UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

DEPARTAMENTO DE COMPUTAÇÃO

PROGRAMA DE PÓS–GRADUAÇÃO EM INFORMÁTICA APLICADA

DIEGO RIBEIRO GOMES

AVALIAÇÃO DE CONFORMIDADE DE REQUISITOS DE AUTENTICAÇÃO EM GATEWAYS IOT

RECIFE – PE

2022

AVALIAÇÃO DE CONFORMIDADE DE REQUISITOS DE AUTENTICAÇÃO 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 Prof. Dr. Fernando Antônio Aires Lins e coorientação do Prof. Dr. Obionor de Oliveira Nóbrega.

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)

G633a Gomes, Diego Ribeiro
Avaliação de conformidade de requisitos de autenticação em gateways IOT / Diego Ribeiro Gomes. - 2022.
78 f. : il.

Orientador: Fernando Antonio Aires Lins.
Coorientador: Obionor de Oliveira Nobrega.
Inclui referências e apêndice(s).

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 autenticação. I. Lins, Fernando Antonio Aires, orient. II. Nobrega, Obionor de Oliveira, coorient. III. Título

CDD 004

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

DIEGO RIBEIRO GOMES

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

Profª. Dra. Jeísa Pereira de Oliveira Domingues
Universidade Federal Rural de Pernambuco - UFRPE

Prof. Dr. Jorge da Silva Correia Neto
Universidade Federal Rural de Pernambuco - UFRPE

Prof. Dr. Nelson Souto Rosa
Universidade Federal de Pernambuco - UFPE

Recife, 13 de julho de 2022

Dedicatória

*A minha querida mãe, **Claúdia Maria**, por sempre acreditar em mim, muitas vezes sem entender os meus sonhos. No entanto, dedicou a sua vida em proveito das realizações e felicidade de seus filhos.*

*Aos meus irmãos, **Tiago e Adriano**, pela amizade, força e incentivo.*

*Ao meu eterno amigo **João Barbosa** (in memoriam), que esteve comigo em vários momentos significativos.*

*Ao meu amigo e professor **Oswaldo Sérgio,** pelo apoio, dedicação e parceria. Nada disso teria sentido se vocês não existissem em minha vida.*

Agradecimento

Nestes anos de mestrado, de muito aprendizado, dedicação e empenho, também foram momentos de inúmeros desafios, perdas, dúvidas e alegrias. No entanto, tiveram pessoas especiais em cada um desses momentos. Portanto, expresso aqui, através de palavras, a importância delas no meu crescimento pessoal e profissional.

A Deus, pelo dom Vida e por me permitir realizar tão grandes sonhos. A Nossa Senhora das Graças por sempre está me guiando, abençoando e protegendo das diversas armadilhas da vida.

À minha família, meu porto seguro, meu expressivo agradecimento, por todas as vezes que precisei de carinho, compreensão e atenção. Agradeço sempre a Deus por ter vocês ao meu lado, pois nunca foi fácil a nossa caminhada.

Ao Prof. Fernando Aires, pela orientação, dedicação, profissionalismo e por todo conhecimento compartilhado, tão importantes em minha vida acadêmica. Diversos momentos, em nossas reuniões online, cheguei desanimado e sem entender o que estava fazendo. No entanto, o senhor sempre com palavras de incentivo que resultavam em força e ânimo para continuar. Eu tenho a certeza de que sem o seu amparo, confiança e apreço nada disso seria possível. O senhor é mais do que um orientador, um verdadeiro amigo e mestre. Meu muito obrigado!

Aos membros da banca examinadora, Profª Jeísa Pereira de Oliveira Domingues, Prof. Jorge da Silva Correia Neto e Prof. Nelson Souto Rosa, que tão gentilmente aceitaram participar e contribuir com esta dissertação. Não poderia deixar de agradecer ao Prof. e coorientador Obionor de Oliveira Nobrega pelas contribuições significativas em minha pesquisa.

Aos professores das disciplinas eletivas, Prof. Glauco Gonçalves, Prof. George Valença, Prof. Gilberto Cysneiros e ao Prof. Wilson Júnior, meu muito obrigado pelo conhecimento compartilhado em minha formação acadêmica.

Ao meu grande mestre e professor, Oswaldo Sérgio, que me incentivou a ingressar no magistério. O seu conhecimento e dedicação profissional sempre foi um grande exemplo para mim, e hoje, agradeço por ter sempre me motivado a seguir no caminho da docência. Meus sinceros agradecimentos.

A querida irmã fraterna em Cristo, Eliane Souto Carvalho, um anjo que Deus colocou em meu caminho. Obrigado pelos conselhos, disponibilidade e ensinamento, em momentos essenciais desta minha jornada. Meu eterno agradecimento.

Ao eterno amigo João Barbosa (in memoriam), pelos inúmeros conselhos e ensinamentos que me foi proporcionado. Agradeço a Deus a oportunidade de vivenciar tantos momentos significativos em sua vida. Que Deus lhe conceda o descanso eterno e conserve em mim as melhores memórias da grande amizade que nos aproximou.

Aos meus amigos, Valder Tabosa, Waldyr Siqueira, José Américo, Valber Marcel, Paulo Afonso (in memoriam), Osvaldo Boracini, Marcus Tayah e a Lindomar Panzuty que mesmo distantes, sempre estiveram presentes no meu crescimento profissional. Meu muito obrigado pelos ensinamentos, companheirismo e principalmente pela amizade construída ao longo dessa jornada.

Por fim, a todos aqueles que contribuíram, direta ou indiretamente, para a realização desta dissertação, o meu sincero agradecimento.

Epígrafe

“O conhecimento é em si mesmo um poder.”

(Francis Bacon)

Resumo

Dentro da Internet das Coisas, os gateways são dispositivos que exercem uma função estratégica na comunicação dos dispositivos com o ambiente externo. Gateways ajudam no problema da heterogeneidade, atuando para realizar a comunicação de dispositivos mesmo que os mesmos utilizem protocolos distintos. Contudo, dada a sua posição centralizada e estratégica em uma rede da Internet das Coisas (IoT), a segurança do gateway se torna ainda mais relevante. Um ataque bem-sucedido a este dispositivo pode deixar vulnerável todas as coisas dentro do sistema IoT. Neste contexto, considerando os requisitos de segurança tradicionais, a autenticação se apresenta com elevada importância em sistemas IoT, visto que é importante que os dispositivos passem por um processo de autenticação antes de serem inseridos no ambiente. Nesta dissertação, o objetivo principal é avaliar os níveis de conformidade de autenticação em gateways IoT atualmente utilizados na comunidade. Para isto, foi desenvolvida uma metodologia de avaliação, descrita em Notação para Modelagem de Processos de Negócio (BPMN), para avaliação de requisitos de autenticação em gateways IoT. Consequentemente, foi possível analisar e selecionar diversos requisitos em autenticação publicados por organizações técnicas internacionalmente reconhecidas, como IoTSF e OWASP. Os gateways atualmente usados em IoT foram levantados, instalados e configurados, e o processo de inspeção dos requisitos foi executado. Em termos de resultados, foi possível observar que os gateways atuais, em sua configuração padrão, só conseguem atender aproximadamente 66% dos requisitos de autenticação apresentados pelas organizações técnicas.

Palavras-chave: Segurança, Internet das Coisas, Gateway, Requisitos de Autenticação

Abstract

Within the Internet of Things, gateways are devices that play a strategic role in the communication of devices with the external environment. Gateways help with the problem of heterogeneity, acting to conduct the communication of devices even if they use different protocols. However, given its centralized and strategic position in an IoT network, gateway security becomes even more relevant. A successful attack on this device could leave everything inside the Internet of things (IoT) system vulnerable. In this context, considering traditional security requirements, authentication is incredibly important in IoT systems, since it is important that devices go through an authentication process before being inserted into the environment. In this dissertation, the main objective is to evaluate the authentication compliance levels of IoT gateways currently used in the community. For this, an evaluation methodology was developed, described in Business Process Model and Notation (BPMN), to evaluate authentication requirements in IoT gateways. Consequently, it was possible to analyze and select several authentication requirements published by internationally recognized technical organizations, such as IoTSF and OWASP. The gateways currently used in IoT were surveyed, installed, and configured, and the requirements inspection process was performed. In terms of results, it was possible to observe that current gateways, in their default configuration, can only meet approximately 66% of the authentication requirements presented by technical organizations.

Keywords: Security, Internet of Things, Gateway, Authentication requirements.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

2FA	Two-Factor Authentication
AAL	Authenticator Assurance Level
BPMN	Business Process Model and Notation
CSA	Cloud Security Alliance
CSP	Credential Service Provider
DFR	Digital Forensic Readiness
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
FAL	Federation Assurance Level
FR	Functional Requirement
GAR	Gateway Authentication Requirement
GSMA	GSM Association
GW	Gateway
IAL	Identity Assurance Level
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoTSF	IoT Security Foundation
ITC	Information and Communications Technology
ITL	Information Technology Laboratory
KBV	Knowledge-Based Verification
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OPC UA	Open Platform Communication Unified Architecture
OTA	Online Trust Alliance
OTP	One-Time Password
OWASP	OWASP IoT Security Verification Standard
PIN	Personal Identification Number
SFA	Single-Factor Authentication
SRE	Security Requirements Engineering

Sumário

1. Introdução

Atualmente, o número de objetos conectados à Internet está crescendo a uma proporção relevante. A Internet das Coisas (IoT) visa expandir a Internet não apenas conectando dispositivos computacionais à mesma, mas também ampliando a conexão de dispositivos do dia a dia como lâmpadas, ventiladores, geladeiras e ar-condicionados [1]. Neste contexto, sistemas baseados em IoT têm sido fundamentais para o avanço de temáticas relevantes, como redes veiculares, *smart health*, casas e cidades inteligentes, dentre outros [2]. Dentre os setores que mais realizaram investimentos em dispositivos IoT se destacam BSFS (Bancos, serviços financeiros e seguros), Varejo, Governo, Saúde, Manufatura, Agricultura, Energia Sustentável, Transporte, TI e Telecom [3].

Em um sistema IoT, os dispositivos podem ser divididos em três grupos básicos: sensores, atuadores e gateways [4]. Os sensores são responsáveis pelos processos de monitoramento, medição e coleta de dados em ambientes, e eles atuam medindo, por exemplo, movimentos, temperatura, umidade e localização. Os atuadores têm a função de realizar ações no ambiente, como desligar uma lâmpada ou acionar o motor de um portão. Por fim, os gateways exercem a função de mediador no processo de comunicação das coisas, auxiliando principalmente na heterogeneidade através do tratamento de diversos padrões e protocolos, mas também contribuindo na questão de segurança [5].

Em entrevista com diversos especialistas na área de segurança foi entregue um questionário estruturado para avaliar os principais ativos de IoT de acordo com a sua criticidade. A coleta dos dados revela que os protocolos de comunicação, os gateways e os aplicativos e serviços foram citados por 67%, isso é, o correspondente a mais de dois terços dos entrevistados [6]. Portanto, considerando a posição estratégica e centralizada do gateway em um sistema IoT, a adoção de medidas de segurança se torna essencial, visto que um ataque bem-sucedido ao gateway pode comprometer o sistema IoT como um todo. E, neste contexto, a autenticação se reveste de significativa relevância. Por exemplo, a *OWASP IoT Mapping Project* [7] possibilita que os fabricantes, as empresas e os consumidores tomem as melhores medidas de segurança na construção, implantação e na avaliação das tecnologias IoT. Na edição em 2018, a autenticação foi relacionada como a mais crítica, visto que sua priorização se encontra em três seções: ocupando o topo de criticidade as senhas fracas, adivinhadas ou codificação(A1); a Interfaces de ecossistema(A3); estando na terceira posição e a nona posição a Configuração padrão(A9). Essas medidas são apresentadas como TOP10 [8] que tem como objetivo priorizar

as dez questões mais críticas no ecossistema IoT. Portanto, a autenticação é considerada o ponto mais crítico no ranking do TOP10.

Neste contexto, a adoção de medidas de autenticação aparece com destaque, pois diminuirá as chances de que o gateway seja logicamente acessado por atacantes. Existem diversos métodos de autenticação, como; dois fatores, multifator, baseada em token, baseada em certificado, biometria e outros [9]. Inclusive, várias organizações divulgam recomendações importantes relacionadas à autenticação, que são descritas como requisitos em ambientes IoT (*Open Web Application Security Project* (OWASP) [10]–[11], *IoT Security Foundation* (IoTSF) [12], *European Union Agency for Network and Information Security* (ENISA) [6], *European Telecommunications Standards Institute* (ETSI) [13], *Online Trust Alliance* (OTA) [14], *GSM Association* (GSMA) [15] e *Cloud Security Alliance* (CSA) [16]). Essas recomendações são fundamentais na melhoria da autenticação em IoT, pois abordam diversas questões sobre a qualidade do processo de autenticação. Contudo, a literatura atual não aborda, com profundidade, os aspectos de segurança para gateways IoT, especialmente requisitos de autenticação.

1.1. Motivação

Em geral, sistemas e dispositivos precisam passar por um serviço de autenticação, visto que este recurso proporciona uma garantia de que a ação ou comunicação é legítima. Mas, para isso, dois pontos são necessários. O primeiro é garantir que as duas entidades são autênticas, e o segundo é proteger a conexão de interferência de terceiros [17]. Diante disso, surgiram diversas propostas de melhorias no serviço de autenticação, dentre eles o desenvolvimento de novos métodos de autenticação [1], protocolos [18] e algoritmos criptográficos [19]. Portanto, foi realizado um mapeamento sistemático, para compreender o atual estado da arte. Para isso, a Tabela 1 apresenta o protocolo de mapeamento.

Tabela 1 – Protocolo para o mapeamento sistemático da literatura.

Objeto de Pesquisa: Quais referências abordam os principais aspectos de autenticação em um ambiente IoT?

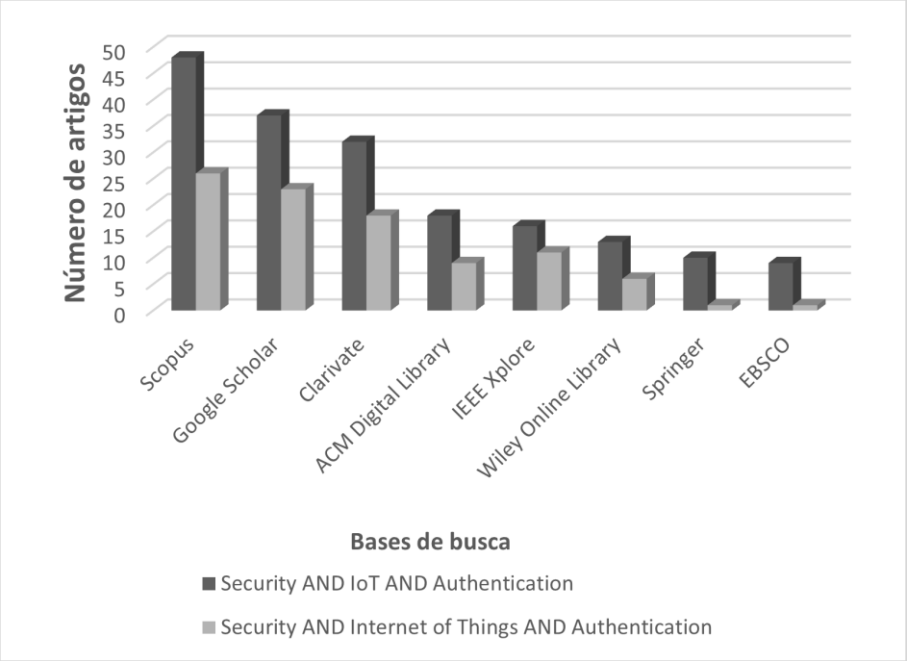
Estratégia de Busca			
Bases de Dados Científicas		**Keywords**	
IEEE Xplore Digital Library; Springer Link; ACM Digital Library; Scopus; Google Scholar; Clarivate; Wiley Online Library; EBSCO.		[*"Security AND IoT AND Authentication"*] *OR* [*"Security AND Internet of Things AND Authentication"*]	
Anos de Publicação	**Tipo de documentos**	**Idioma**	**Critério**
2016 a 2021	**Artigos**	**Inglês**	**Títulos**

Fonte: O Autor (2022).

O ponto de partida do protocolo foi a definição do objetivo da pesquisa, para logo em seguida se determinar a estratégia de busca. Os descritores foram fundamentais para se delimitar o escopo da pesquisa.

A Figura 1 demonstra a quantidade de artigos científicos encontrados nas bases de buscas: Scopus Preview [20], Google Scholar [21], Clarivate [22], ACM Digital Library [23], IEEE Xplore [24], Wiley Online Library [25], Springerlink [26] e EBSCO [27]. As bases Scopus e Google Scholar retornaram o maior quantitativo de referências observando o protocolo definido na Tabela 1.

Figura 1 – Número de artigos encontrados em bases científicas.



Fonte: O autor (2022).

A busca de artigos foi dividida em duas etapas. Na primeira consulta, foram definidas

as palavras-chaves (*Security*, IoT, *Authentication*). Esta primeira etapa retornou um total de 183 artigos. Porém, uma outra consulta foi realizada, visto que a palavra IoT tem o mesmo significado que o termo "*Internet of Things*"; logo, as palavras-chaves desta nova consulta foram: *Security, Internet of Things* e *Authentication*. Nesta nova consulta, foram identificados mais 95 documentos que totalizaram, em conjunto com os da primeira pesquisa, um total de 278 artigos. Por fim, foi identificado que diversos artigos se repetiam nas duas consultas; desta forma, foram analisados os títulos e o resumo com a finalidade de excluir os artigos repetidos. Depois deste processo, foram identificados 156 documentos duplicados, restando um total de 122 artigos para serem analisados.

Para a segunda etapa é importante considerar quais artigos apresentam o gateway IoT em sua topologia, visto que ele é considerado um componente de alto valor no processo de segurança e tem uma função vital no processo de comunicação das coisas. Diante deste contexto, a Tabela 2 apresenta 19 artigos que especificam o gateway IoT em sua topologia. Após uma análise aprofundada, foram identificados quatro objetivos relevantes, a saber: métodos de autenticação, protocolos de autenticação, ataques e vulnerabilidades e requisitos de segurança.

Tabela 2 – Comparativo dos artigos selecionados.

Nº	Artigos Selecionados	Métodos de autenticação	Protocolos de autenticação	Ataques e Vulnerabilidades	Requisitos de Segurança
1	Aski et al. [28]	Sim	-	-	-
2	Chatterjee et al. [29]	Sim	-	Sim	-
3	Ferdowsi e Saad [30]	-	Sim	Sim	-
4	Kumar et al. [31]	Sim	Sim	-	-
5	Ghosh e Ruj [32]	Sim	-	-	Sim
6	Dhillon e S. Kalra [33]	Sim	-	Sim	Sim
7	Chen et al. [34]	Sim	-	Sim	-
8	Jabbari e Mohasefi [35]	Sim	Sim	Sim	-
9	Wu et al. [36]	Sim	-	Sim	Sim
10	Moon et al. [37]	Sim	-	Sim	-
11	Chuang et al. [38]	-	Sim	Sim	-
12	Parne et al. [39]	-	Sim	Sim	-
13	Alzahrani et al. [40]	-	Sim	Sim	-
14	Nandy et al. [1]	Sim	-	Sim	-
15	Vorugunti et al. [41]	Sim	Sim	Sim	-
16	Fan e Niu et al. [42]	-	Sim	Sim	-
17	Sheron et al. [43]	Sim	-	-	Sim
18	Rattanalerdnusorn et al. [44]	Sim	-	-	-
19	Showkat et al. [45]	Sim	-	-	Sim

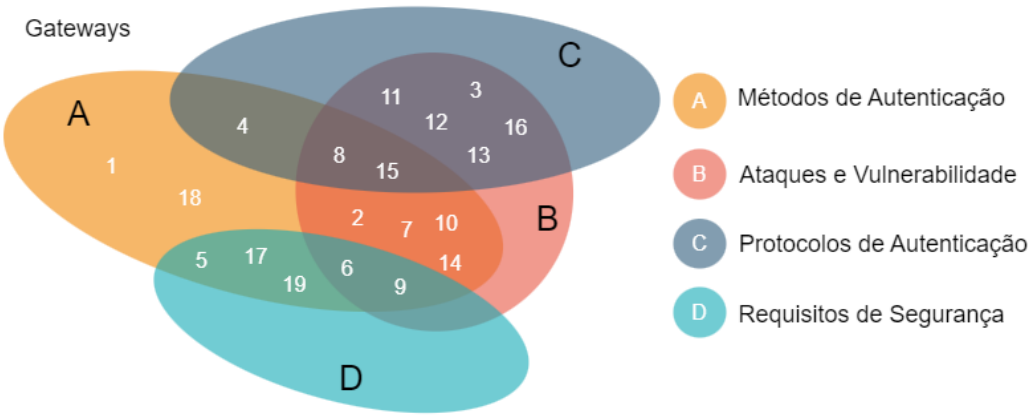
Fonte: O autor (2022).

Na Tabela 2, é possível observar que alguns artigos só apresentam um dos objetivos relevantes, entretanto a maioria apresenta mais de um. Assim sendo, todos têm sua importância

no sistema IoT, visto que os métodos não padronizados de autenticação em dispositivos de IoT proporcionam diversos riscos que comprometem a confidencialidade, integridade, disponibilidade e confiança dos dados [46]. Já no contexto de protocolos de autenticação no ambiente IoT, o usuário se autentica enviando mensagens entre os sensores e os gateways; por sua vez, os sensores se autenticam comunicando-se com os gateways [1]. No entanto, esse processo de comunicação ocorre em diversos ambientes, de modo que sejam ponto focal para diversos ataques [33]. Porém, os requisitos de segurança garantem uma maior proteção na arquitetura IoT, visto que eles possibilitam que todas as partes integrantes dos sistemas estejam mais seguros [45].

Outra forma de observar esses dados é utilizando um diagrama de Venn. Através dele, é possível evidenciar que todas as interseções possíveis entre conjuntos, mesmo que não existam na entrada [47]. Portanto, a Figura 2 apresenta os 19 artigos selecionados e os objetivos relevantes entre eles.

Figura 2 – Diagrama de Venn dos objetivos relevantes.



Fonte: O autor (2022).

O objetivo “requisitos de segurança” foi o que apresentou a menor quantidade de artigos no diagrama de Venn. Contudo, para o desenvolvimento dessa pesquisa, ele acabou sendo priorizado. Diversas organizações técnicas de segurança divulgam normas com diversos requisitos de segurança e suas recomendações, com a finalidade de propor uma maior proteção na construção do *hardware* e *software* das coisas [4]. No entanto, pouco se comenta na literatura sobre a inspeção dos requisitos de autenticação nos gateways IoT. Neste contexto, surge a questão de como avaliar o nível de segurança de gateways IoT considerando requisitos de autenticação.

Para solucionar esta questão, este trabalho busca pesquisar as organizações técnicas de segurança, analisando e selecionando os requisitos de autenticação publicados em suas normas. Além disso, será feita uma seleção, instalação e configuração dos gateways IoT em *software*, com o objetivo de inspecionar os requisitos indicados. Para isso, uma metodologia de avaliação de requisitos de autenticação foi desenvolvida com a finalidade de registrar todos os processos de inspeção.

1.2. Objetivos

A seguir são especificados os objetivos deste trabalho.

1.2.1. Objetivo geral

Avaliar o nível de segurança de gateways IoT considerando requisitos de autenticação.

1.2.2. Objetivos específicos

- Pesquisar entidades de padronização que propuseram requisitos relacionados a IoT, analisando e selecionando os requisitos de segurança em autenticação publicados pelas normas técnicas;
- Desenvolver uma metodologia para avaliação de requisitos de autenticação em gateways IoT;
- Realizar a inspeção dos requisitos de autenticação nos gateways selecionados para o estudo.

1.3. Organização

O restante desta dissertação está estruturado da forma que se segue.

O Capítulo 2 descreve os conceitos fundamentais para o entendimento desta pesquisa.

O Capítulo 3 apresenta os trabalhos relacionados ao uso de requisitos de autenticação em gateways IoT. O objetivo da avaliação dos trabalhos relacionados é destacar os artigos que abordam os requisitos de segurança, bem como evidenciar se alguma metodologia de avaliação é discutida na literatura corrente. Outro ponto que a ser observado na seleção desses artigos é se eles apresentam algum processo de inspeção de requisitos em autenticação e, por fim, se esta inspeção foi aplicada em gateway IoT.

O Capítulo 4 detalha a metodologia proposta. Essa metodologia auxilia no processo de

definir as metas de avaliação, bem como, pesquisar e priorizar referências, analisar e priorizar os requisitos, realizar a seleção de gateways, executar a inspeção de requisitos e realizar a comparação e avaliação de resultados.

No Capítulo 5 é apresentada a principal contribuição desta dissertação, que é a avaliação do nível de conformidade de gateways IoT considerando requisitos de autenticação apresentados por diversas organizações técnicas relevantes na área de Internet das Coisas e Segurança.

No Capítulo 6 são apresentadas as conclusões, as principais contribuições, limitações e os trabalhos futuros que poderão ser realizados com base nesta dissertação.

2. Fundamentação Teórica

Neste capítulo, são descritos conceitos fundamentais para o entendimento deste trabalho. Na Seção 2.1, é apresentado o conceito de Internet das Coisas e sua arquitetura. A Seção 2.2 aborda os gateways usados frequentemente em várias áreas de IoT. Na Seção 2.3, são apresentadas as diretrizes de identidade digital e os três níveis de garantia de conformidade: inscrição, autenticação e federação e asserções. A Seção 2.4 apresenta as sete organizações técnicas que propõem requisitos de segurança para IoT. Por fim, a Seção 2.5 apresenta as considerações finais deste capítulo.

2.1. Internet das Coisas

A Internet das Coisas é uma concepção tecnológica em que objetos da vida cotidiana estão conectados à uma rede de computadores ou à Internet, atuando de uma forma sensorial e inteligente [48]. A principal ideia por trás da IoT é a união do mundo real com o digital, resultando em novas experiências de comunicação e interação com outras pessoas ou objetos [48]. Diversas áreas estão trazendo várias soluções de IoT [49]:

- Na área de manufatura/indústria, existem várias maneiras de utilizar IoT, como monitoramento, realidade aumentada, automatização de controle de qualidade e outros.
- Na área de transporte/mobilidade, IoT vem sendo usada para rastreamento do veículo, monitoramento do motorista, gerenciamento de frota, monitoramento de recursos (ex.: bateria e pneus) e outros [49].
- No setor energético, as soluções IoT têm impacto direto na geração, transmissão e distribuição de energia, bem como, manutenção preventiva, monitoramento e no gerenciamento remoto de ativos [49].
- No varejo, estão adotando IoT para o monitoramento de produtos, gestão de estoque, máquinas de venda inteligentes, entre outros [49].
- Na área de cidades inteligentes (*Smart Cities*), soluções baseadas em IoT estão sendo propostas para o gerenciamento de tráfego, o descarte de resíduos, a vigilância pública e poluição do ar [49].
- Na área médica, hospitais e clínicas utilizam IoT para o monitoramento de dispositivos médicos e pacientes, coordenação de equipes, fluxo de trabalho, atendimento a idosos, gerenciamento de medicamentos, entre outros [49].

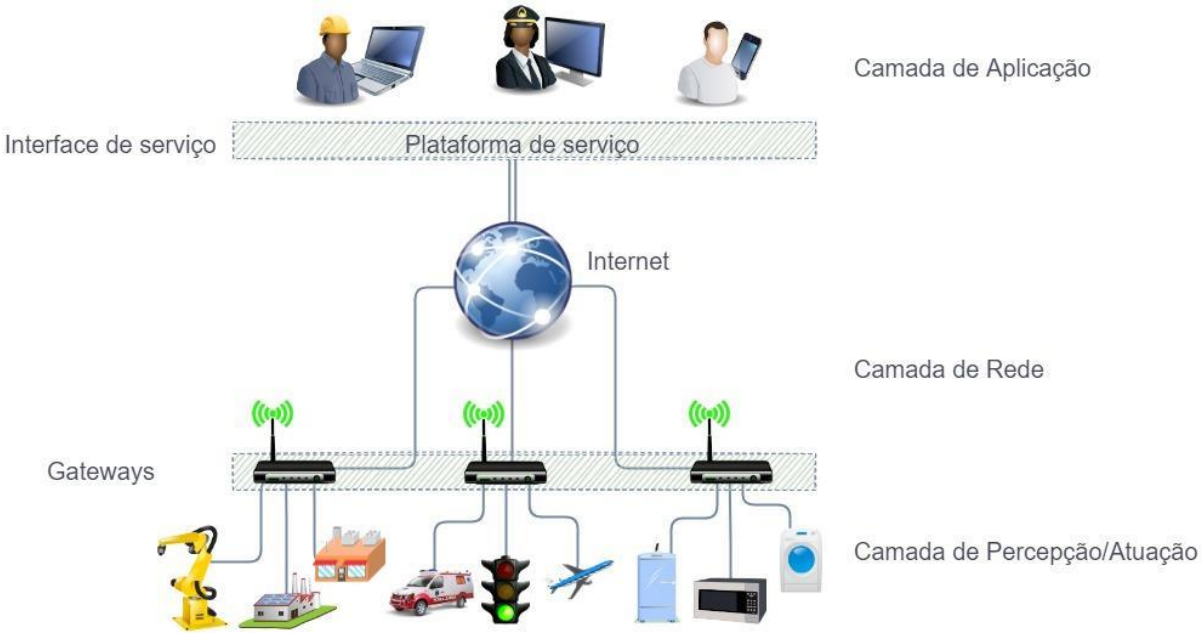
Com a expansão desses setores, o mercado global da Internet das Coisas teve um

crescimento de 8% em 2021. A expectativa para 2022 é de 18% e espera-se que, até 2025, um crescimento de aproximadamente 27 bilhões de dispositivos IoT conectados [50].

2.1.1. Arquitetura de referência para IoT

Em IoT não existe uma arquitetura padrão, visto que existem pesquisadores que propõem a utilização de uma arquitetura de três camadas (percepção/atuação, rede e aplicação), e outras que propõem cinco camadas (que incluem a camada de processamento e negócios) [51]. A Figura 3 apresenta uma visão geral da arquitetura mais básica, que é composta de três camadas.

Figura 3 – Arquitetura de referência para IoT de três camadas.



Fonte: O autor (2022).

A seguir são detalhadas destas camadas.

- **Camada de percepção/atuação.** É a parte do sistema de IoT que detecta parâmetros físicos ou identifica outros objetos inteligentes no ambiente. Geralmente, as "coisas" da IoT estão inseridas nessa camada (ex.: sensores, geladeiras, semáforos e máquinas industriais). O elemento de percepção tem a finalidade de coletar informações do ambiente, e esta coleta permite inclusive que as coisas atuem em situações reais; essa ação de mudança é conhecida como atuação, e realizada por meio de atuadores.
- **Camada de rede.** Proporciona a conexão entre as coisas, dispositivos de rede e servidores. Seus recursos são usados para transmissão e processamento de dados usando a Internet; portanto, é fundamental definir como esta conexão será realizada. Alguns dos

componentes que fazem parte desta camada são: gateways/concentradores, padrões de comunicação e equipamentos de rede como roteadores.

- **Camada de aplicação.** Responsável por entregar serviços específicos aos usuários. Para isto, utiliza as camadas de percepção/atuação e de rede para definir como os diferentes serviços ou processos vão se comunicar. Componentes de *software*/aplicativos e protocolos de comunicação do nível de aplicação fazem parte dessa camada.

2.2. Gateways IoT

No sistema IoT, os objetos podem ter alto poder de processamento, como por exemplo o dispositivo Alexa que tem a capacidade de organizar *playlist* pessoal, alertar sobre previsão do tempo, organizar agenda telefônica e realizar chamadas. No entanto, nem todos os dispositivos são assim, visto as suas limitações de *hardware* e/ou *software*, como os sensores, semáforos e outros.

Neste contexto, os gateways auxiliam estes dispositivos a se conectarem à rede de comunicação, ainda que nem todos os dispositivos necessitem de um gateway. O gateway tem o papel de estabelecer a comunicação com diversos dispositivos inteligentes ou objetos que não tenham acesso direto à Internet [48]. Os dispositivos IoT enviam os dados ao gateway, onde são pré-processados, convertidos para outro protocolo se necessário, e enviados para a Internet.

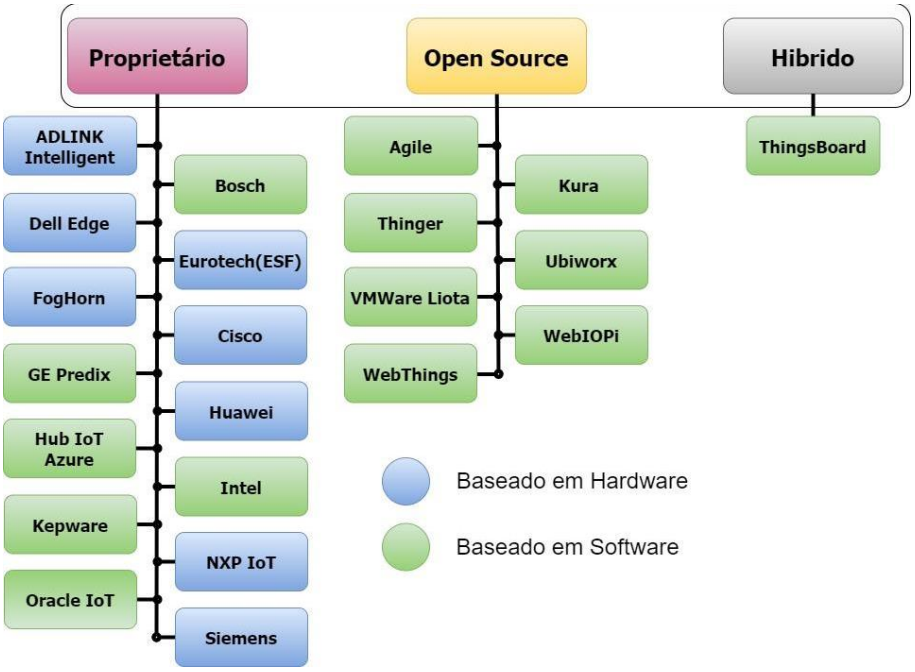
Nessa comunicação dos dispositivos IoT, em redes de curta e longa distância [52], o gateway proporciona a tradução dos protocolos de comunicação, que tem como objetivo permitir a conexão de diversas coisas, solucionando o problema da heterogeneidade [5]. No entanto, ele também fornece diversos outros recursos, como: autenticação [1], segurança no geral [33], monitoramento [32], criptografia [37] e outros. Os gateways IoT são comumente usados em várias áreas, como: *Smart home* [53]-[54], Agricultura [34], Saúde [55] e *Smart city* [56]. Os gateways podem ser classificados como:

- **Proprietário.** É qualquer gateway baseado em *software* de funcionamento exclusivo de quem produziu, sendo pessoa ou empresa. Para o uso de terceiros, é necessária uma solicitação ou mesmo a compra de uma licença.
- ***Open Source*.** Refere-se a distribuição de forma gratuita. De forma geral, existe uma comunidade, sem fins lucrativos, que disponibiliza o código-fonte do *software*. Sendo assim, o usuário pode utilizar, alterar, adaptar à sua necessidade ou até mesmo ajudar a comunidade na melhoria das funcionalidades desse *software*.
- **Híbrido.** No contexto de híbrido, se cria um modelo único de *software* proprietário e

Open Source. No entanto, em sua versão proprietária, há uma equipe de suporte ao usuário.

Em termos de implementação, os gateways podem ser de dois tipos: *hardware*, quando o gateway já vem instalado em um equipamento proprietário, e *software*, quando é disponibilizado o código-fonte ou executável do gateway para ser instalado em um *hardware* de propósito geral, como *Arduino* ou *Raspberry*. A Figura 4 apresenta um total de 22 gateways IoT ordenados de acordo com a sua classificação.

Figura 4 – Gateways IoT mais importantes e sua classificação.



Fonte: O autor (2022).

Na Figura 4, oito gateways são baseados em *hardware*, ou seja, o usuário tem que comprar o hardware físico para ter acesso ao produto. No entanto, 14 gateways são baseados em *software*, e seis deles necessitam de licença de uso para que o usuário utilize todas as funcionalidades. Finalmente, a Internet disponibiliza 8 gateways baseado em *software* com todos os recursos disponíveis de forma gratuita.

2.3. Autenticação

A autenticação é um dos recursos fornecidos pelos gateways IoT, visto que o processo de confirmação da identidade de uma pessoa ou dispositivo é fundamental na segurança das redes IoT. Neste contexto, pode-se afirmar que diversos ataques têm objetivo de roubar credenciais de dispositivos IoT. O Laboratório de Tecnologia da Informação (ITL) do NIST

publica três séries SP 800-63-3[1] de diretrizes de Identidade Digital relacionadas a autenticação em sistemas para organizações setoriais, governamentais e acadêmicas. Essas diretrizes definem requisitos técnicos em prova de identidade, registro, autenticadores, processos de gerenciamento, protocolos de autenticação, federação e assuntos relacionados [57].

- **Nível de garantia de identidade (IAL ou SP 800-63A[2]).** Apresenta os requisitos necessários pelos quais os usuários podem comprovar sua identidade e se registrarem em um dos três níveis distintos de conformidade. Estes três níveis são: I) Não há a exigência de associar o solicitante a uma identidade particular da vida real. Portanto, um e-mail é um atributo válido. II) Exigem atributos que comprovem a identidade do solicitante no mundo real, como por exemplo a verificação baseada no conhecimento (KBV), e, por fim, III) A presença física do solicitante é necessária na confirmação de sua identidade, e atributo como biometria é requerido. Esses três níveis visam garantir a prova de identidade [58].
- **Nível de garantia de autenticador (AAL ou SP 800-63B[3]).** Aborda como um indivíduo pode se autenticar de forma segura em um serviço ou um conjunto de serviços digitais. Para isto, três níveis são apresentados baseado no risco e o impacto causado por um invasor. I) Proporcionar ao usuário uma autenticação de fator único (SFA), senha de uso único (OTP) ou autenticação multifator (MFA) em sua conta digital. II) Promover uma maior confiança do usuário ao sistema, solicitando a posse de uma autenticação de dois fatores distintos. III) Fornecer ao usuário a posse e o controle de uma autenticação de dois fatores distinta através de um protocolo criptográfico.

- **Nível de garantia da federação (FAL ou SP 800-63C[4]).** A federação é um processo que autoriza o transporte de atributos dos usuários e de autenticação através de sistemas em rede. Esse documento fornece diretrizes de requisitos técnicos para agências federais que implementam serviços de identidade digital. No entanto, o FAL é opcional, em virtude que nem todos os sistemas digitais incentivam a arquitetura de identidade

[1] SP 800-63-3 - Diretrizes de Identidade Digital. Disponível em:<https://doi.org/10.6028/NIST.SP.800-63-3>. Último acesso em 06 de junho de 2022.
[2] SP 800-63A - Inscrição e Prova de Identidade. Disponível em:<https://doi.org/10.6028/NIST.SP.800-63a>. Último acesso em 06 de junho de 2022.
[3] SP 800-63B - Autenticação e gerenciamento do ciclo de vida. Disponível em:<https://doi.org/10.6028/NIST.SP.800-63b>. Último acesso em 06 de junho de 2022.
[4] SP 800-63C - Federação e afirmações. Disponível em:<https://doi.org/10.6028/NIST.SP.800-63b>. Último acesso em 06 de junho de 2022.

federada [59].

2.3.1. Níveis de Garantia do Autenticador

A identidade digital é um meio de identificar um usuário envolvido em uma transação online. A prova de identidade comprova que este usuário é de fato quem afirma ser. O documento NIST SP 800-63B [60] requer que os indivíduos tenham que ser autenticados com pelo menos um dos três níveis de garantia [60]. O nível ALL1 apresenta diversos autenticadores, como por exemplo segredos memorizados, que são geralmente chamados de senha ou, se for número, de PIN. Esse nível informa que as senhas devem conter no mínimo 8 caracteres, maiúsculos, minúsculo, número e caracteres especiais. Classificados como *algo que você sabe*, a composição desses 8 caracteres não deve aceitar senha digitadas anteriormente, palavras compostas do dicionário, caracteres repetidos ou sequenciais e palavras específicas. Para os autenticadores no nível ALL2, o nível de complexidade aumenta. Um exemplo é um dispositivo de senha descartável (OTP) de fator único, que são senhas de 6 caracteres de uso único, baseado em um relógio em tempo real, produzidas por *software*, que é instalada em um *hardware*. Classificados como *algo que você tem*, essas senhas de uso único devem ser trocadas pelo menos uma vez a cada 2 minutos.

Por fim, o ALL3 é o maior nível de autenticação. Nesse nível são utilizados dispositivos criptográficos multifatoriais que solicitam a posse do dispositivo de *hardware* e o controle de duas autenticações distintas. Este nível é caracterizado como *algo que você tem*, e será ativado por *algo que você sabe* ou *algo que você é*. Os provedores de serviços credenciais (CSPs) utilizam dispositivos como *pendrive* ou cartão inteligente para encapsular uma ou mais chaves privadas do autenticador e somente acessíveis, por um fator adicional que seja um segredo memorizado ou a biometria (impressão digital, reconhecimento de retina, facial, íris ou voz). A Tabela 3 apresenta os tipos de processos de autenticação, os autenticadores usados em cada nível e o ciclo de vida dos autenticadores.

Tabela 3 – Resumo dos três níveis de garantia do autenticador.

Requisito	AAL1	AAL2	AAL3
Autenticadores	**Memorized Secret;** Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	**MF OTP Device;** MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	**MF Crypto Device;** SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
Reautenticação	30 dias	12 horas ou 30 minutos de inatividade; PODE exigir apenas um fator de autenticação.	12 horas ou 15 minutos inatividade; DEVE usar ambos os fatores autenticação.

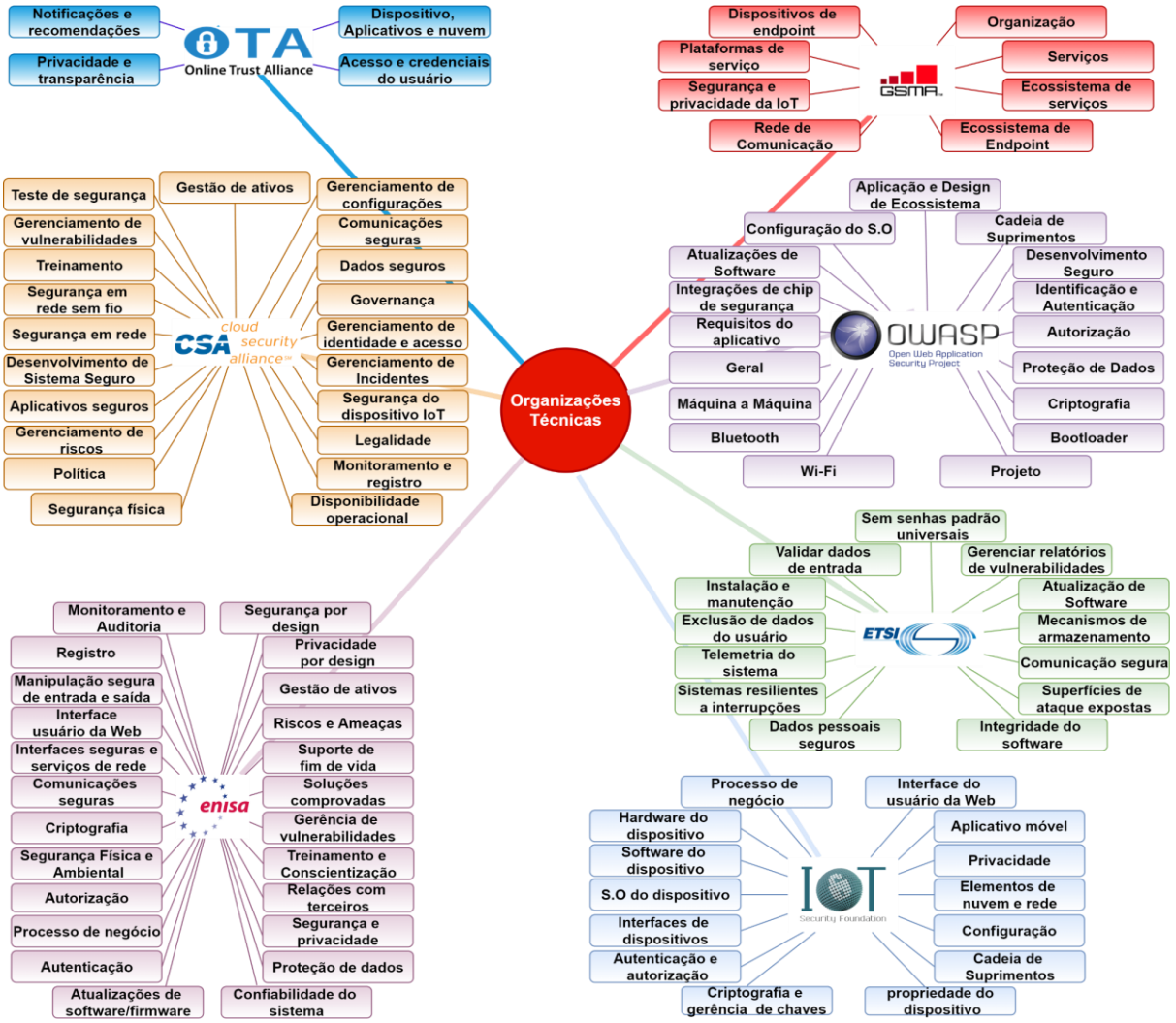
Fonte: O autor (2022).

Cada autenticador tem características e complexidade distintas, e os níveis apresentados pelos autenticadores garantem uma maior segurança no processo de autenticação. Portanto, quanto mais alto for o nível de autenticação menor será o risco de ataques.

2.4. Organizações Técnicas em IoT

As organizações técnicas relacionadas à segurança em IoT fornecem documentos fundamentais que possibilitam a verificação das melhores práticas de segurança em IoT para a comunidade [4]. Neste contexto, a *Open Web Application Security Project* (OWASP) [10], a *IoT Security Foundation* (IoTSF) [12], a *European Union Agency for Network and Information Security* (ENISA) [6], a *European Telecommunications Standards Institute* (ETSI) [13], a *Online Trust Alliance* (OTA) [14], a *GSM Association* (GSMA) [15] e a *Cloud Security Alliance* (CSA) [16] apresentam, em suas documentações, recomendações relevantes acerca da segurança em IoT. Essas boas práticas são discutidas e propostas pela literatura como requisitos ou recomendações de segurança. A Figura 5 apresenta as organizações técnicas mencionadas e suas seções de requisitos de segurança.

Figura 5 – Organizações Técnicas e suas seções de requisitos de segurança.



Fonte: O autor (2022).

As Seções 2.4.1 até 2.4.7 contextualizam as organizações, explicando requisitos e técnicas.

2.4.1. Open Web Application Security Project (OWASP)

A OWASP (*Open Web Application Security Project*) é uma fundação que colabora para o desenvolvimento de *software* seguro. A OWASP Foundation oferece, em seus capítulos, diversas ferramentas e projetos de *software* de código aberto liderados pela comunidade IoT [61]. Um dos seus capítulos é *OWASP Internet of Things* [7], que auxilia os fabricantes, desenvolvedores e consumidores a identificarem os problemas e soluções de segurança em IoT. A norma *IoT Security Verification Standard* (versão 1.0) [10] apresenta 17 seções com diversos requisitos de segurança. Por exemplo, na seção de Identificação e Autenticação, o requisito 2.1.1 recomenda que “todas as formas de usuários e contas no ecossistema IoT devem ser

identificadas exclusivamente" [10].

2.4.2. Internet of Things Security Foundation (IoTSF)

A IoTSF (*Internet of Things Security Foundation*) tem como finalidade elevar o nível da segurança cibernética em sistemas IoT. A IoTSF é destinada tanto aos usuários iniciantes de IoT quanto a profissionais experientes [62], devido a diversidade de conteúdos publicados, como normas, vídeos, entrevistas, notícias, conferências e eventos. A norma *IoT Security Compliance Framework* (versão 2.1) [12] descreve boas práticas de segurança em IoT, e é composto por 14 seções. Um exemplo é o requisito 2.4.8.6:

> "A entrada de senha segue a prática padrão da indústria, como recomendações da política de senha 3GPP TS 33.117. [ref. 17] ou NIST SP800-63b Digital Identity Guidelines - Authentication and Lifecycle Management "[ref 26] ou NCSC [Ref 48] no comprimento da senha, caracteres dos agrupamentos e caracteres especiais." [12].

O propósito desse requisito é lembrar a importância de implementar uma política de senha forte. Várias organizações recomendam o comprimento mínimo de 8 caracteres na criação da senha, e que também se inclua caracteres especiais, letras maiúsculas, letras minúsculas e números.

2.4.3. European Union Agency for Cybersecurity (ENISA)

A ENISA (*European Union Agency for Cybersecurity*) é outra organização que visa elevar o nível de cibersegurança da sociedade. Para isso, contribui com políticas cibernéticas e análise de confiabilidade dos produtos, serviços e processos de tecnologia da informação e comunicação [63]. A ENISA disponibiliza para a comunidade IoT a norma *Baseline Security Recommendations for IoT* (versão nov. 2017) [6] e este documento apresenta 24 seções com diversos requisitos técnicos. A seção de autenticação, por exemplo, apresenta o seguinte requisito:

> "Proteger contra *ataque de força bruta*[5] e / ou outras tentativas de login abusivas (como bots de login automatizado, etc.) bloqueando ou desabilitando contas de suporte de usuário e dispositivo após um número razoável de tentativas de login inválidas, ou fazendo o usuário esperar um certo tempo para fazer o login novamente após uma tentativa malsucedida. Essa proteção também deve considerar as chaves armazenadas nos dispositivos." [6].

A finalidade desse requisito é a recomendação de uma política de proteção contra

[5] O *Ataque de força bruta* visa testar todas as possibilidades de senha, uma a uma, até que se descubra a senha desejada [64].

inúmeras tentativas seguidas de acesso inválido. Por exemplo, uma ação sugerida é o bloqueio temporário ou permanente do usuário.

2.4.4. European Telecommunications Standards Institute (ETSI)

O ETSI (*European Telecommunications Standards Institute*) é um instituto sem fins lucrativos composto por empresas privadas, entidades de pesquisa, academia, governo e organizações públicas com a finalidade de fornecer oportunidades, recursos, plataformas e padrões globalmente aplicáveis à interoperabilidade e a segurança em ambientes de Tecnologia da Informação e Comunicação (TIC) [65]. Um dos padrões disponibilizado pela ETSI é o documento *Cyber Security for Consumer Internet of Things: Baseline Requirements* (versão 2.1.0) [13], que descreve requisitos (boas práticas) para o desenvolvimento e fabricação de dispositivos IoT. Uma das recomendações presentes neste documento é a 5.1-1:

> "Quando as senhas são usadas em qualquer estado diferente do padrão de fábrica, todas as senhas de dispositivos IoT do consumidor devem ser exclusivas por dispositivo ou definidas pelo usuário. Ex. não a admin/admin. Para maior segurança a implementação do *MFA*[6]." [13].

Esse requisito recomenda senhas exclusivas para qualquer dispositivo IoT ou proporciona ao usuário a mudança da senha padrão, não admitindo o uso de senhas padrões e relativamente simples como usuário e senha "admin/admin".

2.4.5. Online Trust Alliance (OTA)

A OTA (*Online Trust Alliance*) publicou relatórios sobre as melhores práticas de segurança, privacidade e identidade dos usuários [67]. No entanto, em 2019 esse projeto parou de publicar estes relatórios. Contudo, diversas organizações, fornecedores e pesquisadores ainda seguem as orientações e relatórios da OTA na proteção das transações online dos usuários. Um desses relatórios é o *IoT Security & Privacy Trust Framework* (versão 2.5) [14], que contém 4 seções de requisitos necessários na proteção dos dispositivos IoT em todo o seu ciclo de vida. Na seção de Acesso e Credenciais do usuário, o requisito de número 17 descreve a seguinte recomendação:

> "As credenciais de autenticação, incluindo, mas não se limitando a senhas de usuário,

[6] A autenticação multifator(MFA) é um recurso de segurança opcional oferecido por diversos serviços na Internet, como redes sociais e *Internet Banking*, com a finalidade de aumentar a proteção da conta do usuário [66].

> devem conter o *salt*[7], *hash*[8] e/ou criptografadas. Aplica-se a todas as credenciais armazenadas para ajudar a evitar acesso não autorizado e ataques de força bruta.” [14].

O objetivo desse requisito específico é a proteção das credenciais de autenticação dos usuários ou das coisas no ambiente IoT, e indica formas de melhorar o nível de segurança associado a estas credenciais.

2.4.6. GSM Association (GSMA)

A GSMA (GSM Association) é uma organização global que propõe boas práticas para o ecossistema móvel, proporcionando uma maior segurança aos seus membros. Para tal finalidade, a GSMA disponibiliza diretrizes de segurança em IoT com recomendações práticas na construção de dispositivos e soluções de IoT, permitindo que as empresas detectem e minimizem as prováveis falhas de segurança em seus serviços [69]. Dessa forma, a *GSMA IoT Security Assessment Process* (versão 2.0) [15] apresenta 8 seções com diversos requisitos de segurança. Para exemplificar uma das recomendações feitas, o requisito CLP13_6.12.1.14 faz a seguinte pergunta: "Seus *endpoints* que exigem administração remota são arquitetados de forma a garantir que as credenciais administrativas não sejam roubadas por um invasor?” [15]. Para mitigar um possível acesso indevido, é recomendado que se utilize a política de complexidade de senha, a utilização de autenticação multifator e a restrição de acesso administrativo por um canal seguro.

2.4.7. Connectivity Standards Alliance (CSA)

A CSA (*Connectivity Standards Alliance*) desenvolve, promove e certifica padrões abertos que permite os objetos IoT se conectarem e interagirem com segurança. Acerca disso, são divulgados documentos de segurança em IoT que possibilitam ao usuário identificar os controles de segurança adequados aos dispositivos, nuvem e tecnologias de rede [70]. Neste contexto, o documento *IoT Security Controls Framework* (versão 2.0) [16] apresenta 82 controles e diversos requisitos de segurança. No controle de comunicações seguras e confiáveis, o requisito COM-11 sugere que “Configure dispositivos, gateways, serviços e aplicativos de IoT para se comunicarem apenas com *peers* e *endpoints* de serviço autorizados.” [16]. Logo, a recomendação proposta é a implementação do gerenciamento de acesso com objetivo de mitigar

[7] O *salt* é uma técnica usada para adicionar uma proteção a função *hash*, o objetivo dessa técnica é mitigar os ataques de senha, como tabelas de *hash* [17].
[8] O *hash* é a transformação de uma sequência de caracteres em uma sequência de tamanho fixo que representa a sequência original [68].

as possíveis ameaças à segurança em um ecossistema de IoT.

2.5. Considerações Finais

Neste capítulo foram descritos os principais conceitos teóricos que serão importantes para o entendimento deste trabalho e de suas contribuições. No próximo capítulo, serão apontados e detalhados trabalhos que estão relacionados à temática abordada nesta dissertação.

3. Trabalhos Relacionados

A bibliografia atual sobre gateways IoT aborda diferentes perspectivas, como integração [71], protocolos [72]–[71], desempenho [73], latência [74] e consumo de dados móveis [75]. No entanto, a literatura não apresenta, com a merecida profundidade, a avaliação de conformidade de requisitos de autenticação em gateways IoT. Este capítulo objetiva apresentar e discutir artigos relacionados à esta temática.

3.1. Mapeamento sistemático de literatura

Para a busca de trabalhos relacionados relevantes, foi realizado um mapeamento sistemático, através do protocolo apresentado na Tabela 4. Este protocolo detalha o objeto de pesquisa, as estratégias de busca, descritores e os métodos de execução.

Tabela 4 – Protocolo do mapeamento sistemático.

Objeto de Pesquisa: Quais trabalhos apresentam avaliação de segurança em IoT?			
Estratégia de Busca			
Bases de Dados Científicas		**Keywords**	
IEEE Xplore Digital Library; Springer Link; ACM Digital Library; Scopus; Google Scholar; Clarivate; Wiley Online Library; EBSCO.		[*"Gateway AND Evaluation NOT Performance"*] *OR* [*"Gateway AND Analysis NOT Performance"*] *OR* [*"IoT AND "Security requirements" NOT Performance"*]	
Anos de Publicação	**Tipos de documentos**	**Idioma**	**Critério**
2016 a 2021	**Artigos**	**Inglês**	**Títulos**

Fonte: O autor (2022).

Após a execução do protocolo descrito na tabela anterior, foram encontrados um total de 63 trabalhos científicos (artigos) nos últimos 5 anos. No entanto, antes de realizar a leitura completa dos artigos, alguns elementos foram observados, como: resumo, introdução e os resultados apresentados, com a finalidade de identificar os artigos que melhor se adequaram ao contexto desta pesquisa. Após esta análise detalhada, finalmente foram selecionados onze artigos mais relevantes e os mesmos foram avaliados considerando os objetivos desta dissertação.

3.2. Discussão

Imdad *et al.* [76] apresentam uma lista de ameaças às redes IoT por camadas, juntamente com os ataques, a camada comprometida, o impacto na segurança e os componentes afetados. São indicados sete requisitos de segurança, e a solução para cada ameaça se constitui no

atendimento destes requisitos. No entanto, nenhuma metodologia de avaliação de segurança é introduzida e os dispositivos IoT, inclusive o gateway, não são inspecionados.

Hansch *et al.* [77] introduzem uma arquitetura de comunicação unificada para requisitos de segurança em IIoT (OPC UA[9]). O objetivo desta arquitetura é realizar a automatização do processo de verificação dos setes requisitos de segurança, escolhidos pelos autores, em um modelo de dados. Os requisitos (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) são apresentados pela norma técnica IEC 62443 e a inspeção é realizada através de três cenários: I) Transmissão Máquina a Máquina de Requisitos de Segurança em Cadeias de Fornecimento Distribuídas, II) Conformidade da produção com determinados conjuntos de requisitos de processo e III) Verificação automatizada da qualidade do produto por máquinas. Todos eles possuem uma característica em comum: a substituição dos processos manuais por uma abordagem totalmente automatizada. Os requisitos são aplicados em um sistema de segurança para automação industrial e não existe um foco específico para dispositivos IoT, especialmente gateways IoT. Ou seja, este trabalho relacionado contempla requisitos de autenticação, no entanto eles não são aplicados especificamente em gateways IoT.

Ankele *et al.* [78] definem requisitos e recomendações de modelos de sistemas IoT/IIoT para automatizar o processo de modelagem de ameaças, análise de segurança e teste de penetração, visando garantir uma maior segurança ao longo do processo de desenvolvimento de *software*. Os requisitos são classificados em cinco propriedades: rede, *hardware*, *software* e operação, segurança e desempenho. Assim sendo, os autores apresentam seis componentes IoT/IIoT e os relacionam com os requisitos. O objetivo é apresentar a priorização desses requisitos por cores (vermelho = alto, amarelo = médio, verde = baixo). O gateway IoT é um dos componentes selecionados e a aplicabilidade dos requisitos são analisadas. Contudo, não se realiza inspeção de segurança. Além disso, as recomendações técnicas dos requisitos de segurança não são especificadas.

Papcun *et al.* [79] propõem uma metodologia para avaliação de gateway IoT com base em funcionalidade. A seleção de 14 critérios (requisitos) dos gateways foram distribuídos em quatro categorias: I) Conectividade do dispositivo: serviços que oferecem ferramentas para padronização e protocolos de rede e a organização dos dispositivos conectados, II) pré-processamento de dados: ferramentas que fornecem filtragem e integração de dados, III)

[9] OPC UA é um protocolo projetado especificamente para a automação industrial.

Análise de dados: ferramentas para pré-analítica de dados, armazenamento local, notificações, compactação de dados, criptografia e a identificação dos dados e IV) Requisitos especiais de *hardware*: Alto poder computacional, fonte de alimentação de longa duração e mais de uma conexão de Internet. Cada critério foi avaliado individualmente em uma escala de 1 a 5, levando em consideração a dificuldade e o número estimado de horas de implementação, necessidade financeira de execução e o impacto no custo final do gateway IoT. O resultado desta avaliação serviu de insumo para determinar os pesos de cada fase durante o processamento de dados e com isso classificar os gateways IoT como normal, inteligente e de borda. A inspeção foi realizada, no entanto poucos requisitos de segurança, como criptografia de dados, são efetivamente descritos e analisados.

Kamalrudin *et al.* [80] apresentam uma biblioteca de requisitos de segurança para aplicações IoT, com o intuito de auxiliar os engenheiros de *softwares*. A biblioteca indica qual requisito deve ser atribuído ao dispositivo específico, mas não oferece recursos ou realiza nenhum processo de inspeção deste requisito. Além disso, gateways IoT não são diretamente abordados, mas apresenta os requisitos de autenticação.

Kebande *et al.* [81] destacam a importância de existir uma abordagem digital forense para a identificação de incidentes de segurança em dispositivos IoT. Uma metodologia de Prontidão Forense Digital (DFR-IoT) é descrita e os requisitos de IoT, requisitos proativos e a extração de evidência Digital (Logs) fazem parte do fluxo dos processos. Esses processos apresentados estão em consonância com a norma técnica ISO/IEC 27043:2015, com diversos requisitos funcionais (FRs) na investigação de incidentes. Mesmo assim, só os requisitos sobre *hash* e seus algoritmos têm relação direta com segurança. Além disso, nenhum dispositivo IoT foi considerado no processo de inspeção.

Lins *et al*. [2], ao considerarem que a literatura relacionada à melhoria de segurança de gateways IoT ainda é limitada, propõem uma metodologia para avaliar e priorizar requisitos de segurança para gateways IoT. Uma metodologia de engenharia de requisitos de segurança é proposta e diferentes entidades técnicas e normas de segurança são apresentadas como referências básicas para estes requisitos. No entanto, a metodologia não é direcionada ao processo de inspeção dos requisitos de autenticação e poucos requisitos de autenticação são elencados. Por fim, a inspeção dos requisitos de autenticação nos gateways em si não foi priorizada no artigo.

Ali *et al.* [82] verificam requisitos de segurança e propõem soluções para diversos tipos de ataques em ambientes *Smart Home*. Alguns cenários, ameaças e impactos causados pelos ataques são evidenciados e analisados. Um medidor inteligente de rede elétrica é usado em

todos os cenários para ilustrar as questões de segurança e a seleção dos requisitos. No entanto, somente os requisitos de autenticação, autorização, confidencialidade, integração e disponibilidade são apresentados. Além disto, a importância do gateway IoT é mencionado no documento, mas nenhuma inspeção de segurança é realizada neste dispositivo especificamente.

Oh e Kim [83] propõem a análise de três características principais do ecossistema IoT, I) heterogeneidade, II) restrição de recursos e III) ambiente dinâmico, e apresentam seis elementos chaves em IoT (rede IoT, nuvem, usuário, atacante, serviço e plataforma). Para cada elemento, uma descrição dos requisitos de segurança é realizada. Os autores também apresentam os resultados da comparação entre os artigos existentes na literatura e o proposto por eles. No entanto, os requisitos apresentados não são relacionados a nenhuma norma técnica reconhecida na área de segurança ou IoT e o processo de inspeção destes requisitos não foi efetivamente aplicado em dispositivos IoT.

Jaiswal e Gupta [84] sugerem diversos requisitos de segurança que se aplicam ao sistema de monitoramento remoto de pacientes. Os componentes do sistema e as recomendações técnicas dos requisitos são listadas e detalhadas. Alguns algoritmos criptográficos também são propostos na implementação dos requisitos de segurança. Os requisitos identificados são aplicados a cada componente do sistema de monitoramento. Contudo, o critério de seleção dos requisitos não é descrito. É válido destacar também que o gateway IoT é inspecionado, mas o processo de inspeção não é detalhado.

Parra Rodriguez *et al.* [85] desenvolveram uma arquitetura de segurança centrada em privacidade dos dados para sistemas que usam gateways IoT, possibilitando que os usuários controlem quem tem acesso aos seus dados. Os requisitos de privacidade e controle de acesso foram selecionados; no entanto, diversos outros requisitos não são considerados. Os autores também expõem possíveis soluções para os requisitos, porém o processo de inspeção não é documentado.

3.3. Visão Comparativa

A Tabela 5 apresenta os trabalhos citados nesta seção, observando os seguintes critérios de comparação: I) se os artigos buscam por requisitos de segurança em organizações técnicas reconhecidas nas áreas de segurança, como IoTSF e OWASP; II) se alguma metodologia de avaliação e seu processo são detalhados; III) se houve uma inspeção nos requisitos de segurança em autenticação; e IV) se as inspeções dos requisitos foram aplicadas em gateways IoT.

O primeiro critério busca avaliar se os requisitos de segurança são divulgados por organizações e normas técnicas conhecidas na área, com o intuito de buscar as melhores práticas em segurança em IoT. Demonstrar uma metodologia detalhada também se mostra importante, pois permite que a comunidade possa compreender e reproduzir as etapas de avaliação. O penúltimo critério de comparação busca avaliar se os trabalhos têm um foco específico na inspeção dos requisitos de autenticação em dispositivos IoT. Por fim, o último critério avalia se os requisitos de segurança apresentados nas normas técnicas são efetivamente inspecionados em gateways IoT.

Tabela 5 – Comparativo dos trabalhos relacionados.

Trabalhos Relacionados	Se baseia em organizações técnicas reconhecidas	Apresenta metodologia de avaliação detalhada	Propõe avaliação de requisitos de autenticação	Realiza a inspeção de requisitos em gateways IoT
Imdad et al. [76]	Não	Não	Parcialmente	Não
Hansch et al. [77]	Sim	Não	Parcialmente	Não
Ankele et al. [78]	Sim	Não	Não	Não
Papcun et al. [79]	Não	Sim	Não	Não
Kamalrudin et al. [80]	Não	Não	Não	Não
Kebande et al. [81]	Sim	Sim	Não	Não
Lins et al. [2]	Sim	Sim	Parcialmente	Parcialmente
Ali et al. [82]	Não	Não	Não	Não
Oh e Kim [83]	Sim	Não	Não	Não
Jaiswal e Gupta [84]	Não	Não	Não	Não
Parra Rodriguez et al. [85]	Sim	Não	Não	Não

Fonte: O autor (2022).

Inicialmente, dois trabalhos propuseram os seus requisitos de segurança baseados em normas técnicas; porém, somente um analisou mais de uma organização técnica. Alguns artigos apresentaram e detalharam metodologias, contudo, apenas um artigo utilizou um processo de engenharia de requisitos de segurança (SRE) para dar suporte a seleção e priorização de requisitos de segurança em IoT [2]. Apesar disto, nenhum trabalho desenvolveu uma metodologia de avaliação de requisitos específica para gateways IoT. Já no processo de inspeção, apenas três artigos realizaram parcialmente uma avaliação prática dos requisitos de autenticação; no entanto, apenas um tem o foco específico em gateways IoT. Deste modo, é possível observar a lacuna existente na atual literatura relativa a uma metodologia ou abordagem, suficientemente detalhada e completa, para avaliação de requisitos de autenticação em gateways IoT que observe os pontos discutidos nesta seção. Além disto, uma avaliação mais aprofundada sobre conformidade de requisitos de autenticação em gateways IoT também se mostra ausente.

3.4. Considerações Finais

Este capítulo apresentou uma visão geral do estado da arte sobre a avaliação de conformidade de requisitos de autenticação em gateways IoT. Algumas propostas até apresentam requisitos de autenticação em IoT; no entanto, poucos trabalhos se baseiam em normas técnicas conhecidos para a escolha dos requisitos a serem considerados. Outro ponto a ser observado é que as metodologias desenvolvidas não descrevem com a devida profundidade o processo de inspeção de requisitos. Por fim, é visível o número reduzido de trabalhos que apresentam foco específico em gateways IoT. Toda está problemática serve de motivação para a contribuição principal desta dissertação, que será apresentada no próximo capítulo.

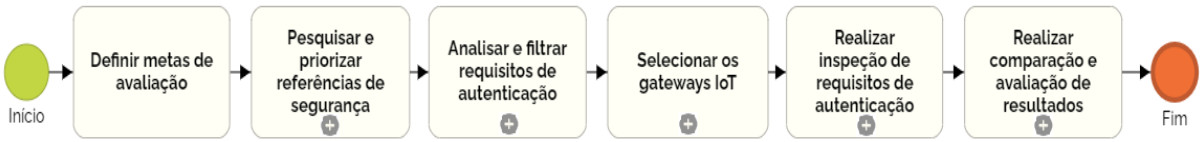
4. Metodologia para Avaliação de Conformidade de Requisitos de Autenticação em Gateways IoT

O objetivo principal desta dissertação é à avaliação de conformidade de requisitos de autenticação em gateways IoT. Para atingir este objetivo, e para melhor estruturar a avaliação, uma metodologia é proposta. Além disso, a metodologia possibilitar que a avaliação seja replicável.

Neste capítulo, a metodologia proposta para avaliação de requisitos de autenticação em gateways IoT é detalhada. As Seções 4.1 até 4.6 detalham a metodologia e a Seção 4.7 apresenta as considerações finais deste capítulo.

A tarefa de avaliação de conformidade de requisitos de autenticação em gateways IoT não é trivial, pois atividades como seleção de conjunto de requisitos, priorização de requisitos e inspeção apresentam graus variáveis e consideráveis de complexidade. Neste contexto, a metodologia proposta visa especificar as etapas necessárias para esta avaliação. Para a especificação desta metodologia, foi usado um padrão amplamente adotado – *Business Process Model and Notation* (BPMN), que possui uma notação semelhante a um fluxograma. BPMN vêm sendo amplamente adotado para modelagem de processos de negócios [86]. Além disso, a metodologia também contribui para a pesquisa ser reproduzível (compatível com o conceito de *reproducible research*), permitindo que outros pesquisadores interessados possam reproduzir a avaliação em outros cenários. A Figura 6 apresenta as atividades da metodologia proposta.

Figura 6 – Metodologia proposta.



Fonte: O autor (2022).

A primeira atividade foca em definir quais metas deverão nortear o estudo a ser realizado. Vale ressaltar que essa atividade é a única que não tem subprocesso de avaliação, por ser uma atividade basilar. A segunda atividade define as referências de segurança para a avaliação. A terceira atividade, que também é um subprocesso, define quais requisitos de autenticação devem ser analisados e priorizados, considerando as referências selecionadas anteriormente. Por sua vez, a seleção dos gateways a serem considerados na avaliação é realizada na próxima atividade. Na quinta atividade, os requisitos são efetivamente

inspecionados nos gateways escolhidos. Neste momento, é avaliado se os gateways estão "conforme", "parcialmente conforme" e "não conforme" em relação aos requisitos de autenticação selecionados e priorizados. Por fim, na última atividade, os resultados obtidos através do processo de inspeção são evidenciados e analisados.

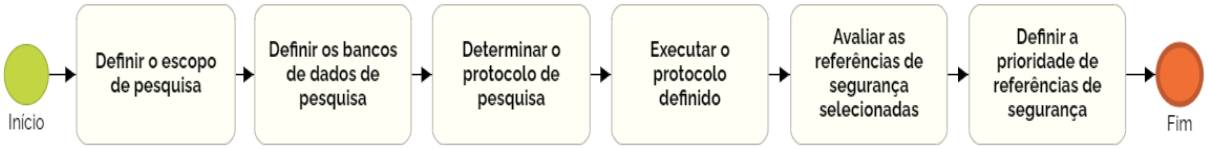
4.1. Definir metas de avaliação

Determinar as metas da avaliação de segurança é o ponto de partida para alcançar o(s) objetivo(s) do estudo. As metas definidas nesta atividade guiarão a execução das demais atividades da metodologia. Por exemplo, uma meta pode ser avaliar o nível de conformidade de um determinado gateway IoT em relação a requisitos de autenticação retirados de uma referência específica. Outra poderia ser envolver uma avaliação mais abrangente, visando saber o nível de maturidade de autenticação em gateways IoT. As metas ajudarão a definir mais claramente o escopo da avaliação.

4.2. Pesquisar e priorizar referências de segurança

A pesquisa de referenciais de segurança determina os tipos de documentos e referências que serão utilizados como base para o levantamento de requisitos de autenticação. A Figura 7 apresenta as seis atividades que dão suporte à busca e priorização de referenciais teóricos.

Figura 7 – Pesquisar e priorizar referências de segurança.



Fonte: O autor (2022).

Definir o escopo da pesquisa é uma forma de restringir o campo de pesquisa. Outro ponto importante é definir as bases de busca que serão consideradas. Estas bases, em geral, têm diversos filtros que auxiliam na busca, como filtro de tempo (ano) e filtro de idioma. Estes campos são importantes para a proposição dos protocolos de busca a serem executados nas bases. O protocolo de busca visa especificar quais os critérios de busca e de inclusão/exclusão das referências encontradas. Após a execução deste protocolo, é realizada uma avaliação técnica dos referenciais de segurança em IoT encontrados para verificar se eles estão de acordo com as metas da pesquisa. Por fim, possivelmente surjam várias referências interessantes, mas apenas um subconjunto possa ou deva ser utilizado. Neste caso, a priorização das referências ajuda na

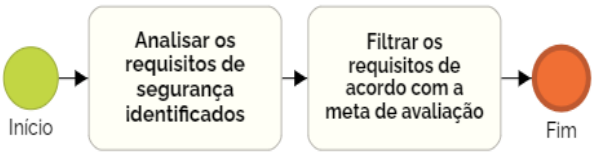
tarefa não trivial de arbitrar que referências devem ser utilizadas e quais devem ser deixadas para um estudo futuro.

4.3. Analisar e filtrar requisitos de autenticação

As entidades técnicas divulgam normas e relatórios técnicos que definem diversos conjuntos de requisitos de segurança. Artigos científicos e outras bibliografias também apresentam requisitos e recomendações.

Considerando o contexto das normas técnicas, os requisitos são usualmente apresentados por seções e subdivididos em tópicos, como: *software* do dispositivo, aplicativo móvel, privacidade, configuração, autenticação, dentre outros [12]. Para cada tópico apresentado são definidas recomendações técnicas publicadas como requisitos de segurança. Neste contexto, a Figura 8 apresenta o processo proposto para analisar e filtrar requisitos de autenticação.

Figura 8 – Analisar e filtrar requisitos de autenticação.



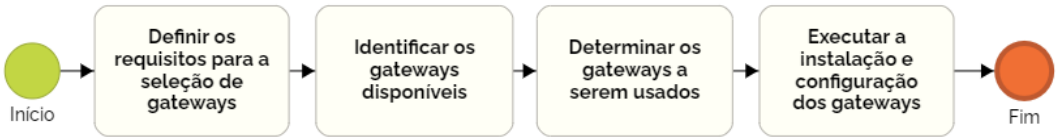
Fonte: O autor (2022).

A primeira atividade se destina a buscar e registrar os requisitos. Contudo, este conjunto ainda não está focado exclusivamente em autenticação. Por isso, a última atividade deste processo se destina a filtragem de requisitos exclusivos da área de autenticação em si. Estes requisitos de autenticação serão registrados e priorizados de acordo com os objetivos da avaliação.

4.4. Selecionar os gateways IoT

Existem diversos tipos de gateway, incluindo gateways baseados em *software*, que executam sobre plataformas como *Raspberry*, e gateways baseados em hardware, que executam sobre plataformas proprietárias. Além disso, existem também diversos fabricantes neste contexto. Neste momento, os gateways serão buscados, selecionados (seguindo requisitos a serem definidos), instalados e configurados. A Figura 9 apresenta as atividades contidas no presente subprocesso.

Figura 9 – Selecionar os gateways IoT.



Fonte: O autor (2022).

Definir um conjunto de requisitos de seleção de gateways, como domínio, serviços, suporte e custo fazem parte da primeira atividade. Estes requisitos devem ser aderentes em relação às metas da avaliação em si. Em seguida, deve-se realizar uma busca para identificar quais gateways estão atualmente disponíveis para sistemas IoT. A escolha dos gateways a serem avaliados ocorre através da análise dos requisitos apresentados em relação aos gateways disponíveis, e isto constitui a terceira atividade. Por fim, os gateways são efetivamente instalados e configurados; para isto, se realiza verificação de documentações técnicas, sites e fóruns de discussão que detalham os procedimentos de instalação e configuração dos gateways escolhidos.

4.5. Realizar inspeção de requisitos de autenticação

Após a escolha dos requisitos de autenticação e dos gateways a serem avaliados, o subprocesso de inspeção pode finalmente iniciar. A Figura 10 apresenta as atividades deste subprocesso.

Figura 10 – Realizar inspeção de requisitos de segurança.

Fonte: O autor (2022).

Para a realização da inspeção, três atividades são propostas. Obter acesso e entender os recursos, as documentações técnicas e o código-fonte do gateway instalado fazem parte da primeira atividade. A próxima atividade é a avaliação da conformidade dos requisitos de autenticação nos gateways escolhidos. Antes de iniciar a inspeção em si, é importante ressaltar que a qualidade da configuração do gateway pode influenciar diretamente no resultado da inspeção. Por exemplo, pode ser que a instalação padrão deste gateway não satisfaça. Contudo, se o usuário analisar manuais de instalação ou fóruns de Internet e atualizar as configurações, o mesmo possa atender. Por isso, para analisar com mais profundidade a qualidade da autenticação provida por estes gateways, consideram-se três níveis de configurações possíveis

neste trabalho (ressaltando que mais níveis podem ser propostos, a depender dos objetivos da avaliação).

O **Nível I** corresponde a configuração padrão de fábrica, ou seja, é a configuração resultante da instalação padrão do gateway. Já o **Nível II** considera que melhorias de configuração são feitas com o objetivo de tentar aumentar o nível de segurança do dispositivo. Para estas melhorias, são analisados recursos como documentações técnicas e fóruns. Por fim, o **Nível III** é caracterizado por modificação no código-fonte do gateway para o atendimento de requisitos específicos, considerando que nos níveis anteriores não foi possível atender aos mesmos. Esta atividade pode requerer uma quantidade significativa de tempo, a depender dos requisitos que serão avaliados.

Por fim, a produção de relatórios com os resultados de inspeção dos requisitos de autenticação é uma forma de documentar o nível atual de segurança dos gateways considerando requisitos de autenticação.

4.6. Realizar comparação e avaliação de resultados

Após a realização da inspeção, resultados relacionados à conformidade dos requisitos são obtidos. Neste último subprocesso, estes resultados são usados para fins comparativos entre os gateways escolhidos e para a produção do relatório final. Além disso, na última atividade, diversas ações podem ser propostas para melhorar o nível de segurança dos gateways avaliados. A Figura 11 apresenta a modelagem deste subprocesso.

Figura 11 – Realizar comparação e avaliação de resultados.

Fonte: O autor (2022).

Inicialmente, a primeira atividade realiza uma comparação dos resultados obtidos para cada gateway IoT. Essa comparação é interessante para analisar, o nível de segurança dos gateways avaliados. A segunda atividade foca na elaboração do relatório final de inspeção, que servirá tanto para documentar os resultados e avaliações obtidas como também no suporte do processo de melhoria de segurança do gateway IoT. Esta melhoria se dá através da proposição de um plano, composto por diversas ações, para melhorar o nível atual de segurança dos gateways avaliados.

4.7. Considerações Finais

Neste capítulo foi detalhada a metodologia proposta para avaliação de requisitos de autenticação de gateways IoT. Para este fim, foi utilizada a notação BPMN para modelagem desta metodologia. Uma vez que a metodologia foi modelada e detalhada, ela será ilustrada na prática (através de estudo de caso) e avaliada no capítulo seguinte.

5. Avaliando o Nível de Segurança de Gateways IoT Considerando Requisitos de Autenticação

Neste capítulo, é apresentada a contribuição principal desta dissertação, que é a avaliação de conformidade de requisitos de autenticação em gateways IoT atualmente utilizados pela comunidade. Esta avaliação será realizada seguindo a metodologia proposta no capítulo anterior.

5.1. Definir metas de avaliação

Como visto no capítulo anterior, ao se definir as metas de avaliação o escopo fica mais claro. A principal meta da avaliação a ser conduzida nesta dissertação é realizar a avaliação de gateways IoT que estão sendo comumente utilizados pelos usuários da área considerando requisitos de autenticação. Com isto, o resultado desta avaliação terá uma contribuição temporal interessante para a comunidade de IoT, pois serão focados justamente os gateways que estão sendo usados por esta comunidade.

Além disto, se objetiva avaliar gateways que podem ser instalados em dispositivos de propósito geral (como *Raspberry*), pois os mesmos podem ser utilizados por um conjunto maior de usuários em comparação a gateways físicos proprietários.

5.2. Pesquisar e priorizar referências de segurança

Neste subprocesso, se inicia a busca, definição e priorização de referências técnicas de segurança que serão utilizadas no processo de avaliação.

Considerando que, em IoT, poucas referências falam unicamente de autenticação em si, é importante primeiro selecionar e priorizar as referências sobre segurança em IoT. Depois disto, no subprocesso posterior, será possível extrair os requisitos de autenticação em si.

Este subprocesso se inicia com a definição do escopo da pesquisa. Neste trabalho, objetivando buscar requisitos discutidos e aceitos pelo maior número de usuários possível, se optou por buscar requisitos de organizações técnicas que contribuem na área de segurança e IoT, como IoT Security Foundation [12] e Open Web Application Security Project [10]–[11]. Para isso, foram definidas bases de dados e *string* de busca capazes de evidenciar as principais organizações que propõem requisitos de segurança para IoT.

Após a execução da busca, foram encontradas e analisadas diversas organizações e

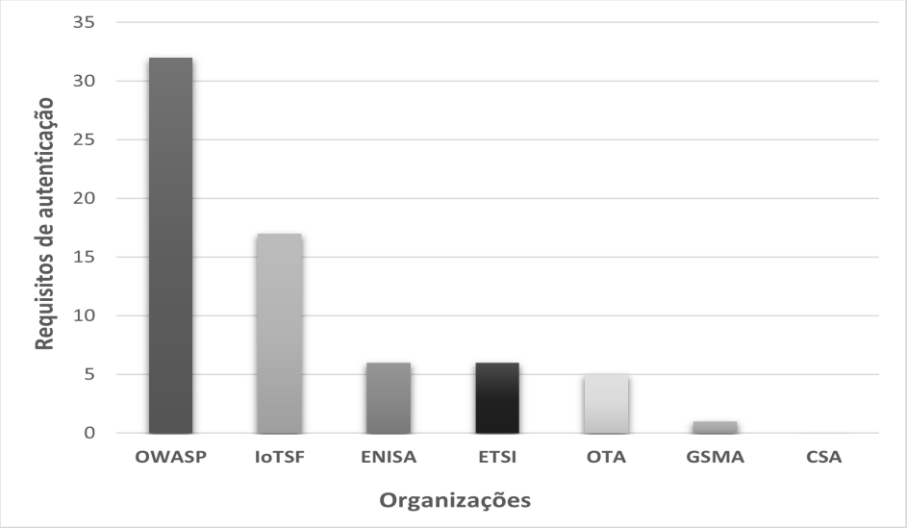
empresas da área. Após isso, como critério de priorização, foi decidido priorizar as que atendam a um grupo significativo de usuários e que descrevem os requisitos de segurança em algum documento oficial da própria organização. Ao final deste subprocesso, as organizações priorizadas foram: IoTSF [12], OWASP [10]–[11], ENISA [6], OTA [14], ETSI [13], CSA [16] e GSMA [15].

5.3. Analisar e filtrar requisitos de autenticação

Considerando as organizações de segurança em IoT priorizadas na atividade anterior, foram analisados quais requisitos de segurança são especificados por elas. No total, estas organizações divulgaram juntas, em suas normas, aproximadamente 1.038 requisitos de segurança para sistemas IoT.

Após o levantamento desses requisitos, foram buscados os requisitos que se referiam especificamente a autenticação em IoT. Baseado neste critério, foram filtrados 67 requisitos de autenticação. A distribuição destes requisitos pelas organizações pesquisadas se encontra na Figura 12.

Figura 12 – Número de requisitos de autenticação por organização.



Fonte: O autor (2022).

Como pode ser observado na Figura 12, a OWASP apresenta um maior número de requisitos, seguido pela IoTSF. Um ponto a ser destacado é que a CSA não apresentou nenhum requisito específico em autenticação. Sendo assim, esta organização não será utilizada nas próximas etapas.

Os requisitos selecionados foram renomeados como GAR (*Gateway Authentication*

Requirement[10]) 01 a 67, ordenados na mesma sequência das organizações técnicas e disponibilizados na nota de rodapé e no apêndice A deste trabalho.

5.4. Selecionar os gateways IoT

O primeiro passo considerado na escolha dos gateways IoT é distinguir os que são baseados em *software*. Nesse contexto, a Figura 4 apresenta 14 gateways IoT com essa característica. O segundo passo observado tem relação com o Nível III de configurações possíveis; tendo em vista a possível necessidade de inspecionar o código-fonte destes gateways, foi dada prioridade aos gateways que permitem o acesso ao código-fonte. Sendo assim, os gateways Agile, Kura, Thinger, ThingsBoard, Ubiworx, Vmware Liota, WebIOPi e WebThings, classificados como *Open Source* e Híbrido, foram selecionados.

No entanto, por motivo de limitação de tempo de pesquisa, 4 entre os 8 gateways foram escolhidos aleatoriamente para participar do processo de inspeção dos requisitos de autenticação. São eles: Eclipse Kura (versão 4.1.2) [87], ThingsBoard (versão 3.2.1) [88], WebIOPi (versão 0.7.1) [89] e WebThings (versão 1.0.0) [90]. Depois da escolha dos gateways, eles foram instalados e configurados. Todos os gateways escolhidos foram instalados em um *Raspberry* Pi 3 modelo B v1.2, com CPU Quad Core 1.2GHz Broadcom BCM2837 64bit, 1 GB de RAM e cartão MicroSDHC Classe 10 de 16 GB em um sistema operacional *Raspberry* Pi OS, baseado em Debian.

No processo de instalação dos gateways, o Eclipse Kura (versão 4.1.2), em comparação com os demais gateways, foi o mais complexo, visto a necessidade de configurações adicionais de interface de rede local, o acesso SSH e as configurações de redes sem fio. A documentação técnica disponibilizada pelo site oficial dos gateways, de forma isolada, não garante o êxito da instalação. Portanto, o usuário precisa, considerando a versão avaliada do gateway, analisar as informações complementares na comunidade do GitHub e dos fóruns de discussões.

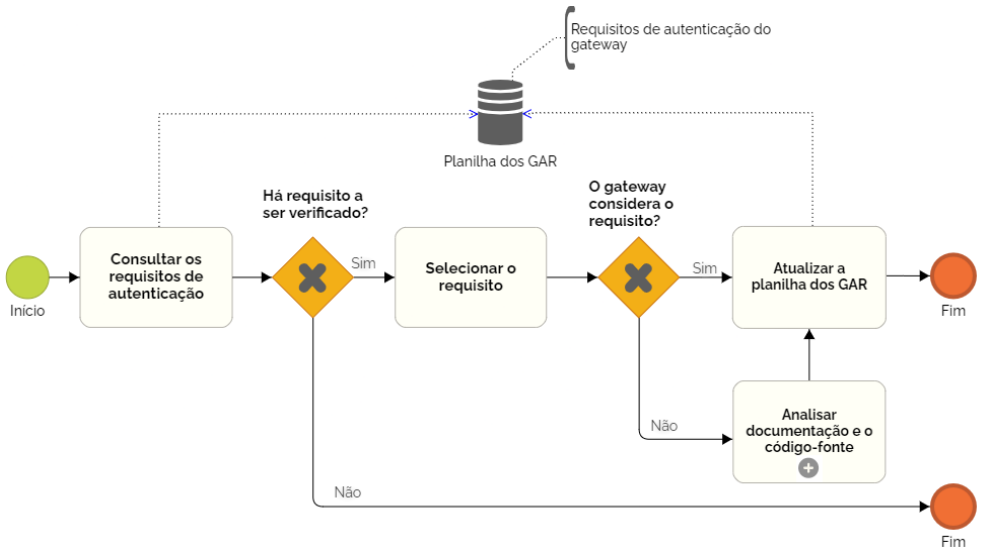
É importante registrar que o objetivo da avaliação não é apontar que um determinado gateway é mais seguro que outros, e sim mostrar como os gateways atuais estão em nível de conformidade com requisitos de autenticação. Por isso, nas atividades seguintes desta avaliação, eles serão chamados de GW_01, GW_02, GW_03 e GW_04. Cada gateway foi associado aleatoriamente a cada uma destas denominações.

[10] Gateway Authentication Requirement. Disponível em:<https://bit.ly/3HD7rYy>. Último acesso em 18 de junho de 2022.

5.5. Realizar inspeção de requisitos de autenticação

Após a definição do conjunto de requisitos de autenticação e a seleção dos gateways, o subprocesso de inspeção pode ser iniciado. A primeira atividade é relacionada ao acesso dos recursos dos gateways que poderão ser utilizados na inspeção. Recursos como documentação técnica e código-fonte são buscados e catalogados para cada gateway, com a finalidade de analisar a conformidade dos requisitos inspecionados. A Figura 13 descreve parte do subprocesso de inspeção de requisitos de autenticação.

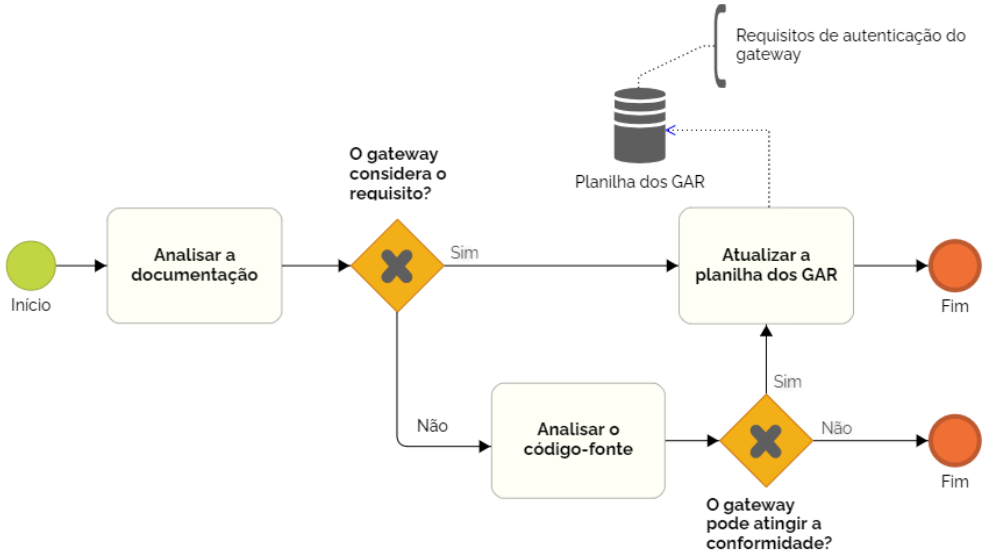
Figura 13 – Inspeção dos requisitos de autenticação considerando o Nível I de configuração.



Fonte: O autor (2022).

O subprocesso inicia-se com a consulta aos requisitos de autenticação registrados na planilha dos GAR. Essa atividade tem como objetivo verificar se há algum requisito que ainda não passou pela inspeção. Se o retorno desta consulta for “não” é porque todos os requisitos já foram inspecionados. Portanto, o subprocesso é finalizado. Mas, se a resposta for "sim", segue para a próxima atividade, que tem como finalidade selecionar o requisito para inspeção. Se o gateway em sua configuração padrão (configuração de fábrica) atender ao requisito selecionado, o resultado da inspeção será registrado na GAR como “Conforme”, finalizando o fluxo, retornando para o início do subprocesso e consultando mais requisitos de autenticação (se houverem). No entanto, se o gateway em sua configuração padrão não atender ao requisito inspecionado, ele continuará sendo inspecionado nos níveis II e III de configurações possíveis. Caso o requisito continue não sendo atendido, mesmo nestes outros níveis de configuração, o resultado é registrado como “Não Conforme” e a inspeção deste GAR específico é finalizada. A Figura 14 descreve as atividades de inspeção nos níveis II e III.

Figura 14 – Inspeção dos requisitos de autenticação considerando os níveis II e III de configuração.



Fonte: Autor (2022).

O subprocesso de analisar a documentação e o código-fonte inicia com a não conformidade do requisito na configuração padrão de fábrica. Portanto, a primeira atividade tem como propósito averiguar as documentações técnicas e os fóruns relacionados ao gateway avaliado. Se após essas consultas o gateway atender ao requisito solicitado, o resultado da inspeção registrado na GAR será de "Parcialmente Conforme[1]". Portanto, o Nível II para esse requisito é aceitável. No entanto, se mesmo assim, ainda não for possível confirmar a conformidade do requisito na atividade anterior, o código-fonte do gateway será explorado. A inspeção no Nível III se mostra mais complexa, visto que será examinado a programação do gateway em si (que pode ser em diferentes linguagens, como Python, Java, JavaScript, C# e C). Nesta atividade, o gateway pode atender ao requisito completamente ou em parte; para ambos os casos, o registro na GAR será de "Parcialmente Conforme[2]". Finalmente, se após as inspeções dos Níveis I, II e III o gateway não alcançar a conformidade, o requisito é registrado como "Não conforme".

Resumindo: no resultado da inspeção, quatro saídas são possíveis: conforme, parcialmente conforme[1], parcialmente conforme[2] e não conforme. Caso o requisito seja atendido já no primeiro nível, o resultado é conforme. Caso sejam necessárias configurações adicionais (Nível II), o resultado é parcialmente conforme[1]. No entanto, se houver a necessidade de melhoria no código-fonte (Nível III), o resultado associado é parcialmente conforme[2]. Finalmente, caso o requisito não seja atendido em nenhuma das configurações possíveis (I, II e III), ele será considerado não conforme. É importante que a conformidade seja atingida logo no primeiro nível, pois nem sempre o usuário se interessa ou é capaz de realizar novas configurações ou modificar o código-fonte do gateway.

Para ilustrar os resultados possíveis das inspeções dos requisitos GAR, sete requisitos foram escolhidos aleatoriamente para serem mostrados na Tabela 6. Estes sete requisitos fazem parte do subconjunto de 67 selecionados neste trabalho, e foram inicialmente apresentados pela OWASP, IoTSF, ENISA e ETSI. Na Tabela 6, são apresentados o identificador do requisito, a sua descrição e os resultados das inspeções nos gateways avaliados (GW_01, GW_02, GW_03 e GW_04).

Tabela 6 – Requisitos de autenticação em gateway (GAR).

Número	Descrição	GW_01	GW_02	GW_03	GW_04
GAR 01	Verifique se todas as formas de usuários e contas no ecossistema IoT podem ser identificadas exclusivamente.	Conforme	Não Conforme	Conforme	Conforme
GAR 36	O produto não aceita o uso de senhas nulas ou em branco.	Conforme	Parcialmente Conforme[2]	Conforme	Conforme
GAR 37	O produto não permitirá novas senhas contendo o nome da conta de usuário ao qual a conta de usuário está associada.	Parcialmente Conforme[2]	Não Conforme	Parcialmente Conforme[2]	Parcialmente Conforme[2]
GAR 39	O produto tem defesa contra tentativas repetidas de login por força bruta, como atrasos exponencialmente crescentes a cada nova tentativa.	Parcialmente Conforme[2]	Não Conforme	Parcialmente Conforme[2]	Parcialmente Conforme[1]
GAR 47	Onde as senhas são inseridas em uma interface de usuário, a senha real é ocultada por padrão.	Conforme	Conforme	Conforme	Conforme
GAR 52	Os mecanismos de autenticação devem usar senhas fortes ou números de identificação pessoal (PINs) e devem considerar o uso de autenticação de dois fatores (2FA) ou autenticação multifator (MFA) como smartphones, biometria etc., além de certificados.	Parcialmente Conforme[1]	Não Conforme	Parcialmente Conforme[2]	Parcialmente Conforme[1]
GAR 56	Quando as senhas são usadas e em qualquer estado que não seja o padrão de fábrica, todas as senhas do dispositivo IoT do consumidor devem ser exclusivas por dispositivo ou definidas pelo usuário.	Conforme	Não Conforme	Parcialmente Conforme[2]	Conforme

Fonte: O autor (2022).

Para exemplificar a inspeção, vamos descrever o caso do requisito GAR 39, proposto inicialmente pela IoTSF. Este requisito recomenda que o gateway tenha defesa contra tentativas repetitivas de acesso, com atraso crescente a cada nova tentativa. O GW_04 só atinge a conformidade do requisito após alteração na sua configuração padrão. Portanto o requisito em questão, neste gateway, está registrado como Parcialmente Conforme[1].

No entanto, outros gateways, como o GW_03, não conseguiram atender a conformidade

após alteração da configuração do gateway. Neste momento, o processo de inspeção se torna mais profundo, pois será verificada a possibilidade de atendimento através de melhoria no código-fonte. Por exemplo, o GW_01 aplica uma política de segurança de que a cada 10 tentativas repetitivas ocorre uma indisponibilidade no acesso por um tempo de 15 minutos fixos. Por sua vez, o GW_03 toma uma ação de segurança após um número máximo de 5 tentativas repetidas. Contudo, ambos não garantem um atraso crescente a cada nova tentativa. Para adicionar esta funcionalidade é preciso modificar o código-fonte dos gateways. Desta forma, eles foram registrados como Parcialmente Conforme[2] (ou seja, eles têm a capacidade de atender ao requisito com melhorias pontuais no código-fonte).

Por fim, se o gateway não conseguiu atender ao requisito solicitado em nenhum dos níveis (I, II ou III), o resultado da inspeção é não conforme. Este foi o caso do GW_02.

A última atividade desse subprocesso tem por finalidade produzir os resultados de inspeção. A Tabela 6 apresentou uma amostragem de sete requisitos e os resultados das 28 inspeções realizadas nos quatros gateways. Nesta amostragem, os GW_01 e GW_04 apresentaram um melhor nível de segurança considerando os requisitos de autenticação selecionados, visto que ambos atingiram a conformidade em quatro dos sete requisitos inspecionados. Já o GW_03 tem capacidade para atender os requisitos, mas é necessário ajustar o código-fonte para atingir este objetivo. Por fim, o GW_02 se apresenta como o nível de conformidade mais crítico, pois dos requisitos inspecionados cinco não apresentaram conformidade.

O *Gateway Authentication Requirement Evaluation Report*[11] é uma planilha completa dos 67 requisitos GAR juntamente com a respectiva inspeção, disponibilizado na nota de rodapé e no apêndice B deste trabalho. Nesta planilha, é possível observar que todos os gateways acabaram falhando em atender algum dos requisitos de autenticação selecionados.

5.6. Realizar comparação e avaliação de resultados

Após definir os três níveis de configurações possíveis nos gateways e apresentar a lista completa dos 67 requisitos inspecionados, o subprocesso de comparação e avaliação de resultados pode finalmente ser iniciado. Nas subseções a seguir são apresentados, de forma comparativa, os resultados das inspeções dos requisitos de autenticação apresentados pelas normas técnicas (OWASP, IoTSF, ENISA, ETSI, OTA e GSMA) com objetivo de mostrar a

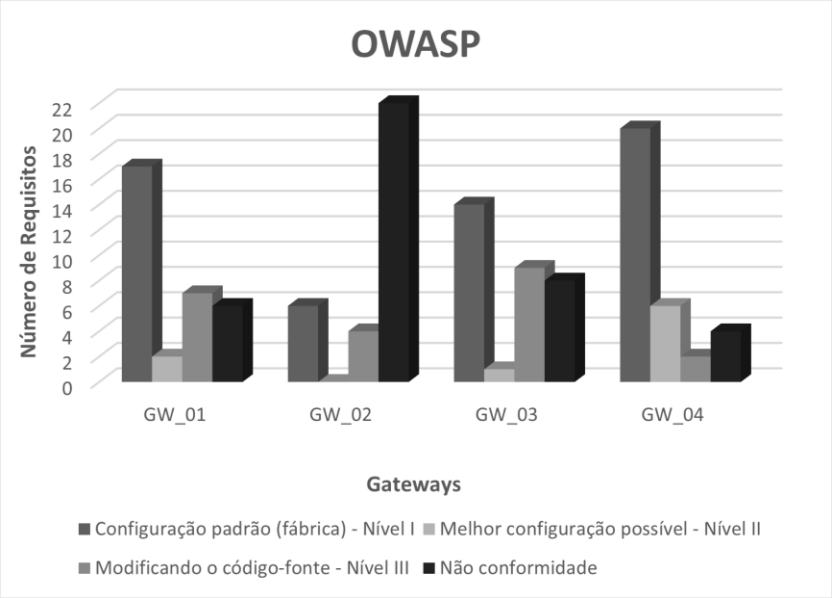
[11] Gateway Authentication Requirement Evaluation Report. Disponível em:< https://bit.ly/3O3Kmk9>. Último acesso em 18 de junho de 2022.

conformidade dos gateways de acordo com cada organização técnica.

5.6.1. Comparar os resultados da inspeção

A *Open Web Application Security Project* apresenta, em sua norma *IoT Security Verification Standard* (versão 1.0) [10], um total de 32 requisitos de autenticação. A Figura 15 apresenta estes requisitos e as suas quatros saídas possíveis de conformidade. Nesta Figura 15, é possível observar que o GW_04 atende a maior quantidade de requisitos em conformidade, enquanto o GW_02 tem o resultado comparativo mais fraco.

Figura 15 – Resultado comparativo da inspeção dos 32 requisitos de autenticação proposto pela OWASP.

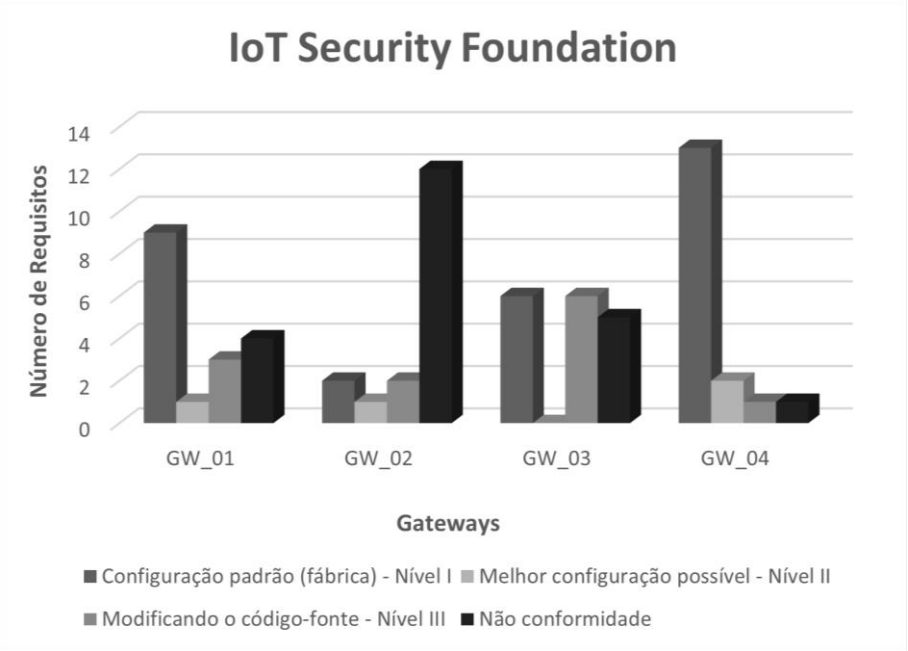


Fonte: O autor (2022).

O GW_04, em sua configuração padrão (fábrica), apresentou uma conformidade em 20 requisitos, 3 a mais do GW_01 e 14 em relação ao gateway mais crítico. No GW_02, por exemplo, 22 requisitos não alcançaram a conformidade, seguido pelo GW_03 com 8 requisitos não conforme. Um ponto a ser observado é que todos os gateways apresentam a não conformidade em um ou mais requisitos.

A IoTSF apresenta um total de 17 requisitos de autenticação. Depois da realização da atividade de inspeção, chegou-se aos resultados explicitados na Figura 16. É possível observar que os gateways GW_01 e GW_04 atendem a maior parte dos requisitos em sua configuração padrão.

Figura 16 – Resultado comparativo da inspeção dos 17 requisitos de autenticação proposto pela IoTSF.

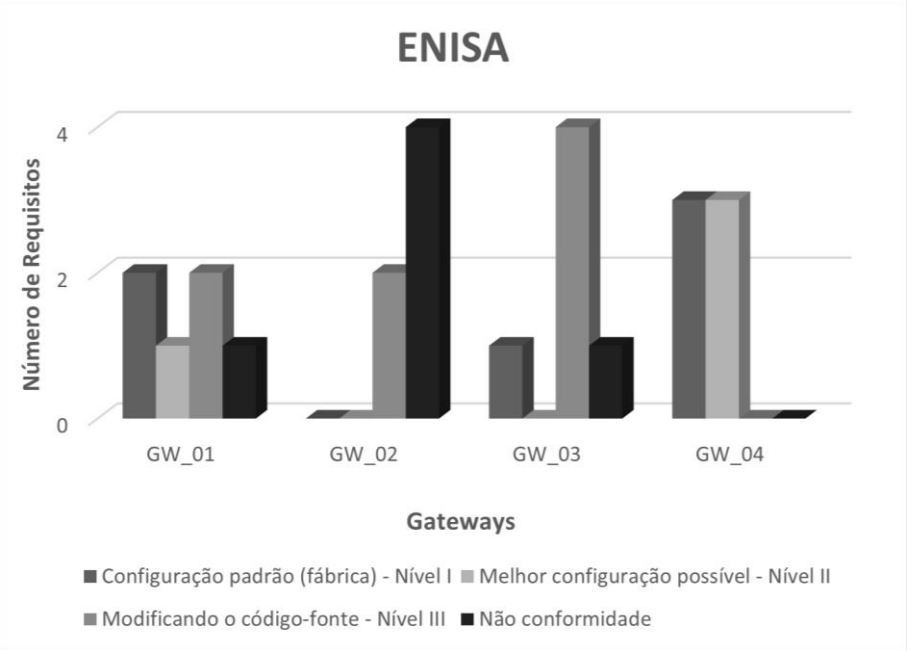


Fonte: O autor (2022).

O GW_02 tem o pior resultado em relação aos demais gateways, visto que apresentou 12 requisitos como não conformidade, sendo 8 a mais em relação ao GW_01 e 07 no que se refere ao GW_03. Observando os níveis de configurações possíveis, o GW_04 apresenta 02 requisitos que conseguem atingir a conformidade na melhor configuração possível, seguido pelos GW_01 e GW_02, ambos com 01 requisito.

A ENISA apresenta 6 requisitos em autenticação. A Figura 17 apresenta o resultado da inspeção destes requisitos nos gateways selecionados. Nesta figura, é possível observar que o GW_04 atinge a conformidade em todos os requisitos considerando os níveis de configuração I e II.

Figura 17 – Resultado comparativo da inspeção dos 6 requisitos de autenticação proposto pela ENISA.

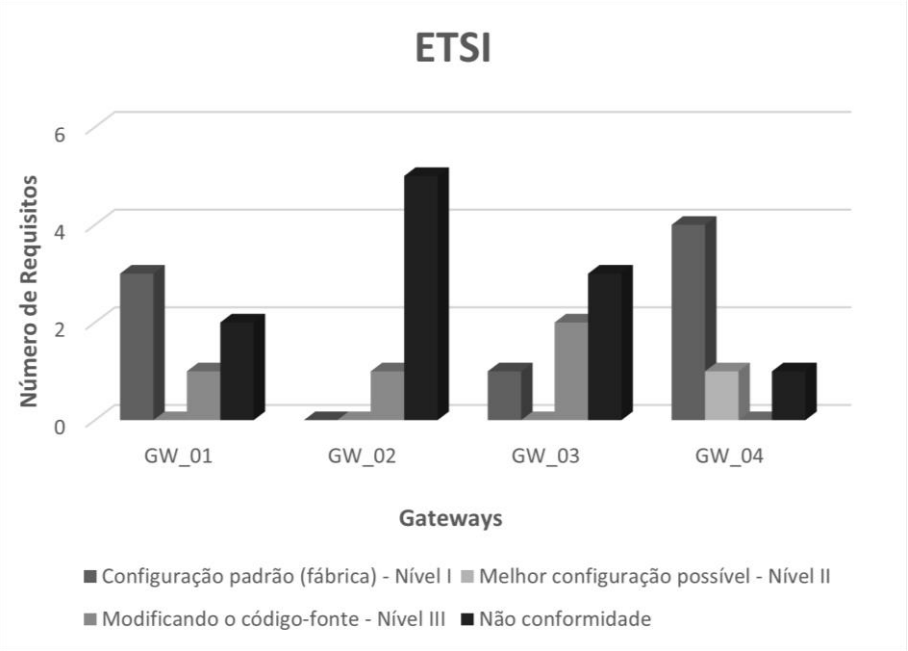


Fonte: O autor (2022).

O GW_01, em sua configuração padrão (fábrica), apresentou conformidade em 2 requisitos, 1 a mais em relação ao GW_03. É possível verificar que os GW_01 e GW_03 podem alcançar mais da metade da conformidade dos requisitos através da modificação/melhoria do código-fonte dos gateways. Por fim, o GW_02 não apresentou nenhuma conformidade considerando os Níveis I e II de configurações possíveis.

A ETSI apresenta 6 requisitos em autenticação. A Figura 18 explicita o resultado comparativo obtido através das inspeções realizadas. Nesta figura, é possível observar que os GW_04 e GW_01, em sua configuração padrão (fábrica), alcançaram conformidade, no mínimo, em metade dos requisitos em autenticação. Entretanto, todos os gateways inspecionados apresentaram não conformidade em algum dos requisitos apresentados.

Figura 18 – Resultado comparativo da inspeção dos 6 requisitos de autenticação proposto pela ETSI.

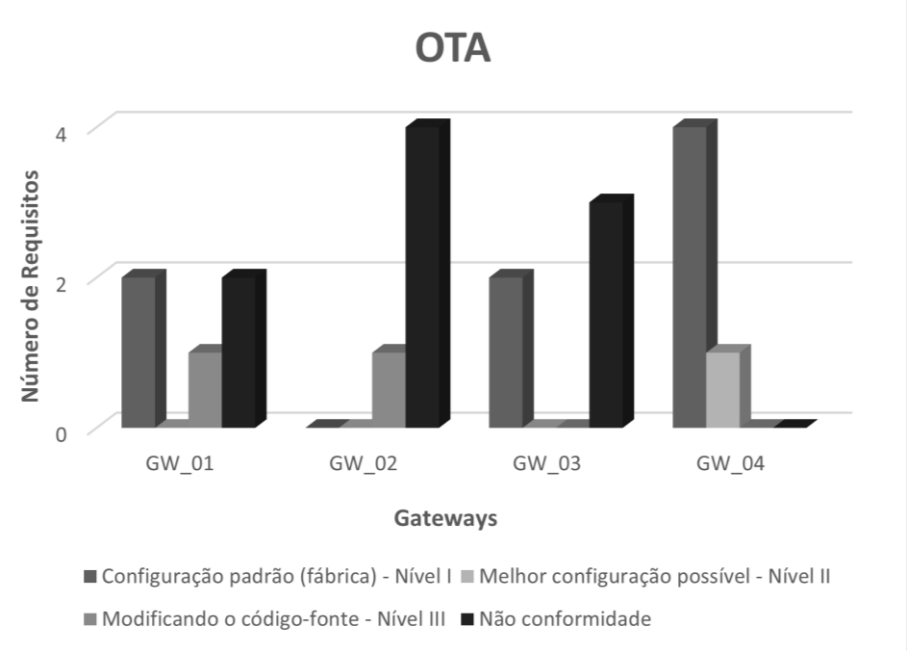


Fonte: O autor (2022).

É importante destacar também que o GW_02 não apresentou conformidade em nenhum requisito considerando os Níveis I e II de configurações possíveis. Entretanto, também pode ser observado na figura que o GW_03 apresentou metade dos requisitos avaliados com não conformidade.

A OTA apresenta 5 requisitos em autenticação. A Figura 19 ilustra o resultado comparativo obtido através da inspeção destes requisitos. É possível observar que os gateways GW_01 e GW_03, nos níveis I e II de configuração, atendem ao mesmo número de requisitos; no entanto, é possível observar que GW_03 apresenta um maior número de requisitos em não conformidade que o GW_01.

Figura 19 – Resultado comparativo da inspeção dos 5 requisitos de autenticação proposto pela OTA.

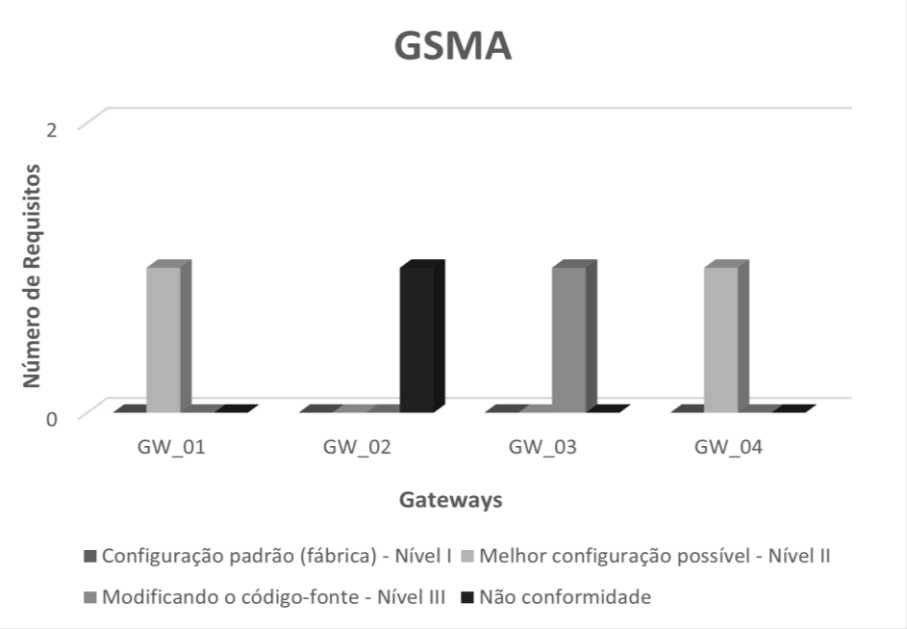


Fonte: O autor (2022).

É possível verificar que o GW_04 apresentou um maior nível de conformidade em relação aos demais gateways. É importante observar que, para obter 100% de conformidade, só foi necessário averiguar a melhor configuração possível. Por outro lado, o GW_02 não apresentou conformidade considerando os níveis I e II de configurações; sendo assim, pode-se afirmar que este gateway obteve o resultado mais crítico diante dos requisitos inspecionados.

A GSM Association, em sua norma *GSMA IoT Security Assessment Process* (versão 2.0) [15], só apresentou um único requisito em autenticação. A Figura 20 apresenta o resultado comparativo da inspeção deste requisito nos gateways avaliados. É possível observar que nenhum dos gateways inspecionados apresentou conformidade no Nível I de configurações. Porém, os gateways GW_01 e o GW_04 conseguem a conformidade do requisito através da análise da melhor configuração possível. Adicionalmente, é possível observar que o GW_03 cumpre a conformidade do requisito apenas através da modificação do seu código-fonte. No entanto, o GW_02 não apresentou conformidade em nenhum dos três níveis de configurações possíveis.

Figura 20 – Resultado comparativo da inspeção de 1 requisito de autenticação proposto pela GSMA.

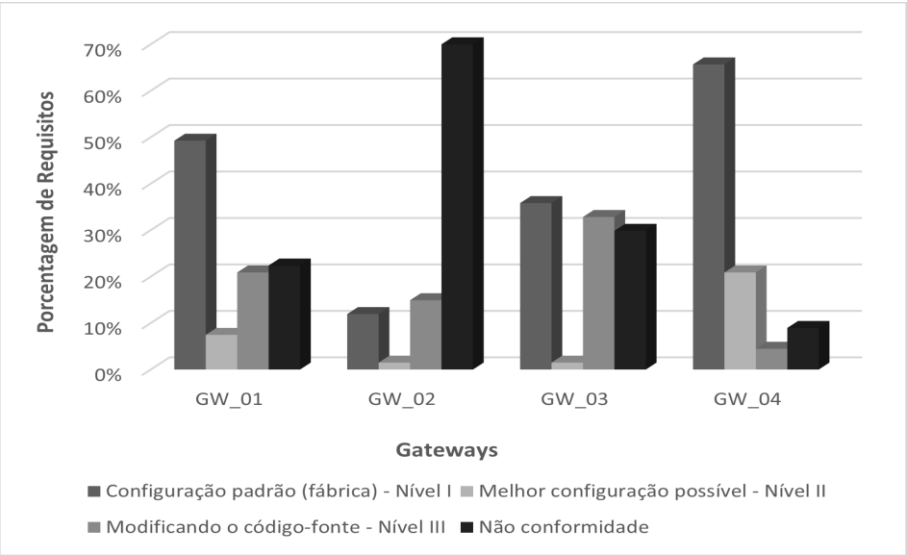


Fonte: O autor (2022).

5.6.2. Produzir relatório final de inspeção

Nesta segunda atividade do último subprocesso da metodologia, são demonstrados os resultados das inspeções dos 67 requisitos de autenticação destacados pelas entidades técnicas e considerados nesta avaliação. A Figura 21 apresenta o percentual para cada etapa das conformidades, examinando todos os requisitos apresentados.

Figura 21 – Resultado comparativo da inspeção dos 67 requisitos de autenticação propostos pelas OWASP, IoTSF, ENISA, ETSI, OTA e GSMA.

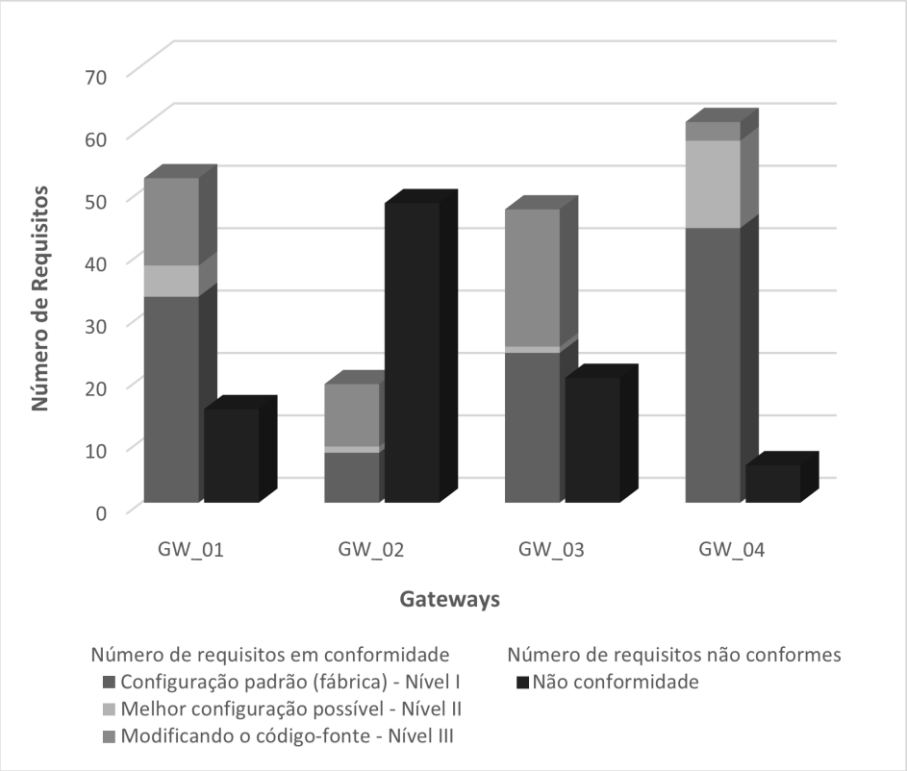


Fonte: O autor (2022).

Através da observação da Figura 21, análises interessantes podem ser realizadas. Por exemplo, no melhor cenário possível, o GW_04, em sua configuração padrão (fábrica), só consegue alcançar, no máximo, 66% de conformidade em relação aos requisitos considerados.

Outra análise a ser observada é o número máximo de requisitos que esses gateways conseguem obter, considerando a possibilidade de alterar as configurações de fábrica e modificar o código-fonte para atingir a conformidade. Para isso, a Figura 22 apresenta a junção dos três níveis de configuração (I, II e III).

Figura 22 – Resultado comparativo da inspeção dos 67 requisitos de autenticação.



Fonte: O autor (2022).

Deste modo, é possível afirmar que, para obter a maior segurança possível considerando os requisitos de autenticação selecionados, o usuário necessita também adotar as melhores configurações possíveis e modificar o código-fonte para aperfeiçoar as funcionalidades de segurança. No entanto, como pode ser visto na figura, mesmo assim isto não garante a conformidade de todos os requisitos de autenticação. Para isto, os desenvolvedores precisam adicionar funcionalidades de segurança que não estão disponíveis atualmente.

5.6.3. Propor ações para melhorar o nível de segurança

Uma abordagem, dentre várias possíveis, para proposição de ações é analisar quais os requisitos que mais se repetem nos documentos oficiais considerados. Esta abordagem

considera que, se um requisito é proposto por mais do que uma organização, ele tem uma importância relativa maior em relação a outro que foi citado por apenas uma organização. Neste contexto, a Tabela 7 apresenta os requisitos que são propostos por mais de uma organização técnica. Essa análise é fundamental, visto que, quando um requisito é citado em mais de uma organização técnica, é possível argumentar que ele se torna mais relevante em relação aos demais requisitos apresentados. No total, dos 67 requisitos considerados inicialmente, foram identificados 10 requisitos semelhantes.

Tabela 7 – Requisitos de autenticação mais citados pelas organizações consideradas neste trabalho.

Nº	Visão geral do requisito	**OWASP**	**IoTSF**	**ENISA**	**ETSI**	**OTA**	**GSMA**
1º	Use senhas fortes ou (PINs) e considere o uso de autenticação de dois fatores (2FA) ou multifator (MFA).	Sim	Sim	Sim	Sim	Sim	Sim
2º	Limite o número de solicitações para evitar ataques de força bruta ou ataques de negação de serviço.	Sim	Sim	Sim	Sim	Não	Não
3º	Certifique-se de que as senhas e nomes de usuário padrão sejam alterados e que senhas fracas, nulas ou em branco não sejam permitidas.	Sim	Sim	Sim	Sim	Não	Não
4º	Armazene qualquer senha usando um algoritmo criptográfico padrão, como NIST SP800-63b [ref 26] ou similar.	Sim	Sim	Sim	Sim	Não	Não
5º	Certifique-se de que o mecanismo de recuperação ou redefinição de senha seja robusto e não forneça informações da conta do usuário.	Sim	Sim	Sim	Não	Sim	Não
6º	As credenciais de autenticação, incluindo, mas não se limitando a senhas de usuário, devem ser salgadas, hash e/ou criptografadas.	Sim	Não	Sim	Não	Sim	Não
7º	Suporte a alteração de uma ou todas as senhas de login de usuário padrão de fábrica quando instaladas ou comissionadas.	Não	Sim	Sim	Sim	Não	Não
8º	Certifique-se de que a senha emitida ou de redefinição de fábrica seja exclusiva para cada dispositivo da família de produtos.	Não	Sim	Não	Sim	Sim	Não
9º	Verifique se as boas políticas de senha são aplicadas em todo o ecossistema de IoT.	Sim	Sim	Não	Não	Não	Não
10º	Verifique se todas as páginas/funções que exigem que um usuário insira credenciais são feitas usando um link criptografado.	Sim	Não	Não	Não	Sim	Não

Fonte: O autor (2022).

A Tabela 7 apresenta o resumo dos 10 requisitos, ordenados de forma quantitativa, e quais as organizações que indicam, em suas normas, estas recomendações técnicas. Diversas considerações importantes podem ser feitas. Uma delas é que o primeiro requisito tem como objetivo o controle de acesso do usuário ao gateway, sendo recomendada por 100% das organizações técnicas. No entanto, nenhum dos gateways atende por completo a este requisito. Por exemplo, o GW_01 e GW_04, no Nível I de configuração (configuração padrão ou de

fábrica), não impõem ao usuário a criação de uma senha forte para o acesso ao gateway. Entretanto, o GW_04 consegue atingir a conformidade considerando o Nível II e o GW_01 o nível III de configuração. Mas, para o recurso de autenticação 2FA e MFA, ambos os gateways só conseguem atingir a conformidade considerando o Nível II.

Outro exemplo a ser apresentado é o sexto requisito, que tem como objetivo proteger as credenciais de autenticação, sendo sugerida pelas organizações técnicas OWASP, ENISA e OTA. No entanto, só os gateways GW_03 e GW_04 atendem o requisito em sua configuração padrão (fábrica) e os GW_01 e GW_02 somente atendem através da alteração do código-fonte. Na inspeção do requisito é possível observar que GW_03 implementa a classe *MessageDigest*, em java, usado para garantir a segurança de uma mensagem. O *MessageDigest* habilita o *hash* com complemento do *salt* com função criptográfica SHA-1, que recebe uma entrada de dados de tamanho variável e produz uma saída de *hash* de 160 bits de tamanho fixo.

No entanto, o GW_04 aplica, nas suas credenciais de acesso, o utilitário *werkzeug.security.generate_password_hash*, que é um método em *hash* com *salt* e função criptográfica SHA-1 com o objetivo de garantir uma maior segurança em uma senha. Enquanto isso, os GW_01 e GW_02 utilizam a função de *hash bcrypt* em suas credenciais. Entretanto, não está habilitado o *salt* no código.

5.7. Considerações Finais

Neste capítulo, foi apresentada a contribuição principal desta dissertação, que é a avaliação dos níveis de segurança de gateways IoT considerando requisitos de autenticação. Neste contexto, a principal meta da avaliação foi verificar os níveis de conformidades dos gateways IoT. Para isso, foram priorizadas organizações técnicas em IoT, e estas referências geraram um total de 67 requisitos de autenticação (chamados de GAR neste trabalho). O subprocesso de inspeção considerou três níveis de configurações possíveis na avaliação do requisito e com o resultado desses dados foi possível realizar comparações e avaliações entre os gateways IoT. Por fim, foram apresentados dez requisitos de autenticação mais citados pelas organizações técnicas com a finalidade de se discutir quais os objetivos mais urgentes, em termos de importância relativa.

6. Conclusões e Trabalhos Futuros

Neste capítulo, são descritas as conclusões, as contribuições, as limitações encontradas e os trabalhos futuros desta dissertação. Na Seção 6.1, são mostradas as conclusões acerca da pesquisa desenvolvida nesta dissertação. Na Seção 6.2, são apresentadas as contribuições científicas deste trabalho. Na Seção 6.3, são expostas as limitações associadas aos resultados desta pesquisa. Por fim, na Seção 6.4 são descritas e detalhadas as oportunidades de trabalhos futuros a serem realizados como complemento a esta pesquisa.

6.1. Conclusões

Este trabalho teve como objetivo avaliar os níveis de segurança de gateways IoT baseados em *software* considerando requisitos de autenticação propostos e divulgados por organizações técnicas internacionais reconhecidas. A princípio foi realizada uma pesquisa bibliográfica, com a finalidade de entender o atual estado da arte sobre os principais aspectos de autenticação em um ambiente IoT, e foi possível observar a falta de propostas direcionadas a avaliar o contexto específico de autenticação em gateways IoT.

Este contexto específico de autenticação foi escolhido por ser o primeiro fator de entrada dos usuários e das coisas em um sistema IoT. Para avaliar a qualidade do atendimento a requisitos de autenticação em gateways IoT, foi proposta uma metodologia, que sistematizou os procedimentos de inspeção e avaliação dos requisitos de autenticação apresentados pelas organizações técnicas.

As organizações técnicas em IoT divulgam, em suas normas, diversas seções com recomendações técnicas de segurança. As seções dos requisitos de autenticação serviram de base para compreender as boas práticas na construção de um sistema IoT mais seguro. Para se avaliar o nível de segurança destes gateways considerando requisitos de autenticação, foram priorizados 67 requisitos, e todo o processo para a obtenção destes requisitos foi detalhado.

Para realização do processo de inspeção, foi necessário analisar com mais detalhes as características de autenticação fornecida pelos gateways. Portanto, foi de fundamental importância adotar três níveis de configurações possíveis (configuração padrão, melhor configuração possível e modificação do código-fonte), pois estes níveis deixam claro o esforço adicional (ex.: alteração de configuração padrão) que o usuário deverá empreender para melhorar o nível de conformidade.

Por fim, este trabalho proporcionou avanços ao atual estado da arte, visto que foi a única

pesquisa, até o momento, que apresentou uma inspeção de requisitos de autenticação em gateways IoT. Com os resultados apresentados, a comunidade poderá tanto entender qual o nível atual de qualidade relacionada a atendimento de requisitos de autenticação como também usar os resultados obtidos na avaliação para escolher um gateway que melhor atenda às necessidades de segurança do usuário/projeto.

6.2. Contribuições

A principal contribuição deste trabalho foi a avaliação do nível de conformidade de requisitos de autenticação em gateways IoT. Foram utilizados requisitos provenientes de organizações técnicas, pois se considera que estes requisitos foram debatidos e aceitos por um número maior de pesquisadores e usuários.

Como resultado, foi observado que os quatro gateways avaliados apresentaram um nível bastante variado de atendimento aos requisitos, o que reforça a necessidade de se avaliar aspectos de autenticação. Além disso, em seu conjunto, nenhum gateway conseguiu alcançar um índice global de atendimento superior a 91%. Por fim, nenhum gateway conseguiu nível de atendimento superior a 66% quando se considera apenas a configuração padrão (*factory*), o que mostra a importância de se avaliar e melhorar a qualidade da configuração de segurança do mesmo.

Outra contribuição interessante deste trabalho foi a metodologia de avaliação proposta. Ela não apenas torna a pesquisa reproduzível, como também pode servir como base para a avaliação do nível de segurança de gateways IoT em outros projetos. Por exemplo, o protocolo da avaliação pode ser alterado para incluir novos gateways ou mesmo novos requisitos.

6.3. Limitações

A principal dificuldade encontrada neste trabalho foi o fato de que diversas documentações de instalação e configuração dos gateways IoT estavam incompletas ou muitas vezes imprecisas. Outra limitação encontrada foi a decisão de limitar a quantidade de gateways avaliados, considerando a falta de tempo hábil para o processo de inspeção; dos 8 gateways inicialmente selecionados, apenas 4 puderam ser efetivamente avaliados. Por fim, não foram considerados outros gateways (especialmente os não baseados em software), o que pode limitar a abrangência do resultado obtido nesta avaliação realizada.

6.4. Trabalhos Futuros

Como trabalhos futuros, a primeira proposta é o desenvolvimento de uma ferramenta para automatizar o processo de inspeção dos requisitos de autenticação em gateways IoT. Esta ferramenta ajudaria na redução dos recursos empregados no processo manual de inspeção. A ferramenta, inclusive, está em fase de desenvolvimento. Para o desenvolvimento dela, foi utilizado o *Robot Framework*, que é uma estrutura, aberta e extensível, de automação de código aberto, que pode ser integrado a outras ferramentas para criar soluções de automação flexíveis [91]. O *Robot Framework* permite que os usuários criem scripts de testes com palavras-chaves sem a necessidade de experiência prévia profunda em programação [92]. A Figura 23 é um teste primário de dois requisitos (GAR 36 e 37) sendo inspecionados no GW_01.

Figura 23 – Caso de testes de credenciais inválidas.

```
1  *** Settings ***
2  Documentation     Caso de testes de credenciais invalidas
3
4  Suite Setup       Open Browser To Login Page
5  Suite Teardown    Close Browser
6  Test Setup        Go To Login Page
7  Test Template     Login With Invalid Credentials Should Fail
8  Resource          resource.robot
9
10 *** Test Cases ***               USER NAME        PASSWORD
11 Invalid Username                 invalid          ${VALID PASSWORD}
12 Invalid Password                 ${VALID USER}    invalid
13 Invalid Username And Password    invalid          whatever
14 Empty Username                   ${EMPTY}         ${VALID PASSWORD}
15 Empty Password                   ${VALID USER}    ${EMPTY}
16 Empty Username And Password      ${EMPTY}         ${EMPTY}
17 Empty Username And Password      ${VALID USER}    ${VALID USER}
18
19 *** Keywords ***
20 Login With Invalid Credentials Should Fail
21     [Arguments]    ${username}    ${password}
22     Input Username    ${username}
23     Input Password    ${password}
24     Submit Credentials
25     Login Should Have Failed
26
27 Login Should Have Failed
28     Location Should Be    ${LOGIN URL}
29     Title Should Be    Login - GW_01
```

Fonte: O autor (2022).

Para os testes de credenciais inválidas, foi utilizado o *Selenium Library* [93]-[94], que é uma biblioteca de teste para Robot Framework. É possível observar, na Figura 23, os sete testes de credenciais com as palavras-chave {username} e {password}. Estes testes têm como objetivo validar os resultados das inspeções do GW_01 apresentado pela planilha GAR (*Gateway Authentication Requirement Evaluation Report*) considerando o Nível I de configurações possíveis (Configuração padrão). O resultado dos sete testes confirmou os resultados apresentados pela avaliação manual realizada nesta dissertação. Por exemplo, a primeira análise ocorreu nas linhas 11-16 do código apresentado pela Figura 23, e o teste confirma que o gateway não admite usuário e/ou senha em branco ou inválidos. Portanto, o GW_01 está “conforme” e

confirma o resultado registrado na GAR 36.

Já o teste da linha 17 tem como objetivo validar o requisito que informa que não é recomendado criar uma senha a partir do mesmo nome do usuário (exemplo: brseclab/brseclab). Portanto, GW_01 não atende o requisito solicitado, visto que é possível a criação. Neste contexto, o resultado obtido confirma a resposta registrada na GAR 37 que é "parcialmente conforme²". Entretanto, ainda precisam ser implementados no *Robot Framework* os testes de níveis II e III de configurações possíveis. As Figuras 24 e 25, localizadas no Apêndice C deste trabalho, contém os recursos de palavras-chave, variáveis reutilizáveis e os testes de credenciais válidas.

Além disso, outra proposta de trabalho futuro é analisar e inspecionar outras seções de conjuntos de requisitos apresentados pelas organizações técnicas, como privacidade e transparência, proteção de dados, elementos de nuvem e rede, gestão de risco, atualização de software, monitoramento e auditoria, entre outros. Esta análise propiciará uma visão mais abrangente do nível de segurança em si, e não apenas dos requisitos de autenticação.

A terceira proposta de continuidade da pesquisa é mensurar a segurança dos gateways proprietários baseados em *software* e *hardware* não cobertos pela pesquisa deste artigo. Isto ajudaria na obtenção de resultados mais abrangentes, que poderiam representar maior precisão no contexto geral da área de segurança de gateways IoT considerando requisitos de autenticação.

Por fim, se vislumbra também a avaliação do nível de segurança em autenticação através da realização de ataques conhecidos em gateways IoT, como: I) *Masquerade attack* (ataque baseado na identidade, que tem como objetivo usar credenciais de autenticação falsa para se passar como coisa/usuário autêntico na rede IoT), II) *Man-in-the-middle attack* (ataque onde o invasor captura os dados de comunicação entre duas partes diretamente conectadas e se comunicando), III) *Distributed denial of service* (ataque que nega um serviço para um coisa/usuário autorizado, enviando milhares de solicitação de acesso em curto espaço de tempo, ocasionando a indisponibilidade do sistema), e IV) *Guessing attack* (ataque que o adversário tenta obter informações de autenticação como ID do usuário e dispositivo, chave secreta e senha do usuário que são armazenados no servidor de autenticação IoT). Outros ataques a autenticação podem ser realizados, como: *Forging attack, Physical attacks* e *Routing attack.*

Referências

[1] T. Nandy *et al.*, "Review on Security of Internet of Things Authentication Mechanism", *IEEE Access*, vol. 7, p. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.

[2] F. A. A. Lins e M. Vieira, "Security Requirements and Solutions for IoT Gateways: A Comprehensive Study", *IEEE Internet Things J.*, vol. 8, nº 11, p. 8667–8679, jun. 2021, doi: 10.1109/JIOT.2020.3041049.

[3] AT&T 2021 - Intelligent Business. Acessado: 03 de setembro de 2021. [Online]. Disponível em: https://www.business.att.com/learn/researchreports/att-intelligent-business-report.html.

[4] IoT Security Foundation - Secure Design Best Practice Guides - Release v2 - Nov_2019. Acessado: 23 de junho de 2021. [Online]. Disponível em: https://www.iotsecurityfoundation.org/wp-content/uploads/2019/03/Best-Practice-Guides-Release-1.2.1.pdf.

[5] S. Narayanaswamy e A. V. Kumar, "Application Layer Security Authentication Protocols for the Internet of Things: A Survey", *Adv. Sci. Technol. Eng. Syst. J.*, vol. 4, nº 1, p. 317–328, 2019, doi: 10.25046/aj040131.

[6] European Union Agency for Network and Information Security., *Baseline security recommendations for IoT in the context of critical information infrastructures.* LU: Publications Office, 2017. Acessado: 21 de junho de 2021. [Online]. Disponível em: https://data.europa.eu/doi/10.2824/03228

[7] OWASP Internet of Things | OWASP Foundation. https://owasp.org/www-project-internet-of-things/ (acessado 16 de maio de 2021).

[8] OWASP Top 10 Internet of Things. Acessado: 03 de setembro de 2021. [Online]. Disponível em: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

[9] L. Prathibha e K. Fatima, "Exploring Security and Authentication Issues in Internet of Things", em *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, jun. 2018, p. 673–678. doi: 10.1109/ICCONS.2018.8663111.

[10] A. Guzman e C. Bassem, "OWASP IoT Security Verification Standard", p. 29.

[11] V2 Authentication verification requirements — OWASP Annotated Application Security Verification Standard 3.0.0 documentation. https://owasp-aasvs.readthedocs.io/en/latest/v2.html (acessado 16 de maio de 2021).

[12] IoTSF IoT Security Compliance Framework Release 2.1 May 2020. Acessado: 13 de maio de 2021. [Online]. Disponível em: https://www.iotsecurityfoundation.org/tag/release-2-1/

[13] Cyber Security for Consumer Internet of Things - Baseline Requirements 2020. Acessado: 07 de junho de 2021. [Online]. Disponível em: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

[14] IoT Security & Privacy Trust Framework v2.5. Acessado: 06 de junho de 2021. [Online]. Disponível em: https://www.internetsociety.org/wp-content/uploads/2018/05/iot_trust_framework2.5a_EN.pdf

[15] GSMA IoT Security Assessment_Checklist. Acessado: 08 de abril de 2021. [Online]. Disponível em: https://www.gsma.com/security/resources/clp-17-gsma-iot-security-assessment-checklist-v3-0/

[16] CSA IoT Security Controls Framework Version 2. Acessado: 06 de junho de 2021. [Online]. Disponível em: https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2/

[17] W. Stallings, *Criptografia e Segurança de Redes: princípios e práticas*, 6º ed. 2015.

[18] Y.-H. Chuang, N.-W. Lo, C.-Y. Yang, e S.-W. Tang, "A Lightweight Continuous Authentication Protocol for the Internet of Things", *Sensors*, vol. 18, nº 4, p. 1104, abr. 2018, doi: 10.3390/s18041104.

[19] I. Bhardwaj, A. Kumar, e M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs", em *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, solan, India, set. 2017, p. 504–509. doi: 10.1109/ISPCC.2017.8269731.

[20] “Scopus Preview”. https://www.scopus.com/home.uri (acessado 25 de fevereiro de 2021).
[21] “Google Scholar”. https://scholar.google.com/ (acessado 27 de fevereiro de 2021).
[22] “Clarivate Home”, *Clarivate*. https://clarivate.com/ (acessado 1º de março de 2021).
[23] “ACM Digital Library”. https://dl.acm.org/ (acessado 4 de março de 2021).
[24] “IEEE Xplore”. https://ieeexplore.ieee.org/Xplore/home.jsp (acessado 7 de março de 2021).
[25] “Wiley Online Library”, *Wiley Online Library*. https://onlinelibrary.wiley.com/ (acessado 10 de março de 2021).
[26] “Springer Link”. https://link.springer.com/ (acessado 12 de março de 2021).
[27] “EBSCO”, *EBSCO Information Services, Inc. | www.ebsco.com*. https://www.ebsco.com/ (acessado 15 de março de 2021).
[28] V. J. Aski, S. Gupta, e B. Sarkar, “An Authentication-Centric Multi-Layered Security Model for Data Security in IoT-Enabled Biomedical Applications”, em *2019 IEEE 8th Global Conference on Consumer Electronics (GCCE)*, Osaka, Japan, out. 2019, p. 957–960. doi: 10.1109/GCCE46687.2019.9015217.
[29] B. Chatterjee, D. Das, S. Maity, e S. Sen, “RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes using In-situ Machine Learning”, 2018, doi: 10.48550/ARXIV.1805.01374.
[30] A. Ferdowsi e W. Saad, “Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems”, *IEEE Trans. Commun.*, vol. 67, nº 2, p. 1371–1387, fev. 2019, doi: 10.1109/TCOMM.2018.2878025.
[31] M. Kumar, H. K. Verma, e G. Sikka, “A secure lightweight signature based authentication for Cloud-IoT crowdsensing environments”, *Trans. Emerg. Telecommun. Technol.*, vol. 30, nº 4, p. e3292, abr. 2019, doi: 10.1002/ett.3292.
[32] S. Ghosh e S. Ruj, “Fast Real-Time Authentication Scheme for Smart Grids”, em *Proceedings of the ACM Workshop on Internet of Things (IoT) Security: Issues and Innovations*, Chennai India, jul. 2017, p. 1–7. doi: 10.1145/3084030.3084033.
[33] P. K. Dhillon e S. Kalra, “Secure multi-factor remote user authentication scheme for Internet of Things environments”, *Int. J. Commun. Syst.*, vol. 30, nº 16, p. e3323, nov. 2017, doi: 10.1002/dac.3323.
[34] M. Chen, T.-F. Lee, e J.-I. Pan, “An Enhanced Lightweight Dynamic Pseudonym Identity Based Authentication and Key Agreement Scheme Using Wireless Sensor Networks for Agriculture Monitoring”, *Sensors*, vol. 19, nº 5, p. 1146, mar. 2019, doi: 10.3390/s19051146.
[35] A. Jabbari e J. B. Mohasefi, “Improvement of a User Authentication Scheme for Wireless Sensor Networks Based on Internet of Things Security”, *Wirel. Pers. Commun.*, vol. 116, nº 3, p. 2565–2591, fev. 2021, doi: 10.1007/s11277-020-07811-3.
[36] F. Wu, L. Xu, S. Kumari, e X. Li, “A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security”, *J. Ambient Intell. Humaniz. Comput.*, vol. 8, nº 1, p. 101–116, fev. 2017, doi: 10.1007/s12652-016-0345-8.
[37] J. Moon, Y. Lee, H. Yang, T. Song, e D. Won, “Cryptanalysis of a privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security”, em *2018 International Conference on Information Networking (ICOIN)*, Chiang Mai, jan. 2018, p. 432–437. doi: 10.1109/ICOIN.2018.8343154.
[38] Y.-H. Chuang, N.-W. Lo, C.-Y. Yang, e S.-W. Tang, “A Lightweight Continuous Authentication Protocol for the Internet of Things”, *Sensors*, vol. 18, nº 4, p. 1104, abr. 2018, doi: 10.3390/s18041104.
[39] B. L. Parne, S. Gupta, e N. S. Chaudhari, “PSE-AKA: Performance and security enhanced authentication key agreement protocol for IoT enabled LTE/LTE-A networks”, *Peer--Peer Netw. Appl.*, vol. 12, nº 5, p. 1156–1177, set. 2019, doi: 10.1007/s12083-019-00785-5.
[40] B. A. Alzahrani, A. Irshad, K. Alsubhi, e A. Albeshri, “A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT”, *Int. J. Commun. Syst.*, vol. 33, nº 11, p. e4423, jul. 2020, doi: 10.1002/dac.4423.
[41] C. S. Vorugunti, B. Mishra, R. Amin, R. P. Badoni, M. Sarvabhatla, e D. Mishra, “Improving Security of Lightweight Authentication Technique for Heterogeneous Wireless Sensor Networks”, *Wirel. Pers. Commun.*, vol. 95, nº 3, p. 3141–3166, ago. 2017, doi: 10.1007/s11277-017-3988-7.

[42] X. Fan e B. Niu, “Security of a new lightweight authentication and key agreement protocol for internet of things”, em *2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, Guangzhou, maio 2017, p. 107–111. doi: 10.1109/ICCSN.2017.8230088.
[43] P. S. F. Sheron, K. P. Sridhar, S. Baskar, e P. M. Shakeel, “A decentralized scalable security framework for end-to-end authentication of future IoT communication”, *Trans. Emerg. Telecommun. Technol.*, vol. 31, nº 12, dez. 2020, doi: 10.1002/ett.3815.
[44] E. Rattanalerdnusorn, P. Thaenkaew, e C. Vorakulpipat, “Security Implementation For Authentication In Iot Environments”, em *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, Singapore, fev. 2019, p. 678–681. doi: 10.1109/CCOMS.2019.8821686.
[45] D. Showkat, S. Som, S. K. Khatri, e A. S. Ahluwalia, “Security Implications in IoT using Authentication and Access Control”, em *2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, ago. 2018, p. 689–694. doi: 10.1109/ICRITO.2018.8748731.
[46] S. Venkatraman e A. Overmars, “IoT Authentication and Security Challenges”, p. 11.
[47] J. G. Pérez-Silva, M. Araujo-Voces, e V. Quesada, “nVenn: generalized, quasi-proportional Venn and Euler diagrams”, *Bioinformatics*, vol. 34, nº 13, p. 2322–2324, jul. 2018, doi: 10.1093/bioinformatics/bty109.
[48] “Code IoT”. https://codeiot.org.br/ (acessado 9 de junho de 2022).
[49] “Top 10 IoT applications in 2020”, *IoT Analytics*, 8 de julho de 2020. https://iot-analytics.com/top-10-iot-applications-in-2020/ (acessado 9 de junho de 2022).
[50] “State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally”, *IoT Analytics*, 18 de maio de 2022. https://iot-analytics.com/number-connected-iot-devices/ (acessado 9 de junho de 2022).
[51] P. Sethi e S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications”, *J. Electr. Comput. Eng.*, vol. 2017, p. 1–25, 2017, doi: 10.1155/2017/9324035.
[52] “Tecnologias e protocolos de IoT | Microsoft Azure”. https://azure.microsoft.com/pt-br/overview/internet-of-things-iot/iot-technology-protocols/ (acessado 11 de junho de 2022).
[53] D. Minoli, “Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach”, *Internet Things*, vol. 10, p. 100147, jun. 2020, doi: 10.1016/j.iot.2019.100147.
[54] E. Kim e C. Keum, “Trustworthy gateway system providing IoT trust domain of smart home”, em *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, Milan, jul. 2017, p. 551–553. doi: 10.1109/ICUFN.2017.7993848.
[55] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, e C.-M. Chen, “An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System”, *Sensors*, vol. 17, nº 7, p. 1482, jun. 2017, doi: 10.3390/s17071482.
[56] S. S. Alotaibi, “Registration Center Based User Authentication Scheme for Smart E-Governance Applications in Smart Cities”, *IEEE Access*, vol. 7, p. 5819–5833, 2019, doi: 10.1109/ACCESS.2018.2884541.
[57] P. A. Grassi, M. E. Garcia, e J. L. Fenton, “Digital Identity Guidelines: Revision 3”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63-3, jun. 2017. doi: 10.6028/NIST.SP.800-63-3.
[58] P. A. Grassi *et al.*, “Digital Identity Guidelines: Enrollment and Identity Proofing Requirements”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63a, jun. 2017. doi: 10.6028/NIST.SP.800-63a.
[59] P. A. Grassi *et al.*, “Digital Identity Guidelines: Federation and Assertions”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63c, jun. 2017. doi: 10.6028/NIST.SP.800-63c.
[60] P. A. Grassi *et al.*, “Digital Identity Guidelines: Authentication and Lifecycle Management”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63b, jun. 2017. doi: 10.6028/NIST.SP.800-63b.
[61] “OWASP Foundation | Open Source Foundation for Application Security”. https://owasp.org/ (acessado 5 de março de 2022).

[62] “IoT Security Foundation – The Global Home of IoT Cybersecurity”. https://www.iotsecurityfoundation.org/ (acessado 5 de março de 2022).
[63] “European Union Agency for Cybersecurity (ENISA)”, *ENISA*. https://www.enisa.europa.eu (acessado 5 de março de 2022).
[64] P. T. Mascarenhas Neto e W. J. de Araújo, *Segurança da informação: uma visão sistêmica para implantação em organizações*. figshare, 2020. doi: 10.6084/m9.figshare.11825559.v1.
[65] “ETSI - European Telecommunications Standards Institute”, *ETSI*. https://www.etsi.org/ (acessado 6 de junho de 2022).
[66] CERT.br, “Fascículos da Cartilha de Segurança para Internet”, *Cartilha de Segurança para Internet*. https://cartilha.cert.br/fasciculos/ (acessado 6 de março de 2022).
[67] “Online Trust Alliance (OTA)”, *Internet Society*. https://www.internetsociety.org/ota/ (acessado 5 de março de 2022).
[68] J. Hintzbergen, K. Hintzbergen, A. Smulders, e H. Baars, *Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002*. Rio de Janeiro: Brasport, 2018. Acessado: 5 de março de 2022. [Online]. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2115716
[69] “GSM Association”, *GSMA*. https://www.gsma.com/ (acessado 6 de março de 2022).
[70] “Connectivity Standards Alliance (CSA)”, *CSA-IOT*. https://csa-iot.org/ (acessado 6 de junho de 2022).
[71] S. K. Y. Donzia, H.-K. Kim, e H. J. Hwang, “A Software Model for Precision Agriculture Framework Based on Smart Farming System and Application of IoT Gateway”, em *Computational Science/Intelligence & Applied Informatics*, vol. 787, R. Lee, Org. Cham: Springer International Publishing, 2019, p. 49–58. doi: 10.1007/978-3-319-96806-3_4.
[72] H. Dickel, V. Podolskiy, e M. Gerndt, “Evaluation of Autoscaling Metrics for (stateful) IoT Gateways”, em *2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)*, Kaohsiung, Taiwan, nov. 2019, p. 17–24. doi: 10.1109/SOCA.2019.00011.
[73] M. Poess, R. Nambiar, K. Kulkarni, C. Narasimhadevara, T. Rabl, e H.-A. Jacobsen, “Analysis of TPCx-IoT: The First Industry Standard Benchmark for IoT Gateway Systems”, em *2018 IEEE 34th International Conference on Data Engineering (ICDE)*, Paris, abr. 2018, p. 1519–1530. doi: 10.1109/ICDE.2018.00170.
[74] O. Ali, M. K. Ishak, L. Wuttisittikulkij, e T. Z. B. Maung, “IoT Devices and Edge gateway provisioning, realtime analytics for simulated and virtually emulated devices”, em *2020 International Conference on Electronics, Information, and Communication (ICEIC)*, Barcelona, Spain, jan. 2020, p. 1–5. doi: 10.1109/ICEIC49074.2020.9051037.
[75] M. F. Quiñones, H. P. Pachar Bravo, J. Martínez-Curipoma, L. Quiñones, e R. Torres, “Desarrollo y evaluación de un gateway móvil IoT para redes 4G LTE”, *Enfoque UTE*, vol. 11, nº 4, p. 16–26, out. 2020, doi: 10.29019/enfoqueute.v11n4.634.
[76] M. Imdad, D. W. Jacob, H. Mahdin, Z. Baharum, S. M. Shaharudin, e M. S. Azmi, “Internet of things: security requirements, attacks and counter measures”, *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, nº 3, p. 1520, jun. 2020, doi: 10.11591/ijeecs.v18.i3.pp1520-1530.
[77] G. Hansch, P. Schneider, K. Fischer, e K. Bottinger, “A Unified Architecture for Industrial IoT Security Requirements in Open Platform Communications”, em *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Zaragoza, Spain, set. 2019, p. 325–332. doi: 10.1109/ETFA.2019.8869524.
[78] R. Ankele, S. Marksteiner, K. Nahrgang, e H. Vallant, “Requirements and Recommendations for IoT/IIoT Models to automate Security Assurance through Threat Modelling, Security Analysis and Penetration Testing”, em *Proceedings of the 14th International Conference on Availability, Reliability and Security*, Canterbury CA United Kingdom, ago. 2019, p. 1–8. doi: 10.1145/3339252.3341482.
[79] P. Papcun, E. Kajati, D. Cupkova, J. Mocnej, M. Miskuf, e I. Zolotova, “Edge-enabled IoT gateway criteria selection and evaluation”, *Concurr. Comput. Pract. Exp.*, vol. 32, nº 13, jul. 2020, doi: 10.1002/cpe.5219.
[80] M. Kamalrudin, A. A. Ibrahim, e S. Sidek, “A Security Requirements Library for the Development of Internet of Things (IoT) Applications”, em *Requirements Engineering for*

Internet of Things, vol. 809, M. Kamalrudin, S. Ahmad, e N. Ikram, Orgs. Singapore: Springer Singapore, 2018, p. 87–96. doi: 10.1007/978-981-10-7796-8_7.
[81] V. R. Kebande, N. K. Menza, e H. S. Venter, "Functional Requirements for Adding Digital Forensic Readiness as a Security Component in IoT Environments", *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, nº 2, p. 342, mar. 2018, doi: 10.18517/ijaseit.8.2.2121.
[82] W. Ali, G. Dustgeer, M. Awais, e M. A. Shah, "IoT based Smart Home: Huddersfield, UK, 7-8 September 2017 Security Challenges, Security Requirements and Solutions", p. 6.
[83] S.-R. Oh e Y.-G. Kim, "Security Requirements Analysis for the IoT", p. 6.
[84] S. Jaiswal e D. Gupta, "Security Requirements for Internet of Things (IoT)", em *Proceedings of International Conference on Communication and Networks*, vol. 508, N. Modi, P. Verma, e B. Trivedi, Orgs. Singapore: Springer Singapore, 2017, p. 419–427. doi: 10.1007/978-981-10-2750-5_44.
[85] J. D. Parra Rodriguez, D. Schreckling, e J. Posegga, "Addressing Data-Centric Security Requirements for IoT-Based Systems", em *2016 International Workshop on Secure Internet of Things (SIoT)*, Heraklion, 2016, p. 1–10. doi: 10.1109/SIoT.2016.007.
[86] "Business Process Model and Notation (BPMN)", p. 538.
[87] "Eclipse Kura™ Documentation". http://eclipse.github.io/kura/ (acessado 27 de março de 2021).
[88] "ThingsBoard IoT Gateway Documentation", *ThingsBoard*. https://thingsboard.io/docs/iot-gateway/ (acessado 21 de março de 2021).
[89] "WebIOPi Gateway Documentation". http://webiopi.trouch.com/ (acessado 21 de março de 2021).
[90] "WebThings Documentation", *WebThings Documentation*. https://webthings.io/docs/ (acessado 20 de março de 2021).
[91] "Robot Framework". https://robotframework.org/ (acessado 3 de março de 2022).
[92] W.-K. Chen, C.-H. Liu, W. W.-Y. Liang, e M.-Y. Tsai, "ICAT: An IoT Device Compatibility Testing Tool", em *2018 25th Asia-Pacific Software Engineering Conference (APSEC)*, Nara, Japan, dez. 2018, p. 668–672. doi: 10.1109/APSEC.2018.00087.
[93] "Selenium Library". https://github.com/robotframework/SeleniumLibrary (acessado 3 de março de 2022).
[94] "Selenium Library". https://robotframework.org/SeleniumLibrary/SeleniumLibrary.html (acessado 3 de março de 2022).

Apêndice A

Gateway Authentication Requirement (GAR)

NUMBER	ORIGIN	REQUIREMENT DESCRIPTION
GAR 01	OWASP, 2.1.1	Verify that all forms of users and accounts in the IoT ecosystem can be uniquely identified.
GAR 02	OWASP, 2.1.2	Verify that all connected devices within the IoT ecosystem can be uniquely identified including connected to the cloud, hubs, as well as to other devices (sensors).
GAR 03	OWASP, 2.1.3	Verify strong user and device authentication is enforced across the IoT ecosystem.
GAR 04	OWASP, 2.1.4	Verify that user, services, and device authentication schemes share a common framework centrally managed in the IoT ecosystem.
GAR 05	OWASP, 2.1.5	Verify certificate-based authentication is preferred over password-based authentication within the IoT ecosystem.
GAR 06	OWASP, 2.1.6	Verify good password policies are enforced throughout the IoT ecosystem by disallowing hardcoded passwords and provisioning duplicate identities or passwords across devices.
GAR 07	OWASP, 2.1	Verify all pages and resources by default require authentication except those specifically intended to be public (Principle of complete mediation).
GAR 08	OWASP, 2.2	Verify that all password fields do not echo the user's password when it is entered.
GAR 09	OWASP, 2.4	Verify all authentication controls are enforced on the server side.
GAR 10	OWASP, 2.6	Verify all authentication controls fail securely to ensure attackers cannot log in.
GAR 11	OWASP, 2.7	Verify password entry fields allow, or encourage, the use of passphrases, and do not prevent long passphrases/highly complex passwords being entered.
GAR 12	OWASP, 2.8	Verify all account identity authentication functions (such as update profile, forgot password, disabled / lost token, help desk or IVR) that might regain access to the account are at least as resistant to attack as the primary authentication mechanism.
GAR 13	OWASP, 2.9	Verify that the changing password functionality includes the old password, the new password, and a password confirmation.
GAR 14	OWASP, 2.12	Verify that all suspicious authentication decisions are logged. This should include requests with relevant metadata needed for security investigations.
GAR 15	OWASP, 2.13	Verify that account passwords make use of a sufficient strength encryption routine and that it withstands brute force attack against the encryption routine.
GAR 16	OWASP, 2.16	Verify that credentials are transported using a suitable encrypted link and that all pages/functions that require a user to enter credentials are done so using an encrypted link.
GAR 17	OWASP, 2.17	Verify that the forgotten password function and other recovery paths do not reveal the current password and that the new password is not sent in clear text to the user.
GAR 18	OWASP, 2.18	Verify that information enumeration is not possible via login, password reset, or forgot account functionality.
GAR 19	OWASP, 2.19	Verify there are no default passwords in use for the application framework or any components used by the application (such as "admin/password").
GAR 20	OWASP, 2.20	Verify that request throttling is in place to prevent automated attacks against common authentication attacks such as brute force attacks or denial of service attacks.

GAR 21	OWASP, 2.21	Verify that all authentication credentials for accessing services external to the application are encrypted and stored in a protected location.
GAR 22	OWASP, 2.22	Verify that forgotten password and other recovery paths use a soft token, mobile push, or an offline recovery mechanism.
GAR 23	OWASP, 2.23	Verify that account lockout is divided into soft and hard lock status, and these are not mutually exclusive. If an account is temporarily soft locked out due to a brute force attack, this should not reset the hard lock status.
GAR 24	OWASP, 2.24	Verify that if knowledge-based questions (also known as "secret questions") are required, the questions should be strong enough to protect the application.
GAR 25	OWASP, 2.25	Verify that the system can be configured to disallow the use of a configurable number of previous passwords.
GAR 26	OWASP, 2.26	Verify re-authentication, step up or adaptive authentication, two factor authentication, or transaction signing is required before any application-specific sensitive operations are permitted as per the risk profile of the application.
GAR 27	OWASP, 2.27	Verify that measures are in place to block the use of commonly chosen passwords and weak passphrases.
GAR 28	OWASP, 2.28	Verify that all authentication challenges, whether successful or failed, should respond in the same average response time.
GAR 29	OWASP, 2.29	Verify that secrets, API keys, and passwords are not included in the source code, or online source code repositories.
GAR 30	OWASP, 2.30	Verify that if an application allows users to authenticate, they use a proven secure authentication mechanism.
GAR 31	OWASP, 2.31	Verify that if an application allows users to authenticate, they can authenticate using two-factor authentication or other strong authentication, or any similar scheme that provides protection against username + password disclosure.
GAR 32	OWASP, 2.32	Verify that administrative interfaces are not accessible to untrusted parties
GAR 33	IoTSF, 2.4.8.1	The product contains a unique and tamper-resistant device identifier (e.g. the chip serial number or other unique silicon identifier) for example binding code and data to a specific device hardware. This is to mitigate threats from cloning.
GAR 34	IoTSF, 2.4.8.2	Where the product has a secure source of time there is a method of validating its integrity, such as Secure NTP: https://www.ntpsec.org.
GAR 35	IoTSF, 2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is unique to each device in the product family. If a password-less authentication is used the same principles of uniqueness apply.
GAR 36	IoTSF, 2.4.8.4	The product does not accept the use of null or blank passwords.
GAR 37	IoTSF, 2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.
GAR 38	IoTSF, 2.4.8.6	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 password policy [ref 17] or NIST SP800-63b Digital Identity Guidelines - Authentication and Lifecycle Management" [ref 26] or NCSC [ref 48] on password length, characters from the groupings and special characters.
GAR 39	IoTSF, 2.4.8.7	The product has defense against brute force repeated login attempts, such as exponentially increasing delays with each retry attempt.
GAR 40	IoTSF, 2.4.8.8	The product securely stores any passwords using an industry standard cryptographic algorithm, compliant with an industry standard such as NIST SP800-63b [ref 26] or similar.
GAR 41	IoTSF, 2.4.8.9	The product supports access control measures to the root/highest privilege account to restrict access to sensitive information or system processes.

GAR 42	IoTSF, 2.4.8.10	The access control privileges are defined, justified, and documented.
GAR 43	IoTSF, 2.4.8.11	The product only allows controlled user account access; access using anonymous, or guest user accounts is not supported without justification.
GAR 44	IoTSF, 2.4.8.12	The product allows the factory issued or OEM login accounts to be disabled, erased, or renamed when installed or commissioned.
GAR 45	IoTSF, 2.4.8.13	The product supports having any or all of the factory default user login passwords altered when installed or commissioned.
GAR 46	IoTSF, 2.4.8.14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism cannot readily be abused by an unauthorized party.
GAR 47	IoTSF, 2.4.8.15	Where passwords are entered on a user interface, the actual pass phrase is obscured by default.
GAR 48	IoTSF, 2.4.8.16	The product allows an authorized and complete factory reset and all of the device's authorization information.
GAR 49	IoTSF, 2.4.8.17	Where the product has the ability to remotely recover from attack, it should rely on a known good state, to enable safe recovery and updating of the device
GAR 50	ENISA, GP-TM-21	Design the authentication and authorization schemes (unique per device) based on the system-level threat models.
GAR 51	ENISA, GP-TM-22	Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.
GAR 52	ENISA, GP-TM-23	Authentication mechanisms must use strong passwords or personal identification numbers (PINs) and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates.
GAR 53	ENISA, GP-TM-24	Authentication credentials shall be salted, hashed and/or encrypted.
GAR 54	ENISA, GP-TM-25	Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.
GAR 55	ENISA, GP-TM-26	Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.
GAR 56	ETSI, Provisão 5.1-1	Where passwords are used and, in any state, other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.
GAR 57	ETSI, Provisão 5.1-2	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.
GAR 58	ETSI, Provisão 5.1-3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk, and usage.
GAR 59	ETSI, Provisão 5.1-4	Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.
GAR 60	ETSI, Provisão 5.1-5	When the device is not a constrained device, it shall have a mechanism available which makes brute force attacks on authentication mechanisms via network interfaces impracticable.
GAR 61	ETSI, Provisão 5.5-5	Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate

GAR 62	OTA, 03	All IoT support websites must fully encrypt the user session from the device to the backend services. Current best practices include HTTPS and HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.1
GAR 63	OTA, 13	Include strong authentication by default, including providing unique, system-generated, or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets.
GAR 64	OTA, 14	Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential reset using multi-factor verification and authentication (email and phone, etc.) where no user password exists.
GAR 65	OTA, 16	Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).
GAR 66	OTA, 17	Authentication credentials, including but not limited to user passwords, shall be salted, hashed and/or encrypted. Applies to all stored credentials to help prevent unauthorized access and brute force attacks.
GAR 67	GSMA, CLP13_6. 12.1.14	Are your endpoints that require remote administration architecture in a way that ensures that administrative credentials cannot be abused by an attacker?

Fonte: O autor (2022).

Apêndice B

Gateway Authentication Requirement Evaluation Report

NUMBER	ORIGIN	REQUIREMENT DESCRIPTION	GATEWAYS			
			GW_01	GW_02	GW_03	GW_04
GAR 01	OWASP, 2.1.1	Verify that all forms of users and accounts in the IoT ecosystem can be uniquely identified.	Compliant	Not Compliant	Compliant	Compliant
GAR 02	OWASP, 2.1.2	Verify that all connected devices within the IoT ecosystem can be uniquely identified including connected to the cloud, hubs, as well as to other devices (sensors).	Compliant	Not Compliant	Compliant	Compliant
GAR 03	OWASP, 2.1.3	Verify strong user and device authentication is enforced across the IoT ecosystem.	Partially Compliant[2]	Not Compliant	Partially Compliant[2]	Partially Compliant[1]
GAR 04	OWASP, 2.1.4	Verify that user, services, and device authentication schemes share a common framework centrally managed in the IoT ecosystem.	Compliant	Compliant	Compliant	Compliant
GAR 05	OWASP, 2.1.5	Verify certificate-based authentication is preferred over password-based authentication within the IoT ecosystem.	Partially Compliant[1]	Not Compliant	Partially Compliant[1]	Partially Compliant[1]
GAR 06	OWASP, 2.1.6	Verify good password policies are enforced throughout the IoT ecosystem by disallowing hardcoded passwords and provisioning duplicate identities or passwords across devices.	Partially Compliant[2]	Partially Compliant[2]	Partially Compliant[2]	Partially Compliant[1]
GAR 07	OWASP, 2.1	Verify all pages and resources by default require authentication except those specifically intended to be public (Principle of complete mediation).	Compliant	Not Compliant	Compliant	Compliant
GAR 08	OWASP, 2.2	Verify that all password fields do not echo the user's password when it is entered.	Compliant	Compliant	Compliant	Compliant
GAR 09	OWASP, 2.4	Verify all authentication controls are enforced on the server side.	Compliant	Not Compliant	Compliant	Compliant
GAR 10	OWASP, 2.6	Verify all authentication controls fail securely to ensure attackers cannot log in.	Compliant	Not Compliant	Compliant	Compliant
GAR 11	OWASP, 2.7	Verify password entry fields allow, or encourage, the use of passphrases, and do not prevent long passphrases/highly complex passwords being entered.	Partially Compliant[2]	Not Compliant	Partially Compliant[2]	Partially Compliant[2]
GAR 12	OWASP, 2.8	Verify all account identity authentication functions (such as update profile, forgot password, disabled / lost token, help desk or IVR) that might regain access to the account are at least as resistant to attack as the primary authentication mechanism.	Partially Compliant[2]	Not Compliant	Not Compliant	Compliant
GAR 13	OWASP, 2.9	Verify that the changing password functionality includes the old password, the new password, and a password confirmation.	Compliant	Partially Compliant[2]	Partially Compliant[2]	Compliant

GAR 14	OWASP, 2.12	Verify that all suspicious authentication decisions are logged. This should include requests with relevant metadata needed for security investigations.	Compliant	Not Compliant	Compliant	Compliant
GAR 15	OWASP, 2.13	Verify that account passwords make use of a sufficient strength encryption routine and that it withstands brute force attack against the encryption routine.	Partially Compliant[2]	Partially Compliant[2]	Compliant	Compliant
GAR 16	OWASP, 2.16	Verify that credentials are transported using a suitable encrypted link and that all pages/functions that require a user to enter credentials are done so using an encrypted link.	Compliant	Compliant	Compliant	Compliant
GAR 17	OWASP, 2.17	Verify that the forgotten password function and other recovery paths do not reveal the current password and that the new password is not sent in clear text to the user.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 18	OWASP, 2.18	Verify that information enumeration is not possible via login, password reset, or forgot account functionality.	Compliant	Compliant	Compliant	Compliant
GAR 19	OWASP, 2.19	Verify there are no default passwords in use for the application framework or any components used by the application (such as “admin/password”).	Compliant	Not Compliant	Not Compliant	Not Compliant
GAR 20	OWASP, 2.20	Verify that request throttling is in place to prevent automated attacks against common authentication attacks such as brute force attacks or denial of service attacks.	Compliant	Not Compliant	Partially Compliant[2]	Partially Compliant[1]
GAR 21	OWASP, 2.21	Verify that all authentication credentials for accessing services external to the application are encrypted and stored in a protected location.	Compliant	Not Compliant	Compliant	Compliant
GAR 22	OWASP, 2.22	Verify that forgotten password and other recovery paths use a soft token, mobile push, or an offline recovery mechanism.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 23	OWASP, 2.23	Verify that account lockout is divided into soft and hard lock status, and these are not mutually exclusive. If an account is temporarily soft locked out due to a brute force attack, this should not reset the hard lock status.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 24	OWASP, 2.24	Verify that if knowledge-based questions (also known as “secret questions”) are required, the questions should be strong enough to protect the application.	Not Compliant	Not Compliant	Not Compliant	Not Compliant
GAR 25	OWASP, 2.25	Verify that the system can be configured to disallow the use of a configurable number of previous passwords.	Partially Compliant[2]	Not Compliant	Partially Compliant[2]	Partially Compliant[2]
GAR 26	OWASP, 2.26	Verify re-authentication, step up or adaptive authentication, two factor authentication, or transaction signing is required before any application-specific sensitive operations are permitted as per the risk profile of the application.	Not Compliant	Not Compliant	Not Compliant	Not Compliant
GAR 27	OWASP, 2.27	Verify that measures are in place to block the use of commonly chosen passwords and weak passphrases.	Partially Compliant[2]	Partially Compliant[2]	Partially Compliant[2]	Partially Compliant[1]
GAR 28	OWASP, 2.28	Verify that all authentication challenges, whether successful or failed, should respond in the same average response time.	Compliant	Compliant	Compliant	Compliant
GAR 29	OWASP, 2.29	Verify that secrets, API keys, and passwords are not included in the source code, or online source code repositories.	Compliant	Compliant	Compliant	Compliant

GAR 30	OWASP, 2.30	Verify that if an application allows users to authenticate, they use a proven secure authentication mechanism.	Partially Compliant[1]	Not Compliant	Partially Compliant[2]	Partially Compliant[1]
GAR 31	OWASP, 2.31	Verify that if an application allows users to authenticate, they can authenticate using two-factor authentication or other strong authentication, or any similar scheme that provides protection against username + password disclosure.	Compliant	Not Compliant	Partially Compliant[2]	Compliant
GAR 32	OWASP, 2.32	Verify that administrative interfaces are not accessible to untrusted parties	Not Compliant	Not Compliant	Not Compliant	Not Compliant
GAR 33	IoTSF, 2.4.8.1	The product contains a unique and tamper-resistant device identifier (e.g. the chip serial number or other unique silicon identifier) for example binding code and data to a specific device hardware. This is to mitigate threats from cloning	Compliant	Not Compliant	Compliant	Compliant
GAR 34	IoTSF, 2.4.8.2	Where the product has a secure source of time there is a method of validating its integrity, such as Secure NTP: https://www.ntpsec.org.	Compliant	Not Compliant	Compliant	Compliant
GAR 35	IoTSF, 2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is unique to each device in the product family. If a password-less authentication is used the same principles of uniqueness apply.	Compliant	Not Compliant	Partially Compliant[2]	Compliant
GAR 36	IoTSF, 2.4.8.4	The product does not accept the use of null or blank passwords.	Compliant	Partially Compliant[2]	Compliant	Compliant
GAR 37	IoTSF, 2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.	Partially Compliant[2]	Not Compliant	Partially Compliant[2]	Partially Compliant[2]
GAR 38	IoTSF, 2.4.8.6	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 password policy [ref 17] or NIST SP800-63b Digital Identity Guidelines - Authentication and Lifecycle Management" [ref 26] or NCSC [ref 48] on password length, characters from the groupings and special characters.	Partially Compliant[2]	Not Compliant	Partially Compliant[2]	Partially Compliant[1]
GAR 39	IoTSF, 2.4.8.7	The product has defense against brute force repeated login attempts, such as exponentially increasing delays with each retry attempt.	Partially Compliant[2]	Not Compliant	Partially Compliant[2]	Partially Compliant[1]
GAR 40	IoTSF, 2.4.8.8	The product securely stores any passwords using an industry standard cryptographic algorithm, compliant with an industry standard such as NIST SP800-63b [ref 26] or similar.	Compliant	Partially Compliant[2]	Compliant	Compliant
GAR 41	IoTSF, 2.4.8.9	The product supports access control measures to the root/highest privilege account to restrict access to sensitive information or system processes.	Compliant	Not Compliant	Partially Compliant[2]	Compliant
GAR 42	IoTSF, 2.4.8.10	The access control privileges are defined, justified, and documented.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 43	IoTSF, 2.4.8.11	The product only allows controlled user account access; access using anonymous, or guest user accounts is not supported without justification.	Partially Compliant[1]	Not Compliant	Partially Compliant[2]	Compliant
GAR 44	IoTSF, 2.4.8.12	The product allows the factory issued or OEM login accounts to be disabled, erased, or renamed when installed or commissioned.	Compliant	Partially Compliant[1]	Not Compliant	Compliant

GAR 45	IoTSF, 2.4.8.13	The product supports having any or all the factory default user login passwords altered when installed or commissioned.	Compliant	Compliant	Compliant	Compliant
GAR 46	IoTSF, 2.4.8.14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism cannot readily be abused by an unauthorized party.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 47	IoTSF, 2.4.8.15	Where passwords are entered on a user interface, the actual pass phrase is obscured by default.	Compliant	Compliant	Compliant	Compliant
GAR 48	IoTSF, 2.4.8.16	The product allows an authorized and complete factory reset and all the device's authorization information.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 49	IoTSF, 2.4.8.17	Where the product has the ability to remotely recover from attack, it should rely on a known good state, to enable safe recovery and updating of the device	Not Compliant	Not Compliant	Not Compliant	Not Compliant
GAR 50	ENISA, GP-TM-21	Design the authentication and authorization schemes (unique per device) based on the system-level threat models.	Compliant	Not Compliant	Partially Compliant[2]	Compliant
GAR 51	ENISA, GP-TM-22	Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null, or blank passwords are not allowed.	Partially Compliant[2]	Partially Compliant[2]	Partially Compliant[2]	Partially Compliant[1]
GAR 52	ENISA, GP-TM-23	Authentication mechanisms must use strong passwords or personal identification numbers (PINs) and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates.	Partially Compliant[1]	Not Compliant	Partially Compliant[2]	Partially Compliant[1]
GAR 53	ENISA, GP-TM-24	Authentication credentials shall be salted, hashed and/or encrypted.	Partially Compliant[2]	Partially Compliant[2]	Compliant	Compliant
GAR 54	ENISA, GP-TM-25	Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.	Compliant	Not Compliant	Partially Compliant[2]	Partially Compliant[1]
GAR 55	ENISA, GP-TM-26	Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 56	ETSI, Provisão 5.1-1	Where passwords are used and, in any state, other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.	Compliant	Not Compliant	Partially Compliant[2]	Compliant
GAR 57	ETSI, Provisão 5.1-2	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 58	ETSI, Provisão 5.1-3	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk, and usage.	Partially Compliant[2]	Partially Compliant[2]	Compliant	Compliant
GAR 59	ETSI, Provisão	Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value	Compliant	Not Compliant	Not Compliant	Compliant

	5.1-4	used.				
GAR 60	ETSI, Provisão 5.1-5	When the device is not a constrained device, it shall have a mechanism available which makes brute force attacks on authentication mechanisms via network interfaces impracticable.	Compliant	Not Compliant	Partially Compliant[2]	Partially Compliant[1]
GAR 61	ETSI, Provisão 5.5-5	Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate	Not Compliant	Not Compliant	Not Compliant	Not Compliant
GAR 62	OTA, 03	All IoT support websites must fully encrypt the user session from the device to the backend services. Current best practices include HTTPS and HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.1	Compliant	Not Compliant	Compliant	Compliant
GAR 63	OTA, 13	Include strong authentication by default, including providing unique, system-generated, or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets.	Compliant	Not Compliant	Not Compliant	Compliant
GAR 64	OTA, 14	Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential reset using multi-factor verification and authentication (email and phone, etc.) where no user password exists.	Not Compliant	Not Compliant	Not Compliant	Compliant
GAR 65	OTA, 16	Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	Not Compliant	Not Compliant	Not Compliant	Partially Compliant[1]
GAR 66	OTA, 17	Authentication credentials, including but not limited to user passwords, shall be salted, hashed and/or encrypted. Applies to all stored credentials to help prevent unauthorized access and brute force attacks.	Partially Compliant[2]	Partially Compliant[2]	Compliant	Compliant
GAR 67	GSMA, CLP13_6.12.1.14	Are your endpoints that require remote administration architecture in a way that ensures that administrative credentials cannot be abused by an attacker?	Partially Compliant[1]	Not Compliant	Partially Compliant[2]	Partially Compliant[1]

Fonte: O autor (2022).

Apêndice C

Figura 24 – Recurso com palavras-chave e variáveis reutilizáveis

```
*** Settings ***
Documentation     Recurso com palavras-chave e variaveis reutilizaveis.

Library           SeleniumLibrary

*** Variables ***
${SERVER}         localhost:4443
${BROWSER}        Chrome
${DELAY}          0.2
${VALID USER}     brseclab@ufrpe.br
${VALID PASSWORD} brseclab
${LOGIN URL}      https://localhost:4443/login/
${Main URL}    https://localhost:4443/

*** Keywords ***
Open Browser To Login Page
    Open Browser    ${LOGIN URL}    ${BROWSER}      options=add_argument("--ignore-certificate-errors")
    Set Selenium Speed    ${DELAY}
    Set Selenium Timeout  2
    Login Page Should Be Open

Login Page Should Be Open
    Title Should Be    Login - GW_01

Go To Login Page
    Go To    ${LOGIN URL}
    Login Page Should Be Open

Input Username
    [Arguments]    ${username}
    Input Text    email   ${username}

Input Password
    [Arguments]    ${password}
    Input Text    password   ${password}

Submit Credentials
    Click Button    login-button

Main Page Should Be Open
    Location Should Be    ${Main URL}
    Title Should Be    GW_01
```

Fonte: O autor (2022).

Figura 25 – Caso de testes de credenciais válidas

```
*** Settings ***
Documentation     Caso de testes de credenciais validas

Resource          resource.robot

*** Test Cases ***
Valid Login
    Open Browser To Login Page
    Input Username    ${VALID USER}
    Input Password    ${VALID PASSWORD}
    Submit Credentials
    Main Page Should Be Open
    [Teardown]    Close Browser
```

Fonte: O autor (2022).