UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

DEPARTAMENTO DE COMPUTAÇÃO

PROGRAMA DE PÓS–GRADUAÇÃO EM INFORMÁTICA APLICADA

EDUARDO FERREIRA FELIX

AVALIAÇÃO DE CONFORMIDADE DE REQUISITOS DE SEGURANÇA CRIPTOGRÁFICA EM GATEWAYS IOT

RECIFE - PE

2022

AVALIAÇÃO DE CONFORMIDADE DE REQUISITOS DE SEGURANÇA CRIPTOGRÁFICA EM GATEWAYS IOT

Trabalho de Dissertação submetido à Universidade Federal Rural de Pernambuco, como requisito necessário para obtenção do grau de Mestre em Informática Aplicada sob a orientação do professor Dr. Fernando Antônio Aires Lins e coorientação do professor Dr. Obinor de Oliveira Nobrega.

RECIFE – PE

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

F316a Felix, Eduardo Ferreira
AVALIAÇÃO DE CONFORMIDADE DE REQUISITOS DE SEGURANÇA CRIPTOGRÁFICA EM GATEWAYS IOT / Eduardo Ferreira Felix. - 2022.
78 f. : il.

Orientador: Fernando Antonio Aires Lins.
Coorientador: Obionor de Oliveira Nobrega.
Inclui referências.

Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Pós-Graduação em Informática Aplicada, Recife, 2022.

1. Segurança. 2. Internet das Coisas. 3. Gateway. 4. Requisitos de Criptografia. I. Lins, Fernando Antonio Aires, orient. II. Nobrega, Obionor de Oliveira, coorient. III. Título

CDD 004

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

EDUARDO FERREIRA FELIX

Este Trabalho de Dissertação foi julgado adequado para a obtenção do título de Mestre em Informática Aplicada, sendo aprovado em sua forma final pela banca examinadora:

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. Fernando Antônio Aires Lins
Universidade Federal Rural de Pernambuco - UFRPE

_____

Prof. Dra. Erica Teixeira Gomes de Sousa
Universidade Federal Rural de Pernambuco - UFRPE

_____

Prof. Dra. Juliana Regueira Basto Diniz
Universidade Federal Rural de Pernambuco - UFRPE

_____

Prof. Dr. Robson Wagner Albuquerque de Medeiros
Universidade Federal Rural de Pernambuco - UFRPE

RECIFE - PE

2022

Dedico este trabalho, primeiramente, a Deus, segundo a minha mãe Damiana Ferreira Felix por fazer dos meus sonhos seus sonhos e por não medir esforços para realizá-los.

Agradecimentos

Em primeiro lugar agradeço a Deus e a Maria santíssima por ter me dado forças para concluir este trabalho. Conseguir realizar este sonho diante de uma pandemia não foi fácil, foram muitas dificuldades enfrentadas e muitos medos vencidos.

Agradeço, aos meus pais, Cícero Jerônimo Sobrinho e Damiana Ferreira Felix por incentivar a trilhar esse caminho que escolhi, não me deixando desistir nunca dos meus sonhos, mesmo quando o desânimo e as dificuldades apareciam.

Agradeço, aos meus professores que percorreram comigo essa caminhada acadêmica, especialmente, ao meu orientador e amigo Dr. Fernando Antônio Aires Lins, pelo seu tempo dedicado a este trabalho, pelas correções realizadas, pelos conhecimentos transmitidos, pelas palavras de sabedoria nos momentos difíceis, pela sua disponibilidade e por procurar sempre me orientar da melhor forma possível.

Agradeço também a todos que compõem o meu grupo de estudos, vocês são muito importantes para mim e para conclusão deste trabalho. Agradeço ao meu coorientador Dr. Obionor de Oliveira Nóbrega, pelas contribuições e disponibilidade.

Agradeço aos meus irmãos e sobrinhos pelo apoio, em especial às minhas irmãs caçulas Káttylla Maria Ferreira Felix e Thays Ferreira Felix por estarem sempre ao meu lado me incentivando a lutar pelos meus sonhos. Amo vocês imensamente!

Por fim, agradeço a todos que contribuíram direto ou indiretamente para o fechamento deste ciclo.

“Se eu vi mais longe, foi por estar sobre ombros de gigantes.”

(Isaac Newton)

Resumo

A Internet das Coisas é uma das novas tendências tecnológicas que vem chamando atenção pela sua rápida disseminação e aceitação. No entanto, não saber se, por exemplo, dados e informações pessoais estão seguros pode dificultar uma aceitação mais generalizada desta tecnologia por parte dos usuários. Neste contexto, a segurança de um dos principais componentes do sistema IoT, o gateway, se torna ainda mais relevante, pois o mesmo é essencial na conexão de dispositivos IoT heterogêneos. O gateway IoT acaba centralizando a comunicação e o gerenciamento do sistema, tornando-se assim um alvo de alto valor em termos de segurança. Para ajudar na melhoria da segurança de gateways IoT é essencial que esses dispositivos façam uso de serviços criptográficos implementados com configurações adequadas, baseado preferencialmente em organizações ou padrões técnicos aceitos pela comunidade científica. Baseado neste contexto, o objetivo principal desta dissertação é avaliar o nível de segurança de gateways IoT considerando requisitos de criptografia. Para isto, um subconjunto de requisitos de criptografia sugeridos por organizações técnicas internacionais, como IoTSF e OWASP, são selecionados e priorizados. Para melhor compreensão do processo de avaliação e inspeção de requisitos de criptografia, foi desenvolvida uma metodologia descrita no padrão *Business Process Model and Notation* (BPMN). Esta metodologia é instanciada na avaliação de quatro gateways IoT atualmente usados pela sociedade. Nenhum dos gateways atingiu mais que 80% de conformidade nos requisitos avaliados, o que causa preocupação em relação à segurança dos dados dos seus usuários.

Palavras-chave: Segurança, Internet das Coisas, *Gateway,* Requisitos de Criptografia.

Abstract

The Internet of Technological Things coming to new attention for its rapid dissemination and innovation. However, there is no secure if, for example, they can make data and more generalized personal information of this technology by part of the users. In this context, the security of one of the main components of the IoT system, the gateway, becomes even more relevant, as it is essential in the connection of heterogeneous IoT devices. The IoT gateway centralizing the communication and system management, thus becoming a high-value target in terms of security. To help improve of the security of IoT gateways is that these devices allow the use of cryptographic services with custom settings, preferably in organizations or technicians accepted scientific community. Based on this context, the main objective of this dissertation is to evaluate the level of IoT considering gateway security requirements. For this, prioritize a set of encryption requirements recommended by international techniques, such as IoTSF and OWASP, are selected and defined. To understand the assessment process and encryption requirements, a better methodology was developed described in the standard business process model and business process model (BPMN). This methodology is instantiated in the evaluation of four IoT gateways currently used by society. Gateways have achieved more than 80% compliance with the requirements, which causes concern about their users' security data.

Keywords: Security, Internet of Things, Gateway, Cryptography Requirements.

Lista de Figuras

Lista de Tabelas

Lista de Siglas

IoT	*Internet of Things*
IoTSF	*IoT Security Foundation*
OWASP	*Open Web Application Security Project*
BPMN	*Business Process Model and Notation*
NIST	*National Institute of Standards and Technology*
ISO/IEC	*International Organization of Standardization/ International Electrotechnical Commission*
FIPS	*Federal Information Processing Standard Publication*
FIPS PUB	*Federal Information Processing Standards Publication*
ENISA	*European Union Agency for Cybersecurity*
ETSI	*European Telecommunications Standards Institute*
IETF	*Internet Engineering Task Force*
CCF	Criptografia de Campo Finito
TCP1	Tamanho da Chave Pública
TCP2	Tamanho da Chave Privada
CFI	Criptografia de Fatoração Inteira
CCE	Criptografia de Curva Elíptica

Sumário

1. Introdução

O advento da Internet das Coisas (*Internet of Things - IoT*) vem sendo cada vez mais observado no cotidiano das pessoas, que encontram na IoT uma maneira de permanecerem conectadas entre si ou com dispositivos inteligentes. Segundo Menegatti (2022) o uso de dispositivos IoT sairá de 17,7 bilhões em 2020 para 36,8 bilhões em 2025 atingindo um crescimento superior a 100% em comparação com os anos anteriores e que esse crescimento no uso de dispositivos IoT é previsto em diferentes áreas. Esse aumento no número de usuários proporciona um aumento na economia do país, onde, de acordo com VIVO (2022), no Brasil a economia anual com IoT em 2025 deve ficar entre 50 e 200 bilhões de dólares. Nesse sentido, com o crescimento acelerado da IoT, mais informações estarão na rede através das conexões IoT gerando em 2025 um volume de informações em torno de 79,4 zettabytes (VIVO, 2022). Assim sendo, é fundamental reforçar a privacidade dos dados que trafegam entre as conexões IoT. Possibilitando aos usuários usufruir dos recursos oferecidos pela IoT sem se preocupar com o vazamento de informações pessoais ou sigilosas através de ações de *hackers*.

Neste contexto, três elementos básicos são comuns em sistemas IoT: sensores, atuadores e gateways. Os sensores são responsáveis pela captura de informações específicas do ambiente, como temperatura, pressão e umidade. Os atuadores são responsáveis por executar ações no ambiente, como acender uma lâmpada ou abrir uma porta. Por sua vez, gateways atuam como um mediador na comunicação entre as coisas, dando suporte para heterogeneidade de padrões e protocolos (LINS; VIEIRA, 2021). Em outras palavras, o gateway atua como um *middleware* que facilita a comunicação entre coisas que utilizam protocolos distintos.

Por ser um elemento centralizador dentro de sistemas IoT, é vital que medidas de segurança sejam tomadas para tornar o gateway mais seguro. Uma forma de melhorar o nível de segurança de gateways IoT é fazendo uso de recursos criptográficos tanto na comunicação como no próprio armazenamento interno do gateway. No entanto segundo o padrão criptográfico NIST 800 - 57 Parte I (BARKER, 2020), existem diferentes algoritmos de criptografia, como por exemplo o AES - 128, AES - 192, AES 256, 2TDEA, 3TDEA, SHA - 1, SHA - 224, SHA - 256, SHA - 384, SKIPJACK, e muitos desses algoritmos não são considerados seguros atualmente pelo padrão criptográfico, como exemplo, podemos citar o

2TDEA, SHA - 1 e o SKIPJACK, que possuem forças de segurança frágeis aos mecanismos de invasões utilizados por *hackers*.

Para que o usuário não caia na falsa ideia de segurança, existem institutos internacionais de padrões e tecnologia renomados, como por exemplo o *National Institute of Standards and Technology* (NIST), que sugere diversos padrões e configurações de segurança. As organizações técnicas *IoT Security Foundation* (IoTSF) e *Open Web Application Security Project* (OWASP) focam inclusive no estudo de segurança em IoT, e sugerem requisitos de segurança para *software, hardware,* sistema operacional e interfaces da IoT. Os requisitos de criptografia destas organizações recomendam seguir padrões como por exemplo as recomendações dos seguintes documentos: FIPS 140 - 2 (TECHNOLOGY, 2002), FIPS PUB 46 - 3 (TECHNOLOGY, 1999), FIPS PUB 81 (TECHNOLOGY, 1980), FIPS PUB 180 - 1 (TECHNOLOGY, 1995), FIPS PUB 186-2 (TECHNOLOGY, 2000), NIST 800-131A (BARKER; ROGINSKY, 2019), e o NIST 800-57 Parte 1 (BARKER, 2020). Esses documentos sugerem e apresentam algoritmos e configurações de proteção criptográfica.

No entanto, apesar de ser peça chave no funcionamento da Internet das Coisas, a segurança de gateways IoT ainda não é abordada com profundidade pelas organizações técnicas relevantes da área. Este fato acaba dificultando a adoção de recursos criptográficos pelos gateways, e isso acaba contribuindo ainda mais para a sensação de falta de segurança por parte dos usuários. Por isso, é vital se avaliar o nível de conformidade dos gateways em relação a requisitos de criptografia e indicar possíveis ações para melhoria. Neste contexto, o objetivo principal deste trabalho é avaliar o nível de segurança de gateways IoT atualmente disponíveis considerando requisitos de criptografia.

1.1. Motivação

O relatório *Nokia Threat Intelligence Report* (NOKIA, 2020) alerta sobre o crescimento expressivo de ataques cibernéticos em dispositivos IoT. Segundo o relatório, em 2020, 33% dos dispositivos infectados foram dispositivos IoT, um aumento de 17% em relação ao ano de 2019. As informações presentes no relatório foram possíveis através do monitoramento do tráfego de rede em 150 milhões de equipamentos no mundo em que está presente o produto *NetGuard Endpoint Security* da Nokia. Diante do alto índice de ataques *hackers* em dispositivos conectados via Internet das Coisas surgiram diversos

questionamentos sobre o que poderia estar facilitando o acesso de ciberpiratas às informações pessoais e sigilosas dos usuários.

A Internet das Coisas pode tornar-se mais segura através do uso de recursos criptográficos. No entanto, dependendo do dispositivo IoT, nem todo algoritmo e protocolo criptográfico é adequado, devido a fatores como, heterogeneidade, baixa capacidade computacional e consumo energético dos dispositivos, sendo necessário realizar avaliações dos diferentes algoritmos de criptografia e protocolos (ALBARELLO; OYAMADA; CAMARGO, 2020). Nesse contexto, é válido ressaltar também a importância da criptografia para os gateways IoT, responsáveis em desempenhar um papel central no sistema IoT, resolvendo problemas de heterogeneidade. O seu comprometimento pode ser uma fonte de ameaça à segurança do sistema como um todo, devido, por exemplo, à sua característica de dar suporte para conexão entre dispositivos IoT e os serviços em nuvem. Desta forma, é possível afirmar que a criptografia é fundamental na segurança tanto dos gateways como do próprio sistema IoT como um todo, pois a segurança criptográfica ajuda a manter o sigilo e integridade das informações coletadas e as protege contra invasores.

Porém, nem todo algoritmo criptográfico é adequado para ser utilizado em gateways IoT. A escolha equivocada de um algoritmo ou o uso de uma configuração inadequada (ex.: tamanho de chave menor que o recomendado) pode levar a sérios problemas para a confidencialidade dos dados, tanto na comunicação como no armazenamento dos mesmos. Por outro lado, diversas referências relevantes na literatura como por exemplo, IOTSF e OWASP sugerem requisitos e técnicas para serem seguidas em relação a segurança criptográfica de *hardware e software*. No entanto, requisitos de criptografia para gateway IoT não são priorizados ou mesmo inspecionados efetivamente. Por outro lado, alguns trabalhos propõem requisitos ou recomendam seguir organizações técnicas que sugerem requisitos de criptografia para ambientes IoT. Choi *et al.* (2018) analisam e inspecionam requisitos de criptografia de uma organização técnica internacional em plataformas IoT. Lins e Vieira (2021) apresentam e utilizam uma metodologia de engenharia de requisitos para a avaliação de segurança de gateways IoT; no entanto, demonstram apenas dois requisitos de criptografia e a inspeção de requisitos de segurança criptográfica em gateways IoT não é o foco principal do artigo. Ning *et al.* (2020) apresentam uma estratégia de avaliação de segurança criptográfica para segurança de dispositivos IoT na área da saúde. Em resumo, nenhum dos trabalhos encontrados atualmente na literatura são voltados especificamente à inspeção de

requisitos de criptografia em gateways IoT.

Neste contexto, torna-se necessária a adoção de medidas de segurança que proporcionem uma criptografia de melhor qualidade para gateways IoT, evitando assim vazamento de dados ou informações pessoais dos usuários. Assim, este trabalho busca avaliar o nível de segurança criptográfica em gateways IoT atualmente utilizados pela comunidade. Para tal fim, inicialmente busca-se as principais entidades ou órgãos regulamentadores internacionais que propõem requisitos de criptografia para Internet das Coisas. Esta busca objetiva conduzir a análise e seleção de requisitos de criptografia propostos em documentos técnicos que sejam aplicáveis aos gateways IoT. Na etapa seguinte, busca-se realizar pesquisa dos principais gateways IoT baseados em *software*, selecionar os mais utilizados, efetuar instalação e configuração em um raspberry pi. Dando seguimento, busca-se sugerir, descrever e desenvolver uma metodologia de avaliação de requisitos de criptografia em gateways IoT. Esta metodologia tanto servirá como descrição e detalhamento do processo de avaliação como também poderá ser utilizada para realizar esta avaliação em outros contextos. Por fim, busca-se realizar inspeção e avaliação de requisitos de criptografia em gateways IoT baseados em software. Esta avaliação e inspeção servirá para diagnosticar como está a segurança criptografia utilizada pelos principais desenvolvedores de gateways IoT atualmente.

1.2. Objetivos

A seguir são apresentados os objetivos propostos para o desenvolvimento deste trabalho.

1.2.1. Objetivo Geral

Avaliar o nível de segurança criptográfica de gateways IoT.

1.2.2. Objetivo Específico

- ➢ Propor e descrever uma metodologia de avaliação de requisitos de criptografia em gateways IoT. Esta metodologia tanto servirá como descrição e detalhamento do processo de avaliação como também poderá ser utilizada para realizar esta avaliação em outros contextos (pesquisa reproduzível);
- ➢ Pesquisar, analisar e selecionar requisitos de criptografia sugeridos por organizações técnicas internacionais reconhecidas pela comunidade científica. A decisão de se

buscar estas organizações se baseia no fato que elas, em geral, representam um número representativo de pessoas interessadas;

- ➢ Pesquisar, analisar, selecionar e configurar gateways IoT baseados em *software* e de código aberto. Essa pesquisa, análise e seleção ajudará localizar, priorizar e configurar adequadamente os gateways IoT mais utilizados pela comunidade;
- ➢ Realizar a inspeção dos requisitos de criptografia selecionados em gateways IoT. Esta inspeção proporcionará avaliações mais assertivas dos gateways IoT, possibilitando diagnosticar possíveis pontos de melhorias em relação a segurança criptográfica.

1.3. Organização

A seguir será apresentada a estruturação do restante deste documento.

O Capítulo 2 apresenta a fundamentação teórica, proporcionando compreender o cenário atual em relação a segurança criptográfica e como se encontram os estudos a respeito do tema, descrevendo conceitos fundamentais para o entendimento deste trabalho.

O Capítulo 3 apresenta os trabalhos relacionados a segurança criptográfica e inspeção de requisitos de criptografia em dispositivos IoT. São apresentados exemplos de trabalhos que utilizam criptografia para diversas finalidades e que possui relação com a IoT, como para inspeção de requisitos de segurança criptográfica em plataformas IoT, metodologia de engenharia de requisitos para avaliação de segurança de gateways IoT e estratégia de avaliação de criptografia para segurança de dispositivos IoT.

O Capítulo 4 descreve a metodologia, modelada em BPMN, para avaliação de requisitos de segurança criptográfica em gateway IoT. O padrão BPMN foi escolhido para representação da metodologia proposta devido sua larga adoção pela comunidade, facilitando o entendimento das atividades e processos.

O Capítulo 5 apresenta em detalhes as etapas realizadas para a execução da avaliação de segurança de gateways IoT considerando requisitos de criptografia. Esta avaliação é executada baseada na metodologia proposta no capítulo 4.

Por fim, o Capítulo 6 apresenta as conclusões obtidas, as contribuições realizadas e os trabalhos futuros sugeridos para a realização de novas pesquisas relacionadas a esta dissertação.

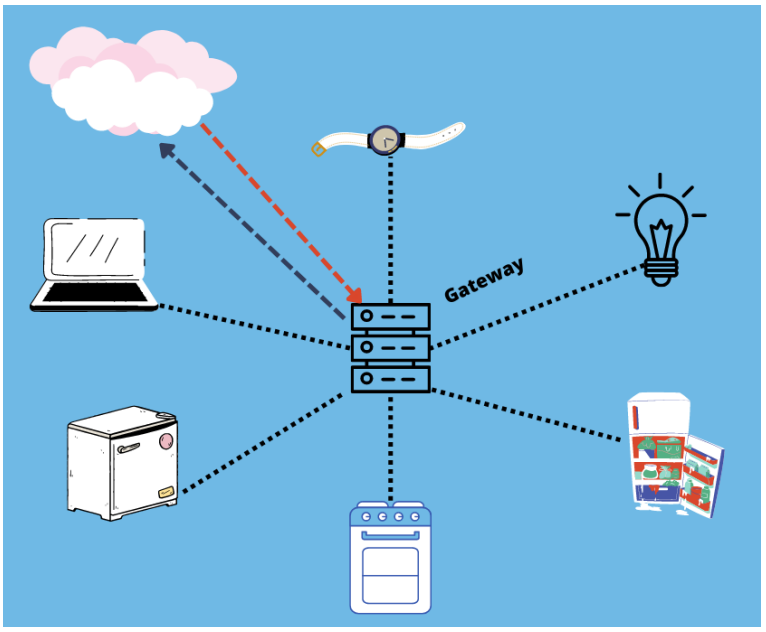
2. Fundamentação Teórica

Neste capítulo são apresentados os principais conceitos necessários para a compreensão desta dissertação. A Seção 2.1 apresenta conceitos básicos relacionados à Internet das Coisas. A Seção 2.2 apresenta e detalha gateways no contexto da Internet das Coisas; este tópico é especialmente interessante porque os gateways são o foco deste trabalho. Por sua vez, a Seção 2.3 descreve o que é criptografia e a sua importância para Internet das Coisas. Por fim, a Seção 2.4 apresenta as considerações finais deste capítulo.

2.1. Internet das Coisas

A Internet das Coisas pode ser considerada uma extensão da Internet atual, que proporciona aos objetos do dia-a-dia capacidade computacional e de comunicação (SANTOS *et al*., 2016). Esta conexão proporciona aos usuários estar em constante comunicação com outras pessoas ou objetos. Para Noleto (2020) a Internet das Coisas vai muito além de computadores, celulares ou tablets; ela engloba outros equipamentos como carros, aparelhos de som e geladeiras. Por sua vez, Luiz (2020) define Internet das Coisas como sendo uma tecnologia emergente que fornece a todos os objetos físicos presença virtual na internet. Compreender o funcionamento de um sistema IoT é importante para identificar as necessidades de segurança de determinados objetos. Assim sendo, a Figura 1 apresenta um exemplo de um sistema IoT composto por 6 dispositivos IoT, um gateway e a nuvem (internet).

Figura 1 – Rede IoT, processo de comunicação entre dispositivos.



Fonte: O autor (2022).

Através do exemplo da Figura 1 é possível observar a importância de um gateway para um sistema IoT. Neste exemplo, cada dispositivo utiliza um protocolo de comunicação diferente e para que a comunicação entre os dispositivos aconteça é necessário o auxílio de um gateway, atuando como um mediador. Assim sendo, os sensores de cada dispositivo com o auxílio dos atuadores enviam as informações através da rede interna da residência para o gateway IoT que realiza a tradução para o protocolo nativo de cada dispositivo, possibilitando que a comunicação entre os objetos (“coisas”) aconteça.

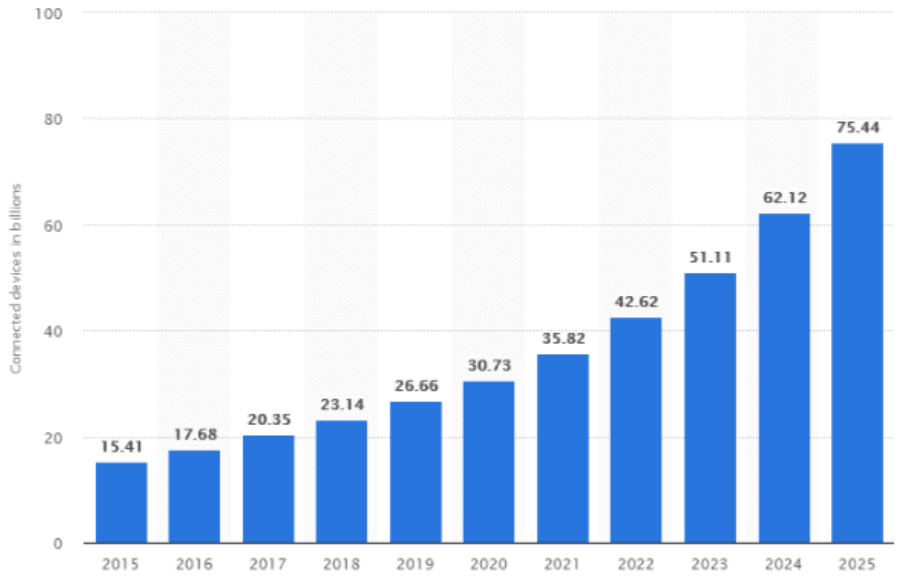
Neste exemplo, também é possível perceber que o gateway IoT na maioria das vezes é o responsável por enviar todas as informações dos dispositivos para a nuvem (Internet). Na Internet das Coisas os gateways atuam como um intérprete fazendo a interligação entre redes. Eles fazem uso de dois protocolos de comunicação e realizam a tradução entre eles (CODEIOT, 2022). Deste modo, no exemplo da Figura 1 para que haja comunicação entre os dispositivos (“coisas”) ou com a nuvem (Internet) é necessário fazer uso de um gateway.

Outro fato que tem chamado atenção atualmente é o crescimento acelerado da Internet das Coisas. De acordo com Vailshery (2021), em 2018 já havia mais de 22 bilhões de dispositivos conectados em todo o mundo. E as previsões sugerem que até 2030 sejam mais de 50 bilhões de dispositivos IoT. Este crescimento é notado também por SYDLE (2022), que apresenta dados relevantes em relação a IoT nos últimos anos, através de um relatório feito

por uma empresa especializada em dados de mercado e consumidores (Statista) (“Statista - The Statistics Portal”, [s.d.]) que afirma a existência em 2021 de mais de 35, 8 bilhões de dispositivos IoT conectados no mundo. SYDLE (2022) afirma também que a Internet das Coisas se tornou rapidamente uma das tecnologias mais difundidas do século 21, chegando em diferentes níveis sociais, países ou alcance econômico. E que esse fenômeno pode ser explicado através da computação de baixo custo.

Ao analisar o gráfico apresentado na Figura 2, disponibilizado pelo departamento de pesquisas da Statista, é possível observar dados relevantes em relação ao quantitativo de dispositivos IoT existentes atualmente. A análise da figura proporciona também compreender a curva de crescimento projetada em relação ao número de dispositivos IoT conectados entre os anos de 2015 e 2025.

Figura 2 – Número de dispositivos IoT projetados entre os anos de 2015 e 2025.



Fonte: Statist (2022)[1].

Ao analisar o gráfico da Figura 2, percebemos um crescimento acentuado no número de dispositivos IoT em um intervalo curto de tempo. A previsão é que em 2025 existam mais de 75 bilhões de dispositivos IoT conectados, o que corresponde a mais de 5 vezes o número de dispositivos existentes no ano de 2015.

Com o crescimento da Internet das Coisas cresce também o número de ataques hackers em dispositivos IoT. Se bem-sucedidos, estes ataques podem comprometer o funcionamento

[1] Disponível em: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/> acesso em: 31 maio 2022.

dos dispositivos ou da rede IoT e capturar informações confidenciais dos usuários.Diante destes fatos, é válido enfatizar que os desenvolvedores e fornecedores IoT devem prezar por utilizar algoritmos que façam uso de uma criptografia validada e aprovada por padrões ou organizações técnicas reconhecidas, evitando assim que informações importantes dos usuários sejam capturadas por *hackers* e que dispositivos IoT sejam comprometidos ou inutilizados.

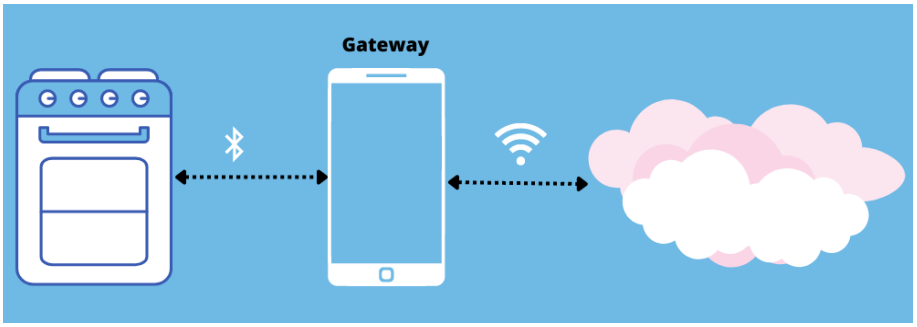
2.2. Gateway

Atualmente, sistemas IoT estão cada vez mais usando gateways para possibilitar a comunicação de equipamentos (“coisas”) em um sistema IoT. As “coisas” podem ser implementadas e se comunicarem utilizando tecnologias distintas, e o gateway é capaz de fazer esta mediação entre estes diferentes contextos.

Na Internet das coisas, em geral, os objetos (“coisas”) se comunicam com um gateway utilizando padrões de comunicação de curta distância, como por exemplo *Bluetooth*, *Bluetooth Low Energy* e *Zigbee*. Já a comunicação entre o gateway e a Internet acontece normalmente utilizando padrões de comunicação de longa distância, como por exemplo: WiFi, *Ethernet*, GPRS, 3G e 4G (CODEIOT, 2022). Desta forma o gateway passa a assumir o papel de um mediador, ajudando na conexão dos objetos (“coisas”) com a Internet.

Segundo Parra Rodrigues *et al*. (2016), o gateway possui dupla função, ele permite que dispositivos com diferentes protocolos se comuniquem entre si e, ao mesmo tempo que, ele pode também processar dados para fins de agregação, análise ou segurança e pré-formar armazenamento temporário de dados. A Figura 3 mostra um exemplo de conexão de um fogão inteligente que utiliza um aparelho celular como gateway para comunicação com a nuvem.

Figura 3 – Exemplo de gateway IoT.



Fonte: O autor (2022).

Na Figura 3, o aparelho celular assume o papel de um gateway ao intermediar a

comunicação entre o fogão e a nuvem. Desta forma, ele recebe os dados enviados pelo fogão através da conexão Bluetooth e os envia para a nuvem utilizando uma rede wifi.

A comunicação de informações deve ocorrer de forma segura, minimizando as chances de violação de dados ou perda de informação. Desta forma, a segurança do gateway IoT deve ser reforçada, pois o mesmo tem um papel central em um sistema IoT. É importante destacar também que milhões de informações, inclusive sigilosas, passam diariamente pelos gateways, e o comprometimento deste dispositivo através de um ataque *hacker* bem-sucedido pode ocasionar perdas irreparáveis para os usuários e para o fornecedor.

Deste modo, o uso de algoritmos de criptografia validados por um padrão de segurança criptográfica reconhecido pela comunidade, proporciona maior segurança e menor risco de obtenção de informações indevida do gateway, pois ao fazer uso de um conjunto de técnicas criptográficas apenas o emissor e o receptor saberão o conteúdo das mensagens trafegadas entre os gateways e os demais dispositivos IoT. Desta forma, a chance de obtenção indevida de dados diminui consideravelmente.

2.3. Criptografia

Com o crescimento expressivo da IoT, diversos questionamentos surgiram em relação à segurança de dispositivos, como por exemplo até que ponto são considerados seguros e o que acontece com as informações trafegadas entre eles. Pensando neste contexto, torna-se necessário implementar o melhor nível de segurança criptográfica possível nestes dispositivos. Como o gateway IoT é um local de convergência de informações, acaba se destacando em relação aos demais dispositivos, e por isso deve receber foco especial em questões de segurança.

Segundo Machado *et al.* (2021), os algoritmos de criptografia de dados são divididos em duas categorias: os simétricos, que possuem apenas uma chave compartilhada entre o emissor e o receptor, e os de criptografia assimétrica, que possui uma chave pública e uma chave privada. No entanto, para realização da avaliação de criptografia, é necessário conhecer um pouco mais sobre quais são os algoritmos de criptografia existentes e quais utilizar no processo criptográfico de determinado sistema ou dispositivo, quais são os tamanhos de chaves considerados ideais para melhorar a segurança dos dispositivos e sistemas, e quais são os padrões e organizações técnicas que devemos seguir neste processo, dentre outras

atividades.

Em termos de padronização, o *National Institute of Standards and Technology* (NIST), em parceria com um conjunto de empresas dos Estados Unidos da América, desenvolveu padrões de criptografia que auxiliam desenvolvedores e fornecedores de recursos tecnológicos a melhorar a segurança criptográfica dos seus produtos. Cada padrão é voltado para um objetivo específico. Por exemplo, o FIPS 140 - 2 apresenta requisitos para segurança de um módulo criptográfico, o FIPS PUB 186-4 é um padrão para assinatura digital e o NIST 800-131A visa dar suporte aos desenvolvedores no processo de transição de algoritmos e comprimento de chave.

Algumas das principais organizações técnicas reconhecidas pela comunidade científica da área de Segurança e IoT, como por exemplo *Internet of Things Security Foundation* (IOTSF), *Open Web Application Security Project* (OWASP), *European Union Agency for Cybersecurity* (ENISA), dentre outras, apresentam requisitos de criptografia avaliados por um conjunto de empresas. Algumas destas organizações apresentam requisitos específicos para dispositivos IoT, como por exemplo, o IOTSF. Estas organizações focam em resolver problemas de vulnerabilidades do cotidiano possibilitando que os dispositivos se conectem de forma segura.

2.4. Considerações finais

Neste capítulo foram descritos os principais conceitos teóricos utilizados nesta dissertação. Foi apresentado o que é a Internet das Coisas, seu funcionamento e conceitos. Descreveu-se a estrutura básica de um sistema IoT e como ocorre o funcionamento de um gateway. Também se realizou uma análise sobre o que é criptografia e a sua importância para o funcionamento da IoT e para sua segurança. Todos estes conceitos serão usados nos próximos capítulos desta dissertação, e seu aprofundamento aqui servirá como base para um entendimento mais profundo das contribuições científicas deste trabalho.

3. Trabalhos Relacionados

A criptografia, quando aplicada da forma recomendada, torna a IoT mais segura e confiável. No entanto, existe uma lacuna na literatura em relação não apenas a avaliação de criptografia em gateways IoT, como também relacionada à definição de requisitos de criptografia para este componente específico. Desta forma, neste capítulo é apresentado como foi conduzida a busca pelos trabalhos relacionados dentro desta temática e quais foram os resultados obtidos. Em especial, é evidenciado como esta lacuna mencionada foi observada. A Seção 3.1 apresenta como foi realizado o mapeamento sistemático da literatura. A Seção 3.2 apresenta uma discussão sobre os principais trabalhos relacionados. A Seção 3.3 realiza uma análise comparativa entre os trabalhos discutidos na seção anterior. Por fim, a Seção 3.4 apresenta as considerações finais referente a este capítulo.

3.1. Mapeamento Sistemático de Literatura

Nesta etapa, é realizado um levantamento da literatura existente relacionado ao tema da pesquisa. Na Tabela 1, é apresentado e detalhado o protocolo do mapeamento sistemático proposto.

Tabela 1 – Protocolo do mapeamento sistemático proposto.

Meta da Pesquisa: buscar material científico que aborde requisitos de segurança e/ou de criptografia em IoT, e/ou que realize inspeção de requisitos de segurança em gateways IoT.			
Local da Pesquisa: Bases de Dados Científicas			
IEEE Xplore Digital Library; Springer Link; ACM Digital Library; Scopus; Google Scholar; Web of Science; Wiley Online Library.			
***Strings* de Busca**			
➢ *IOT AND Gateway AND Evaluation NOT Performance* ➢ *Gateway AND Analysis NOT Performance* ➢ *IoT AND "Requirements Security" NOT Performance* ➢ *"Internet of things" AND "Requirements Security" NOT Performance*			
Critérios de Busca nas Base de Dados Científicas			
Anos de Publicação: 2016 a 2021	Tipo de Documento: Artigo	Idioma do Documento: Todos	Busca Realizada no: Título
Etapas de Buscas e Verificação Documental			
1) Selecionar bases de busca; 2) Realizar pesquisa documental conforme *string* e critérios de busca determinados; 3) Analisar e excluir documentos repetidos; 4) Eliminar artigos que não apresentam resumo em conformidade com os objetivos da pesquisa; 5) Analisar e excluir artigos que não apresentam conclusões em conformidade com este trabalho; 6) Examinar o artigo por inteiro, selecionando trabalhos relacionados aos objetivos da pesquisa.			

Fonte: O autor (2022).

Ao se realizar as buscas das *strings* de palavras nas sete bases de dados científicas, seguindo os protocolos definidos na Tabela 1, obteve se um total de 92 artigos. Ao se efetuar a etapa de verificação documental correspondente a exclusão e retirada dos artigos repetidos, 36 artigos foram retirados, obtendo-se ao final desta etapa 56 documentos. Com a finalização das análises seguindo as demais etapas de verificação documental apresentadas na Tabela 1, foram selecionados e priorizados nove artigos científicos relacionados diretamente aos objetivos desta pesquisa.

3.2. Discussão

Esta seção descreve os principais trabalhos relacionados à inspeção de requisitos de segurança em dispositivos IoT.

Choi *et al*. (2018) analisam e inspecionam requisitos de segurança criptográfica sugeridos pelo padrão de classificação de dispositivos e requisitos de segurança da Internet das Coisas da associação coreana de tecnologia da informação e comunicação (TTAK.KO-12.0298) (TTA, 2016) nas plataformas IoT de código aberto AllJoyn, oneM2M e IoTivity. É possível afirmar que os autores conseguiram classificar e avaliar o nível de segurança criptográfica destas plataformas. Após análise, os autores concluíram que as plataformas oferecem tecnologias criptográficas para suporte a serviços de segurança, como confidencialidade, integridade, autenticação e autorização. Contudo, dispositivos IoT com recursos limitados, como sensores de monitoramento de pressão arterial, apresentam mais dificuldades para a aplicação das técnicas criptográficas existentes. No entanto, a metodologia de avaliação não foi demonstrada e seus requisitos não possuem relação especificamente com uso de criptografia em gateways IoT. Além disso, os autores se limitaram a seguir recomendações de apenas uma um padrão técnico internacional da área.

Lins e Vieira (2021) apresentam e descrevem uma metodologia de engenharia de requisitos para a avaliação de segurança de gateways IoT. Os autores propõem metas de segurança de alto nível para gateways IoT baseadas nos seguintes princípios: comunicações criptografadas multidirecionais; autenticação forte de componentes; armazenamento (quantidade mínima de informações e para armazenar em formato criptografado); negação de serviço e mitigação de ataque de repetição; registro e alerta; detecção de anomalias e recursos de relatório; use os componentes de terceiros mais recentes e atualizados; e atualizações

automáticas e/ou relatórios de versão. Desta forma, são pesquisados, selecionados e priorizados requisitos de segurança que estejam conforme o solicitado nas metas propostas. Os autores apresentam, analisam e especificam mais de uma referência ou padrão técnico internacional para seleção dos requisitos de segurança. No entanto, pode-se afirmar que os mesmos apresentaram poucos requisitos de criptografia em si e efetuaram inspeção de requisitos de forma parcial, limitando-se a verificação de conformidade apenas na documentação dos gateways. Além disso, a inspeção de requisitos de criptografia em gateways IoT não é o foco principal do artigo.

Ning *et al*. (2020) apresentam uma estratégia de avaliação de criptografia para segurança de dispositivos IoT na área da saúde. Segundo os autores a estratégia é focada na avaliação e seleção das melhores cifras criptográficas leves, considerando requisitos como, desempenho, físico e segurança, sugeridos pelo *National Institute of Standards and Technology* (NIST) e pelo padrão *International Standard Organization* ISO/IEC 29192. A estrutura pode ser usada como referência para inspeção e classificação de cifras criptográficas leves na área da saúde ou em qualquer outro ambiente, concentrando-se basicamente nas características físicas e de desempenho das cifras. No entanto, os autores não realizam a inspeção de segurança criptográfica desses requisitos nos dispositivos em si.

Imdad *et al.* (2020) apresentam sete requisitos de segurança que podem ser utilizados para evitar ataques em redes IoT; no entanto, os autores não especificam a fonte dos requisitos. Cada requisito é voltado para segurança do sistema ou de uma camada específica da rede IoT, objetivando alcançar a segurança completa do sistema, desde requisitos de confidencialidade, integridade, disponibilidade, autenticação, autorização, não repúdio até privacidade. Assim sendo, o documento apresenta os desafios de segurança enfrentados por uma rede IoT, os classificando em duas categorias: desafios tecnológicos que surgem devido à heterogeneidade e onipresença dos dispositivos, e os e desafios de segurança voltados para funcionalidades básicas do sistema. Assim, os autores apresentam uma lista de todos os requisitos de segurança, juntamente com os ataques, camada afetada da rede IoT, impacto na segurança, componente do sistema afetado e solução proposta. Por exemplo: um ataque de repetição, pode falsificar a identidade de um ou mais dispositivos, comprometendo a camada de percepção em IoT, prejudicando assim, principalmente a confidencialidade dos sistemas. Entretanto, os autores não propuseram uma metodologia de avaliação que detalhasse como os requisitos podem ser aplicados na segurança da rede e não realizaram inspeção dos requisitos

de segurança.

Ankele *et al*. (2019) realizam análise de segurança e testes de penetração em sistemas IoT, com foco especial em IoT industrial. Nesse contexto, os autores analisam as ferramentas de teste de segurança mais usadas em sistemas e redes IoT. O trabalho proposto ajuda a automatizar o processo de teste de penetração, modelagem de ameaças e análise de segurança em sistemas IoT e IoT industrial. Entre os requisitos apresentados é mencionada a criptografia, porém não são citados quais algoritmos são utilizados, quais são os comprimentos das chaves criptográficas e se os requisitos de criptografia são retirados de organizações ou padrões técnicos bem reconhecidos pela comunidade científica. Os autores exaltam a importância do gateway para a IoT, contudo não especificam se realizam inspeções de requisitos de criptografia nos gateways utilizados.

Hansch *et al*. (2019) apresentam um modelo de arquitetura baseada em *Open Platform Communications Unified Architecture* (OPC UA). A arquitetura OPC UA é composta por um conjunto de padrões e especificações para comunicação industrial que permite a troca de informações, através da integração dos equipamentos de chão de fábrica com os sistemas de controle. A arquitetura proposta pelos autores busca realizar a verificação de requisitos de segurança na IoT industrial. Tendo como objetivo automatizar o processo de verificação de requisitos em conformidade com a norma técnica IEC 62443 (“ISA/IEC 62443 Cybersecurity | ISA São Paulo Section”, [s.d], p. 62443). Essa norma é uma série de padrões que abrange segurança para sistemas de controle industrial através de sete requisitos fundamentais de segurança: controle de identificação e autenticação, controle de uso, integridade do sistema, confidencialidade de dados, fluxo de dados restrito, resposta oportuna a eventos e disponibilidade de recursos. Assim sendo, os autores realizaram testes de segurança em quatro grandes protótipos de IIoT de um projeto de referência realizado por 14 parceiros industriais e 7 laboratórios de pesquisa na Alemanha. Ao todo, são utilizados 418 requisitos de segurança. Alguns dos requisitos descrevem os componentes internos dos sistemas, como criptografía de disco rígido para confidencialidade ou balanceamento de carga para maior disponibilidade. Contudo, os autores não definem uma metodologia de avaliação de requisitos, não apresentam os resultados dos testes realizados durante a inspeção nas máquinas industriais e os testes realizados não estão relacionados exclusivamente com a segurança dos gateways IoT.

Parra Rodriguez *et al.* (2016) propõem uma arquitetura de segurança centrada em dados para sistemas que usam gateways IoT. Assim sendo, os autores apresentam a

arquitetura de segurança como solução para os requisitos de controle de acesso e privacidade de dados em dispositivos IoT, que fazem uso de mecanismos de segurança criptográfica. No artigo são apresentados três requisitos de segurança centrados em dados. 1) um usuário pode conceder acesso a dados a outros usuários enquanto mantendo-o confidencial para entidades não autorizadas. 2) A identidade associada aos dados acessados só pode ser determinada por um conjunto de entidades autorizadas. 3) Um usuário pode expor parcialmente dados a entidades externas a fim de proteger sua privacidade. No entanto, não é especificado a fonte dos requisitos. As soluções de segurança são apresentadas baseadas em perímetro, como por exemplo para um determinado perímetro os autores apresentam uma solução chamada de ambientes de execução confiável, no qual o usuário possui a proteção que necessitam para os seus dados através da junção de algumas tecnologias atualmente existentes. Uma das soluções apresentadas é a SMART, uma primitiva baseada em hardware de microcontrolador de baixo custo e software TCB que protege tarefas por meio de memória somente leitura e fornece mecanismos de atestado. No entanto, não realizam inspeção dos requisitos em gateway IoT e não apresentam uma metodologia de avaliação de requisitos.

Papcun *et al.* (2020) introduzem uma metodologia de avaliação para gateway IoT habilitado para borda da rede. Os autores apresentam um conjunto de 14 critérios para avaliação de uma arquitetura geral IoT habilitada para borda. Os critérios da avaliação são retirados de artigos científicos e são classificados em quatro categorias: conectividade do dispositivo, pré-processamento de dados, análise de dados e requisitos especiais de hardware. Na categoria análise de dados, um dos critérios analisados é a criptografia. É verificado se o gateway faz uso de ferramentas que ofereçam recursos para uma melhor criptografia dos dados. Cada critério é identificado com pesos conforme a sua importância. Entretanto, não existe um aprofundamento e detalhamento da segurança criptográfica dos dispositivos analisados.

Kamalrudin *et al.* (2018) propuseram uma biblioteca de requisitos de segurança de IoT para o desenvolvimento de aplicativos. Segundo os autores, a biblioteca ajuda os engenheiros de software a prover maior segurança no aplicativo logo na fase inicial do desenvolvimento. Para atingir esse objetivo, a biblioteca faz uso da correspondência de palavras para sugerir e categorizar os requisitos de segurança com base nas propriedades de segurança corretas para cada uma das aplicações. Assim sendo, a biblioteca apresenta os atributos que cada uma das aplicações necessitam, como por exemplo, redes de mobilidade, sistemas RFID, wi-fi,

bluetooth e sensores, e os categoriza conforme suas propriedades de segurança (como por exemplo autenticação, confidencialidade, integridade, autorização e controle de acesso). Contudo, requisitos de criptografia não são citados e também não é citado se os requisitos de segurança são retirados de algum padrão ou norma técnica reconhecida pela comunidade científica.

3.3. Visão Comparativa

A Tabela 2 apresenta uma visão geral dos trabalhos relacionados apresentados neste capítulo. Estes trabalhos são avaliados de acordo com os seguintes critérios: I) se os artigos buscam requisitos de segurança apresentados por organizações técnicas ou padrões internacionais; II) Se apresenta uma metodologia de avaliação não necessariamente de requisitos de criptografia; III) se existe uma seleção de requisitos de criptografia; IV) se foi realizado inspeção nos requisitos propostos; e V) se as inspeções foram realizadas em gateways IoT.

Saber se os artigos seguem orientações de organizações técnicas conhecidas é útil para mostrar a origem dos requisitos e se foram sugeridos por uma equipe qualificada de profissionais ou grupo de empresas. O segundo critério busca saber se foi descrita uma metodologia de avaliação. Com uma metodologia bem definida é possível compreender e replicar a avaliação conduzida. O terceiro critério foca na seleção de requisitos de criptografia. O quarto critério tem como objetivo verificar se os autores realizaram inspeções nos dispositivos usando como base os requisitos de criptografia. O último critério avalia se os trabalhos realizam inspeções de requisitos de segurança, ou seja, não necessariamente de criptografia, especificamente em gateways IoT.

Tabela 2 – Trabalhos relacionados.

Trabalho Relatado	Se baseia em padrões internacionais	Apresenta Metodologia Detalhada	Realiza Seleção dos Requisitos de Criptografia	Realiza a Inspeção de Requisitos de criptografia	Realiza a Inspeção de Requisitos de Segurança em Gateways IoT
Ning *et al*. (NING *et al*., 2020)	Sim	Sim	Sim	Não	Não
Imdad *et al*. (IMDAD *et* al., 2020)	Não	Não	Não	Parcialmente	Não
Ankele *et al.* (ANKELE *et al*., 2019)	Não	Não	Não	Não	Não
Papcun *et al*. (PAPCUN *et al*., 2020)	Não	Sim	Não	Não	Não
Kamalrudin *et a*l. (KAMALRUDIN *et al*., 2018)	Não	Não	Não	Não	Não
Choi *et al*. (CHOI *et al.*, 2018)	Sim	Não	Sim	Sim	Não
Lins e Vieira (LINS; VIEIRA, 2021)	Sim	Sim	Parcialmente	Parcialmente	Parcialmente
Hansch e*t al.* (HANSCH e*t al*., 2019)	Sim	Sim	Não	Parcialmente	Não
Parra Rodriguez *et al.* (PARRA RODRIGUEZ *et al*., 2016)	Sim	Não	Não	Não	Não

Fonte: O autor (2022).

Ao se analisar a Tabela 2, pode-se verificar que apenas os trabalhos de Ning et al., Choi et al., Lins e Vieira, Hansch et al. e Parra Rodriguez seguem recomendações de organizações técnicas. É importante ressaltar que, desses cinco trabalhos, apenas dois analisaram mais de uma organização técnica. Por outro lado, apenas os trabalhos de Ning et. al., Papcun et al., Lins e Vieira e Hansch, apresentam e detalham a metodologia de avaliação, e dentre eles apenas um tem foco específico na seleção de requisitos de segurança para gateways IoT.

Em relação ao processo de seleção de requisitos de criptografia, apenas os artigos de Ning et al., Choi et al. e Lins e Vieira. fazem esta atividade. Quando é analisado se os trabalhos realizam inspeção de requisitos, não necessariamente requisito de criptografia, apenas os trabalhos de Imdad et al., Lins e Vieira e Hansch efetuam avaliações, sendo que dois deles o fazem de forma parcial, realizando apenas inspeção de alguns requisitos apresentados ou trabalhando apenas um dos critérios de verificação de conformidade de requisitos, como por exemplo, apenas avaliação documental. Também foi verificado se os

trabalhos realizam inspeções de requisitos de segurança em gateways IoT, e apenas o trabalho de Lins e Vieira faz, e de forma parcial, realizando apenas avaliação documental. Isso mostra a evidente lacuna existente na questão de avaliação de segurança de gateways IoT considerando requisitos criptográficos.

Em contraste ao estado da arte apresentado, esta dissertação apresenta uma metodologia de avaliação, descrita em BPMN, para dar suporte ao processo de pesquisa, seleção, priorização, avaliação e inspeção de requisitos de criptografia. Esta metodologia é utilizada para realizar efetivamente a avaliação de requisitos de criptografia em gateways IoT utilizados atualmente. A avaliação proposta nesta dissertação ajuda a compreender, de forma sistematizada e considerando padrões e documentos amplamente adotados, como se encontra o estado atual da segurança em termos de criptografia de gateways IoT.

3.4. Considerações finais

Este capítulo detalhou como foram conduzidas a pesquisa por trabalhos relacionados a temática desta dissertação. Com o levantamento bibliográfico, foi possível visualizar uma visão geral do estado da arte da área. Com esta visão geral, foi possível observar contribuições científicas e tecnológicas existentes, assim como possíveis lacunas a serem mais bem pesquisadas. Neste contexto, uma destas lacunas foi escolhida como tema principal desta dissertação: a avaliação de requisitos criptográficos em gateways IoT.

4. Metodologia Para Avaliação de Segurança de Gateways IoT Considerando Requisitos de Criptografia

Este capítulo introduz e detalha uma das principais contribuições desta dissertação, a metodologia para avaliação de segurança criptográfica de gateways IoT. A proposição da metodologia visa dois objetivos: estruturar o corpo de conhecimento necessário para a execução da citada avaliação e também tornar a avaliação reproduzível, baseada na ideia do *reproduceable research*[2].

O presente capítulo está estruturado da forma que se segue. A Seção 4.1 apresenta e descreve a metodologia proposta. As Seções 4.2 até a 4.7 descrevem as atividades e subprocessos desta metodologia. Por fim, na Seção 4.8 são apresentadas as considerações finais do capítulo.

4.1. Metodologia proposta

Muitas organizações técnicas desenvolveram documentos que fornecem as melhores práticas de segurança no ambiente IoT. Assim, são propostos e detalhados requisitos de segurança, que ajudam na tomada de decisão dos usuários sobre qual tecnologia adquirir para lidar com os seus dados. Neste contexto, apesar da segurança da IoT despertar preocupação dos usuários, poucas informações, incluindo requisitos, estão disponíveis sobre a segurança do gateway em organizações técnicas. Levando em consideração a importância da segurança do gateway IoT, foi criada uma metodologia de avaliação de requisitos criptográficos visando melhorar a segurança das informações que trafegam pelos gateways.

Esta metodologia é composta por seis atividades, onde algumas delas são subprocessos. Esta metodologia foi projetada tendo como base o padrão *Business Process Model and Notation* (BPMN). Este padrão é bastante utilizado por proporcionar facilidade na compreensão dos seus processos e também porque é vastamente utilizado para a descrição de processos de negócio. A Figura 4 apresenta a metodologia proposta.

[2] Reproduceable research: possibilita ao leitor reproduzir a pesquisa realizada por outro pesquisador. Isto é possível porque o outro pesquisador escreveu sua pesquisa de forma suficientemente completa e estruturada.

Figura 4 – Metodologia para avaliação de segurança de gateways IoT considerando requisitos de criptografia.

Fonte: O autor (2022).

A primeira atividade da metodologia tem foco na definição dos objetivos da avaliação a ser realizada. Em seguida, é realizada a pesquisa e priorização das referências bibliográficas de segurança que nortearão o estudo. Dando seguimento, no próximo subprocesso é feita a análise e seleção dos requisitos de criptografia, e neste momento os requisitos selecionados passam por um filtro que tem como objetivo identificar se o requisito é "entendível", "verificável" e "aplicável" ao contexto da avaliação. Depois disto, é realizada a busca, instalação e configuração dos gateways IoT que serão avaliados no estudo. Após a configuração destes gateways, os requisitos de criptografia podem ser inspecionados. Por fim, no último subprocesso da metodologia, é realizada a comparação dos resultados obtidos considerando os diversos gateways selecionados.

As subseções a seguir detalham as atividades e subprocessos contidos na metodologia proposta.

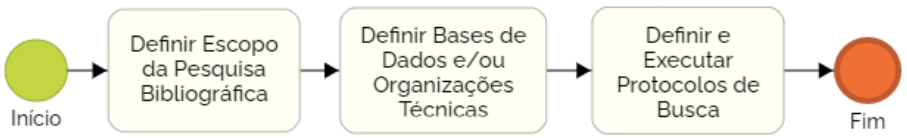
4.2. Definir metas

A definição de metas permite uma melhor compreensão do escopo da avaliação a ser realizada. Por exemplo, é possível ter metas relacionadas tanto a verificar o uso de criptografia como também relacionadas à qualidade desse uso (ex.: algoritmo usado e tamanho de chave). As metas definidas nesta atividade irão guiar o planejamento e execução de todas as atividades seguintes da metodologia proposta.

4.3. Pesquisar e priorizar referências

A pesquisa de referencial teórico é fundamental para a avaliação a ser realizada, pois proporciona a busca de fontes adequadas para nortear os requisitos técnicos a serem considerados na inspeção e avaliação. A Figura 5 apresenta a modelagem do subprocesso correspondente.

Figura 5 – Pesquisar e priorizar referências.



Fonte: O autor (2022).

A definição do escopo da pesquisa visa definir, de forma assertiva, o escopo da pesquisa bibliográfica a ser realizada. A depender das metas de pesquisa, este escopo pode abranger artigos científicos, normas técnicas, relatórios técnicos, notícias, dentre outros. A segunda atividade se refere a definição das bases de dados científicas e técnicas que serão consideradas. Esta definição é importante para definir o tipo de documentação e requisitos que serão usados na avaliação. Bases de dados científicas ajudam a identificar requisitos oriundos de pesquisas acadêmicas. Por sua vez, documentos técnicos oriundos de organizações técnicas como IoTSF e OWASP proporcionam diretrizes e experiências já validadas por profissionais qualificados e consórcios de empresas.

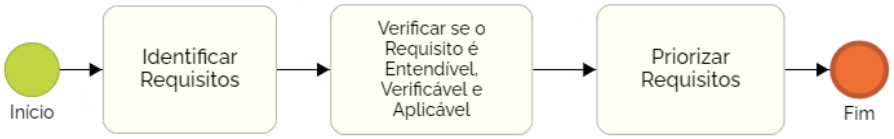
A próxima atividade foca na definição e execução do protocolo de busca. Informações como palavras de busca e critérios de inclusão e exclusão são definidos neste momento. Além disso, cada base de dados tem suas peculiaridades (ex.: formatos de strings de busca), e é importante compreender o funcionamento de cada uma. Por fim, as referências são buscadas através do protocolo de busca definido.

A principal saída (*output*) deste subprocesso é uma lista de referências a serem usadas nas próximas atividades da metodologia.

4.4. Analisar e priorizar requisitos de criptografia

As normas técnicas possuem requisitos de segurança diversos, que podem ser aplicados em diferentes contextos. Por isso, é necessário verificar se os requisitos de segurança que tratam do contexto criptográfico podem ser usados, ou mesmo adaptados, para avaliar a segurança de gateways IoT. O subprocesso que trata da análise e priorização de requisitos de segurança criptográfica está modelado na Figura 6.

Figura 6 – Analisar e priorizar requisitos de criptografia.



Fonte: O autor (2022)

A primeira atividade do subprocesso exposto na Figura 6 é responsável por listar os requisitos de segurança criptográfica encontrados nas referências do subprocesso passado. As referências podem apresentar requisitos de diversas subáreas de segurança (ex.: autenticação e atualização de software), e pode ser necessário avaliar todos estes requisitos e filtrar aqueles que propõem requisitos ligados à qualidade da criptografia. Após esta atividade, a próxima etapa é identificar se o requisito é entendível, verificável e aplicável considerando o contexto da pesquisa. O requisito é considerado "entendível" se está descrito de forma que permita o seu entendimento pelos usuários. Por sua vez, o requisito é considerado "verificável" se pode ser inspecionado usando técnicas e ferramentas conhecidas. Por fim, o requisito é considerado "aplicável" se ele está dentro do escopo da avaliação realizada. Por fim, é possível que a importância dos requisitos selecionados não seja uniforme, ou seja, um requisito tenha mais relevância para o estudo do que outro. Por isso, na última atividade do subprocesso, é realizada a priorização dos requisitos mais relevantes considerando as metas do estudo.

4.5. Selecionar e instalar gateways IoT

Após a definição dos requisitos de segurança criptográfica a serem considerados na avaliação, o próximo passo é a escolha, instalação e configuração dos gateways a serem analisados. A Figura 7 mostra o subprocesso de seleção e instalação dos gateways IoT.

Figura 7 – Selecionar e instalar gateways IoT.

Fonte: O autor (2022).

Definir os requisitos a serem considerados para a seleção dos gateways a serem estudados é a atividade inicial deste subprocesso. Existem diferentes tipos de gateways IoT

atualmente disponíveis, por exemplo existem gateways de código aberto e proprietários. Adicionalmente, também existem gateways baseados em software e gateways baseados em *hardware*. Gateways baseados em *software* geralmente são feitos para implantação em dispositivos genéricos como *Raspberry Pi*. Por outro lado, gateways baseados em *hardware* já são vendidos com o *software* integrado ao *hardware* que vai ser utilizado. Neste contexto, é importante definir que tipos de gateways devem ser focados na avaliação. Após a definição dos requisitos ou critérios a serem usados na escolha dos gateways, a segunda atividade, pesquisa e seleção de gateways, pode ser executada.

Por fim, é realizada a instalação e configuração dos gateways selecionados. Considerando que cada gateway tem as suas particularidades em relação às atividades de instalação e configuração (por exemplo, o Kura exige um maior espaço de armazenamento e possui mais etapas de instalação e configuração do que os demais gateways), é necessário verificar todo o material correspondente a estas atividades em cada gateway.

4.6. Realizar Inspeção dos Requisitos de Criptografia

Na etapa de inspeção, cada gateway é observado minuciosamente considerando os requisitos criptográficos selecionados e priorizados. Este processo tem a intenção de verificar se determinado gateway está em conformidade com o que é sugerido pelos requisitos; assim sendo, compreender o objetivo de cada requisito em sua essência é fundamental para uma inspeção de qualidade. Através desta análise, é possível derivar o nível de segurança criptográfica dos gateways IoT e saber se as informações trafegadas nos gateways estão protegidas conforme sugerido por padrões técnicos internacionais de segurança criptográfica.

A Figura 8 apresenta como a atividade de inspeção, descrita como um subprocesso BPMN, pode ser realizada.

Figura 8 – Realizar inspeção dos requisitos de criptografia.

Fonte: O autor (2022).

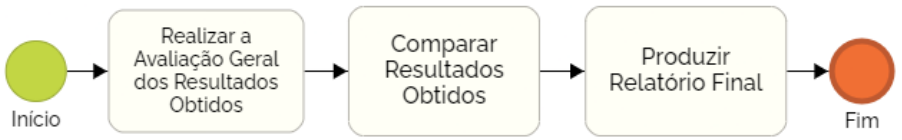
A atividade inicial do subprocesso descrito na Figura 8 indica o acesso a todos os recursos disponíveis do gateway que poderão ser utilizados na inspeção, incluindo

documentação, código executável e código fonte. Estes recursos serão analisados em busca de evidências para fundamentar a avaliação da conformidade do requisito. Na atividade seguinte, todos os requisitos de segurança criptográfica levantados e priorizados anteriormente são efetivamente verificados considerando os recursos disponibilizados pelos próprios gateways. Pode-se adotar escalas variadas de níveis possíveis de conformidade, como por exemplo: conformidade verificada na instalação (IC), conformidade verificada na documentação (CD), conformidade verificada no código fonte (CCF) e não conformidade. Finalmente, é realizado o registro dos resultados da inspeção.

4.7. Realizar avaliação dos resultados

Neste subprocesso, são conduzidas as avaliações dos resultados obtidos durante a inspeção. A Figura 9 apresenta como este subprocesso pode ser executado.

Figura 9 – Realizar avaliação dos resultados.



Fonte: O autor (2022).

Inicialmente, é realizada a avaliação individual dos resultados obtidos em cada gateway IoT analisado. Avaliações quantitativas (ex.: número de requisitos que estão em conformidade) e qualitativas (ex.: nível geral de segurança criptográfica do gateway) podem ser realizadas. Já na atividade seguinte são realizadas comparações entre os resultados das inspeções dos gateways. Busca-se, neste momento, Avaliações quantitativas (ex.: número de requisitos que estão em conformidade) e qualitativas (ex.: nível geral de segurança criptográfica do gateway)avaliar comparativamente o nível de segurança criptográfica do gateway em relação a outros atualmente disponíveis. Finalmente, é produzido o relatório final com as informações de todo o processo de avaliação, incluindo as avaliações feitas neste subprocesso.

4.8. Considerações finais

Neste capítulo foi apresentada e detalhada a metodologia proposta para avaliação de

requisitos de segurança criptográfica em gateways IoT. Essa metodologia foi desenvolvida utilizando o padrão *Business Process Model and Notation* (BPMN), e com o uso deste padrão foi possível estruturar e descrever cada atividade da citada metodologia. Com a metodologia bem definida, as atividades e processos se ajustam e se conectam entre si, facilitando a compreensão e possível reprodução do mesmo por pesquisadores interessados.

No próximo capítulo, a metodologia proposta será tanto ilustrada como avaliada através da execução de estudo de caso.

5. Avaliação de Requisitos de Segurança Criptográfica em Gateways IoT

Este capítulo apresenta, em detalhes, a contribuição principal deste trabalho, que é a avaliação de segurança criptográfica de gateways IoT considerando requisitos de criptografia. Esta avaliação é executada baseada na metodologia proposta no capítulo anterior. A avaliação feita neste capítulo ajuda tanto a ilustrar a execução da metodologia proposta como também observar a sua eficácia.

O restante deste capítulo está estruturado da forma que se segue. A Seção 5.1 apresenta as metas traçadas para a avaliação a ser realizada. A Seção 5.2 descreve como foram executadas as atividades referente a pesquisa e priorização de referências. A Seção 5.3 analisa, detalha e prioriza os requisitos de criptografia compatíveis com os objetivos da pesquisa. Na Seção 5.4 são apresentadas as atividades referentes à seleção e instalação dos gateways IoT. A Seção 5.5, por sua vez, apresenta e detalha como ocorreu o processo de inspeção dos requisitos de criptografia nos gateways IoT. Na Seção 5.6 é apresentado como foi realizada a avaliação dos resultados obtidos. Por fim, na Seção 5.7 são apresentadas as considerações finais do capítulo.

5.1. Definir Metas

A principal meta desta avaliação é realizar a avaliação da segurança criptográfica de gateways IoT atualmente disponíveis no mercado. A ideia é avaliar o nível destes gateways e evidenciar a qualidade de segurança criptográfica usualmente oferecida por eles, e não fazer a avaliação de um gateway específico apenas.

5.2. Pesquisar e Priorizar Referências

Para definição do escopo da pesquisa bibliográfica, foi definido se considerar documentos de organizações técnicas que apresentam requisitos de segurança criptográfica relacionados a IoT. As seguintes organizações técnicas foram selecionadas: IoTSF, OWASP, ENISA, OTA, ETSI, CSA e GSMA. A escolha por essas organizações técnicas foi motivada pelo seu reconhecimento na comunidade científica. Os seguintes protocolos de busca foram traçados: 1) Pesquisar em mecanismos de busca por documentos das organizações ou padrões

técnicos de segurança e 2) Selecionar documentos de organizações que apresentam requisitos de segurança criptográfica em geral, não necessariamente específicos para IoT. A pesquisa retornou os seguintes documentos das organizações técnicas: IoT *security compliance framework* (IoTSF, 2020), *Annotated Application security verification standard* (OWASP, [s.d.]), *Baseline Security Recommendations for* IoT (ENISA, 2017), IoT *Security & Privacy Trust Framework v2.5*(OTA, 2018), *Cyber Security for Consumer Internet of Things: Baseline Requirements* (ETSE, 2020), IoT *Security Controls Framework v2* (CSA, 2021) e IoT *Security Assessment Checklist* (GSMA, 2018). A seguir será apresentada a Tabela 3, que aborda o quantitativo de requisitos de criptografia localizados nos documentos das organizações técnicas IOTSF, OWASP, ENISA, ETSI, OTA, CSA e GSMA.

Tabela 3 – Quantidade de requisitos de criptografia por organização técnica.

Organizações Técnicas	**Título do documento**	**Quantidade de requisitos de criptografia**
OWASP	*Annotated Application security verification standard (version 1.0)*	16
IOTSF	*Security compliance framework (version 2.1)*	10
ETSI	*Cyber Security for Consumer Internet of Things: Baseline Requirements (version 2.1.0)*	05
ENISA	*Baseline Security Recommendations for IoT (version nov. 2017)*	04
CSA	*IoT Security Controls Framework (version 2.0)*	02
OTA	*IoT Security & Privacy Trust Framework (version 2.5)*	01
GSMA	*IoT Security Assessment Checklist (version 2.0)*	00

Fonte: O autor (2022).

Após análise dos requisitos de segurança criptográfica nos documentos das organizações técnicas, os seguintes documentos foram priorizados para esta avaliação: *Security compliance framework (version 2.1)* da IoTF e *Annotated Application security verification standard (version 1.0)* da OWASP. A escolha por estes documentos foi motivada pelo fato de apresentarem maior quantidade de requisitos criptográficos que podem ser utilizados em relação às demais organizações analisadas, como pode ser observado na Tabela 3.

5.3. Analisar e Priorizar Requisitos de Criptografia

Inicialmente, foram selecionados requisitos de segurança criptográfica sugeridos pelas organizações técnicas IoTF e OWASP. Somando os requisitos criptográficos destas duas

organizações, se obteve um total de vinte e seis requisitos. Na fase seguinte, cada um dos requisitos foram submetidos a um filtro que busca identificar se o requisito é entendível, verificável e aplicável. O requisito é considerado “entendível” se está descrito de forma que permita o seu entendimento pelos usuários. Por sua vez, o requisito é considerado “verificável” se pode ser inspecionado usando técnicas e ferramentas conhecidas. Por fim, o requisito é considerado “aplicável” se ele está dentro do escopo da avaliação realizada. A Tabela 4 apresenta tantos estes requisitos como a análise sobre se cada um deles atende aos critérios do filtro.

Tabela 4 – Seleção dos Requisitos de Criptografia.

N°	Requisito	Entendível	Verificável	Aplicável
01	Verifique se os segredos e chaves criptográficos são únicos por dispositivo.	SIM	NÃO	NÃO
02	Verifique o uso adequado da criptografia. Apenas algoritmos padrões e fortes devem ser usados, com tamanho de chave adequado e implementações seguras.	SIM	SIM	SIM
03	Verifique se fontes seguras de aleatoriedade são fornecidas pelo sistema operacional e/ou *hardware* para todas as necessidades de segurança.	SIM	NÃO	NÃO
04	Verifique se os segredos criptográficos usados pelo dispositivo são armazenados com segurança, aproveitando a funcionalidade fornecida por *chips* de segurança dedicados.	SIM	NÃO	NÃO
05	Verifique se as primitivas criptográficas usadas pelo dispositivo são fornecidas por *chips* de segurança dedicados.	SIM	NÃO	NÃO
06	Verifique se as bibliotecas criptográficas usadas são certificadas para serem compatíveis com um padrão de segurança criptográfico reconhecido.	SIM	SIM	SIM
07	Verifique se todos os módulos criptográficos falham com segurança e se os erros são tratados de uma maneira que não ative o oracle *padding*.	SIM	NÃO	NÃO
08	Verifique se todos os números aleatórios, nomes de arquivos aleatórios, GUIDs aleatórios e *strings* aleatórias são gerados usando o gerador de números aleatórios aprovado pelo módulo criptográfico quando esses valores aleatórios não podem ser adivinhados por um atacante.	SIM	NÃO	NÃO
09	Verifique se os algoritmos criptográficos usados pelo aplicativo foram validados em relação ao FIPS 140-2 ou um padrão equivalente.	SIM	SIM	SIM
10	Verifique se os módulos criptográficos operam em seu modo aprovado de acordo com suas políticas de segurança publicadas.	SIM	NÃO	NÃO
11	Verifique se há uma política explícita de como as chaves criptográficas são gerenciadas (por exemplo, geradas, distribuídas, revogadas e expiradas). Verifique se esse ciclo de vida da chave é aplicado corretamente.	SIM	NÃO	SIM
12	Verifique se todos os consumidores de serviços criptográficos não têm acesso direto à material chave. Isole processos criptográficos, incluindo segredos mestres e considere o uso de um cofre de chaves de *hardware* (HSM).	SIM	NÃO	NÃO

N°	Requisito	Entendível	Verificável	Aplicável
13	As informações de identificação pessoal devem ser armazenadas criptografadas em repouso e garantir que a comunicação seja feita por meio de canais protegidos.	SIM	SIM	SIM
14	Verifique se, sempre que possível, chaves e segredos são zerados quando destruídos.	SIM	NÃO	SIM
15	Verifique se todas as chaves e senhas são substituíveis e são geradas ou substituídas no momento da instalação.	SIM	SIM	SIM
16	Verifique se os números aleatórios são criados com a entropia adequada, mesmo quando o aplicativo está sob carga pesada, ou se o aplicativo se degrada normalmente em tais circunstâncias.	SIM	NÃO	NÃO
17	Se presente, uma fonte geradora de números aleatórios verdadeiros foi validada para aleatoriedade verdadeira usando um NIST SP800-22 [ref 4], FIPS 140-2 [ref 5] ou um processo de conformidade semelhante.	SIM	NÃO	SIM
18	Existe um processo de provisionamento seguro de chaves que inclui geração, distribuição, atualização, revogação e destruição. Por exemplo, em conformidade com FIPS 140-2 [ref 5] ou um processo semelhante.	SIM	SIM	SIM
19	Existe um método seguro de inserção de chave que protege as chaves contra cópia.	SIM	NÃO	SIM
20	Todas as funções criptográficas relacionadas ao produto não têm pontos fracos conhecidos publicamente, por exemplo, MD5 e SHA-1 não são usados, conforme estabelecido no NIST SP800-131A [ref 2].	SIM	SIM	SIM
21	Todas as funções criptográficas relacionadas ao produto são suficientemente seguras para o ciclo de vida do produto, por exemplo, aqueles estipulados no NIST SP800-131A [ref 2].	SIM	SIM	SIM
22	O produto armazena todos os parâmetros não criptografados sensíveis, por exemplo, chaves, em um local seguro e inviolável.	SIM	SIM	SIM
23	A cadeia de chaves criptográficas usada para assinar o *software* de produção é diferente daquela usada para qualquer outro teste, desenvolvimento ou outras imagens de *software* ou requisito de suporte.	SIM	NÃO	NÃO
24	Na fabricação de dispositivos, todas as chaves privadas de criptografia assimétrica que são exclusivas de cada dispositivo são protegidas conforme descrito no FIPS 140-2 [ref 5]. Elas devem ser geradas internamente de forma verdadeiramente aleatória ou programadas com segurança em cada dispositivo.	SIM	NÃO	SIM
25	Todos os comprimentos de chave são suficientes para o nível de garantia exigido, conforme detalhado no NIST SP800-57 Parte 1.	SIM	SIM	SIM
26	Em sistemas com muitos sub dispositivos em camadas, o gerenciamento de chaves deve seguir as melhores práticas.	NÃO	NÃO	NÃO

Fonte: O autor (2022).

Como demonstrado na Tabela 4, os requisitos passaram por um filtro que os classifica como: entendível, verificável e aplicável. Essa classificação é utilizada para selecionar e priorizar os requisitos que são classificados simultaneamente como entendível, verificável e aplicável. Para melhor compreensão do porque cada requisito recebeu determinada classificação, a Tabela 5 apresenta as respectivas justificativas. Cada requisito é analisado

considerando a sua utilização em gateways IoT baseados em software (que é foco da presente avaliação).

Tabela 5 – Justificativa de Seleção dos Requisitos de Criptografia.

N°	Requisito	Resultado	Justificativa
01	Verifique se os segredos e chaves criptográficos são únicos por dispositivo.	Não selecionado	É descrito de forma que permite o seu entendimento pelos usuários. No entanto, não é aplicável ao contexto da pesquisa devido ao fato de estar voltado para dispositivos (*hardware)*.
02	Verifique o uso adequado da criptografia. Apenas algoritmos padrões e fortes devem ser usados, com tamanho de chave adequado e implementações seguras.	Selecionado	O requisito está descrito de forma que permita o seu entendimento pelos usuários, pode ser inspecionado usando técnicas conhecidas e está dentro do escopo do estudo realizado.
03	Verifique se as fontes seguras de aleatoriedade são fornecidas pelo sistema operacional e/ou *hardware* para todas as necessidades de segurança.	Não selecionado	É entendível, e está descrito de maneira que permite o seu entendimento. Porém, não é aplicável ao escopo do estudo, por sugerir verificar a criptografia de sistemas operacional e/ou *hardware*.
04	Verifique se os segredos criptográficos usados pelo dispositivo são armazenados com segurança, aproveitando a funcionalidade fornecida por *chips* de segurança dedicados.	Não selecionado	Não é aplicável ao trabalho por estar sugerindo verificar a criptografia fornecida pelos *chips* dos dispositivos.
05	Verifique se as primitivas criptográficas usadas pelo dispositivo são fornecidas por *chips* de segurança dedicados.	Não selecionado	Está descrito de forma que permite o seu entendimento pelos usuários. Entretanto, não é aplicável por estar voltado para segurança fornecidas pelos *chips* dos dispositivos.
06	Verifique se as bibliotecas criptográficas usadas são certificadas para serem compatíveis com um padrão de segurança criptográfico reconhecido.	Selecionado	Está descrito de forma que permite o seu entendimento pelos usuários, pode ser inspecionado usando padrões criptográficos reconhecidos e está dentro do escopo do estudo do estudo.
07	Verifique se todos os módulos criptográficos falham com segurança e os erros são tratados de uma maneira que não ative o *oracle padding*.	Não selecionado	É apresentado e descrito de forma que permite o seu entendimento pelos usuários. Contudo, não é aplicável por sugerir realização de ataques.
08	Verifique se todos os números aleatórios, nomes de arquivos aleatórios, GUIDs aleatórios e *strings* aleatórias são gerados usando o gerador de números aleatórios aprovado pelo módulo criptográfico quando esses valores aleatórios não podem ser adivinhados por um atacante.	Não selecionado	Não é verificável ao projeto por ser necessário informações que abrangem desde o desenvolvimento do software, e por não existir uma técnica ou ferramenta que auxilie nesta função. E também, por estar voltado para verificação de segurança através de ataques à aplicação.

N°	Requisito	Resultado	Justificativa
09	Verifique se os algoritmos criptográficos usados pelo aplicativo foram validados em relação ao FIPS 140-2 ou um padrão equivalente.	Selecionado	O requisito é entendível e está descrito de forma compreensível. Ele também é verificável, pois pode ser inspecionado usando FIPS 140-2, um padrão criptográfico reconhecido pela comunidade científica. Por fim, é aplicável, por estar dentro do escopo do estudo.
10	Verifique se os módulos criptográficos operam em seu modo aprovado de acordo com suas políticas de segurança publicadas.	Não selecionado	Não é verificável, por depender de informações referente ao ambiente em que cada aplicação será inserida.
11	verifique se há uma política explícita de como as chaves criptográficas são gerenciadas (por exemplo, geradas, distribuídas, revogadas e expiradas). Verifique se esse ciclo de vida da chave é aplicado corretamente.	Não selecionado	O requisito não é verificável, devido ao fato de necessitar de informações do desenvolvedor do gateway.
12	Verifique se todos os consumidores de serviços criptográficos não têm acesso direto ao material de chave. Isole processos criptográficos, incluindo segredos mestres e considere o uso de um cofre de chaves de *hardware* (HSM).	Não selecionado	É entendível, porém, não aplicável ao estudo devido ao fato de sugerir o uso de um cofre de chave de *hardware*, e o escopo abranger apenas gateways baseados em *software*.
13	As informações de identificação pessoal devem ser armazenadas criptografadas em repouso e garantir que a comunicação seja feita por meio de canais protegidos.	Selecionado	É verificável através de uma busca no código fonte e está dentro do escopo do projeto pela necessidade de verificar como as informações pessoais dos usuários estão sendo armazenadas nos gateways IoT.
14	Verifique se, sempre que possível, chaves e segredos são zerados quando destruídos.	Não selecionado	Não é verificável pela necessidade de informações do desenvolvimento do gateway e também por não ser possível realizar a inspeção usando uma técnica ou ferramenta conhecida para verificação de destruição de chaves.
15	Verifique se todas as chaves e senhas são substituíveis e são geradas ou substituídas no momento da instalação.	Selecionado	O requisito está descrito de forma que permita o seu entendimento pelos usuários, pode ser inspecionado no momento da instalação e está dentro do escopo do estudo realizado.
16	Verifique se os números aleatórios são criados com a entropia adequada, mesmo quando o aplicativo está sob carga pesada, ou se o aplicativo se degrada normalmente em tais circunstâncias.	Não selecionado	Não é aplicável por sugerir a verificação da entropia de acordo com a carga da aplicação, fugindo do escopo do estudo.
17	Se presente, uma fonte geradora de números aleatórios verdadeiros foi validada para aleatoriedade verdadeira usando um NIST SP800-22 [ref 4], FIPS 140-2 [ref 5] ou um processo de conformidade semelhante.	Não selecionado	Não é verificável por necessitar de informações dos desenvolvedores do gateway.

N°	Requisito	Resultado	Justificativa
18	Existe um processo de provisionamento seguro de chaves que inclui geração, distribuição, atualização, revogação e destruição. Por exemplo, em conformidade com FIPS 140-2 [ref 5] ou um processo semelhante.	Não selecionado	Não é verificável, por necessitar de informações referente ao desenvolvimento do gateway, ou por não existir uma ferramenta conhecida que possibilite localizar essas informações.
19	Existe um método seguro de inserção de chave que protege as chaves contra cópia.	Não selecionado	Não é verificável por ser necessário informações do desenvolvimento do *software* do gateway.
20	Todas as funções criptográficas relacionadas ao produto não têm pontos fracos conhecidos publicamente, por exemplo, MD5 e SHA-1 não são usados, conforme estabelecido no NIST SP800-131A [ref 2].	Selecionado	O requisito está descrito de forma que permita o seu entendimento pelos usuários, pode ser inspecionado usando as sugestões do NIST SP800-131 para uso de algoritmos criptográficos e é aplicável ao contexto da avaliação proposta.
21	Todas as funções criptográficas relacionadas ao produto são suficientemente seguras para o ciclo de vida do produto, por exemplo, aqueles estipulados no NIST SP800-131A [ref 2].	Selecionado	O requisito está descrito de forma que permita o seu entendimento pelos usuários, pode ser inspecionado usando as sugestões do NIST SP800-131 para uso de funções criptográficas e é aplicável ao contexto da avaliação proposta.
22	O produto armazena todos os parâmetros não criptografados sensíveis, por exemplo, chaves, em um local seguro e inviolável.	Selecionado	É entendível, está descrito de forma compreensível e pode ser inspecionado através de uma busca minuciosa no código do gateway. Também é aplicável ao escopo do projeto.
23	A cadeia de chaves criptográficas usada para assinar o software de produção é diferente daquela usada para qualquer outro teste, desenvolvimento ou outras imagens de *software* ou requisito de suporte.	Não selecionado	O requisito sugere verificar se a cadeia de chaves criptográficas utilizadas para assinar o *software* é diferente das demais. Desta forma, se torna impossível a sua verificação, pois são necessário informações referentes ao desenvolvimento do *software*.
24	Na fabricação de dispositivos, todas as chaves privadas de criptografia assimétrica que são exclusivas de cada dispositivo são protegidas conforme descrito no FIPS 140-2 [ref 5]. Elas devem ser geradas internamente de forma verdadeiramente aleatória ou programadas com segurança em cada dispositivo.	Não selecionado	Não é aplicável ao escopo do estudo, por estar voltado para *hardware* e por necessitar de informações referente a fabricação do dispositivo.
25	Todos os comprimentos de chave são suficientes para o nível de garantia exigido, conforme detalhado no NIST SP800-57 Parte 1.	Selecionado	O requisito está descrito de forma que permita o seu entendimento pelos usuários, pode ser inspecionado usando as sugestões do NIST SP800-57 para verificação do comprimento de chaves e é aplicável ao contexto desta avaliação.

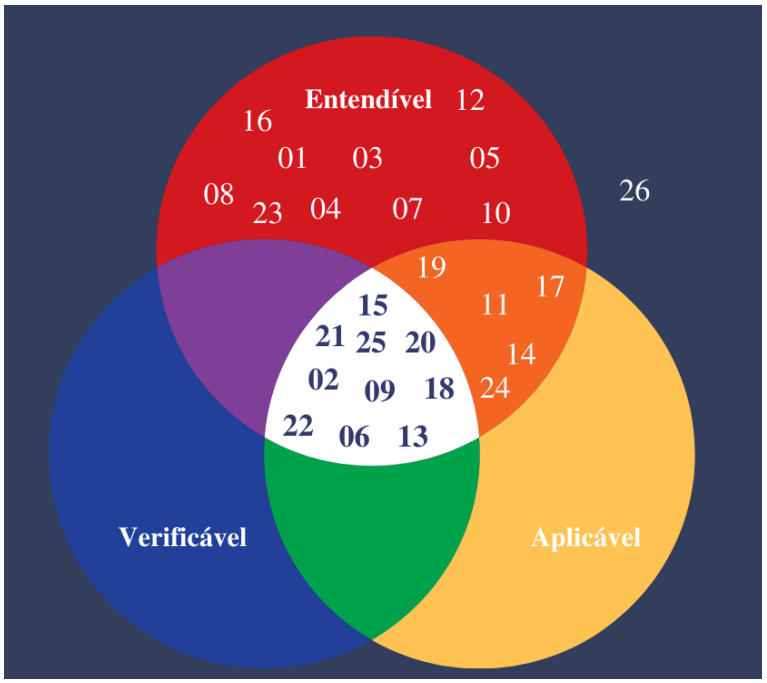
N°	Requisito	Resultado	Justificativa
26	Em sistemas com muitos sub dispositivos em camadas, o gerenciamento de chaves deve seguir as melhores práticas.	Não selecionado	O requisito não está descrito de forma que permita o seu entendimento exato pelos usuários.

Fonte: O autor (2022).

Após as justificativas apresentadas na Tabela 5, é possível agrupar os requisitos por critérios de seleção. A Figura 10, com este intuito, apresenta um diagrama de Venn[3] com três círculos distintos nas cores vermelho, azul e amarelo. Cada cor corresponde, respectivamente, aos conjuntos de requisitos “entendível”, “verificável” e “aplicável”. Assim sendo, no círculo vermelho estão agrupados os requisitos classificados como entendíveis, no círculo azul os requisitos classificados como verificáveis e no círculo amarelo os requisitos classificados como aplicáveis. As áreas de interseção estão com cores laranja, branca, verde e azul-claro. A área laranja pertence aos requisitos classificados como entendíveis e aplicáveis. A área branca pertence aos requisitos classificados como entendíveis, verificáveis e aplicáveis. A área verde pertence aos requisitos classificados como verificáveis e aplicáveis e a área azul-claro pertence aos requisitos classificados como verificáveis e entendíveis. Se o requisito não está localizado em nenhum dos conjuntos possíveis significa que ele não pertence a nenhum dos grupos, e passa a ser entendido e classificado como não entendível, não verificável e não aplicável.

[3] O diagrama de Venn é um gráfico utilizado para organizar e explicar as relações lógicas entre dois ou mais conjuntos de itens.

Figura 10 – Classificação de requisitos utilizando diagrama de Venn.

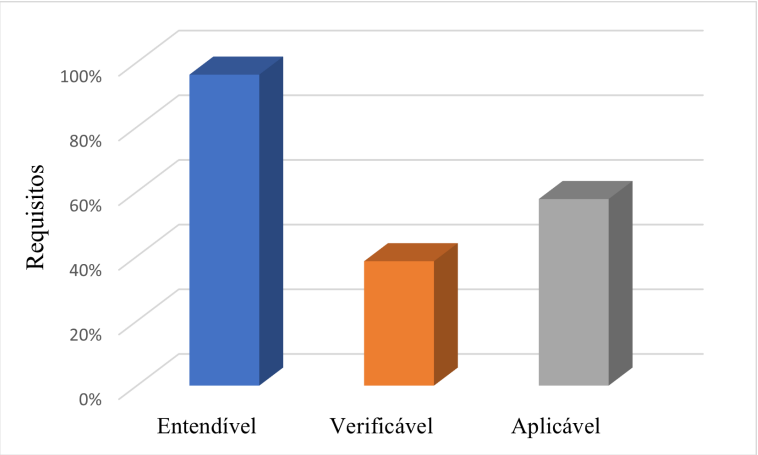


Fonte: O autor (2022).

Ao analisar a Figura 10, obtemos os seguintes conjuntos: Entendível = { 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25 }, Verificável = { 02, 06, 09, 13, 15, 18, 20, 21, 22, 25 } , Aplicável = { 11, 14, 17, 19, 24 }, ~Entendível ∩ - ~Verificável ∩ ~ Aplicável = {26}, entendível ∩ verificável = { }, verificável ∩ aplicável = { }, Entendível ∩ Aplicável = { 11, 14, 17, 19, 24 } Entendível ∩ Verificável ∩ Aplicável = { 02, 06, 09, 13, 15, 18. 20, 21, 22, 25 }. Deste modo, temos os resultados que seguem. Os requisitos, em sua maioria, são classificados como entendíveis. Apenas um dos requisitos analisados pertencem ao grupo de requisitos não entendíveis, não verificáveis e não aplicáveis.

A Figura 11 apresenta o percentual de requisitos pertencentes aos conjuntos: entendível, verificável e aplicável. Nesta etapa da análise, cada conjunto é avaliado individualmente sem ser levado em consideração a intersecção entre eles. Por exemplo: se um requisito é classificado como entendível e verificável ao mesmo tempo, então no gráfico ele será contabilizado nos requisitos classificados como entendíveis e nos classificados como verificáveis.

Figura 11 – Avaliação de requisitos pertencentes aos conjuntos: entendível, verificável e aplicável.



Fonte: O autor (2022).

Ao se analisar a Figura 11, pode-se concluir que 96% dos requisitos são entendíveis, 38% são verificáveis e 58% são aplicáveis.

Para que um requisito seja adotado/priorizado é necessário que ele faça parte da intersecção entre os conjuntos entendível, verificável e aplicável. Ao analisar o conjunto formado pela intersecção Entendível ∩ Verificável ∩ Aplicável, pode-se perceber que apenas 38,5% dos requisitos atendem ao critério de ser entendível, verificável é aplicável, o que corresponde a 10 requisitos. Este número representa menos da metade dos requisitos de segurança criptográfica inicialmente selecionados, o que mostra a importância de se avaliar e filtrar os mesmos antes da atividade de inspeção para garantir que os requisitos selecionados estejam de acordo com as metas do estudo.

5.4. Selecionar e instalar gateways IoT

Para atingir as metas definidas no início da avaliação, é necessário definir os gateways que serão utilizados dentro da avaliação. No caso da presente pesquisa, os seguintes requisitos são considerados: 1) o gateway deve estar atualmente disponível para uso, 2) o gateway deve possuir código aberto e 3) o gateway deve ser baseado em software. Para o requisito 1), é suficiente verificar se o gateway disponibiliza uma versão atual de seu software para *download* e uso. Em relação ao requisito 2), a ideia de se usar softwares com código aberto é o de facilitar ou até mesmo possibilitar a inspeção do código do mesmo. Por fim, o requisito 3) busca filtrar gateways que podem ser utilizados pela comunidade através de hardware de

propósito geral como Raspberry Pi. Desta forma, usuários não precisarão comprar o hardware específico de um gateway, mas sim fazer o *download* do seu software e implantar em hardwares de propósito geral como o Raspberry Pi.

Após uma análise detalhada dos gateways, levando em consideração os requisitos especificados anteriormente, os seguintes gateways foram selecionados: Eclipse Kura 5.0.0 (MAIERO, 2021), WebThings 1.0.0 (WEBTHINGS, 2020), ThingsBoard 3.2.1 (THINGSBOARD, 2022) e WebIOPI 0.7.1 (WEBIOPI, 2015). Em relação ao processo de instalação, foi utilizado o sistema operacional Raspbian e o seguinte hardware: Raspberry Pi 3 modelo B v1.2, com CPU Quad Core 1.2GHz Broadcom BCM2837 64 bit, 1 GB de RAM e cartão MicroSDHC Classe 10 de 16 GB.

Durante o processo de instalação, três dos quatro gateways apresentaram um nível maior de dificuldade. Este fato ocorreu principalmente devido a falta de instruções de como realizar a instalação na documentação fornecida pelo desenvolvedor. Neste contexto, foi necessário realizar buscas em sites, blogs e fóruns. No entanto, é válido salientar que os gateways apresentam documentação, porém incompleta ou muito complexa para instalação por usuários com pouco conhecimento tecnológico. Um dos gateways em especial chamou muito atenção pelo fato de apresentar dificuldades extremas no processo de instalação, não só para usuários leigos tecnologicamente, mas também para usuários com mais conhecimento técnico.

É importante ressaltar que o objetivo desta avaliação não é sugerir um produto específico, mas sim verificar o nível de conformidade que os gateways avaliados tem atualmente em relação às organizações técnicas. Desta forma, os gateways selecionados foram nomeados de forma aleatória, e serão referenciados nas seções posteriores como Gateway A, Gateway B, Gateway C e Gateway D.

5.5. Realizar inspeção de requisitos de Criptografia

As subseções a seguir apresentam, em detalhes, como foi conduzido o processo de inspeção dos requisitos de criptografia. Na Subseção 5.5.1, são apresentados os 10 requisitos de criptografia e as formas de verificação de conformidade dos requisitos nos gateways IoT. A Subseção 5.5.2 apresenta em detalhes o processo de inspeção dos requisitos e os recursos criptográficos localizados em cada um dos gateways. Por fim, na Subseção 5.5.3 é

apresentado como foi realizado o registro dos resultados da inspeção.

5.5.1. Acessar documentação, código e funcionalidades dos gateways IoT selecionados

Com os requisitos selecionados e priorizados e os gateways IoT instalados e configurados, iniciou-se a etapa de inspeção de requisitos de criptografia. Na Tabela 6 são apresentados os requisitos selecionados e priorizados na etapa de análise e priorização de requisitos de criptografia.

Tabela 6 – Requisitos de Criptografia priorizados.

N°	Requisitos
RC-01	Verifique o uso adequado da criptografia. Apenas algoritmos padrões e fortes devem ser usados, com tamanho de chave adequado e implementações seguras.
RC-02	Verifique se as bibliotecas criptográficas usadas são certificadas para serem compatíveis com um padrão de segurança criptográfico reconhecido.
RC-03	Verifique se os algoritmos criptográficos usados pelo aplicativo foram validados em relação ao FIPS 140-2 ou um padrão equivalente.
RC-04	As informações de identificação pessoal devem ser armazenadas criptografadas em repouso e garantir que a comunicação seja feita por meio de canais protegidos.
RC-05	Verifique se todas as chaves e senhas são substituíveis e são geradas ou substituídas no momento da instalação.
RC-06	Existe um processo de provisionamento seguro de chaves que inclui geração, distribuição, atualização, revogação e destruição. Por exemplo, em conformidade com FIPS 140-2 [ref 5] ou um processo semelhante.
RC-07	Todas as funções criptográficas relacionadas ao produto não têm pontos fracos conhecidos publicamente, por exemplo, MD5 e SHA-1 não são usados, conforme estabelecido no NIST SP800-131A [ref 2].
RC-08	Todas as funções criptográficas relacionadas ao produto são suficientemente seguras para o ciclo de vida do produto, por exemplo, aqueles estipulados no NIST SP800-131A [ref 2].
RC-09	O produto armazena todos os parâmetros não criptografados sensíveis, por exemplo, chaves, em um local seguro e inviolável.
RC-10	Todos os comprimentos de chave são suficientes para o nível de garantia exigido, conforme detalhado no NIST SP800-57 Parte 1.

Fonte: O autor (2022).

A inspeção dos requisitos de segurança criptográfica nos gateways ocorre da seguinte maneira: inicialmente é verificada a sua conformidade no processo de instalação e através da navegação pela interface gráfica. Caso a conformidade seja atendida nesta fase, é realizado o registro deste resultado. Caso contrário, é dado início à fase de verificação de conformidade através da documentação disponibilizada pelo fornecedor do gateway. Mas, se mesmo assim não for possível efetuar a verificação de conformidade, é realizada verificação também através do código fonte. Se a conformidade não puder ser verificada em nenhuma destas

inspeções, é obtido o resultado de não conformidade. Este procedimento de inspeção ocorreu nos quatro gateways selecionados e observou os 10 requisitos de criptografia apresentados na Tabela 5. Assim sendo, a seguir será apresentado como ocorreu o processo de inspeção dos requisitos em cada gateway IoT considerando cada requisito individualmente.

5.5.2. Verificar conformidade de requisitos

Nas subseções a seguir será detalhado como ocorreu o processo de inspeção dos requisitos de criptografia apresentados na Tabela 6. Com estes resultados, será possível alcançar um melhor entendimento de como se encontra o nível de segurança criptográfica dos gateways IoT.

5.5.2.1. Verifique o uso adequado da criptografia. Apenas algoritmos padrões e fortes devem ser usados, com tamanho de chave adequado e implementações seguras.

Ao analisar o requisito, percebeu-se que não é sugerido um padrão criptográfico específico para ser utilizado como validador dos algoritmos e comprimentos de chaves. Desta forma, para esse requisito em especial, será feito uso do padrão NIST 800 - 57 Parte I. A escolha por este documento de criptografia foi motivada pelo fato dele ser sugerido por algumas das organizações que foram adotadas como referência para este trabalho, por exemplo IoTSF e OWASP . O NIST 800 - 57 fornece orientações sobre o gerenciamento de chaves criptográficas em todo o seu ciclo de vida, incluindo sua geração, armazenamento, distribuição, uso e destruição. A Tabela 7 apresenta os algoritmos de criptografia e as forças de segurança que as chaves criptográficas devem ter para serem consideradas seguras e aprovadas pelo padrão.

Tabela 7 – Força de segurança comparável de criptografia de bloco simétrico e algoritmos de chave assimétrica.

Força de segurança	**Algoritmos de chave simétrica**	**CCF (DSA, DH, MQV)**	**CFI (RSA)**	**CCE (ECDSA, EdDSA, DH, MQV)**
112	3 TDEA	TCP1 = 2048 TCP2 = 224	k = 2048	f = 224-255
128	AES-128	TCP1 = 3072 TCP2 = 256	k = 3072	f = 256-383
192	AES-192	TCP1 = 7680 TCP2 = 384	k = 7680	f = 384-511
256	AES-256	TCP1 = 15360 TCP2 = 512	k = 15360	f = 512+

Fonte: Elaborada pelo autor com base no NIST 800 - 57 parte I ,2022.

A primeira coluna apresenta o tamanho das chaves (forças de segurança máxima) estimada (em bits) fornecida pelos algoritmos. A segunda coluna apresenta os algoritmos de chave simétrica que podem fornecer a força de segurança especificada na coluna 1. Na terceira coluna, estão os tamanhos mínimos dos parâmetros associados aos padrões que usam criptografía de campo finito (CCF), onde TCP1 corresponde ao tamanho da chave pública e TCP2 corresponde ao tamanho da chave privada. A quarta coluna indica o valor de k (o tamanho da chave) para algoritmos baseados em criptografia de fatoração inteira (CFI), por exemplo, algoritmo RSA. Por fim, a última coluna indica o intervalo de f (o tamanho da chave) para algoritmos baseados em criptografia de curva elíptica (CCE).

O padrão NIST 800 - 57 Parte I apresenta também os algoritmos que fazem uso das funções *hashes* aprovadas pelo NIST. Assim sendo, a força de segurança estimada para esses algoritmos depende do comprimento do bloco de saída da função *hash,* que é indicado pelos três últimos dígitos do nome da função *hash*, por exemplo, SHA-224 tem um comprimento de bloco de saída de 224 bits. A Tabela 8 exibe as funções de *hash* aprovadas e o menor comprimento de bloco de saída que pode ser usado para fornecer cada força de segurança identificada para várias aplicações de função de *hash:* assinaturas digitais, HMAC, KMAC, derivação de chave e geração de bits aleatórios.

Tabela 8 – Funções *hashes* aprovadas pelo padrão.

Força de segurança	**Assinaturas digitais e outras aplicações que exigem resistência a colisões**	**HMAC, KMAC, funções de derivação de chave, geração de bits aleatórios**
112	SHA-224, SHA-512/224, SHA3-224	
128	SHA-256, SHA-512/256, SHA3-256	SHA-1, KMAC128
192	SHA-384, SHA 3-384	SHA-224, SHA-512/224, SHA3-224
≥ 256	SHA-512, SHA3-512	SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512, KMAC 256

Fonte: Elaborada pelo autor com base no NIST 800 - 57 parte I ,2022.

Com o passar do tempo, a força de segurança dos algoritmos pode sofrer modificações, tornando-os mais suscetíveis a ataques bem-sucedidos de hackers. A Tabela 9 apresenta uma projeção do período de tempo que determinada força de segurança criptográfica é considerada eficiente. Após esse período, estima-se ser necessário realizar uma nova configuração de proteção criptográfica. A primeira coluna da tabela é dividida em duas;

a primeira indica a força de segurança a ser fornecida para que determinado algoritmo seja considerado eficiente e a segunda indica se a proteção criptográfica está sendo utilizada no processo de criptografia ou descriptografia. Já as demais colunas exibem os prazos durante os quais a força de segurança é aceita. Os seguintes termos são usados:

- "Aceitável" significa que o algoritmo ou comprimento da chave é atualmente considerado seguro.
- “Uso legado” significa que um algoritmo ou comprimento de chave pode ser usado apenas no processo de descriptografia.
- "Não permitido" significa que um algoritmo ou comprimento de chave não devem ser mais usados.

Tabela 9 – Períodos de tempo de força de segurança.

<table>
<tr><th colspan="2">Força de segurança</th><th>Até 2030</th><th>A Partir 2031</th></tr>
<tr><td rowspan="2">< 112</td><td>Criptografia</td><td colspan="2">Não permitido</td></tr>
<tr><td>Descriptografia</td><td colspan="2">Uso legado</td></tr>
<tr><td rowspan="2">112</td><td>Criptografia</td><td rowspan="2">Aceitável</td><td>Não permitido</td></tr>
<tr><td>Descriptografia</td><td>Uso legado</td></tr>
<tr><td>128</td><td rowspan="3">Aplicação de proteção e processamento de informações que já estão protegidas</td><td>Aceitável</td><td>Aceitável</td></tr>
<tr><td>192</td><td>Aceitável</td><td>Aceitável</td></tr>
<tr><td>256</td><td>Aceitável</td><td>Aceitável</td></tr>
</table>

Fonte: Elaborada pelo autor com base no NIST 800 - 57 parte I ,2022.

Todas as informações apresentadas nas tabelas 7, 8 e 9 podem serem consultadas e acessadas entre as páginas 54 à 59 do NIST SP 800 - 57[4].

Após apresentação dos algoritmos e tamanho de chaves criptográficas aprovadas pelo NIST, a Tabela 10 apresenta os recursos criptográficos localizados nos gateways IoT através do processo de inspeção do requisito RC-01 da Tabela 6. Na primeira coluna desta tabela, estão localizados os gateways IoT. Na segunda coluna, são apresentados os recursos criptográficos encontrados durante a inspeção. Por fim, na terceira coluna, são apresentadas breves observações referentes a cada recurso criptográfico localizado durante o processo de inspeção nos gateways.

[4] Disponível para acesso em: <https://doi.org/10.6028/NIST.SP.800-57pt1r5>. Último acesso em 17 de junho de 2022.

Tabela 10 – Inspeção do requisito de criptografia RC-01.

Gateway	Recursos criptográficos localizados	Observações da inspeção
Gateway A	SHA-256, P 256 (NIST), SSL e TLS	Utiliza recursos criptográficos aprovados pelo NIST 800 - 57, como por exemplo o algoritmo que faz uso das funções *hashes*. Também utiliza algoritmos baseados em criptografia de curva elíptica como a curva P 256 (NIST) e para configuração de certificados são utilizados os protocolos SSL e TLS.
Gateway B	Não utiliza criptografia	-
Gateway C	SHA-256, AES 128 e RSA 4096	Para segurança criptográfica, o gateway faz uso de algoritmos aprovados pelo NIST 800 - 57, como por exemplo o algoritmo de chave simétrica AES, o algoritmo de chave assimétrica RSA e as funções *hashes*.
Gateway D	SHA - 256, RSA 2048 e SSL	O gateway faz uso das funções *hashes* e algoritmos de chaves assimétricas aprovados pelo NIST 800 - 57, como por exemplo o algoritmo RSA 2048 e da função *hash* SHA - 256. Para configuração de certificados, é utilizado o protocolo SSL.

Fonte: O autor (2022).

Ao analisar a Tabela 10, é possível perceber que três dos quatro gateways utilizam algoritmos e comprimentos de chave aprovados pelo NIST SP 800 - 57. No entanto, é importante registrar que não é possível afirmar se cada gateway faz uso apenas de recurso criptográfico aprovado pelo padrão; para isto, seria necessário documentações específicas dos fabricantes sobre o uso da criptografia. No caso, esta avaliação se baseou se o gateway possui o recurso necessário para estar em conformidade com o requisito RC-01.

5.5.2.2. Verifique se as bibliotecas criptográficas usadas são certificadas para serem compatíveis com um padrão de segurança criptográfico reconhecido.

A Tabela 11 apresenta as bibliotecas utilizadas pelos gateways em seus processos criptográficos, possibilitando a realização de uma análise detalhada dos recursos utilizados por cada gateway. Deste modo, na primeira coluna, estão localizados os gateways IoT, na segunda coluna, são apresentadas as bibliotecas criptográficas localizadas durante a inspeção e na terceira coluna são apresentadas breves observações referentes a cada biblioteca criptográfica localizada durante o processo de inspeção nos gateways.

Tabela 11 – Inspeção do requisito de criptografia RC-02.

Gateway	Bibliotecas criptográficas localizadas	Observações da inspeção
Gateway A	*OpenSSL*, *Let's encrypt*, *hash bcrypt*	O gateway A utiliza três bibliotecas criptográficas. A primeira é o *OpenSSL*, utilizado para geração de certificados de autenticação de serviços, através dos protocolos SSL e TLS.

Gateway	Bibliotecas criptográficas localizadas	Observações da inspeção
		A segunda é o *Let 's Encrypt,* uma autoridade certificadora que trabalha com geração de certificados utilizando o protocolo TLS. E, por fim, a *hash bcrypt,* utilizada para geração de senhas criptografadas, é também usada.
Gateway B	Não utiliza criptografia	-
Gateway C	*OpenSSL* e *Keytool*	*Keytool* é utilizada para o gerenciamento de chaves e certificados SSL. *OpenSSL* é utilizado para gerar certificados de autenticação de serviços, através dos protocolos SSL e TLS.
Gateway D	*OpenSSL* e *Keytool*	O gateway D faz uso das mesmas bibliotecas criptográficas utilizadas pelo gateway C.

Fonte: O autor (2022).

Ao se analisar a Tabela 11, é possível perceber que os recursos criptográficos utilizados por cada gateway são semelhantes. Inclusive, uma das bibliotecas é utilizada por todos eles (com exceção do gateway B, que não faz uso de criptografia). Através de uma verificação detalhada da documentação e do código fonte de cada biblioteca utilizada por cada um dos gateways que estão citadas na Tabela 11 foram localizados algoritmos e tamanhos de chaves compatíveis com os sugeridos pelo NIST SP 800 - 57. É válido ressaltar que não é possível afirmar se todos os algoritmos utilizados pelas bibliotecas criptográficas são certificados por um padrão de segurança criptográfico reconhecido; na prática se buscou saber se, pelo menos, os algoritmos certificados estão disponíveis.

5.5.2.3. Verifique se os algoritmos criptográficos usados pelo aplicativo foram validados em relação ao *FIPS* 140 - 2 ou um padrão equivalente.

No enunciado do requisito é citado o *FIPS* 140 - 2 e, para melhor compreensão deste padrão criptográfico, a seguir será apresentado um breve resumo sobre o que ele é. Assim sendo, o FIPS 140 - 2 especifica os requisitos de segurança para um módulo criptográfico que pode ser utilizado em: sistemas de segurança, sistemas de proteção de informações confidenciais e sistemas de computadores e telecomunicações. Para melhor classificar o nível de segurança criptográfica fornecida por cada módulo criptográfico, o padrão desenvolveu quatro níveis qualitativos crescentes de segurança. Assim sendo, segundo o FIPS 140 - 2:

> O nível de segurança 1 fornece o nível mais baixo de segurança. Os requisitos básicos de segurança são especificados para um módulo criptográfico (por exemplo, pelo menos um algoritmo aprovado ou função de segurança aprovada deve ser usado)[...] O nível de segurança 2 aprimorar os mecanismos de segurança física de

> um módulo criptográfico de nível de segurança 1 adicionando o requisito de evidência de violação, que inclui o uso de revestimentos ou selos à prova de violação ou para fechaduras anti-arrombamento em tampas removíveis ou portas do módulo[...] Além dos mecanismos de segurança física invioláveis exigidos no nível de segurança 2, o nível de segurança 3 tenta impedir que o invasor obtenha acesso aos CSPs mantidos no módulo criptográfico. Os mecanismos de segurança física exigidos no Nível de Segurança 3 destinam-se a ter uma alta probabilidade de detectar e responder a tentativas de acesso físico, uso ou modificação do módulo criptográfico[...] O nível de segurança 4 fornece o mais alto nível de segurança definido neste padrão. Nesse nível de segurança, os mecanismos de segurança física fornecem um envelope completo de proteção ao redor do módulo criptográfico com a intenção de detectar e responder a todas as tentativas não autorizadas de acesso físico (TECHNOLOGY, 2002, tradução livre do autor).

Ao compreender do que se trata o FIPS 140 - 2, é possível prosseguir com a inspeção do requisito RC-03 da Tabela 6, que sugere uma verificação de conformidade dos algoritmos criptográficos usados pela aplicação com os algoritmos aprovados pelo FIPS 140 - 2 ou um padrão equivalente. Deste modo, a verificação foi conduzida através da comparação entre os algoritmos localizados nos gateways com os algoritmos aprovados pelo padrão *FIPS* 140 - 2.

É válido mencionar que o FIPS 140 - 2 não apresenta nenhum algoritmo de criptografia em sua documentação, porém direciona o leitor para *links* de padrões pertencentes a mesma organização técnica que o desenvolveu, como por exemplo os padrões de criptografia NIST SP 800 - 57 e NIST SP 800 - 131 A, especificados nos anexos A, C e D[5] como documentos de algoritmos de criptografia aprovados. Deste modo, os algoritmos disponíveis nas Tabelas 7 ,8, 9, 13,14 e 15 pertencentes aos documentos NIST SP 800 - 57 e NIST SP 800 - 131 A são também aprovados pelo FIPS 140 - 2 e podem ser utilizados como verificadores de conformidade para o solicitado pelo requisito. Para maiores informações consultar o *FIPS* 140 - 2[6].

A lista com os algoritmos localizados durante a inspeção em cada gateway está disponível na Tabela 10. Deste modo, após realizar análises nas tabelas foram observados os seguintes resultados: todos os participantes do processo de inspeção, com exceção do gateway B, fizeram uso ao menos de um algoritmo aprovado pelo *FIPS* 140 -2. Porém, devido à falta de informações nas documentações, nas interfaces gráficas e nos códigos fontes de cada gateway sobre os recursos criptográficos utilizados por eles, não é possível garantir que "todos" os algoritmos criptográficos utilizados pelos gateways são aprovados pelo padrão. É

[5] Disponível para acesso em: <https://csrc.nist.gov/publications/detail/fips/140/2/final>. Último acesso em 17 de junho de 2022.
[6] Disponível para acesso em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>. Último acesso em 17 de junho de 2022.

possível que algum algoritmo não aprovado seja também utilizado e este fato não tenha sido identificado na inspeção.

Em relação aos níveis de segurança criptográfica orientados pelo FIPS 140 - 2, com exceção do gateway B, que não atende ao solicitado em nenhum dos níveis, todos os demais estão em conformidade apenas com o nível 1. Segundo o FIPS 140 - 2, para conformidade com o nível de segurança 2 é necessário que o módulo criptográfico possua, no mínimo, autenticação baseada em funções, no qual para que um usuário tenha acesso a determinado módulo do sistema é necessário que ele realize autenticação e receba aprovação de um operador para que possa assumir uma função específica e executar um conjunto correspondente de ações. Nenhum dos gateways analisados possuem esse tipo de autenticação de usuários.

Para conformidade com o nível de segurança 3, é necessário que a conformidade do nível de segurança 2 seja atendida e que o módulo possua mecanismos de autenticação baseados em identidade, aumentando a segurança fornecida pelo nível de segurança 2. O mesmo ocorre com o nível de segurança 4, para que a conformidade seja atendida é necessário que a conformidade com o nível de segurança 3 seja atendida e sejam realizados mecanismos de segurança física. Assim sendo, a não conformidade dos gateways com o nível 2 impossibilita a conformidade com os demais níveis de segurança do FIPS 140 - 2.

5.5.2.4. As informações de identificação pessoal devem ser armazenadas criptografadas em repouso e garantir que a comunicação seja feita por meio de canais protegidos.

A Tabela 12 apresenta como cada gateway se comporta em relação ao armazenamento de informações pessoais. Na primeira coluna da tabela, estão localizados os gateways IoT. Na segunda coluna, são apresentados os recursos utilizados para o armazenamento de informações sigilosas localizados durante o processo de inspeção. Por fim, na terceira coluna são apresentadas informações referentes aos recursos utilizados para o armazenamento de informações pessoais.

Tabela 12 – Requisito de criptografia RC-04.

Gateway	Local de armazenamento	Observações da inspeção
Gateway A	Banco de dados	*hash bcrypt* é utilizado também para armazenar informações criptografadas em um banco de dados. Assim sendo, todas as informações pessoais dos usuários são armazenadas no banco de dados já criptografadas.

Gateway	Local de armazenamento	Observações da inspeção
Gateway B	-	Não foram localizadas informações sobre o processo de armazenamento de informações pessoais dos usuários.
Gateway C	-	Não foram localizadas informações sobre o processo de armazenamento de informações pessoais dos usuários.
Gateway D	RAM e Arquivo	O Gateway D armazena os dados em memória - os dados recebidos são salvos na memória RAM. Ou armazena em arquivos - os dados recebidos são salvos no disco rígido. Dependendo do tipo de armazenamento utilizado pelo usuário do *software* no momento da instalação três formas de segurança podem ser atendidas:Token de acesso, TLS + Token de acesso, TLS + Chave privada.

Fonte: O autor (2022).

O requisito sugere que as informações pessoais devem ser armazenadas e criptografadas em repouso fazendo uso de canais protegidos. Na Tabela 12, é possível observar que o Gateway A faz uso da ferramenta *hash bcrypt* para armazenar as informações do usuário em um banco de dados. Para o processo de criptografia a ferramenta utiliza algoritmos *hashes,* possibilitando que as informações sejam criptografadas antes do armazenamento no banco de dados. Nos gateways B e C, não foram localizadas informações sobre o processo de criptografia de informações pessoais durante a inspeção. Por fim, temos o gateway D que utiliza armazenamento em memória (*RAM*) e armazenamento em arquivos. Para garantir a segurança dos dados, o gateway disponibiliza três formas de proteção: Token de acesso, TLS + Token de acesso e TLS + Chave privada.

5.5.2.5. Verifique se todas as chaves e senhas são substituíveis e são geradas ou substituídas no momento da instalação.

Através da análise no momento da instalação dos gateways percebeu-se que, com exceção do gateway B, nos demais é possível criar uma nova senha durante o processo de instalação e efetuar a sua substituição conforme solicitado no requisito. No entanto, o requisito sugere também que a verificação seja feita com as chaves. Neste caso, o único gateway que disponibiliza esse recurso de geração e substituição de chaves no momento da instalação é o gateway C. Nos demais, não é possível afirmar que não fazem, porém, não foram localizadas evidências referente a esse processo durante a avaliação.

5.5.2.6. Existe um processo de provisionamento seguro de chaves que inclui geração, distribuição, atualização, revogação e destruição. Por exemplo, em conformidade com FIPS 140-2 [ref 5] ou um processo semelhante.

Não foi possível localizar as informações solicitadas pelo requisito independentemente

da forma de inspeção utilizada nos gateways. Inicialmente, foi realizada verificação de conformidade na documentação, em seguida no momento da instalação e na interface gráfica e, por fim, foi realizada a verificação no código fonte de cada um dos gateways. Em nenhuma destas formas de inspeção foram localizadas informações sobre o processo de distribuição, atualização, revogação ou destruição de chaves.

5.5.2.7. Todas as funções criptográficas relacionadas ao produto não têm pontos fracos conhecidos publicamente, por exemplo, MD5 e SHA-1 não são usados, conforme estabelecido no NIST SP 800-131A [rev 2].

O requisito sugere o uso de algoritmos aprovados pelo NIST SP 800 - 131A. Assim sendo, a seguir serão apresentadas tabelas com o status de aprovação de cada algoritmo, possibilitando ao usuário saber se os algoritmos ou funções localizadas nos gateways são aprovados pelo padrão NIST. A Tabela 13 exibe o status de aprovação dos algoritmos de cifra simétrica. A coluna 1 apresenta os algoritmos de criptografia analisados pelo NIST e a coluna 2 os termos de aprovação de status: “aceitável”, “uso legado” e “não permitido”. Estas possibilidades de status são entendidas da forma que se segue:

- Aceitável: significa que o algoritmo e o comprimento da chave em um FIPS ou SP (*special publication*) são seguros de usar.
- Uso legado: denota que o algoritmo ou o comprimento da chave podem ser usados apenas para processar informações já protegidas.
- Não permitido: significa que o algoritmo ou o comprimento da chave não são mais recomendados para a realização de proteção criptográfica.

Tabela 13 – Status de aprovação de algoritmos simétricos usados para criptografia e descriptografia.

Algoritmo	Status
Criptografia TDEA de duas chaves	Não permitido
Descriptografia TDEA de duas chaves	Uso legado
Criptografia TDEA de três chaves	Descontinuado e não permitido após 2023
Descriptografia TDEA de três chaves	Uso legado
Criptografia SKIPJACK	Não permitido
Descriptografia SKIPJACK	Uso legado
Criptografia e descriptografia AES-128	Aceitável
Criptografia e descriptografia AES-192	Aceitável
Criptografia e descriptografia AES-256	Aceitável

Fonte: Elaborada pelo autor com base no NIST 800 - 131A ,2022.

Ao analisar a Tabela 13, é possível perceber que os algoritmos considerados mais

eficientes e seguros, segundo o padrão NIST em relação ao processo de criptografia e descriptografia, são da família AES. É possível notar também que alguns dos algoritmos da tabela atualmente não são considerados seguros, como por exemplo o TDEA de duas chaves e o SKIPJACK.

Por sua vez, a Tabela 14 fornece o status de aprovação dos algoritmos e comprimentos de chave usados na geração e verificação de assinaturas digitais. Na primeira coluna da tabela, está o tipo de processo de assinatura digital. Na segunda coluna, são apresentados os parâmetros de domínios de cada algoritmo. Por fim, na terceira coluna, são apresentados os status de aprovação dos algoritmos e comprimentos de chaves para o processo de assinatura digital.

Tabela 14 – Status de aprovação de algoritmos usados para geração e verificação de assinatura digital.

Processo de Assinatura Digital	**Parâmetros de domínio**	**Status**
Geração de Assinatura Digital	< 112 bits de força de segurança: DSA: (L, N) ≠ (2048, 224), (2048, 256) ou (3072, 256) ECDSA: len(n) < 224 RSA: len(n) < 2048	Não permitido
	≥ 112 bits de força de segurança: DSA: (L, N) = (2048, 224), (2048, 256) ou (3072, 256) ECDSA ou EdDSA: len(n) ≥ 224 RSA: len(n) ≥ 2048	Aceitável
Verificação de assinatura digital	< 112 bits de força de segurança: DSA: ((512 ≤ L < 2048) ou (160 ≤ N < 224)) ECDSA: 160 ≤ len(n) < 224 RSA: 1024 ≤ len(n) < 2048	Uso legado
	≥ 112 bits de força de segurança: DSA: (L, N) = (2048, 224), (2048, 256) ou (3072, 256) ECDSA e EdDSA: len(n) ≥ 224 RSA: len(n) ≥ 2048	Aceitável

Fonte: Elaborada pelo autor com base no NIST 800 - 131A, 2022.

Ao analisar a Tabela 14, é possível perceber que o comprimento de chave privada para geração de assinatura digital, independente do método utilizado, não deve ser inferior a 112 bits. Nota-se também que, para verificação de assinatura digital, forças de segurança menores que 112 bits são aceitas apenas para uso legado. Segundo o NIST, nestes casos, o usuário do sistema estará aceitando alguns riscos que, com o tempo e evolução da capacidade de processamento e armazenamento dos computadores, poderá tornar-se maiores. Deste modo, fica a critério do usuário decidir se vale a pena correr estes riscos.

Na Tabela 15, são exibidas as funções *hash* e o status de aprovação de cada uma destas funções. Na primeira coluna da tabela, está o tipo de função *hash* e a qual família ela pertence. Na segunda coluna, estão os tipos de uso das funções. Por fim, na terceira coluna, são apresentados os status de aprovação de cada função.

Tabela 15 – Status de aprovação das funções de *hash.*

Função de *hash*	**Uso**	**Status**
SHA-1	Geração de assinatura digital	Não permitido
	Verificação de assinatura digital	Uso legado
	Aplicativos sem assinatura digital	Aceitável
Família SHA-2 (SHA 224, SHA-256, SHA-384, SHA-512, SHA-512/224 e SHA-512/256)	Aceitável para todos os aplicativos de função *hash*	
Família SHA-3 (SHA3-224, SHA3-256, SHA3-384 e SHA3-512)	Aceitável para todos os aplicativos de função *hash*	

Fonte: Elaborada pelo autor com base no NIST SP 800 - 131A, 2022.

Ao se analisar a Tabela 15, percebe-se que existem alguns tipos de funções *hash* que, dependendo da finalidade de uso, podem não serem consideradas seguras segundo o NIST SP 800 - 131A, como por exemplo a função SHA-1. Todas as informações apresentadas nas Tabelas 13, 14 e 15 podem ser acessadas no NIST SP 800 - 131 A[7].

Durante o processo de avaliação dos gateways IoT, não foram localizadas funções ou algoritmos não aprovados pelo NIST SP 800 - 131A. Deste modo, todas as funções e algoritmos localizados durante a inspeção do requisito são considerados fortes e aprovados pelo NIST, como por exemplo, as funções *hashes* e algoritmos AES. Este é um resultado interessante e importante. Porém, não é possível afirmar que todas as funções e algoritmos utilizados pelos gateways são considerados seguros e aprovados por um padrão criptográfico reconhecido, devido a dificuldade de identificação destes padrões na codificação e a falta de informações nas documentações disponibilizadas pelos desenvolvedores dos gateways.

5.5.2.8. Todas as funções criptográficas relacionadas ao produto são suficientemente seguras para o ciclo de vida do produto, por exemplo, aqueles estipulados no NIST SP 800 - 131A [ref 2].

Ao se analisar a Tabela 8, que apresenta as funções *hashes*, é possível perceber que todos os gateways, com exceção do gateway B, utilizam funções aprovadas pelo NIST SP 800

[7] Disponível para acesso em: <https://doi.org/10.6028/NIST.SP.800-131Ar2>. Último acesso em 19 de junho de 2022.

- 131A, como por exemplo, SHA - 256, localizada no código fonte dos gateways A, C e D. Assim sendo, constatamos que os gateways avaliados, com exceção do gateway B, fazem uso de funções suficientemente seguras. No entanto, não é possível afirmar se todas as funções utilizadas no processo de criptografia são aprovadas pelo NIST SP 800 - 131A.

5.5.2.9. O produto armazena todos os parâmetros não criptografados sensíveis, por exemplo, chaves, em um local seguro e inviolável.

O gateway A faz uso da *Bcrypt* para armazenar os dados em um banco de dados. *Bcrypt* é utilizada para armazenar senhas e dados sensíveis em um banco de dados fazendo uso de algoritmos *hashes*. Por sua vez, os gateways C e D utilizam a *Keytool* para armazenar chaves e certificados. *Keytool* faz parte das distribuições do Java fornecidas pela empresa Oracle, sendo usada para gerenciar bases de dados. Por fim, o gateway B, não faz uso de recursos criptográficos.

Não foram localizadas informações afirmando que as bibliotecas utilizadas pelo gateways fazem uso de um padrão de criptografia reconhecido fornecido pela comunidade, no entanto também não foram localizadas informações afirmando que as bibliotecas são inseguras. Assim sendo, com exceção do gateway B, que não faz uso de criptografia, os demais armazenam dados sensíveis em bancos de dados utilizando bibliotecas consideradas seguras pelos desenvolvedores de software.

5.5.2.10. Todos os comprimentos de chave são suficientes para o nível de garantia exigido, conforme detalhado no NIST SP 800 - 57 Parte 1.

Ao analisar o tamanho das chaves criptográficas localizadas nos gateways A, C e D, encontram-se chaves com forças de segurança de 128 bits. Essa força de segurança é considerada aprovada pelo NIST SP 800 - 57, conforme especificado na Tabela 8 ou na documentação do padrão criptográfico. Já no gateway B não foram localizadas chaves.

5.5.3. Registrar os resultados da Inspeção

Ao finalizar a inspeção dos requisitos em cada um dos quatro gateways, é realizado o registro em uma tabela. A Tabela 16 apresenta os 10 requisitos de criptografia e o registro da inspeção nos gateway IoT. Com relação ao resultado da verificação, a Tabela 16 apresenta 2 possibilidades:

- **Conforme:** O requisito foi verificado integralmente nos gateways IoT conforme o solicitado em seu enunciado;
- **Não Conforme:** O requisito não foi verificado, devido a não conformidade dos gateways IoT com o solicitado no enunciado do requisito.

Tabela 16 – Verificação de conformidade de requisitos nos gateways avaliados.

N°	Requisitos	Gateway A	Gateway B	Gateway C	Gateway D
RC-01	Verifique o uso adequado da criptografia. Apenas algoritmos padrões e fortes devem ser usados, com tamanho de chave adequado e implementações seguras.	Conforme	Não Conforme	Conforme	Conforme
RC-02	Verifique se as bibliotecas criptográficas usadas são certificadas para serem compatíveis com um padrão de segurança criptográfico reconhecido.	Não Conforme	Não Conforme	Não Conforme	Não Conforme
RC-03	Os módulos de criptografia foram validados em relação ao FIPS 140-2 ou equivalente: Verifique se os algoritmos criptográficos usados pelo aplicativo foram validados em relação ao FIPS 140-2 ou um padrão equivalente.	Conforme	Não Conforme	Conforme	Conforme
RC-04	As IIP são criptografadas em repouso e protegidas durante a comunicação: as informações de identificação pessoal devem ser armazenadas criptografadas em repouso e garantir que a comunicação seja feita por meio de canais protegidos.	Conforme	Não Conforme	Não Conforme	Conforme
RC-05	Os segredos são substituíveis e colocados na instalação: Verifique se todas as chaves e senhas são substituíveis e são geradas ou substituídas no momento da instalação.	Não Conforme	Não Conforme	Conforme	Não Conforme
RC-06	Existe um processo de provisionamento seguro de chaves que inclui geração, distribuição, atualização, revogação e destruição. Por exemplo, em conformidade com FIPS 140-2 [ref 5] ou um processo semelhante.	Não Conforme	Não Conforme	Não Conforme	Não Conforme
RC-07	Todas as funções criptográficas relacionadas ao produto não têm pontos fracos conhecidos publicamente, por exemplo, MD5 e SHA-1 não são usados, por exemplo, conforme estabelecido no NIST SP800-131A [ref 2].	Conforme	Não Conforme	Conforme	Conforme
RC-08	Todas as funções criptográficas relacionadas ao produto são suficientemente seguras para o ciclo de vida do produto, por exemplo, aqueles estipulados no NIST SP800-131A [ref 2].	Conforme	Não Conforme	Conforme	Conforme
RC-09	O produto armazena todos os parâmetros não criptografados sensíveis, por exemplo, chaves, em um local seguro e inviolável.	Conforme	Não Conforme	Conforme	Conforme
RC-10	Todos os comprimentos de chave são suficientes para o nível de garantia exigido,	Conforme	Não Conforme	Conforme	Conforme

N°	Requisitos	Gateway A	Gateway B	Gateway C	Gateway D
	conforme detalhado no NIST SP800-57 Parte 1.				

Fonte: O autor (2022).

Ao analisar a Tabela 16, é possível observar que nenhum dos *gateways* atingiu 100% de conformidade dos requisitos, fator que desperta preocupação quanto a segurança criptográfica dos gateways. Para melhor compreender o processo de avaliação dos requisitos e acompanhar cada detalhe das etapas da inspeção, a Tabela 16 apresenta 4 possibilidades possíveis de verificação dos requisitos, que estão descritas a seguir:

- **Conformidade verificada na instalação (CI):** A verificação do requisito foi possível na instalação do gateway IoT.
- **Conformidade verificada na documentação (CD):** A verificação do requisito foi possível através da documentação fornecida pelo desenvolvedor do gateway ou através de fórum ou materiais disponíveis na Internet.
- **Conformidade verificada no código fonte (CCF):** A verificação do requisito foi possível através do código fonte do gateway IoT.
- **Não conformidade (NC):** Não foi possível efetuar a verificação de conformidade e, por falta de evidências, se considera que o gateway não está em conformidade com o requisito.

Inicialmente, se buscou verificar a conformidade do requisito no gateway no momento da instalação do gateway e através da navegação pela interface gráfica. Se a conformidade for atendida, é realizado o registro deste resultado na tabela. Caso contrário, é iniciada a verificação de conformidade através da documentação disponibilizada pelo fornecedor do gateway. Mas, se mesmo assim não for possível efetuar a verificação de conformidade, é realizada verificação através do código fonte. Por fim, se a conformidade do requisito não for atendida em nenhuma destas etapas, é realizado o registro na tabela informado que o gateway não possui conformidade com o requisito.

Tabela 17 – Avaliação de Conformidade dos Requisitos por Formas de Verificação

N°	Requisitos	Gateway A	Gateway B	Gateway C	Gateway D
RC-01	Verifique o uso adequado da criptografia. Apenas algoritmos padrões e fortes devem	CCF	NC	CCF	CCF

N°	Requisitos	Gateway A	Gateway B	Gateway C	Gateway D
	ser usados, com tamanho de chave adequado e implementações seguras.				
RC-02	Verifique se as bibliotecas criptográficas usadas são certificadas para serem compatíveis com um padrão de segurança criptográfico reconhecido.	NC	NC	NC	NC
RC-03	Os módulos de criptografia foram validados em relação ao FIPS 140-2 ou equivalente: Verifique se os algoritmos criptográficos usados pelo aplicativo foram validados em relação ao FIPS 140-2 ou um padrão equivalente.	CCF	NC	CCF	CCF
RC-04	As IIP são criptografadas em repouso e protegidas durante a comunicação: as informações de identificação pessoal devem ser armazenadas criptografadas em repouso e garantir que a comunicação seja feita por meio de canais protegidos.	NC	NC	NC	NC
RC-05	Os segredos são substituíveis e colocados na instalação: Verifique se todas as chaves e senhas são substituíveis e são geradas ou substituídas no momento da instalação.	NC	NC	CCF	NC
RC-06	Existe um processo de provisionamento seguro de chaves que inclui geração, distribuição, atualização, revogação e destruição. Por exemplo, em conformidade com FIPS 140-2 [ref 5] ou um processo semelhante.	NC	NC	NC	NC
RC-07	Todas as funções criptográficas relacionadas ao produto não têm pontos fracos conhecidos publicamente, por exemplo, MD5 e SHA-1 não são usados, por exemplo, conforme estabelecido no NIST SP800-131A [ref 2].	CD	NC	CCF	CCF
RC-08	Todas as funções criptográficas relacionadas ao produto são suficientemente seguras para o ciclo de vida do produto, por exemplo, aqueles estipulados no NIST SP800-131A [ref 2].	CCF	NC	CCF	CCF
RC-09	O produto armazena todos os parâmetros não criptografados sensíveis, por exemplo, chaves, em um local seguro e inviolável.	CCF	NC	CCF	CCF
RC-10	Todos os comprimentos de chave são suficientes para o nível de garantia exigido, conforme detalhado no NIST SP800-57 Parte 1.	CCF	NC	CCF	CCF

Fonte: O autor (2022).

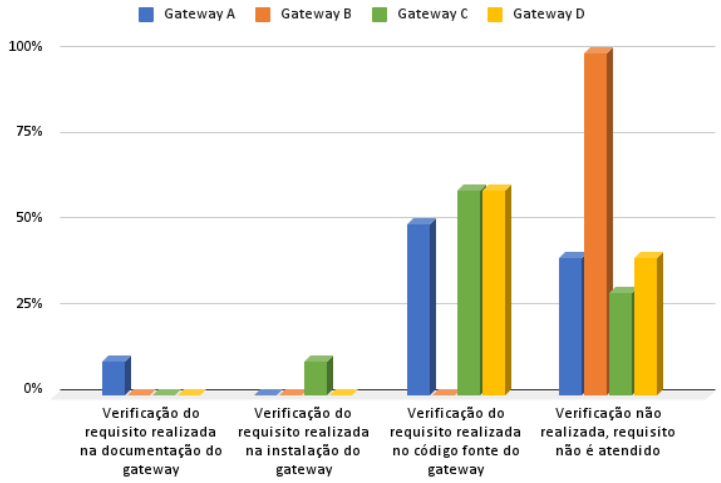
Pode-se afirmar que, em geral, pouca ou nenhuma informação foi localizada em relação à segurança criptográfica na documentação dos gateways. Situação similar ocorre em relação à verificação no momento da instalação ou através da navegação da interface gráfica.

Como é possível perceber na Tabela 17, para um usuário identificar o nível de segurança criptográfica dos gateways, é usualmente necessário analisar o código fonte associado ao gateway.

5.6. Realizar Avaliação dos Resultados

A Figura 12 apresenta e avalia a conformidade dos requisitos levando em consideração quatro critérios: verificação do requisito na documentação, na instalação, pelo código fonte e a não conformidade do requisito.

Figura 12 – Forma de verificação de conformidade dos requisitos.

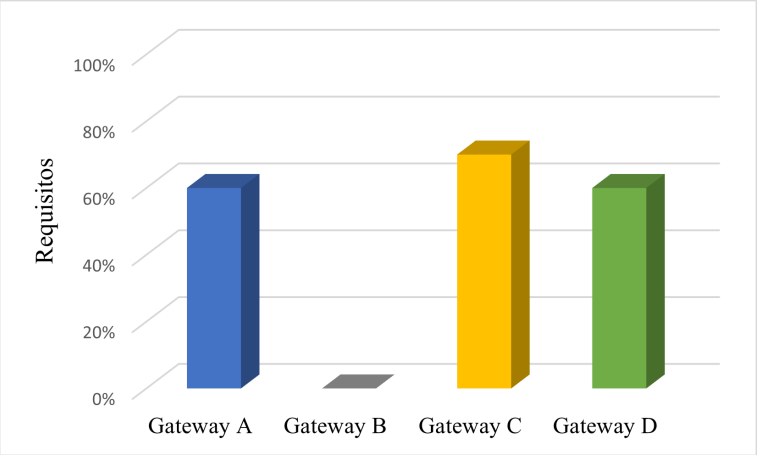


Fonte: O autor (2022).

Na Figura 12, é possível notar que todos os gateways apresentam não conformidade com pelo menos um requisito. É possível observar também que o Gateway B apresentou não conformidade em relação a todos os requisitos avaliados. Outro fato a ser mencionado é que nenhum dos gateways apresenta conformidade superior a 25% no processo de instalação ou através da verificação na documentação. Logo, um usuário com pouco conhecimento em programação não conseguiria identificar qual gateway utilizar para garantir a segurança dos seus dados.

A Figura 13 exibe o resultado referente ao nível de conformidade de cada gateway considerando os 10 requisitos de segurança criptográfica selecionados.

Figura 13 – Nível de conformidade de requisitos por gateway.



Fonte: O autor (2022).

Ao se analisar a Figura 13, é possível perceber o nível de conformidade que cada gateway apresenta em relação aos requisitos priorizados. Os gateways A e D atendem 70% dos requisitos, enquanto o gateway C está em conformidade com 80% dos requisitos. Por sua vez, o gateway B não atende nenhum dos requisitos. Diante dos resultados expostos é possível verificar o status da segurança criptográfica atual dos gateways IoT comumente utilizados. Devido a importância do gateway para um sistema IoT, é interessante que a conformidade esteja próxima do valor máximo. Considerando os resultados apresentados, não é possível afirmar que as informações trafegadas pelos gateways estão 100% protegidas, visto que nenhum dos gateways atingiu 100% dos requisitos. Mas, é possível afirmar que os gateways A, C e D apresentaram nível que pode ser considerado, de um ponto de vista quantitativo, como regular. É importante ressaltar também que um dos gateways atingiu nível mínimo de conformidade (0%), o que reforça a importância da avaliação realizada neste trabalho para auxiliar na melhor escolha de um gateway IoT.

5.7. Considerações finais

Este capítulo apresentou como foram conduzidos os subprocessos e atividades, descritos na metodologia apresentada no capítulo anterior, necessários para a inspeção e avaliação de requisitos de criptografia em gateways IoT baseados em *software* comumente utilizados. A avaliação realizada gerou resultados que podem ser usados para entender como está o estado atual da segurança criptográfica em gateways IoT. Além disto, esta avaliação

também propicia uma melhor escolha de gateway baseado no melhor nível de conformidade em relação a requisitos de segurança. Por fim, a avaliação realizada serviu tanto para ilustrar como também analisar a metodologia proposta no capítulo anterior.

No capítulo seguinte, as conclusões gerais desta dissertação são destacadas. Além disso, possibilidades de trabalhos futuros são introduzidas e detalhadas.

6. Conclusões e Trabalhos Futuros

Neste capítulo são apresentadas as conclusões, contribuições e trabalhos futuros desta dissertação. Na Seção 6.1 são exibidas as conclusões acerca da pesquisa realizada nesta dissertação. Na Seção 6.2 são apresentadas as contribuições científicas deste trabalho. Por fim, não menos importante, na Seção 6.3 são descritas as possibilidades de trabalhos futuros a serem realizados como complemento para esta pesquisa.

6.1. Conclusões

Este trabalho buscou evidenciar o nível atual de segurança criptográfica de gateways IoT baseados em software comumente utilizados no mercado. Inicialmente foi realizada uma pesquisa bibliográfica com intuito de se conhecer e aprofundar sobre o estado da arte da Internet das Coisas. Foi realizado também um levantamento do estado da arte sobre segurança de gateways IoT, o que permitiu perceber que diversas referências relevantes, como organizações técnicas e padrões internacionais, apresentam significativa preocupação com a segurança da Internet das Coisas. No entanto, ficou claro que a segurança dos gateways IoT em si não é priorizada e que dificilmente se sugere requisitos de segurança criptográfica direcionados para verificação de segurança destes gateways IoT.

Os requisitos priorizados e utilizados neste trabalho são de organizações de renome internacional, como IoTSF e OWASP. Estes requisitos passaram por uma rigorosa seleção, objetivando selecionar apenas requisitos de criptografia que pudessem ser utilizados, em termos práticos, para verificação de segurança criptográfica especificamente dos gateways IoT. Estes requisitos selecionados podem ser utilizados para verificação de segurança criptográfica dos demais gateways IoT que não fizeram parte desta pesquisa, bem como ajudar os fabricantes e desenvolvedores a fazerem uso dos recursos criptográficos validados por organizações técnicas reconhecidas pela comunidade científica, possibilitando assim estar em conformidade com os principais padrões de segurança criptográfica.

Para facilitar a compreensão do processo de avaliação proposto e permitir a sua reprodução (de forma alinhada à ideia de pesquisa reproduzível), foi descrita uma metodologia baseada em BPMN para avaliação de segurança criptográfica de gateways IoT. O processo modelado serviu não apenas para melhor ilustrar e estruturar a avaliação feita, mas

também para facilitar que outros pesquisadores possam a utilizar para realizar avaliações de segurança de gateways considerando requisitos de criptografia. A aplicação da metodologia proposta possibilitou uma avaliação mais assertiva a respeito do objetivo do estudo, e também trouxe resultados interessantes sobre o nível de segurança criptográfica de gateways IoT atualmente utilizados pela comunidade.

Por fim, a proposta apresentada neste trabalho possibilitou avanço ao estado da arte da área, pois apresentou uma avaliação técnica e reproduzível do nível de conformidade apresentado por gateways IoT considerando requisitos de segurança criptográfica.

6.2. Contribuições

A principal contribuição científica apresentada neste trabalho é a avaliação de segurança criptográfica de gateways IoT baseados em software considerando requisitos de criptografia. Essa avaliação possibilitou saber como está o nível de segurança criptográfica de gateway IoT atualmente utilizados na comunidade. Também é possível utilizar o conjunto de requisitos selecionados nesta pesquisa na avaliação da segurança criptográfica de outros gateways IoT.

Esta dissertação apresentou também outras contribuições relevantes, como a revisão de literatura sobre o atual estado da arte em relação à segurança criptográfica dos gateways IoT. Outra contribuição interessante foi a metodologia proposta para avaliação de segurança criptográfica de gateways IoT. A metodologia possibilitou estruturar todo o conhecimento necessário para se realizar a avaliação desejada.

Por fim, este trabalho demonstrou a importância de se avaliar o nível de segurança criptográfica de gateways IoT, apresentando as limitações de segurança criptográficas localizadas em quatro gateways utilizados atualmente, considerando dez requisitos de criptografia que foram priorizados dentre vinte e seis inicialmente selecionados.

6.3. Trabalhos futuros

Como trabalho futuro, se vislumbra aumentar o número de organizações técnicas consideradas para avaliação de requisitos de criptografia. Assim sendo, se almeja incluir, dentre outras, as seguintes organizações: *European Telecommunications Standards Institute* (ETSI), *European Union Agency for Cybersecurity* (ENISA), *Cloud Security Alliance* (CSA)

e *Online Trust Alliance* (OTA). A inclusão destas organizações é importante para se obter um conjunto mais rico de requisitos, objetivando-se assim, conseguir resultados mais abrangentes em relação à segurança criptográfica dos gateways IoT. Esses resultados podem ser obtidos através da realização das inspeções utilizando as sugestões e técnicas apresentadas por esse conjunto maior de requisitos, possibilitando assim localizar um número maior de possíveis falhas ou qualidades que o sistema de um gateway possa apresentar.

Além disso, também está planejada a expansão do número de gateways IoT baseados em *software*, através da inclusão do Agile, Thinger, Liota VMware, Ubiworx entre outros. O aumento no número de gateways é interessante devido ao fato de ser possível obter resultados mais expressivos através de uma amostra maior de gateways. Como se pretende aumentar o número de requisitos de segurança criptográfica, estes outros gateways poderão também ser avaliados com o novo conjunto de requisitos.

Também se almeja conduzir testes de penetração para identificar possíveis vulnerabilidades dos gateways. Podem ser utilizados testes dos seguintes tipos: testes de quebra de criptografia, testes de força bruta e teste de quebra de senha. Realizar esses tipos de ataques é interessante também para avaliar como o gateway reage diante de situações de estresse

Por fim, também se planeja avaliar se a configuração criptográfica adotada (exemplo: algoritmo criptográfico e tamanho de chave) está condizente tanto com o nível de segurança desejado como também com o impacto de desempenho observado. Neste caso, é válido salientar que, o ideal é que o sistema possua apenas a segurança necessária para se proteger de possíveis ataques. Pois, quanto mais seguro for o sistema (exemplo: chave com tamanho elevado), maior será o tempo de execução da solução de segurança e pior será o desempenho (em termos de tempo de execução). Este contexto pode ser extremamente crítico para sistemas baseados em IoT. Diante de tal situação é interessante pesquisar uma solução que apresenta melhor custo benefício para o usuário ou desenvolvedor do sistema.

Referências

ALBARELLO, R.; OYAMADA, M.; CAMARGO, E. DE. **Avaliação de Algoritmos de Criptografia e Implementação de um Protocolo Leve para Comunicação entre Dispositivos IoT**. Anais Estendidos do Simpósio Brasileiro de Engenharia de Sistemas Computacionais (SBESC). **Anais**... Em: ANAIS ESTENDIDOS DO X SIMPÓSIO BRASILEIRO DE ENGENHARIA DE SISTEMAS COMPUTACIONAIS. SBC, 23 nov. 2020. Disponível em: <https://sol.sbc.org.br/index.php/sbesc_estendido/article/view/13092>. Acesso em: 5 mar. 2022

ANKELE, R. et al. **Requirements and Recommendations for IoT/IIoT Models to automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing**. Proceedings of the 14th International Conference on Availability, Reliability and Security. **Anais**...: ARES '19.New York, NY, USA: Association for Computing Machinery, 26 ago. 2019. Disponível em: <https://doi.org/10.1145/3339252.3341482>. Acesso em: 9 fev. 2022

BARKER, E. **Recommendation for Key Management: Part 1 – General**. [s.l.] National Institute of Standards and Technology, 4 maio 2020. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>. Acesso em: 19 fev. 2022.

BARKER, E.; ROGINSKY, A. **Transitioning the Use of Cryptographic Algorithms and Key Lengths**. [s.l.] National Institute of Standards and Technology, 21 mar. 2019. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final>. Acesso em: 19 fev. 2022.

CHOI, J.-I. et al. Analysis of IoT Open-Platform Cryptographic Technology and Security Requirements. **KIPS Transactions on Computer and Communication Systems**, v. 7, n. 7, p. 183–194, 31 jul. 2018.

CODEIOT. **Gateway | Aula 8 - Gateways na IoT | Material didático IOT101 | Code IoT**. Disponível em: <https://codeiot.org.br/courses/course-v1:LSI-TEC+IOT101+2020_O1/courseware/88349d2e8b8d49dbad5036adbe7435d4/828ce99ce1f64477a9f8b82176f3b25e/1?activate_block_id=block-v1%3ALSI-TEC%2BIOT101%2B2020_O1%2Btype%40vertical%2Bblock%4028fd9b057d7e46fa817da317d94b2f7c>. Acesso em: 4 jun. 2022.

CSA. **CSA IoT Security Controls Framework v2**. Disponível em: <https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2/>. Acesso em: 18 jun. 2022.

ENISA. **Baseline Security Recommendations for IoT**. Report/Study. Disponível em: <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>. Acesso em: 18 jun. 2022.

GSMA. **GSMA IoT Security Assessment ChecklistSecurity** , 30 set. 2018. Disponível em: <https://www.gsma.com/security/resources/clp-17-gsma-iot-security-assessment-checklist-v3-0/>. Acesso em: 18 jun. 2022

HANSCH, G. et al. **A Unified Architecture for Industrial IoT Security Requirements in Open Platform Communications**. 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). **Anais**... Em: 2019 24TH IEEE INTERNATIONAL CONFERENCE ON EMERGING TECHNOLOGIES AND FACTORY AUTOMATION (ETFA). set. 2019.

IMDAD, M. et al. Internet of things: security requirements, attacks and counter measures. **Indonesian Journal of Electrical Engineering and Computer Science**, v. 18, p. 1520, 1 jun. 2020.

IOTSF. **IoT security compliance framework**, 2020. Disponível em: <https://www.iotsecurityfoundation.org/iotsf-issues-update-to-popular-iot-security-compliance-framework/undefined>. Acesso em: 17 jun. 2022

IOTSF. **IoT Security Foundation – The Global Home of IoT Cybersecurity**, [s.d.]. Disponível em: <https://www.iotsecurityfoundation.org/>. Acesso em: 20 jun. 2022

ISA/IEC 62443 Cybersecurity | ISA São Paulo Section. , [s.d.]. Disponível em: <http://isasp.org.br/isa-iec-62443-cybersecurity/>. Acesso em: 3 mar. 2022

KAMALRUDIN, M.; IBRAHIM, A. A.; SIDEK, S. **A Security Requirements Library for the Development of Internet of Things (IoT) Applications**. (M. Kamalrudin, S. Ahmad, N. Ikram, Eds.)Requirements Engineering for Internet of Things. **Anais**...: Communications in Computer and Information Science.Singapore: Springer, 2018.

LINS, F. A. A.; VIEIRA, M. Security Requirements and Solutions for IoT Gateways: A Comprehensive Study. **IEEE Internet of Things Journal**, v. 8, n. 11, p. 8667–8679, jun. 2021.

LUIZ, E. DE O. B. M. Sistema de Detecção de Intrusão Baseado em Criptografia Simétrica para Redes IoT de Baixa Potência. p. 74, 10 abr. 2020.

MACHADO, J. DOS S. et al. UM ESTUDO DOS ALGORITMOS DE CRIPTOGRAFIA LEVE PARA DISPOSITIVOS IOT. **Revista Expressão Científica (REC)**, v. 6, n. 2, p. 71–86, 27 out. 2021.

MAIERO, M. **5.0.0**. Text. Disponível em: <https://projects.eclipse.org/projects/iot.kura/releases/5.0.0>. Acesso em: 15 jun. 2022.

MENEGATTI, F. **Crescimento do IoT no Brasil abre oportunidades de negócios em rastreamento veicular e gestão de frotasTI INSIDE Online**, 15 fev. 2022. Disponível em: <https://tiinside.com.br/15/02/2022/crescimento-do-iot-no-brasil-abre-oportunidades-de-negocios-em-rastreamento-veicular-e-gestao-de-frotas/>. Acesso em: 26 maio. 2022

NING, L. et al. A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things. **IEEE Access**, v. 8, p. 220165–220187, 2020.

NIST. **National Institute of Standards and Technology**. text. Disponível em: <https://www.nist.gov/>. Acesso em: 19 fev. 2022.

NOKIA. **Nokia Threat Intelligence Report warns of rising cyberattacks on internet-connected devices**. Disponível em: <https://www.nokia.com/about-us/news/releases/2020/10/22/nokia-threat-intelligence-report-warns-of-rising-cyberattacks-on-internet-connected-devices/>. Acesso em: 1 jun. 2022.

NOLETO, C. **Internet das Coisas: entenda o conceito e confira 6 exemplos!** Disponível em: <https://blog.betrybe.com/tecnologia/internet-das-coisas/>. Acesso em: 30 maio. 2022.

OTA. **IoT Trust FrameworkInternet Society**, 2018. Disponível em: <https://www.internetsociety.org/iot/trust-framework/>. Acesso em: 18 jun. 2022

OWASP. **Fundação OWASP | Fundação de código aberto para segurança de aplicativos**. Disponível em: <https://owasp.org/>. Acesso em: 19 fev. 2022a.

OWASP. **OWASP Annotated Application Security Verification Standard — OWASP Annotated Application Security Verification Standard 3.0.0 documentation**. Disponível em: <https://owasp-aasvs.readthedocs.io/en/latest/index.html>. Acesso em: 18 jun. 2022b.

PAPCUN, P. et al. Edge-enabled IoT gateway criteria selection and evaluation. **Concurrency and Computation: Practice and Experience**, v. 32, n. 13, p. e5219, 2020.

PARRA RODRIGUEZ, J. D.; SCHRECKLING, D.; POSEGGA, J. **Addressing Data-Centric Security Requirements for IoT-Based Systems**. 2016 International Workshop on Secure Internet of Things (SIoT). **Anais**... Em: 2016 INTERNATIONAL WORKSHOP ON SECURE INTERNET OF THINGS (SIOT). set. 2016.

SANTOS, B. P. et al. Internet das Coisas: da Teoria à Prática. p. 50, 2016.

Statista - The Statistics Portal. Disponível em: <https://www.statista.com/>. Acesso em: 31 maio. 2022.

SYDLE. **O que é a Internet das Coisas? Aprenda tudo sobre IoT**. Disponível em: <https://www.sydle.com/br/blog/internet-das-coisas-6239c79c3bbdd676577a1e76/>. Acesso em: 30 maio. 2022.

TEAM, E. C. **ETSI - ETSI releases world-leading Consumer IoT Security standard**. Disponível em: <https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard>. Acesso em: 18 jun. 2022.

TECHNOLOGY, N. I. OF S. AND. **DES Modes of Operation**. [s.l.] U.S. Department of Commerce, 2 dez. 1980. Disponível em:

<https://csrc.nist.gov/publications/detail/fips/81/archive/1980-12-02>. Acesso em: 19 fev. 2022.

TECHNOLOGY, N. I. OF S. AND. **Secure Hash Standard**. [s.l.] U.S. Department of Commerce, 17 abr. 1995. Disponível em: <https://csrc.nist.gov/publications/detail/fips/180/1/archive/1995-04-17>. Acesso em: 19 fev. 2022.

TECHNOLOGY, N. I. OF S. AND. **Data Encryption Standard (DES)**. [s.l.] U.S. Department of Commerce, 25 out. 1999. Disponível em: <https://csrc.nist.gov/publications/detail/fips/46/3/archive/1999-10-25>. Acesso em: 19 fev. 2022.

TECHNOLOGY, N. I. OF S. AND. **Digital Signature Standard (DSS)**. [s.l.] U.S. Department of Commerce, 27 jan. 2000. Disponível em: <https://csrc.nist.gov/publications/detail/fips/186/2/archive/2000-01-27>. Acesso em: 19 fev. 2022.

TECHNOLOGY, N. I. OF S. AND. **Security Requirements for Cryptographic Modules**. [s.l.] U.S. Department of Commerce, 3 dez. 2002. Disponível em: <https://csrc.nist.gov/publications/detail/fips/140/2/final>. Acesso em: 31 dez. 2021.

THINGSBOARD. **Releases · thingsboard/thingsboard**. Disponível em: <https://github.com/thingsboard/thingsboard/releases>. Acesso em: 16 jun. 2022.

TTA. **Associação Coreana de Tecnologia da Informação e Comunicação - Login Integrado**. Disponível em: <http://www.tta.or.kr/loginView.do>. Acesso em: 6 jun. 2022.

VAILSHERY, L. S. V. **Number of connected devices worldwide 2030**. Disponível em: <https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/>. Acesso em: 30 maio. 2022.

VIVO. **Tendências para 2022: a evolução da Internet das Coisas e como ela pode beneficiar sua empresa**. Disponível em: <https://vivomeunegocio.com.br/conteudos-gerais/expandir/evolucao-da-internet-das-coisas/>. Acesso em: 25 maio. 2022.

WEBIOPI. **Download last release**. Disponível em: <https://webiopi.trouch.com/DOWNLOADS.html>. Acesso em: 16 jun. 2022.

WEBTHINGS. **Releases · WebThingsIO/gateway**. Disponível em: <https://github.com/WebThingsIO/gateway/releases>. Acesso em: 16 jun. 2022.