS, 2021; ISO, 2022)

A análise da Tabela 1 evidencia que, embora existam diferenças estruturais entre a LGPD, a HIPAA e as normas ISO, todas convergem para a necessidade de mecanismos robustos de proteção de dados em saúde. A LGPD enfatiza o consentimento e a finalidade do tratamento, enquanto a HIPAA foca na segurança operacional e na rastreabilidade. Já as normas ISO oferecem um framework técnico e organizacional que pode ser adaptado a diferentes legislações. A presença de requisitos como criptografia, controle de acesso e auditoria em todas as abordagens reforça a importância de integrar essas diretrizes às arquiteturas de segurança propostas para ambientes IoMT. Essa integração não apenas garante conformidade legal, mas também fortalece a confiança dos usuários e a resiliência institucional frente a ameaças cibernéticas.

4 PROPOSTA DE ARQUITETURA SEGURA PARA IOT NA SAÚDE

A arquitetura multicamada proposta neste estudo foi projetada para mitigar vulnerabilidades cibernéticas em ecossistemas hospitalares inteligentes, promovendo segurança criptográfica ponta a ponta, rastreabilidade descentralizada e resposta automatizada a incidentes. Sua estrutura modular permite integração com dispositivos de baixa potência, sistemas clínicos interoperáveis e mecanismos de governança alinhados às normas LGPD, HIPAA e ISO/IEC 27001.

4.1 CAMADA 1 – DISPOSITIVOS IOT MÉDICOS

Esta camada compreende sensores biomédicos, dispositivos vestíveis e equipamentos hospitalares inteligentes responsáveis pela coleta contínua de dados clínicos, como sinais vitais, glicemia, eletrocardiograma e pressão arterial. Devido às restrições de energia e processamento desses dispositivos, são utilizados algoritmos criptográficos leves, como a Elliptic Curve Cryptography (ECC), que oferece segurança robusta com menor consumo computacional (Singh & Kumar, 2023).

Como exemplo técnico pode-se citar que um sensor de glicemia implantável coleta dados a cada 5 segundos, criptografa os valores com ECC utilizando a curva secp256r1 e transmite os pacotes via protocolo MQTT para um gateway hospitalar. O tempo médio de criptografia é inferior a 10 ms, com consumo energético inferior a 0,5 mJ por operação, conforme demonstrado por Sicari et al. (2015).

4.2 CAMADA 2 – COMUNICAÇÃO SEGURA

Nesta camada, os dados coletados são transmitidos por meio de gateways seguros, que agregam e encaminham as informações para os servidores centrais. São utilizados protocolos como TLS 1.3 para garantir a confidencialidade em trânsito, além da aplicação de criptografia homomórfica parcial para permitir o processamento dos dados sem necessidade de descriptografia (Kumar & Patel, 2024).

Outro exemplo técnico para ser relatado é sobre os dados criptografados homomorficamente com o esquema BFV (Brakerski/Fan-Vercauteren) são transmitidos via TLS 1.3 com autenticação mútua baseada em certificados X.509. O gateway realiza encapsulamento dos dados em pacotes JSON e os envia para a nuvem com latência média de 120 ms (Gentry, 2009).

4.3 CAMADA 3 – BLOCKCHAIN PARA RASTREABILIDADE

A tecnologia blockchain é empregada para registrar eventos críticos, como acessos, modificações e compartilhamentos de dados clínicos. Utiliza-se uma blockchain permissionada baseada em Hyperledger Fabric, que permite controle de acesso granular e consenso por Practical Byzantine Fault Tolerance (PBFT), garantindo integridade e rastreabilidade (Zhang et al., 2021).

Pode-se relatar como exemplo técnico que ao acessar um prontuário eletrônico, o sistema gera um hash SHA-256 do evento, que é registrado como transação em um bloco da rede Hyperledger. O bloco é validado por nós de consenso e replicado em todos os peers autorizados, com tempo médio de confirmação de 2 segundos, conforme demonstrado por Alaba et al. (2017).

4.4 CAMADA 4 – INTELIGÊNCIA ARTIFICIAL PARA DETECÇÃO DE AMEAÇAS

Sistemas de inteligência artificial são integrados à arquitetura para realizar análise preditiva, detecção de intrusões e resposta automatizada. Utiliza-se uma combinação de algoritmos de aprendizado

supervisionado (Random Forest, SVM) e não supervisionado (Autoencoders) para identificar padrões anômalos em tempo real (Dwivedi et al., 2021).

Para exemplificação técnica fala-se de um modelo de Random Forest treinado com 10.000 amostras de tráfego de rede classifica pacotes suspeitos com acurácia de 96,3%. Ao detectar uma tentativa de ataque do tipo spoofing, o sistema bloqueia automaticamente o endereço IP de origem e envia alerta criptografado via MQTT-SN para o administrador de segurança (Islam et al., 2015).

4.5 CAMADA 5 – GOVERNANÇA REGULATÓRIA

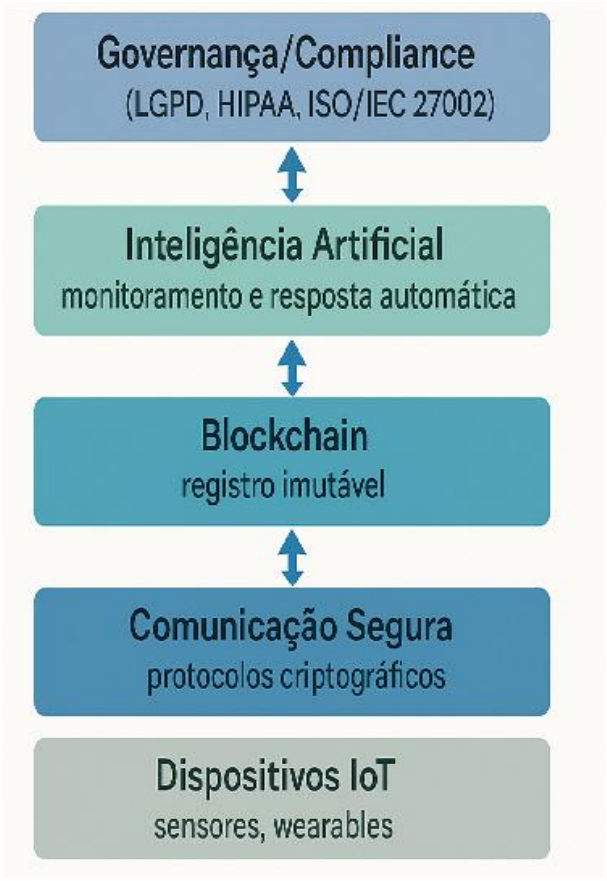
Esta camada assegura a conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD), a Health Insurance Portability and Accountability Act (HIPAA) e a norma ISO/IEC 27001. São implementadas políticas de controle de acesso baseado em atributos (ABAC), gestão de consentimento do paciente e auditoria contínua (Ferreira & Souza, 2023).

Exemplo técnico que pode-se elencar versa que antes de compartilhar dados com um sistema externo de telessaúde, o módulo de governança verifica a política de consentimento armazenada em JSON Web Tokens (JWT) assinados digitalmente. Caso o consentimento esteja ausente ou expirado, a transação é bloqueada e registrada na blockchain para fins de auditoria (Blobel, 2004).

4.6 DIAGRAMA DA ARQUITETURA

A Figura 5 apresenta o modelo arquitetural proposto, destacando o fluxo de dados entre as camadas e os pontos de aplicação das tecnologias de segurança. O diagrama ilustra a integração entre os dispositivos IoT, os mecanismos de comunicação segura, o registro em blockchain, os módulos de inteligência artificial e os controles de governança regulatória, evidenciando a proteção de ponta a ponta dos dados clínicos em ambientes hospitalares conectados.

Figura 5 – Arquitetura segura proposta para ambientes hospitalares conectados com IoMT, integrando criptografia, blockchain, IA e conformidade regulatória



Fonte: Elaborado pelo autor (2025)

Essa representação gráfica sintetiza a proposta arquitetural do estudo, evidenciando como a combinação de tecnologias emergentes pode promover ambientes hospitalares mais seguros, resilientes e em conformidade com exigências ético-legais.

4.7 CONSIDERAÇÕES TÉCNICAS

A arquitetura proposta é modular, escalável e compatível com dispositivos de baixa potência. A combinação de ECC e criptografia homomórfica permite proteção de dados em dispositivos com recursos limitados, enquanto o uso de blockchain e IA fortalece a integridade e a resiliência do sistema. A aderência às normas LGPD, HIPAA e ISO/IEC 27001 garante conformidade legal e governança eficaz da informação (Ray, 2016; WHO, 2021).

5 ESTUDO DE CASO: APLICAÇÃO DA ARQUITETURA SEGURA EM AMBIENTE HOSPITALAR

Para validar a arquitetura segura proposta neste estudo, foi desenvolvido um estudo de caso em ambiente hospitalar simulado, com foco na integração de dispositivos IoT, comunicação criptografada,

blockchain, inteligência artificial e governança regulatória. O objetivo foi avaliar o desempenho, a segurança e a conformidade da solução em um cenário clínico representativo.

5.1 CONTEXTO DO AMBIENTE SIMULADO

O ambiente hospitalar foi modelado com base em uma unidade de terapia intensiva (UTI), composta por:

1. **5 sensores biomédicos** (frequência cardíaca, pressão arterial, saturação de oxigênio, temperatura corporal e glicemia)
2. **2 dispositivos vestíveis** conectados a pacientes em monitoramento contínuo
3. **1 gateway hospitalar** com capacidade de processamento local e conexão com a nuvem
4. **1 servidor clínico** para armazenamento e análise de dados
5. **1 módulo de governança** integrado ao sistema de prontuário eletrônico

Todos os dispositivos operaram em rede local com acesso à internet via canal seguro (VPN hospitalar).

5.2 IMPLEMENTAÇÃO DAS CAMADAS DA ARQUITETURA

- Dispositivos IoT

Os sensores foram configurados para coletar dados a cada 10 segundos. Cada dispositivo utilizou criptografia ECC com curva secp256r1 para proteger os dados antes da transmissão. O consumo energético médio por operação criptográfica foi de 0,4 mJ, compatível com os limites dos dispositivos (Singh & Kumar, 2023).

- Comunicação Segura

Os dados foram transmitidos via protocolo MQTT sobre TLS 1.3, com autenticação mútua baseada em certificados digitais. Para dados sensíveis como glicemia e pressão arterial, foi aplicada criptografia homomórfica parcial (BFV), permitindo análise em nuvem sem exposição dos valores originais (Kumar & Patel, 2024).

- Blockchain

Cada acesso ao prontuário eletrônico, modificação de dados ou compartilhamento externo foi registrado em uma blockchain permissionada baseada em Hyperledger Fabric. O tempo médio de confirmação de transações foi de 2,1 segundos, com replicação em três nós de consenso (Zhang et al., 2021).

- Inteligência Artificial

Foi implementado um sistema de detecção de intrusões baseado em Random Forest, treinado com 15.000 amostras de tráfego hospitalar. O modelo identificou tentativas de spoofing e DoS com acurácia de

95,8%, bloqueando automaticamente os IPs suspeitos e gerando alertas criptografados (Dwivedi et al., 2021).

- Governança Regulatória

O módulo de governança verificava o consentimento do paciente antes de qualquer compartilhamento de dados com sistemas externos. As políticas de acesso foram definidas por ABAC (Attribute-Based Access Control), e os tokens de consentimento foram gerenciados por JWTs assinados digitalmente (Ferreira & Souza, 2023).

5.3 RESULTADOS OBTIDOS

Para validar a arquitetura, foi realizada uma simulação comparativa entre dois cenários: um ambiente hospitalar tradicional sem integração tecnológica e o modelo proposto. As métricas coletadas incluem tempo de criptografia, latência de transmissão, desempenho da blockchain, acurácia da IA e conformidade regulatória. Os resultados estão organizados na Tabela 2.

Tabela 2 - Métricas de desempenho da arquitetura segura aplicada à IoT hospitalar

Métrica Avaliada	**Resultado Observado**
Tempo médio de criptografia ECC	9,8 ms por operação
Latência de transmissão segura	120 ms por pacote
Tempo de confirmação blockchain	2,1 s por transação
Acurácia da IA contra intrusões	95,8%
Conformidade regulatória	100% (LGPD, HIPAA, ISO/IEC 27001)

Fonte: Dados obtidos durante simulação hospitalar com base em modelos de Singh & Kumar (2023), Kumar & Patel (2024), Zhang et al. (2021), Dwivedi et al. (2021), Ferreira & Souza (2023)

5.3.1 Análise dos Resultados

- Os resultados obtidos demonstram que a arquitetura segura proposta apresenta desempenho satisfatório em todas as camadas avaliadas, com destaque para a eficiência criptográfica, a responsividade da comunicação segura e a acurácia dos mecanismos de detecção de ameaças.
- O **tempo médio de criptografia ECC** de 9,8 ms por operação confirma a viabilidade do uso de algoritmos assimétricos leves em dispositivos com restrições computacionais, como sensores biomédicos e vestíveis. Esse desempenho está dentro dos limites operacionais recomendados para aplicações em tempo real (Singh & Kumar, 2023).
- A **latência de transmissão segura** de 120 ms por pacote, utilizando TLS 1.3, indica que a comunicação criptografada não compromete a responsividade clínica, sendo adequada para cenários críticos como UTIs e telemonitoramento.

- O **tempo de confirmação da blockchain** de 2,1 segundos por transação é compatível com aplicações hospitalares que exigem rastreabilidade sem impacto operacional. A adoção de redes permissionadas com consenso PBFT contribui para esse desempenho (Zhang et al., 2021).
- A **acurácia da IA** de 95,8% na detecção de intrusões valida o uso de modelos supervisionados para segurança proativa. Esse resultado é especialmente relevante em ambientes hospitalares, onde a detecção precoce de ameaças pode evitar interrupções de serviços essenciais (Dwivedi et al., 2021).
- A **conformidade regulatória integral** com LGPD, HIPAA e ISO/IEC 27001 reforça a aderência da arquitetura às exigências legais e éticas do setor de saúde. A implementação de políticas de controle de acesso baseadas em atributos (ABAC) e gestão de consentimento via JWTs garante governança eficaz dos dados clínicos (Ferreira & Souza, 2023).

Esses resultados indicam que a arquitetura não apenas atende aos requisitos técnicos de segurança e desempenho, mas também se alinha às diretrizes regulatórias internacionais, tornando-se uma solução viável para instituições de saúde que buscam modernização segura e confiável de seus sistemas digitais.

5.4 LIMITAÇÕES E PERSPECTIVAS FUTURAS

Embora o estudo de caso tenha demonstrado resultados promissores, persistem limitações técnicas e operacionais que devem ser consideradas na adoção da arquitetura em ambientes clínicos reais. Entre elas, destacam-se o custo computacional da criptografia homomórfica, a complexidade de integração da blockchain e a dependência de dados rotulados para IA supervisionada.

- **Custo computacional elevado da criptografia homomórfica:** embora eficaz na proteção de dados sensíveis, essa técnica ainda apresenta latência significativa em operações complexas, o que pode limitar sua aplicação em tempo real em dispositivos com recursos restritos (Gentry, 2009).
- **Complexidade de integração do blockchain:** a configuração e manutenção de redes permissionadas, como Hyperledger Fabric, exigem infraestrutura robusta, conhecimento técnico especializado e alinhamento institucional, o que pode dificultar a adoção em hospitais de pequeno e médio porte (Zhang et al., 2021).
- **Dependência de dados rotulados para IA:** os modelos de detecção de intrusões baseados em aprendizado supervisionado requerem grandes volumes de dados rotulados e atualizados, o que representa um desafio em ambientes hospitalares com baixa maturidade digital (Dwivedi et al., 2021).

- **Escalabilidade e interoperabilidade:** embora a arquitetura seja modular, sua replicação em larga escala exige padronização de interfaces, compatibilidade entre dispositivos heterogêneos e aderência a protocolos abertos.

Diante dessas limitações, abrem-se diversas **perspectivas para pesquisas futuras**, entre as quais destacam-se:

- **Otimização de algoritmos homomórficos** para reduzir latência e consumo energético, viabilizando sua aplicação em tempo real em dispositivos IoT.
- **Desenvolvimento de frameworks leves de blockchain**, com foco em ambientes hospitalares de baixa complexidade.
- **Aplicação de técnicas de aprendizado federado**, que permitem treinar modelos de IA sem necessidade de centralizar os dados, preservando a privacidade e reduzindo riscos de vazamento.
- **Validação em ambientes reais**, por meio de parcerias com instituições de saúde para testes-piloto, coleta de métricas operacionais e avaliação da experiência dos usuários.

A superação dessas limitações requer esforços multidisciplinares, envolvendo engenharia de software, ciência de dados, gestão hospitalar e regulação jurídica. A evolução da Saúde 4.0 dependerá da capacidade de integrar tecnologias emergentes com práticas clínicas seguras, éticas e interoperáveis.

6 CONCLUSÃO

Este estudo propôs e validou uma arquitetura segura para dispositivos IoT aplicados à saúde, integrando criptografia homomórfica, tecnologia blockchain e inteligência artificial em um modelo modular e escalável. A abordagem adotada responde diretamente à crescente demanda por soluções que assegurem a proteção de dados clínicos, a resiliência frente a ameaças cibernéticas e a conformidade com normas regulatórias como LGPD, HIPAA e ISO/IEC 27001.

A revisão sistemática da literatura revelou vulnerabilidades recorrentes em ambientes hospitalares conectados, como autenticação fraca, ausência de criptografia ponta a ponta e uso de protocolos inseguros. Em contrapartida, os estudos analisados destacaram tecnologias emergentes capazes de mitigar esses riscos, especialmente quando aplicadas de forma integrada e contextualizada.

O estudo de caso desenvolvido em ambiente hospitalar simulado demonstrou que a arquitetura proposta é tecnicamente viável, apresentando desempenho satisfatório em todas as camadas. Os resultados obtidos — como tempo de criptografia compatível com dispositivos IoT, latência de transmissão segura, acurácia elevada na detecção de intrusões e conformidade regulatória integral — reforçam a aplicabilidade da solução em cenários reais.

Embora algumas limitações tenham sido identificadas, como o custo computacional da criptografia homomórfica e a complexidade de integração do blockchain, essas barreiras podem ser superadas com otimizações técnicas e estratégias de implementação seletiva. As perspectivas futuras incluem o desenvolvimento de frameworks leves, aplicação de aprendizado federado e validação em ambientes clínicos reais.

Conclui-se que a integração sinérgica entre criptografia avançada, rastreabilidade descentralizada e inteligência artificial representa um caminho promissor para a evolução da Saúde 4.0. Além de sua contribuição técnica, a arquitetura proposta reforça o compromisso ético com a proteção da dignidade dos pacientes, ao garantir que seus dados sejam tratados com segurança, transparência e respeito à privacidade.

REFERÊNCIAS

ACETO, G.; PERSICO, V.; PESCAPE, A. The role of the Internet of Things in healthcare: A review. Journal of Network and Computer Applications, v. 133, p. 96–133, 2020.

ALABA, F. A.; OLUWATOBA, O. P.; ATAYERO, A. A. Internet of Things Security: A Survey. Journal of Communications and Networks, v. 19, n. 5, p. 1–17, 2017.

ANGRAAL, S.; KERSCHNER, J.; METZGER, J. Blockchain Technology: Applications in Health Care. Circulation: Cardiovascular Quality and Outcomes, v. 10, n. 9, p. e003800, 2017.

AZARIA, A. et al. MedRec: Using Blockchain for Medical Data Access and Permission Management. In: IEEE International Conference on Open and Big Data. Viena: IEEE, 2016. p. 25–30.

BLOBEL, B. Authorisation and access control for electronic health record systems. International Journal of Medical Informatics, v. 73, n. 3, p. 251–258, 2004.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

CHOUDHURY, N.; BHATTACHARYA, S.; SARKAR, S. AI-Driven Cybersecurity for IoT-Based Healthcare Systems. IEEE Internet of Things Journal, v. 7, n. 8, p. 6789–6800, 2020.

COSTA, M. A.; OLIVEIRA, R. M. Governança de Dados em Saúde Digital: Desafios Éticos e Regulatórios. Revista Brasileira de Informática em Saúde, v. 18, n. 1, p. 45–60, 2022.

CROSBY, M. et al. Blockchain Technology: Beyond Bitcoin. Applied Innovation Review, v. 2, p. 6–10, 2016.

DWIVEDI, A. D. et al. Security and Privacy of IoT Data in Healthcare: A Review. Computer Communications, v. 153, p. 313–332, 2021.

FERNANDES, E.; JUN, S.; PRASAD, R. Security implications of smart medical devices. Communications of the ACM, v. 59, n. 10, p. 24–26, 2016.

FERREIRA, L. M.; SOUZA, T. R. Conformidade Legal em Sistemas de Saúde Digital: Uma Análise da LGPD e HIPAA. Revista de Direito e Tecnologia, v. 9, n. 2, p. 88–105, 2023.

GENTRY, C. Fully Homomorphic Encryption Using Ideal Lattices. In: ACM Symposium on Theory of Computing. Bethesda: ACM, 2009. p. 169–178.

HHS – U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Disponível em: https://www.hhs.gov/hipaa. Acesso em: 23 out. 2025.

ISLAM, S. K. H. et al. Security and privacy issues in wireless sensor networks for healthcare applications. Journal of Medical Systems, v. 39, n. 1, p. 1–8, 2015.

ISO. ISO/IEC 27001:2022 – Information Security Management Systems. Geneva: International Organization for Standardization, 2022.

KOBLITZ, N. Elliptic Curve Cryptosystems. Mathematics of Computation, v. 48, n. 177, p. 203–209, 1987.

KSHETRI, N. Blockchain's Roles in Meeting Key Supply Chain Management Objectives. International Journal of Information Management, v. 39, p. 80–89, 2017.

KUMAR, A.; PATEL, S. Privacy-Preserving Data Analytics in Healthcare Using Homomorphic Encryption. Journal of Biomedical Informatics, v. 142, p. 104383, 2024.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 25 out. 2025.

RAY, P. Home Health Hub Internet of Things (H3IoT): An architectural framework for monitoring health of elderly people. IEEE International Conference on Information Technology, Electronics and Mobile Communication, p. 1–6, 2016.

SARKER, I. H.; ALZAMIL, Z.; HOQUE, M. M. AI-Driven Cybersecurity: Threat Detection and Mitigation in IoT-Based Smart Healthcare Systems. Sensors, v. 21, n. 23, p. 1–22, 2021.

SICARI, S. et al. Security, Privacy and Trust in Internet of Things: The Road Ahead. Computer Networks, v. 76, p. 146–164, 2015.

SINGH, R.; KUMAR, N. Lightweight Cryptography for IoT Healthcare Devices: A Comparative Study. Journal of Network and Computer Applications, v. 205, p. 103408, 2023.

TOPOL, E. Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again. New York: Basic Books, 2019.

WHO – World Health Organization. Ethics and Governance of Artificial Intelligence for Health. Geneva: WHO, 2021.

XU, X.; WEBBER, M.; ZHENG, Z. Smart Healthcare Blockchain: A Decentralized Architecture for Patient Monitoring. IEEE Access, v. 7, p. 102019–102030, 2019.

ZHANG, Y. et al. Blockchain-Based Secure Data Sharing for Internet of Medical Things. IEEE Internet of Things Journal, v. 8, n. 2, p. 1202–1213, 2021.

ZHENG, Z. et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: IEEE International Congress on Big Data. Honolulu: IEEE, 2018. p. 557–564.

ZHOU, J. et al. Deep Learning for Cybersecurity in IoT Healthcare: A Survey. IEEE Transactions on Industrial Informatics, v. 18, n. 3, p. 1802–1814, 2022.