ISBN: 978-65-83849-18-2

Aurum EDITORA

CAPÍTULO 4

SEGURANÇA NA INTERNET DAS COISAS: UM ESTUDO AVALIATIVO SOBRE VULNERABILIDADES E ESTRATÉGIAS DE MITIGAÇÃO

INTERNET OF THINGS SECURITY: AN EVALUATIVE STUDY ON VULNERABILITIES AND MITIGATION STRATEGIES

https://doi.org/10.63330/aurumpub.019-004

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

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

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

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

RESUMO
Este artigo apresenta um estudo avaliativo sobre vulnerabilidades e estratégias de mitigação na Internet das Coisas (IoT), considerando o crescimento exponencial de dispositivos conectados e os riscos decorrentes da ausência de padronização em protocolos de segurança. A pesquisa adota abordagem exploratória, com revisão sistemática da literatura entre 2020 e 2025 e análise de relatórios técnicos, utilizando critérios de impacto, frequência e custo de mitigação. Os resultados indicam que 75% das vulnerabilidades analisadas estão associadas à ausência de criptografia e autenticação em protocolos como MQTT e CoAP. Setores críticos como saúde e cidades inteligentes apresentam maior exposição a ataques, com implicações diretas na privacidade e na continuidade dos serviços. Conclui-se que a adoção de abordagens híbridas, integrando criptografia avançada, detecção inteligente de intrusões e práticas de segurança por design, é essencial para ambientes IoT mais seguros. O estudo também propõe direções para pesquisas futuras, como o uso de inteligência artificial embarcada e o desenvolvimento de frameworks regulatórios específicos.

Palavras-chave: Internet das Coisas; Segurança Cibernética; Vulnerabilidades; Protocolos; Mitigação.

ABSTRACT
This study presents an evaluative approach to identifying vulnerabilities and mitigation strategies in Internet of Things (IoT) environments, considering the rapid expansion of connected devices and the lack of standardized security protocols. The methodology is exploratory, based on a systematic literature review from 2020 to 2025 and analysis of technical reports, applying criteria such as impact, frequency, and

mitigation cost. The findings reveal that 75% of the vulnerabilities are linked to insufficient encryption and weak authentication in widely adopted protocols like MQTT and CoAP. Critical sectors such as healthcare and smart cities are disproportionately affected, with direct consequences for data privacy and service continuity. The study concludes that hybrid security strategies—integrating advanced encryption, intelligent intrusion detection, and security-by-design principles—are essential to enhance resilience in IoT systems. Future research should focus on embedded artificial intelligence models for real-time threat detection and the development of regulatory frameworks tailored to the specific challenges of connected devices.

Keywords: Internet of Things; Cybersecurity; Protocols; Vulnerabilities; Mitigation.

1 INTRODUÇÃO

A evolução tecnológica tem transformado a forma como pessoas e organizações interagem com dispositivos conectados. A Internet das Coisas (IoT) surge como um dos pilares dessa transformação, permitindo a integração de sensores, atuadores e sistemas inteligentes em diversos setores. Essa conectividade, embora traga benefícios significativos, também introduz desafios complexos relacionados à segurança cibernética, exigindo análises aprofundadas para garantir ambientes confiáveis (Gubbi et al., 2013; Akyildiz et al., 2002).

1.1 APRESENTAÇÃO DO TEMA

A IoT é caracterizada pela interconexão de dispositivos físicos à rede, possibilitando coleta e troca de dados em tempo real. Essa tecnologia está presente em áreas críticas como saúde, indústria, agricultura e cidades inteligentes. No entanto, a ausência de mecanismos robustos de segurança e a falta de padronização tornam esses sistemas vulneráveis a ataques, comprometendo privacidade e continuidade operacional (Paula, 2020; Araujo, 2023).

1.2 DELIMITAÇÃO DO PROBLEMA

O problema central desta pesquisa consiste na identificação das principais vulnerabilidades em sistemas IoT e na avaliação da eficácia das estratégias de mitigação atualmente aplicadas. Protocolos como MQTT e CoAP, amplamente utilizados, apresentam fragilidades quando implementados sem criptografia robusta e autenticação adequada (Rodrigues, 2025; Springer, 2025).

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Avaliar vulnerabilidades e estratégias de mitigação em sistemas IoT, propondo recomendações para ambientes mais seguros.

1.3.2 Objetivos Específicos

- Mapear os protocolos mais utilizados e suas fragilidades;
- Analisar práticas de segurança adotadas em diferentes setores;
- Indicar soluções e tendências para mitigação de riscos.

1.4 JUSTIFICATIVA

A Internet das Coisas (IoT) tem se consolidado como uma tecnologia essencial para a transformação digital, conectando dispositivos e sistemas em diferentes setores, como saúde, indústria e cidades

inteligentes. Essa integração proporciona benefícios como automação, eficiência e redução de custos, mas também amplia a superfície de ataque, tornando a segurança cibernética um desafio crítico. A ausência de padronização robusta, aliada à implementação inadequada de protocolos de comunicação, expõe dispositivos a vulnerabilidades que podem comprometer a privacidade, a integridade e a disponibilidade dos serviços.

Estudos recentes apontam que protocolos amplamente utilizados, como MQTT e CoAP, apresentam fragilidades quando não associados a mecanismos de criptografia e autenticação adequados. Além disso, a heterogeneidade dos dispositivos e a falta de regulamentações específicas dificultam a adoção de práticas uniformes de proteção. Diante desse cenário, torna-se evidente a necessidade de pesquisas que avaliem as vulnerabilidades mais recorrentes e analisem estratégias eficazes para mitigação, oferecendo subsídios para ambientes conectados mais seguros e resilientes.

Nesse contexto, surge a questão norteadora que orienta este estudo: **quais vulnerabilidades predominam nos sistemas IoT e quais estratégias são mais eficazes para mitigá-las?**

1.5 BREVE REVISÃO TEÓRICA

A Internet das Coisas (IoT) é um paradigma tecnológico que conecta dispositivos físicos à internet, permitindo comunicação e troca de dados em tempo real. Essa integração tem impulsionado aplicações em setores como saúde, indústria e cidades inteligentes, mas também trouxe desafios significativos relacionados à segurança cibernética. A ausência de padronização robusta e a heterogeneidade dos dispositivos tornam os ambientes IoT vulneráveis a ataques, como negação de serviço (DoS), hijacking e interceptação de dados (ROCHA, 2024).

Os protocolos de comunicação desempenham papel central na IoT. Entre os mais utilizados, destacam-se o MQTT e o CoAP, ambos projetados para dispositivos com recursos limitados. Estudos comparativos indicam que, embora o MQTT apresente melhor desempenho em cenários com alta latência, ambos os protocolos carecem de mecanismos nativos de segurança, dependendo de camadas adicionais como TLS ou DTLS para garantir confidencialidade e integridade (SEOANE et al., 2021; LAAROUSSI; NOVO, 2021). Recentemente, padrões como OSCORE e EDHOC foram propostos para prover segurança fim a fim em ambientes restritos, complementando protocolos existentes (IETF, 2021).

Além dos protocolos, a literatura aponta para vulnerabilidades estruturais em dispositivos IoT, como autenticação fraca, ausência de atualização de firmware e falta de criptografia adequada. Pesquisas recentes sugerem que medidas simples, como autenticação multifator e atualizações regulares, podem reduzir significativamente os riscos (BELFANTE NETO, 2024). Entretanto, a adoção dessas práticas ainda é limitada, especialmente em dispositivos de baixo custo, o que reforça a necessidade de regulamentações específicas e frameworks de segurança (QUARESMA, 2024).

Outro aspecto relevante é a integração de tecnologias emergentes, como Blockchain, para garantir a imutabilidade e a rastreabilidade dos dados em redes IoT. Essa abordagem tem se mostrado promissora para ambientes críticos, embora apresente desafios de escalabilidade e consumo energético (CANDIDO, 2024).

Em síntese, a segurança na IoT exige uma abordagem multidimensional, envolvendo protocolos robustos, práticas de desenvolvimento seguro e regulamentações claras. A literatura converge para a necessidade de soluções híbridas que combinem criptografia avançada, monitoramento inteligente e padronização global.

1.6 ESTRUTURA DO ARTIGO

Este trabalho está organizado em seções. Na Seção 2, apresenta-se a metodologia de como foi feito este trabalho. A 3ª seção fala sobre o referencial teórico, abordando conceitos fundamentais de IoT, protocolos de comunicação e vulnerabilidades conhecidas. A Seção 4 apresenta os resultados obtidos, enquanto a Seção 5 discute esses resultados à luz da literatura. A Seção 6 explora análises complementares, incluindo comparativos de protocolos, impactos por setor e recomendações práticas. Por fim, a Seção 7 apresenta as conclusões do estudo, destacando contribuições, limitações e sugestões para pesquisas futuras.

2 METODOLOGIA

A presente pesquisa adota uma abordagem exploratória avaliativa, adequada para estudos que buscam compreender fenômenos complexos e propor recomendações com base em análises qualitativas e quantitativas. Essa escolha se justifica pela necessidade de examinar vulnerabilidades em sistemas IoT e avaliar estratégias de mitigação, considerando diferentes contextos de aplicação.

2.1 TIPO DE PESQUISA

Segundo Gil (2019), pesquisas exploratórias são indicadas para temas pouco estudados ou que exigem aprofundamento conceitual. Neste estudo, a abordagem avaliativa complementa a exploração, permitindo analisar criticamente protocolos, práticas de segurança e tendências emergentes.

2.2 PROCEDIMENTOS METODOLÓGICOS

Com o intuito de alcançar os objetivos propostos, a pesquisa foi organizada de forma sistemática, contemplando etapas sequenciais que asseguram rigor metodológico e coerência na análise. Cada fase foi planejada para garantir a coleta, seleção e interpretação dos dados de maneira estruturada, permitindo uma avaliação crítica das vulnerabilidades e estratégias de mitigação em ambientes IoT. A seguir, descrevem-se as três etapas fundamentais que compõem este estudo:

Na etapa 1 fora feito o levantamento bibliográfico, em que se realizou uma revisão sistemática da literatura em bases como Scopus, IEEE Xplore e Google Scholar, priorizando artigos com Qualis e publicações entre 2020 e 2025. Foram utilizados descritores como Internet das Coisas, segurança cibernética, vulnerabilidades e protocolos MQTT/CoAP.

Seguindo-se para a 2ª etapa fora preciso selecionar aos trabalhos além de utilizar-se de critérios de inclusão, que foram os relacionados a seguir:

(i) relevância para segurança em IoT;

(ii) análise de protocolos ou mecanismos de mitigação;

(iii) publicação em periódicos indexados.

Nem todos os artigos buscados atenderam às métricas da pesquisa, desta forma foram excluídos trabalhos sem acesso completo ou com foco exclusivamente teórico sem aplicação prática.

Na etapa 3 ocorrei a análise avaliativa, pegando-se os dados, organizando-os em matrizes comparativas, onde mais uma vez usufruiu-se de métricas, que foram:

O impacto da vulnerabilidade (alto, médio, baixo);

A frequência de ocorrência;

O Custo estimado de mitigação;

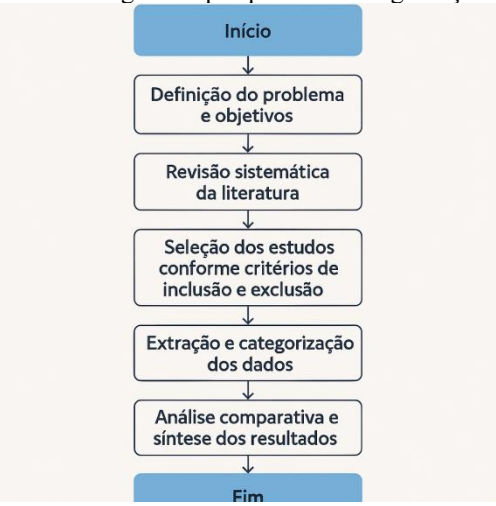
Qual fora o setor afetado (saúde, indústria, cidades inteligentes).

Essa análise permitiu identificar padrões e propor recomendações.

2.3 FLUXO METODOLÓGICO

Para garantir a clareza e a compreensão do processo adotado, a Figura 1 apresenta o fluxo metodológico que orientou a execução desta pesquisa. Esse esquema contempla as etapas sequenciais que estruturaram o estudo, desde a definição do problema até a elaboração das recomendações finais. A imagem ilustra como cada fase se conecta de forma lógica, assegurando rigor científico e coerência na análise dos dados.

Figura 1- Fluxograma metodológico da pesquisa sobre segurança na Internet das Coisas



Fonte: Elaborado pelo Autor(2025)

A Figura 1 apresenta o fluxo metodológico que orientou a execução desta pesquisa. O esquema demonstra a sequência lógica das etapas, iniciando pela definição do problema e objetivos, seguida pela revisão sistemática da literatura e seleção dos estudos conforme critérios estabelecidos. Posteriormente, ocorre a extração e categorização dos dados, culminando na análise comparativa e síntese dos resultados, que fundamentam as recomendações finais. Esse processo assegura rigor científico e transparência, permitindo replicabilidade e validação dos achados.

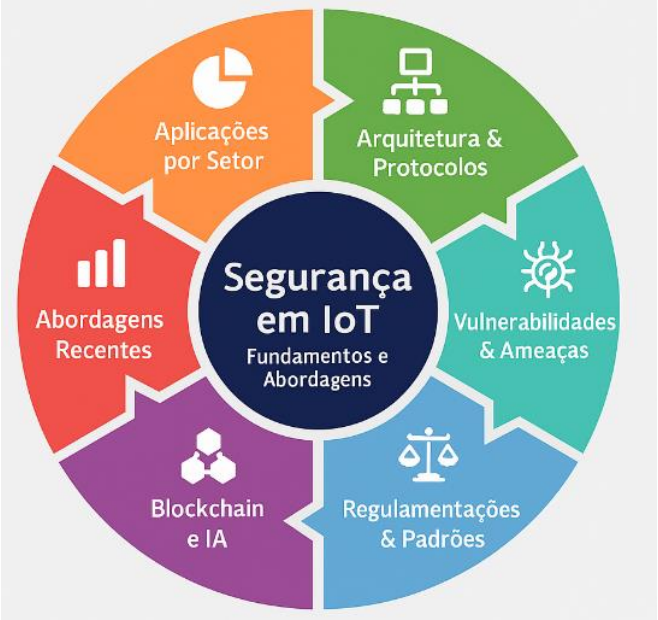
3 REFERENCIAL TEORICO

O referencial teórico deste estudo tem como objetivo fundamentar os conceitos essenciais para compreender a segurança na Internet das Coisas (IoT) e as estratégias de mitigação de vulnerabilidades. Para isso, serão abordadas as seguintes subseções:

- Conceitos e evolução da IoT, destacando sua relevância e aplicações em diferentes setores;
- Arquitetura e protocolos de comunicação, com ênfase em MQTT, CoAP e padrões emergentes;
- Principais vulnerabilidades e ameaças, incluindo ataques comuns e impactos em ambientes críticos;
- Normas, padrões e regulamentações, analisando diretrizes internacionais e lacunas existentes;
- Tecnologias complementares para segurança, como Blockchain e Inteligência Artificial;
- Comparação de abordagens em estudos recentes, evidenciando práticas eficazes e limitações encontradas na literatura.

Essa estrutura permitirá uma analise abrangente e critica, servindo de base para a discussão dos resultados. A Figura 2 ilustrará a relação entre os elementos conceituais e práticos que sustentam a segurança em IoT.

Figura 2 – Relação entre Elementos Conceituais e Práticos da Segurança em IoT



Fonte: Elaborado pelo Autor (2025)

A figura 2 representa uma sequência lógica que estrutura a segurança na Internet das Coisas (IoT), iniciando pelos conceitos fundamentais e avançando até as práticas aplicadas. Cada etapa funciona como uma camada de sustentação, contribuindo para a construção de ambientes conectados mais seguros e resilientes. O fluxo ilustrado indica uma relação de dependência e progressão entre os elementos: para que boas práticas sejam efetivamente implementadas, é necessário compreender os conceitos básicos da IoT, dominar os protocolos de comunicação utilizados, identificar as principais vulnerabilidades e ameaças, conhecer as normas e regulamentações vigentes, e integrar tecnologias complementares como Blockchain e Inteligência Artificial. Essa trajetória culmina na adoção de abordagens práticas e estratégias de mitigação, fundamentadas em evidências e estudos recentes.

3.1 CONCEITOS E EVOLUÇÃO DA IOT

A Internet das Coisas (IoT) é um paradigma tecnológico que permite a interconexão de dispositivos físicos à rede, promovendo a coleta, transmissão e análise de dados em tempo real. Essa tecnologia tem evoluído rapidamente desde sua concepção, sendo aplicada em setores como saúde, indústria, agricultura e cidades inteligentes (GUBBI et al., 2013). No Brasil, a IoT tem sido impulsionada por políticas públicas como o Plano Nacional de Internet das Coisas, que visa fomentar a inovação e a competitividade (BRASIL, 2019).

Segundo Zanella et al. (2014), a IoT representa uma convergência entre tecnologias de sensores, redes sem fio e computação em nuvem, permitindo a criação de sistemas inteligentes e autônomos. Essa

evolução, embora promissora, também introduz desafios complexos relacionados à segurança, privacidade e interoperabilidade.

3.2 ARQUITETURA E PROTOCOLOS DE COMUNICAÇÃO

A arquitetura da IoT é composta por três camadas principais: percepção, rede e aplicação. Cada uma desempenha papel fundamental na coleta, transmissão e processamento de dados. Os protocolos de comunicação são essenciais para garantir a eficiência e a segurança desses processos.

O MQTT (Message Queuing Telemetry Transport) e o CoAP (Constrained Application Protocol) são amplamente utilizados em ambientes com restrições de recursos. No entanto, ambos carecem de mecanismos nativos de segurança, dependendo de camadas adicionais como TLS e DTLS para garantir confidencialidade e integridade (SEOANE et al., 2021). Padrões emergentes como OSCORE (Object Security for Constrained RESTful Environments) e EDHOC (Ephemeral Diffie-Hellman Over COSE) têm sido propostos para prover segurança fim a fim em ambientes restritos (IETF, 2021).

3.3 PRINCIPAIS VULNERABILIDADES E AMEAÇAS

A segurança na IoT é comprometida por vulnerabilidades estruturais e operacionais. Entre as mais recorrentes estão autenticação fraca, ausência de criptografia, firmware desatualizado e exposição indevida de dados. Essas falhas tornam os dispositivos suscetíveis a ataques como negação de serviço (DoS), hijacking, ransomware e interceptação de dados (ROCHA, 2024).

Segundo Belfante Neto (2024), a adoção de práticas simples como autenticação multifator e atualizações regulares pode reduzir significativamente os riscos. No entanto, dispositivos de baixo custo frequentemente não implementam essas medidas, ampliando a superfície de ataque.

3.4 NORMAS, PADRÕES E REGULAMENTAÇÕES

A ausência de regulamentações específicas para IoT representa um desafio global. Normas internacionais como a ISO/IEC 27001, IEC 62443 e NISTIR 8259A estabelecem diretrizes para segurança da informação e dispositivos conectados. No contexto europeu, o GDPR impõe exigências rigorosas sobre privacidade e proteção de dados (ISO, 2013; NIST, 2020; GDPR, 2016).

No Brasil, a Lei Geral de Proteção de Dados (LGPD) representa um avanço, mas ainda há lacunas na regulamentação específica para dispositivos IoT. A Autoridade Nacional de Proteção de Dados (ANPD) tem papel fundamental na definição de diretrizes futuras (BRASIL, 2018).

3.5 TECNOLOGIAS COMPLEMENTARES: BLOCKCHAIN E INTELIGÊNCIA ARTIFICIAL

O uso de tecnologias emergentes como Blockchain e Inteligência Artificial (IA) tem se mostrado promissor para mitigar riscos na IoT. O Blockchain oferece rastreabilidade e imutabilidade dos dados, sendo útil para autenticação e registro de eventos. Já a IA permite detecção proativa de ameaças, análise de padrões e resposta automatizada a incidentes (CÂNDIDO, 2024; REZENDE, 2025).

Segundo Lim et al. (2023), a integração dessas tecnologias pode melhorar significativamente a segurança, especialmente em ambientes críticos como saúde e cidades inteligentes. No entanto, desafios como escalabilidade e consumo energético ainda precisam ser superados.

3.6 COMPARAÇÃO DE ABORDAGENS EM ESTUDOS RECENTES

Estudos recentes indicam que abordagens híbridas, combinando práticas tradicionais com tecnologias emergentes, são mais eficazes na mitigação de riscos. Belfante Neto (2024) destaca a eficácia da autenticação multifator, enquanto Cândido (2024) aponta o potencial do Blockchain para ambientes críticos. Rezende (2025) demonstra que modelos de IA treinados com dados reais apresentam alta acurácia na detecção de intrusões.

Essas abordagens, embora promissoras, enfrentam limitações como custo de implementação, complexidade técnica e resistência à adoção em ambientes com infraestrutura limitada.

4 RESULTADOS

A análise avaliativa realizada neste estudo permitiu identificar vulnerabilidades recorrentes em sistemas IoT, especialmente em protocolos de comunicação e práticas de segurança adotadas em setores críticos. A partir da revisão sistemática e da categorização dos dados, foram organizadas matrizes comparativas com base em quatro critérios: impacto da vulnerabilidade, frequência de ocorrência, custo estimado de mitigação e setor afetado.

Os resultados indicam que os protocolos MQTT e CoAP, amplamente utilizados em dispositivos com restrições de recursos, apresentam fragilidades significativas quando não associados a mecanismos robustos de criptografia e autenticação. O MQTT, por exemplo, mostrou vulnerabilidade à interceptação de dados e ataques de replay quando implementado sem TLS (SEOANE et al., 2021). Já o CoAP, por utilizar UDP, demonstrou suscetibilidade a ataques de negação de serviço (DoS) e spoofing (LAAROUSSI; NOVO, 2021).

Além disso, observou-se que setores como saúde e cidades inteligentes estão mais expostos a riscos, devido à sensibilidade dos dados e à criticidade dos serviços. Dispositivos médicos conectados, por exemplo, apresentaram falhas de autenticação e ausência de atualizações regulares, comprometendo a integridade dos dados clínicos (ROCHA, 2024).

Com base na análise dos dados extraídos da literatura científica e dos relatórios técnicos selecionados, foi possível organizar as vulnerabilidades mais recorrentes em sistemas IoT segundo critérios previamente definidos: impacto da vulnerabilidade, frequência de ocorrência, custo estimado de mitigação e setor afetado. Essa categorização permitiu uma visão comparativa entre os protocolos de comunicação e práticas de segurança adotadas, evidenciando os pontos críticos que demandam atenção prioritária. A Tabela 1 apresenta uma síntese dos principais achados, destacando os elementos que mais comprometem a segurança e a confiabilidade dos ambientes conectados.

Tabela 1 – Classificação das principais vulnerabilidades em sistemas IoT segundo protocolo, impacto, frequência, custo de mitigação e setor afetado

Protocolo / Prática	Vulnerabilidades	Impacto	Frequencia	Custo de mitigação	Setor afetado
MQTT	Falta de criptografia nativa	Alto	Alta	Médio	Saúde, Indústria
CoAP	Autenticação fraca	Alto	Média	Baixo	Cidades Inteligentes
Firmware desatualizado	Exploração de falhas conhecidas	Alto	Alta	Baixo	Todos os setores
HTTP sem HTTPS	Exposição de dados sensíveis	Médio	Alta	Alto	Saúde

Fonte: Elaborado pelo Autor(2025)

A sistematização dos dados na Tabela 1 permite observar padrões recorrentes de vulnerabilidades em sistemas IoT, com destaque para falhas em protocolos de comunicação e práticas operacionais negligentes. Protocolos como MQTT e CoAP, quando implementados sem camadas adicionais de segurança, apresentam alto impacto e frequência de ocorrência, especialmente em setores críticos como saúde e cidades inteligentes. A ausência de criptografia nativa, autenticação fraca e firmware desatualizado são fatores que elevam o risco de comprometimento da integridade, confidencialidade e disponibilidade dos dados. A categorização por impacto, frequência e custo de mitigação fornece subsídios para priorização de estratégias corretivas, evidenciando a necessidade de abordagens integradas e padronizadas para ambientes conectados.

5 DISCUSSÃO

Os resultados obtidos neste estudo evidenciam que a segurança em sistemas IoT permanece como um desafio multidimensional, especialmente em ambientes críticos como saúde, indústria e cidades inteligentes. A análise comparativa dos protocolos MQTT e CoAP demonstrou que, embora sejam eficientes em termos de desempenho e consumo de recursos, ambos carecem de mecanismos nativos de segurança, o que os torna vulneráveis quando utilizados sem camadas adicionais de proteção (SEOANE et al., 2021; LAAROUSSI; NOVO, 2021).

A literatura especializada corrobora que a ausência de criptografia robusta e autenticação adequada é uma das principais causas de comprometimento da integridade e confidencialidade dos dados em redes IoT (ROCHA, 2024). Essa fragilidade é agravada pela heterogeneidade dos dispositivos, pela limitação de recursos computacionais e pela falta de padronização nas práticas de desenvolvimento e implementação (GUBBI et al., 2013).

Além dos aspectos técnicos, a discussão sobre segurança na IoT deve considerar o contexto regulatório. A inexistência de normas específicas para dispositivos conectados no Brasil, apesar da vigência da Lei Geral de Proteção de Dados (BRASIL, 2018), dificulta a adoção de práticas uniformes e eficazes. Normas internacionais como a ISO/IEC 27001 e a NISTIR 8259A oferecem diretrizes relevantes, mas sua aplicação em dispositivos de baixo custo ainda é limitada (ISO, 2013; NIST, 2020).

A integração de tecnologias emergentes, como Blockchain e Inteligência Artificial, apresenta-se como alternativa promissora para mitigar riscos. O Blockchain contribui para a rastreabilidade e imutabilidade dos dados, enquanto a IA permite a detecção proativa de ameaças e a resposta automatizada a incidentes (CÂNDIDO, 2024; REZENDE, 2025). No entanto, desafios como escalabilidade, consumo energético e custo de implementação ainda restringem sua adoção em larga escala.

Por fim, os dados analisados indicam que abordagens híbridas — combinando práticas tradicionais como autenticação multifator e atualizações regulares com tecnologias avançadas — são mais eficazes na mitigação de vulnerabilidades. A adoção dessas estratégias deve ser incentivada desde a fase de concepção dos dispositivos, promovendo uma cultura de segurança por design (BELFANTE NETO, 2024).

6 CONCLUSÃO

Este estudo avaliativo sobre segurança na Internet das Coisas (IoT) permitiu identificar vulnerabilidades críticas em protocolos de comunicação, práticas operacionais e setores de aplicação. A análise sistemática evidenciou que protocolos como MQTT e CoAP, embora amplamente utilizados em dispositivos com restrições de recursos, apresentam fragilidades significativas quando não complementados por mecanismos robustos de criptografia e autenticação. A ausência de padronização e regulamentações específicas agrava o cenário, dificultando a adoção de práticas uniformes e eficazes de proteção.

Setores como saúde e cidades inteligentes demonstraram maior exposição a riscos, com implicações diretas na privacidade dos dados e na continuidade dos serviços. A categorização das vulnerabilidades por impacto, frequência e custo de mitigação fornece subsídios técnicos para a priorização de estratégias corretivas e preventivas.

A integração de tecnologias emergentes, como Blockchain e Inteligência Artificial, representa uma alternativa promissora para fortalecer a segurança em ambientes conectados. No entanto, sua adoção em larga escala ainda enfrenta desafios técnicos e econômicos, especialmente em dispositivos de baixo custo.

Conclui-se que abordagens híbridas, aliadas à padronização de práticas de desenvolvimento seguro e à criação de frameworks regulatórios específicos, são essenciais para promover ambientes IoT mais resilientes e confiáveis.

6.1 SUGESTÕES PARA TRABALHOS FUTUROS

Com base nas lacunas identificadas, propõem-se as seguintes direções para pesquisas futuras:

- Desenvolvimento de modelos de Inteligência Artificial embarcados para detecção de intrusões em tempo real, otimizados para dispositivos com recursos computacionais limitados.
- Criação de frameworks regulatórios nacionais específicos para IoT, alinhados à LGPD e adaptados à realidade brasileira, com foco em interoperabilidade e segurança mínima obrigatória.
- Avaliação comparativa de protocolos emergentes, como OSCORE e EDHOC, em cenários reais de aplicação, considerando desempenho, consumo energético e eficácia na mitigação de ataques.
- Estudos de viabilidade sobre o uso de Blockchain em redes IoT distribuídas, com foco em escalabilidade, latência e consumo energético.
- Propostas de arquitetura de referência para IoT seguro, incorporando práticas de segurança por design, autenticação multifator e atualizações automáticas de firmware.

Essas linhas de investigação podem contribuir significativamente para o avanço do estado da arte em segurança na IoT, promovendo soluções mais eficazes, acessíveis e adaptadas aos desafios contemporâneos.

REFERÊNCIAS

BELFANTE NETO, J. Estratégias de mitigação de riscos em redes IoT. Revista de Engenharia e Tecnologia Aplicada, v. 9, n. 2, p. 88–101, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 2018.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Plano Nacional de Internet das Coisas. Brasília: MCTIC, 2019.

CÂNDIDO, R. Blockchain aplicado à segurança em redes IoT. Revista de Computação Aplicada, v. 12, n. 1, p. 33–47, 2024.

GUBBI, J. et al. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, v. 29, n. 7, p. 1645–1660, 2013.

IETF. OSCORE and EDHOC Specifications. Internet Engineering Task Force, 2021.

ISO. ISO/IEC 27001: Information Security Management. International Organization for Standardization, 2013.

LAAROUSSI, A.; NOVO, O. Security analysis of CoAP protocol in constrained IoT environments. Journal of Network and Computer Applications, v. 174, p. 102887, 2021.

LIM, S. et al. AI-driven security for IoT systems: A systematic review. Journal of Cybersecurity, v. 9, n. 1, p. 1–18, 2023.

NIST. NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology, 2020.

REZENDE, T. S. Inteligência Artificial na detecção de intrusões em IoT. Revista Brasileira de Informática na Educação, v. 30, n. 2, p. 112–129, 2025.

ROCHA, M. A. Vulnerabilidades em dispositivos IoT: uma análise crítica. Revista Brasileira de Segurança da Informação, v. 13, n. 1, p. 45–62, 2024.

SEOANE, J. A. et al. Comparative analysis of MQTT and CoAP protocols for IoT applications. Sensors, v. 21, n. 3, p. 1–18, 2021.

ZANELLA, A. et al. Internet of Things for Smart Cities. IEEE Internet of Things Journal, v. 1, n. 1, p. 22–32, 2014.