



UEPB

**UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS (CCEA)
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO**

CLEIVERSON DE MEDEIROS FRANÇA

**SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS: ESTUDO DE
CASO COM A *THINGER.IO* PLATFORM**

**PATOS - PB
2022**

CLEIVERSON DE MEDEIROS FRANÇA

SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS: ESTUDO DE CASO COM A *THINGER.IO* PLATFORM

Trabalho de Conclusão de Curso apresentado ao curso de Graduação em Bacharel em Ciência da Computação da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Ciência da Computação.

Área de concentração: Internet das Coisas.

Orientador: Prof. MSc. Ingrid Morgane Medeiros de Lucena

**PATOS - PB
2022**

É expressamente proibido a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano do trabalho.

F814s França, Cleiverson de Medeiros.
Segurança e privacidade na internet das coisas
[manuscrito] : estudo de caso com a *Thingier.io Platform* /
Cleiverson de Medeiros Franca. - 2022.
38 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em
Computação) - Universidade Estadual da Paraíba, Centro de
Ciências Exatas e Sociais Aplicadas, 2022.

"Orientação : Profa. Ma. Ingrid Morgane Medeiros de
Lucena, Coordenação do Curso de Computação - CCEA."

1. Internet das Coisas. 2. Thingier. 3. Ambientes
inteligentes. 4. Segurança. I. Título

21. ed. CDD 004.678

CLEIVERSON DE MEDEIROS FRANÇA

SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS: ESTUDO DE CASO COM A THINGER.IO PLATFORM.

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Ciência da Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado em 28/03/2022

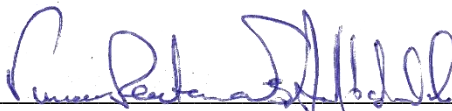
BANCA EXAMINADORA



Prof. Me Ingrid Morgane Medeiros de Lucena
(Orientadora)



Prof. Me Francisco Anderson Mariano da Silva
(Examinador)



Prof. Vinícius Reuteman Feitoza Alves de Andrade
(Examinador)

AGRADECIMENTOS

Agradeço a Deus, por me dar paciência e coragem para persistir nesta jornada.

À minha família, por me apoiar em todos os momentos da minha vida.

À minha noiva, Aline Gírlene, pelo incentivo e apoio a todo momento.

Aos amigos que conquistei ao longo dessa jornada.

Aos professores do curso de Bacharel em Ciência da Computação, em especial a Profa. Ingrid Morgane Medeiros de Lucena, pelo seu tempo e orientações no decorrer deste trabalho.

E a todos, que de forma direta e indireta fizeram parte da minha formação.

RESUMO

A Internet das Coisas vem objetivando ambientes inteligentes e que sejam interativos através de dispositivos denominados de Coisas, a quantidade destes dispositivos tem crescido de forma rápida e o crescimento desenfreado desses dispositivos conectados, somados ao baixo custo e por vezes, o tamanho compacto e multifuncional, fazem com que conseqüentemente ganhe uma relevância junto ao mundo globalizado, e em virtude disso, acaba surgindo um aumento em pesquisas acadêmicas a respeito. Dito isso, essa pesquisa tem o objetivo de analisar as soluções de segurança e privacidade por meio de um estudo de caso da plataforma *Thingier.io*. Neste contexto, as plataformas funcionam como *Softwares Middlewares*, que fazem o papel de intermediador para padronizar e acelerar o desenvolvimento desse paradigma. Sendo assim, o cenário descrito faz com que esse estudo se torne relevante para o desenvolvimento da área e conseqüentemente responder se a plataforma *Thingier.io* pode ser considerada uma boa escolha para o desenvolvimento de aplicações para Internet das Coisas.

Palavras-Chave: Internet das Coisas. *Thingier*. Ambientes inteligentes. Segurança.

ABSTRACT

The Internet of Things has been aiming at intelligent environments that are interactive through devices called Things, the number of these devices has grown rapidly and the unbridled growth of these connected devices, added to the low cost and sometimes the compact and multifunctional size, make it consequently gain relevance in the globalized world, and as a result, there is an increase in academic research on the subject. That said, this research aims to analyze security and privacy solutions through a case study of the Thinger.io platform. In this context, the platforms work as Software Middlewares, which play the role of intermediary to standardize and accelerate the development of this paradigm. Therefore, the scenario described makes this study relevant for the development of the area and, consequently, to answer whether the Thinger.io platform can be considered a good choice for the development of applications for the Internet of Things.

Keywords: Internet of Things. Thing. Smart environments. Security.

LISTA DE ILUSTRAÇÕES

Figura 1 - Principais recursos do <i>Thingier.io</i>	17
Figura 2 - Visão geral da plataforma <i>Thingier.io</i>	22
Figura 3 - Comparação de codificação (bytes)	24
Figura 4 - Funcionamento dos certificados SSL / TLS.....	25
Figura 5 - Conversão de modelo de dispositivo para API REST.....	26
Figura 6 - Arduino com <i>Ethernet Shield</i>	29
Figura 7 - Dispositivo Arduino com biblioteca <i>Thingier.io</i>	29
Figura 8 - Visão geral do armazenamento de <i>Big Data</i> do <i>Thingier.io</i>	30

LISTA DE ABREVIATURAS E SIGLAS

API	Application Programming Interface
CDTI	Centre for the Development of Industrial Technology
CoAP	Constrained Application Protocol
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things (Internet das Coisas)
IP	Internet Protocol
LPWAN	Low Power Wide Area Network
MQTT	Message Queuing Telemetry Transport
OTA	Over-The-Air update
P&G	Procter & Gamble
PaaS	Platform as a Service
RAID	Redundant Array of Inexpensive Disks
REST	Representational State Transfer
RFID	Radio-Frequency Identification
SSL	Secure Sockets Layer
TICs	Tecnologias de informação e comunicação
TLS	Transport Layer Security

SUMÁRIO

1.	INTRODUÇÃO	9
1.1.	Objetivos	10
1.1.1.	Objetivo Geral.....	10
1.1.2.	<i>Objetivos Específicos</i>	11
1.2.	Justificativa	11
2.	INTERNET DAS COISAS	12
2.1.	Aplicações e importância para a sociedade	13
2.2.	Desafios enfrentados pela iot	14
2.3.	Plataformas de IoT	15
2.3.1.	<i>Thingier.io Platform</i>	16
2.4.	Segurança da informação e privacidade dos dados	18
2.4.1.	<i>Confidencialidade</i>	19
2.4.2.	<i>Integridade</i>	19
2.4.3.	<i>Disponibilidade</i>	20
3.	METODOLOGIA	21
4.	AVALIAÇÃO DA PLATAFORMA	22
4.1.	Arquitetura da plataforma	22
4.1.1.	<i>Comunicação bidirecional em tempo real</i>	23
4.1.2.	<i>Protocolos de comunicação</i>	23
4.1.3.	<i>Protocolos de segurança</i>	25
4.1.4.	<i>Interoperabilidade</i>	26
4.1.5.	<i>Tokens de acesso</i>	27
4.1.6.	<i>Over-The-Air update (OTA)</i>	28
4.2.	Compatibilidade com Arduino	28
4.3.	Gerenciamento de armazenamento	30
5.	RESULTADOS	32
6.	CONSIDERAÇÕES FINAIS	34
	REFERÊNCIAS	35

1. INTRODUÇÃO

Mais conhecida como IoT (Internet of *Things*), a Internet das Coisas é considerada por muitos como o futuro da Internet, o termo descreve um cenário onde inúmeros objetos do seu dia a dia estarão conectados à Internet se comunicando mutuamente. Esta tecnologia está em pleno desenvolvimento e tem tudo para mudar a forma como as pessoas veem e usam os seus dispositivos eletrônicos (EVANS, 2011).

A proposta da IoT é tornar objetos considerados comuns em objetos inteligentes, tornando-os mais eficientes recebendo atributos complementares e sendo melhor utilizados (MCEWEN; CASSIMALLY, 2013). Desse modo, o objetivo é fazer com que objetos gerem mais utilidades e conseqüentemente maior interesse do usuário, podendo ser controlados remotamente e usados como forma de auxílio autônomo em diversas outras atividades, em suma, o intuito da IoT é melhorar a qualidade de vida dos usuários através do uso de objetos inteligentes conectados.

Esse paradigma idealizado pela IoT possibilita a criação de um mundo de objetos físicos embarcados com sensores e atuadores, onde uma vez conectados à Internet, formam uma rede de objetos inteligentes capazes de realizar diversos processamentos, capturar variáveis ambientais e reagir a estímulos externos (ATZORI *et al*, 2010).

Esses objetos possuem aplicações para as mais diversas áreas, desde saúde, agropecuária, indústrias, comércio, logística, passando pelas cidades inteligentes onde podemos encontrar o uso de sensores posicionados em pontos estratégicos para detectar eventos da natureza, câmeras auxiliadas por inteligência artificial, semáforos inteligentes, sistemas solares entre outras, fazendo com que a influência da IoT na vida de todas as pessoas seja enorme, mesmo que direta ou indiretamente.

Alguns fatores geram preocupação com a popularização da IoT, pois com o aumento iminente da IoT será preciso que tecnologias existentes sejam adaptadas para suportar o aumento massivo de conexões que serão necessárias, assim como gerenciar o grande volume de dados gerados por esses dispositivos. Outro fator preocupante é a questão da segurança e da privacidade dos dados gerados por esses dispositivos, a Cisco¹, uma das maiores empresas de redes e Internet do mundo,

¹ Disponível em: <https://www.cisco.com>. Acesso em: 27 ago. 2022.

considera que embora exista muito progresso nessa área, ainda não é o suficiente, mas que isso será apenas uma questão de tempo (EVANS, 2011).

Dessa forma, com o objetivo de facilitar a resolução de problemas e contribuir com o aceleração do desenvolvimento de novas aplicações para a IoT surgem no mercado as PaaS (Platform as a Service) ou plataformas como serviço, dedicadas à IoT (BANDYOPADHYAY *et al*, 2011).

Bandyopadhyay *et al* (2011) diz ainda que uma plataforma de IoT é um *software* Middleware que atua como intermediário entre o usuário e suas Coisas, fornecendo uma infinidade de conjuntos de componentes e recursos que possibilita a programação e o gerenciamento completo dos dispositivos a ela conectados. Essas plataformas são inseridas entre as aplicações e a infraestrutura (de comunicação, processamento e sensoriamento) subjacente, com o objetivo de padronizar o acesso aos dados e os serviços fornecidos pelos objetos inteligentes por meio de uma interface de alto nível.

Assim sendo, o objetivo da pesquisa é fazer uma avaliação conceitual sobre as características da plataforma de IoT, *Thingier.io*, tendo como pontos específicos as suas funcionalidades de Segurança da Informação e de privacidade de dados que são implementados pela plataforma. A ideia é contribuir com o desenvolvimento da área da IoT, identificando as melhores práticas e possíveis melhorias e problemas que existem na versão *Open Source* da plataforma.

No desenvolvimento da pesquisa foram feitas buscas literárias sobre os conceitos relacionados a IoT, bem como suas plataformas e privacidade de dados e Segurança da Informação. Em seguida, os conceitos teóricos obtidos foram utilizados para a produção do desenvolvimento da análise, onde serão avaliadas as técnicas de segurança e de privacidade que compõem a plataforma *Thingier.io*.

1.1. Objetivos

1.1.1. Objetivo Geral

Realizar uma avaliação conceitual acerca das configurações de segurança e de privacidade implementadas pela plataforma *Thingier.io* em sua versão 3.4.6.

1.1.2. Objetivos Específicos

- Reconhecer a veracidade das informações contidas na documentação oficial da plataforma;
- Identificar as vantagens e limitações das técnicas de segurança e privacidade utilizadas na plataforma;
- Fazer uma análise das primitivas usadas na plataforma e verificar se a mesma possibilita escalabilidade das soluções de segurança e privacidade.

1.2. Justificativa

O estudo se justifica pelo fato de o tema ser bastante relevante na conjuntura que vivemos, pois cada vez mais se tem um aumento dos dispositivos conectados a Internet, gerando uma maior quantidade de tráfego de dados demandando um aumento na relevância do estudo da privacidade, uma vez que um grande volume de dados gera informações que precisam estar seguras e privadas.

O mundo atualmente está interligando pessoas e dispositivos de tal forma que passamos a viver um paradigma no qual é difícil imaginar o que não estará conectado em um futuro próximo. O avanço da IoT no cotidiano das pessoas proporciona uma vida facilitada e mais prática por meio de ambientes interligados e responsivos e com isso a preocupação com a segurança dos dados passou a ser algo bastante estudado nessa área (OLIVEIRA, 2017).

Sendo assim, se torna relevante analisar e avaliar conceitualmente a plataforma de IoT *Thinger.io* sob a perspectiva da privacidade dos dados gerados pelas Coisas que a ela serão conectados e assim contribuir para o avanço tecnológico da IoT.

2. INTERNET DAS COISAS

A Internet das Coisas é um termo usado para definir o conceito de transformar objetos simples do dia a dia considerados 'burros' em equipamentos inteligentes, embora tenha um crescimento popular atualmente no século XXI. Esse conceito foi apresentado primeiramente por Kevin Ashton da MIT Auto Centre em uma apresentação sobre RFID (*Radio-Frequency Identification*) e a cadeia de suprimentos da empresa Procter & Gamble (P&G), em 1999. (ASHTON, 2009).

Segundo Fleisch (2010), o objetivo da IoT é tornar praticamente todos os objetos físicos em computadores conectados a Internet. Feito isso esses objetos são chamados de Coisas inteligentes e com isso possibilita o aumento da sua utilidade no dia a dia, pois através dessa tecnologia é possível aperfeiçoar os dispositivos e permitir que sejam capazes de realizar várias tarefas para auxiliar as pessoas de acordo com a necessidade, além de permitir que sejam controlados de forma remota de qualquer lugar usando a Internet.

Atualmente é praticamente impossível imaginar uma sociedade vivendo sem acesso a Internet, pois a cada dia que passa mais serviços são ofertados de forma online, trazendo mais comodidade e segurança em alguns casos. A IoT é uma das principais tecnologias emergentes que tem contribuído bastante no intuito de efetivar novos domínios de aplicação das Tecnologias de Informação e Comunicação (TICs), como por exemplo domínio de cidades inteligentes, onde o uso de tecnologias avançadas de comunicação e sensoriamento visa fornecer serviços de valor agregado para os órgãos administrativos dessas cidades e seus cidadãos (ZANELLA *et al*, 2014).

Esses dispositivos chamados de Coisas, se tornaram bastante populares se expandindo pelo mundo todo e atingindo todas as esferas econômicas da sociedade, fazendo com que a Internet passe a ser um recurso indispensável em qualquer sistema computacional (RAJ; RAMAN, 2017). Nesse contexto, a IoT pode ser vista como uma evolução da Internet como se conhece, tendo em vista o rápido aumento no número de dispositivos conectados simultaneamente.

2.1. Aplicações e importância para a sociedade

Tendo em vista a quantidade de dispositivos conectados à Internet nos dias de hoje, é inevitável que a IoT tenha se tornado uma tecnologia indispensável para a sociedade. Segundo Halvorsen *et al* (2017), a IoT no contexto de casas inteligentes é um agrupamento de aparelhos interconectados que interagem entre si e pessoas autorizadas, sendo esses, aparelhos inteligentes e possivelmente autônomos, como aparelhos de eletrodomésticos, de segurança, veículos para que dessa forma pessoas autorizadas possam ter acesso.

Para Ferreira *et al* (2012), ao conectar sensores aos objetos, eles adquirem o conceito de objetos inteligentes, onde possibilita capturar informações de contexto, e fornecer informações que torna possível adaptações e decisões em tempo real. Nesse contexto empresas ou setores estão adotando o uso da IoT para simplificar, automatizar e assim melhorar o controle de diversos processos, possibilitando que máquinas se comuniquem entre si e possam aumentar sua produtividade, ampliando a segurança dos processos de fabricação de um produto e conseqüentemente diminuindo os desperdícios de matéria prima.

A IoT está também está presente no uso de práticas esportivas com acompanhamento em tempo real através de relógios inteligentes, pulseiras e até óculos, bem como o seu uso na área de saúde através de sensores que permitem que os médicos monitorem as condições do paciente em tempo real mesmo estando fora do ambiente hospitalar. Um outro exemplo da importância da IoT é o conceito de cidades inteligentes, que tem se tornado popular graças ao uso da IoT, essa tecnologia tem contribuído bastante no monitoramento em tempo real de diversas atividades cotidianas, automatização de tarefas, criação de soluções sustentáveis e conseqüentemente a melhoria da qualidade de vida de uma população (ZANELLA *et al*, 2014).

O alcance da utilidade da IoT é enorme, já é uma realidade nas nossas vidas e essa importância tende a ficar cada vez mais evidente conforme a tecnologia vai evoluindo e possibilitando novas implementações. (DOMINGOS *et al*, 2013), corroboram com (FERREIRA *et al*, 2010) esclarecendo que a IoT pode ser compreendida como vantagem competitiva, visto que as informações de contexto podem ser utilizadas para permitir e otimizar a adaptação às alterações do ambiente em tempo real.

2.2. Desafios enfrentados pela IoT

Alguns aspectos têm dificultado e até mesmo prejudicado o desenvolvimento da IoT, tendo em vista os múltiplos dispositivos conectados à rede. É importante analisar algumas questões como por exemplo a quantidade de dados que são gerados por esses dispositivos, assim como o tratamento e armazenamento desses dados que são gerados por diversas fontes diferentes. Nesse contexto, soluções baseadas em *Big Data*, assim como computação em nuvem, têm surgido como potencial resposta para solucionar alguns desses desafios, permitindo lidar com um imenso volume de dados diversos e não estruturados (SOLDATOS *et al*, 2012).

Um dos fatores bastante importante e que acaba dificultando ou atrasando o desenvolvimento da IoT é a questão da infraestrutura da rede atual, pois existem inúmeras formas diferentes de tecnologias de conexão, mas apesar disso ainda são bastante limitadas no que se refere a suportar a grande quantidade de dispositivos conectados. Temos avanços nesse sentido com a migração do IPv4 (*Internet Protocol* versão 4) para a versão 6 (IPv6) do protocolo IP (*Internet Protocol*) que utiliza 128 bits para endereçamento, facilitando assim o gerenciamento de redes devido a recursos de autoconfiguração, oferecendo suportes adicionais de segurança (EVANS, 2011).

Será preciso que as tecnologias suportem não apenas a quantidade de dispositivos conectados, mas também a grande largura de banda necessária para atender a demanda de dados que serão gerados por esses dispositivos conectados simultaneamente. Portanto, significa dizer que será necessário manter o funcionamento completo das conexões dos dispositivos sem que ocorra nenhum tipo de interrupção. Nesse sentido, as novas tecnologias como a LPWAN (*Low Power Wide Area Network*), assim como a 5G, são tecnologias que implica dizer que irão contribuir muito para solucionar os problemas de conectividade da IoT (I-SCOOP, 2021).

Outro fator que desafia a IoT é a falta de padronização de uma arquitetura de referência para o desenvolvimento das Coisas, como se trata de uma área nova não existe um padrão a ser seguido, tão pouco existem requisitos delimitados para sua infraestrutura. Para Cloutier *et al* (2010) e Nakagawa *et al* (2011), uma arquitetura de referência compreende-se por ser uma arquitetura abstrata, onde conhecimento e experiências se juntam como solução em um domínio de aplicação específico, possibilitando facilitar e guiar o desenvolvimento, a padronização e

consequentemente a evolução de sistemas de *software* em tal domínio.

Por fim, a IoT necessita que as tecnologias se adaptem de maneira que suportem um cenário onde bilhões de dispositivos estejam conectados simultaneamente. Nesse cenário, vamos discutir as plataformas de IoT e a sua importância no que se refere a resolução dos problemas mencionados.

2.3. Plataformas de IoT

A IoT visa estabelecer um ambiente altamente heterogêneo, onde os componentes que compõem este meio são diversificados umas das outras. Com isso, todos os aplicativos e soluções de problemas precisam ser adaptados para amparar essa diversidade (SUNDMAEKER *et al*, 2010). Desse modo, este capítulo descreve as entidades que integram o ambiente de IoT, assim como apresentar as plataformas de IoT como uma ferramenta importante e completa no gerenciamento dessas entidades.

O princípio básico da IoT é que qualquer coisa possa ser conectada à Internet e nesse contexto o *Hardware* é uma parte importante no desenvolvimento, pois se trata da construção física dos objetos e isso precisa ser feito de maneira que suporte a diversidade dos dispositivos que encontramos no ecossistema da IoT. Sendo assim, se faz necessária uma camada de *software* que forneça abstrações para dispositivos e aplicações, diversos níveis de transparência e interoperabilidade, assim como diversos serviços para usuários finais e aplicações.

Denominada *Middleware*, essa camada oculta dos desenvolvedores de aplicações as complexidades e heterogeneidades referentes ao *Hardware* subjacente, bem como, às camadas de protocolos de rede, às plataformas e dependências do sistema operacional, além de facilitar o gerenciamento de recursos do sistema e por fim aumentar a previsibilidade da execução de aplicações (BERNSTEIN, 1996).

Implementar novos serviços nas redes atuais tem se tornado um grande desafio por vários fatores, como a natureza proprietária dos dispositivos de *Hardware*, a falta de profissionais qualificados, bem como o custo para oferecer espaço físico e energia para vários dispositivos (HAN *et al*, 2015). Para resolver esses problemas é preciso que a IoT ofereça suporte aos paradigmas que fizeram ela se tornar uma realidade, como a *Cloud Computing*, *Web semântica*, *Fog Computing* e a *Big Data*, pois a tendência é que esses problemas aumentem com o aumento da popularidade e

crescimento da IoT (MACHADO, 2018).

As plataformas de IoT surgem com o objetivo de contribuir com a solução dos problemas que acabam atrasando o desenvolvimento da IoT. Essas plataformas são um tipo de *PaaS (Platform as a service)* que são *Softwares Middlewares* que se caracterizam por operarem como um intermediário entre usuário e aplicação ou entre aplicações. Essas plataformas têm surgido como potenciais soluções para fornecer interoperabilidade e gerenciar a demanda crescente de variados dispositivos associados a aplicações, bem como o consumo de dados dos usuários finais (TEIXEIRA *et al*, 2011).

O gerenciamento é composto por várias funcionalidades e pode variar bastante o número de recursos dependendo da versão da plataforma, mas no geral uma plataforma de IoT oferece serviços como autenticação, coleta de dados, configurações, atuação sobre os dispositivos e implementação de protocolos de segurança e técnicas de privacidade.

O uso de uma plataforma de IoT traz como vantagem a simplificação no processo de desenvolvimento, já que a plataforma padroniza o ambiente fazendo com que todas as aplicações necessitam estar de acordo com as características técnicas da plataforma. Além disso, elas permitem o funcionamento de diferentes protocolos de comunicação e de segurança em uma mesma plataforma, criando assim, diferentes níveis de privacidade e segurança, como também podem ser escolhidos de acordo com necessidade e capacidade do dispositivo conectado (PIRES *et al*, 2015).

A tarefa de uma plataforma IoT é tratar, processar e moldar a grande quantidade de dados gerados por certa quantidade de dispositivos, nesse contexto também estão inseridas a segurança e privacidade dos dados. As plataformas IoT normalmente disponibilizam diversas formas de conectividade como: HTTP (*Hypertext Transfer Protocol*) e seu uso sobre o estilo arquitetural REST (*Representational State Transfer*), o MQTT (*Message Queuing Telemetry Transport*) e o CoAP (*Constrained Application Protocol*), que possibilita a interação com uma grande quantidade de dispositivos (FIELDING, 2000).

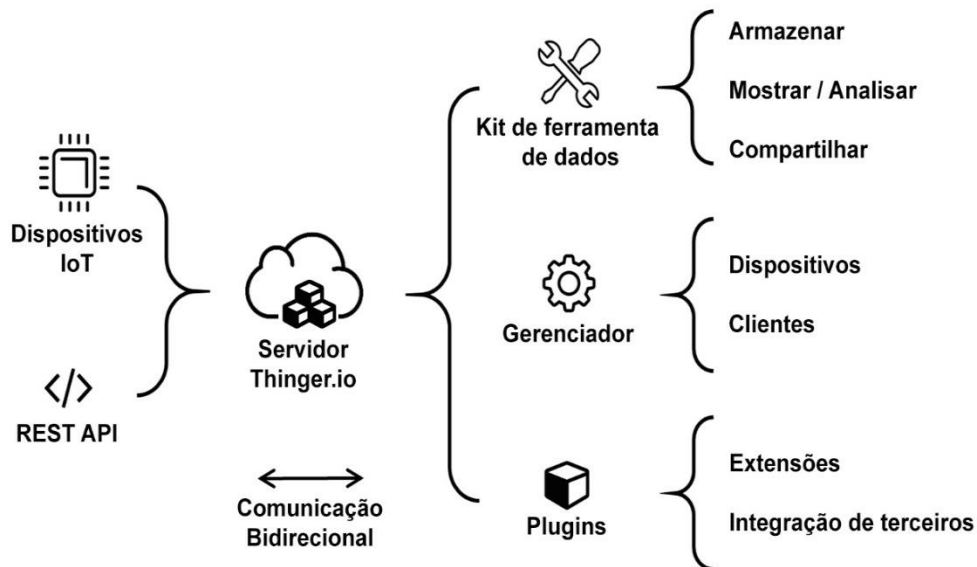
2.3.1. Thinger.io Platform

A plataforma *Thinger.io* é uma plataforma de código aberto para a IoT fundada pela CDTI (*Centre for the Development of Industrial Technology*) com o propósito de

facilitar o desenvolvimento e gerenciamento de produtos conectados de uma maneira muito simples. A plataforma encontra-se atualmente na versão 3.4.6 e conta com vários planos disponíveis. O plano *Free*, é a versão gratuita e conta com algumas limitações para iniciar o aprendizado e a prototipagem, há também os planos *Small*, o *Medium*, o *Large* e o *Unlimited* (THINGER.IO, 2022)

A plataforma *Thinger.io* é formada por um servidor de IoT como *Backend* e um *Frontend* baseado na *web*, tornando mais simples a utilização de todos os recursos independentemente de estar usando computador ou *smartphone*. Na Figura 1 é possível ver os principais recursos da plataforma para criar objetos de IoT.

Figura 1 - Principais recursos do *Thinger.io*



Fonte: *Thinger.io* (2022, com Adaptações)

Os dispositivos IoT são totalmente compatíveis independente do processador, rede ou do fabricante. O recurso de comunicação bidirecional da plataforma permite criar comunicações com dispositivos Linux, Arduino, Raspberry Pi ou MQTT, bem como com tecnologias de ponta como Sigfox ou LoRaWAN. O Servidor *Thinger.io* permite armazenar dados IoT de forma escalável com eficiência e acessibilidade na nuvem, tornando possível agregar os dados em tempo real com apenas alguns cliques (THINGER.IO, 2022).

Já o Kit de ferramentas de dados exibe os dados em tempo real ou armazenados em vários *widgets*, como gráficos de rosca, séries temporais, medidores ou representações personalizadas para criar painéis em minutos. Outro recurso

interessante são os diversos *plug-ins* que a plataforma oferece para integrar projetos de IoT ao *software* de empresas ou qualquer outro serviço de Internet. Por fim, o gerenciador permite introduzir as cores de marca, logotipos e domínios da *web*.

2.4. Segurança da informação e privacidade dos dados

A segurança da informação é a área que estuda mecanismos de proteção de um conjunto de informações. No contexto da computação é a responsável pela proteção de um sistema computacional, ou seja, proteger computadores, dispositivos e os dados que são gerados por esses equipamentos, não restringindo apenas ao meio eletrônico, mas também abrangendo componentes físicos e humanos (SILVA; STEIN, 2007).

Para Miorandi *et al* (2012), uma das principais preocupações éticas dos usuários com relação a IoT é a privacidade, esse é um detalhe crucial que pode distorcer a visão sobre a IoT. Portanto, é necessário que o controle deste novo ambiente complexo, bem como a troca de dados invisível e constante entre as Coisas e outras Coisas, assim como com as pessoas, aconteça anonimamente, sem que o proprietário e criadores tenham qualquer conhecimento desses dados.

A abordagem do anonimato parte do princípio de que o indivíduo não pode ser identificado dentro de um conjunto de usuários. Porém, o nível de anonimato depende diretamente de consequências legais e sociais que possam causar possíveis violações de dados (CHABRIDON *et al*, 2014). Com o decorrer dos anos, a segurança da informação foi obtendo cada vez mais espaço e importância para ser estudada, muito disso devido ao avanço e as inovações tecnológicas em constante crescimento, tornando a prática de preservação da integridade das informações cada vez mais relevantes no contexto digital (BROSTOFF, 2004).

Segundo Shelby e Bormann (2011), para considerarmos um sistema de IoT seguro é necessário estabelecer quais os objetivos de segurança desejáveis. Podemos citar pelo menos três grupos de objetivos desejáveis para a segurança em IoT, são eles: confidencialidade – requisito onde possibilita “escutar” e entender os dados transmitidos por elementos participantes da comunicação; integridade – requisito onde os dados ficam impossibilitados de serem alterados por elementos da rede sem a devida autorização; e disponibilidade – onde o objetivo é manter o sistema sempre disponível e seguro contra ataques maliciosos.

2.4.1. Confidencialidade

A Confidencialidade é a primitiva da segurança da informação responsável por garantir que os dados fiquem disponíveis apenas para pessoas autorizadas. Sendo assim, significa dizer que tem como função manter as informações confidenciais. Para isso é preciso que medidas adicionais sejam aplicadas para evitar que essas informações possam ser lidas e interpretadas por terceiros.

Uma das técnicas utilizadas é a criptografia, ela serve para manter uma comunicação segura entre os participantes, com isso impede que terceiros mal-intencionados possam ter acesso a informações sem a devida autorização. Uma observação a respeito dos processos criptográficos é que geralmente estão divididos em dois elementos, sendo eles: algoritmo e chave, conforme explica (MENDES *et al*, 2011).

O algoritmo é o procedimento que será executado a fim de cifrar a informação. Já a chave, na criptografia, é um valor que é fornecido como uma entrada para um sistema, como uma espécie de manual de como deve ser criptografada a mensagem contendo instruções a respeito do processo (KIM; SOLOMON, 2014).

2.4.2. Integridade

A integridade diz respeito à confiabilidade da informação, onde apenas pessoas que possuem autorização podem modificar os dados utilizados na transmissão. Portanto essa primitiva tem a função de se preocupar com alterações indevidas que possam ocorrer ao realizar o armazenamento das informações ou ao ser enviadas para um destinatário.

Sendo assim, é necessário que se crie mecanismos de controle que impeçam a exclusão e alteração dos dados por pessoas não autorizadas. Para isso é preciso que os sistemas computacionais possuam níveis de segurança em todos os processos em que envolva manipulação de algum tipo de dado, como por exemplo na camada de transporte que é responsável pela transferência dos dados (KIM; SOLOMON, 2014).

2.4.3. Disponibilidade

A disponibilidade é o princípio de que as informações estejam disponíveis para serem acessadas sempre que for preciso, evitando falhas na solicitação ou na disponibilização de uma informação. Nesse cenário se encaixa diversas partes de um sistema computacional como o *Software* e *Hardware*. O uso de funcionalidades de redundância de dados como RAID (*Redundant Array of Inexpensive Disks*) e *Backups* acabam sendo importantes.

Portanto, para garantir o princípio de disponibilidade em um sistema computacional é garantir que os usuários que possuem autorização possam acessar seus dados sempre que necessário, bem como garantir que possíveis falhas de segurança sejam evitadas para que não afete o funcionamento adequado, como por exemplo o DoS (*Denial of Service*) que é um ataque de negação de serviços.

Dito isso, a segurança da informação tem se tornado indispensável principalmente com o avanço da tecnologia e o aumento no número de dispositivos conectados a internet. É essencial que todos os dispositivos utilizem técnicas de segurança ainda na sua construção básica (CABRAL; CAPRINO, 2015).

3. METODOLOGIA

Este capítulo trata da metodologia que foi utilizada durante a pesquisa. Será apresentado as etapas de avaliação que foram usadas para analisar a plataforma de IoT *Thinger.io*, diante disso, validar os objetivos que serão analisados, bem como as suas limitações.

A princípio foi realizada avaliação conceitual a respeito da arquitetura da plataforma. Para tal, utilizamos a literatura e a documentação fornecida pela própria desenvolvedora, sendo assim possível validar os recursos e funcionalidades que são oferecidas pela plataforma *Thinger.io*.

Em seguida, realizamos uma avaliação das configurações gerais de segurança disponibilizadas pela plataforma *Thinger.io*; na sequência pontuamos os recursos de segurança e de privacidade que estão presentes na plataforma e que consequentemente podem impactar diretamente no desenvolvimento de aplicações mais seguras de lot.

Por último, foi feita uma avaliação a respeito do gerenciamento do armazenamento de dados. Nesse sentido, iremos descrever e avaliar as características da funcionalidade através da análise da documentação oficial da plataforma.

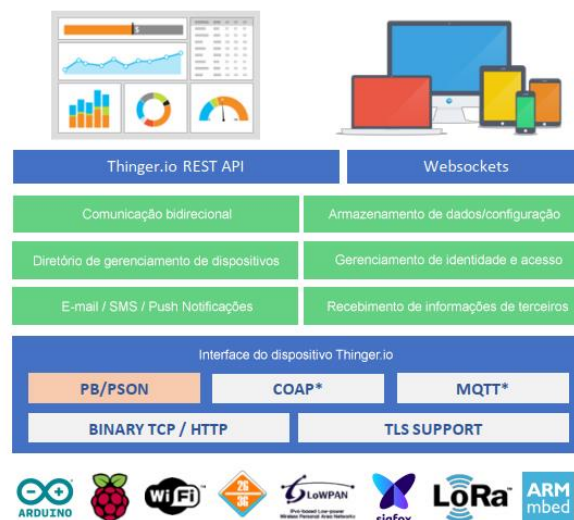
4. AVALIAÇÃO DA PLATAFORMA

Este capítulo tem o propósito de descrever a avaliação conceitual realizada na *Thingier.io* plataforma do ponto de vista da segurança e privacidade dos dados gerenciados pela plataforma. Diante disso, os procedimentos de avaliação realizados serão descritos em tópicos.

4.1. Arquitetura da plataforma

O *Thingier.io* é uma plataforma que tem despertado o interesse da comunidade científica e tecnológica, graças aos diversos projetos que foram bem sucedidos utilizando esta plataforma (LIKOTIKO *et al*, 2018). Um dos principais fatores do sucesso é o fato da plataforma fornecer um serviço de nuvem pronto para usar e conectar dispositivos à Internet para que seja realizado qualquer sensoriamento remoto. Além disso, a plataforma possibilita conectar qualquer dispositivo com conectividade à Internet, desde dispositivos Arduino, Raspberry Pi, a dispositivos Sigfox e ARM, entre outros. A Figura 2 exibe alguns dos recursos disponíveis na plataforma.

Figura 2 - Visão geral da plataforma *Thingier.io*



Fonte: *Thingier.io* (2022, com Adaptações)

. Alguns recursos prontos são oferecidos pela plataforma como: registro de dispositivo; comunicação bidirecional em tempo real, tanto para sensoriamento quanto

para atuação; dados e armazenamento de configuração, tornando possível o armazenamento de dados de séries temporais; gerenciamento de identidade e acesso (IAM), permitindo que entidades de terceiros acessem a plataforma e os recursos do dispositivo por meio de APIs REST/Websocket. Também fornece uma interface web para gerenciar todos os recursos e gerar painéis para monitoramento remoto.

Uma das principais vantagens de usar esta plataforma, além do fato de ser *open source*, é a possibilidade de comunicação bidirecional entre os dispositivos em tempo real, usando o REST-API. Diante disso, é possível desenvolver qualquer aplicação de fusão de dados, ou seja, *desktop, mobile, Webservice*, onde interage com dispositivos usando uma interface comprovada baseada em REST-API (BUSTAMANTE *et al*, 2019). Com isso, os dispositivos podem usar protocolos binários mais eficientes (em termos de largura de banda ou espaço de memória) para se comunicar com a nuvem.

4.1.1. Comunicação bidirecional em tempo real

As plataformas baseadas em HTTP podem ser facilmente desenvolvidas, implantadas e mantidas porque são executadas regularmente. Os servidores HTTP recebem os dados de sensores usando técnicas bem conhecidas, porém, não fornecem um mecanismo eficiente para comunicação bidirecional, ou seja, quando se torna necessário operar sobre um dispositivo ou configurar dispositivos em tempo real.

No geral, plataformas baseadas em HTTP possuem um mecanismo de pesquisa no qual os dispositivos verificam o servidor periodicamente em busca de novos comandos ou atualizações, já o *Thinger.io* oferece um canal de comunicação bidirecional entre o dispositivo e o servidor em nuvem, possibilitando que qualquer aplicativo possa interagir com o dispositivo em tempo real.

4.1.2. Protocolos de comunicação

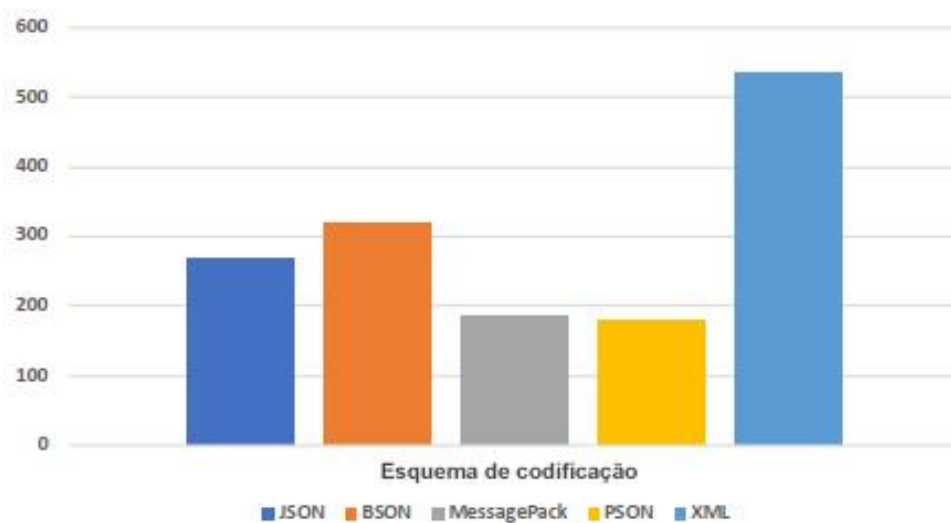
Grande parte das plataformas de IoT utilizam protocolos de transporte tradicionais baseados em HTTP (*Hypertext Transfer Protocol*) ou MQTT (*Message Queuing Telemetry Transport*) para enviar dados dos dispositivos para a nuvem (YASUMOTO *et al*, 2016). No HTTP, os dispositivos emitem uma solicitação HTTP com uma carga personalizada sempre que enviam dados para a nuvem, a plataforma

recebe as informações e as armazena em um banco de dados.

O uso do protocolo citado anteriormente para transmitir informações acaba sendo ineficiente, principalmente quando falamos de largura de banda, latência e consumo de energia, que são restrições para dispositivos IoT (YOKOTANI; SASAKI, 2016). Assim como, se faz necessário a criação de uma nova conexão com a nuvem, e conseqüentemente a criação de uma solicitação HTTP que inclui vários cabeçalhos e uma carga útil geralmente em JSON ou XML, causando uma enorme sobrecarga para enviar cargas pequenas e regulares, como na transmissão de alguns bytes com medições de sensores.

A Figura 3 mostra que a plataforma *Thingier.io* propõe uma solução eficiente utilizando MQTT, através do uso de conexões binárias brutas sem a sobrecarga de HTTP ou a necessidade de mecanismo de assinatura, além do mais, fornece uma melhor eficiência de transmissão usando um esquema de codificação otimizado chamado Photoson (PSON) (THINGER.IO, 2022).

Figura 3 - Comparação de codificação (bytes)



Fonte: Bustamente (2019, com Adaptações)

Na figura acima é possível ver a comparação dos tamanhos de codificações entre os diferentes formatos que são usados pelas plataformas, como o JSON, BSON (JSON Binário), *MessagePack*, XML e o PSON proposto. Uma das grandes vantagens do uso do MQTT é o fato dele ser altamente desacoplado do espaço, pois os sensores que produzem os dados não precisam ter acesso a identidade dos clientes que desejam aquela informação (BELLAVISTA; ZANNI, 2016).

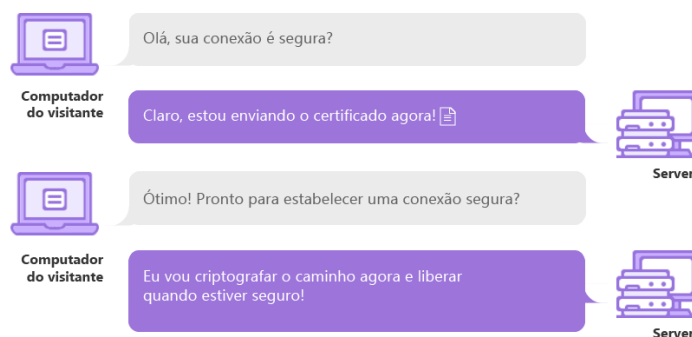
Esse esquema de codificação PSON foi projetado com objetivo de suportar dispositivos com restrições de recursos como memória e poder de processamento, permitindo codificar dados não estruturados como JSON, utilizando um formato binário compacto. Dessa forma, a solução proposta permite reduzir a latência no envio de informações para a nuvem, economizar largura de banda, assim como reduzir o consumo de memória e conseqüentemente oferecer uma economia de bateria nos dispositivos (BUSTAMANTE *et al*, 2019).

4.1.3. Protocolos de segurança

Quando falamos em dispositivos inteligentes é inegável a preocupação de como estão sendo usados e armazenados os dados que são utilizados pelos dispositivos, sendo assim, o fator da segurança desses dados é um ponto importante na hora do desenvolvimento, bem como do seu uso.

As comunicações entre dispositivos e o *Thingier.io* são protegidas através do uso do protocolo TLS (*Transport Layer Security*) SSL (*Secure Sockets Layer*) conforme mostra a documentação da plataforma. O TLS é o protocolo mais atual e responsável por certificar a proteção de dados de maneira semelhante ao SSL que já é bastante utilizado e estabelecido (ATZORI *et al*, 2010). É um tipo de segurança digital que permite comunicação criptografada entre um site e um navegador, como podemos ver na Figura 4.

Figura 4 - Funcionamento dos certificados SSL / TLS.



Fonte: <http://www.hostinger.com.br> (2022)

Nesse sentido, uma lista ordenada dos protocolos de segurança é introduzida por padrão com objetivo de serem usadas para a troca de chaves, onde é possível

equilibrar entre configuração mais segura ou melhor desempenho e compatibilidade apenas modificando a ordem.

4.1.4. Interoperabilidade

Um dos pontos positivos de usar o *Thingier.io* é a possibilidade de ser interoperável com outras plataformas e aplicações. Isso permite que qualquer dispositivo seja acessível, independente se ele for usado para sensoriamento ou para atuação a partir de APIs REST padrão, ocultando a complexidade existente das otimizações de protocolos entre dispositivos e servidor (PIRES *et al*, 2015).

Os *endpoints* REST não são definidos estaticamente ou configurados manualmente para se comunicar com dispositivos no servidor. Pelo contrário, uma vez conectado à nuvem, eles são dinamicamente extraídos a partir da definição do modelo do dispositivo. Com isso, pode-se ter acesso em tempo real a um conjunto de recursos definidos no código do dispositivo a partir dos terminais REST que são gerados, como pode ser observado na Figura 5.

Figura 5 - Conversão de modelo de dispositivo para API REST



Fonte: *Thingier.io* (2022, com Adaptações)

Na figura acima podemos ver um exemplo de um dispositivo que contém um conjunto de sensores (temperatura, umidade e luminosidade) que são definidos no modelo do dispositivo. Quando usada a biblioteca do cliente *Thingier.io*, possibilita que o dispositivo se conecte à nuvem da plataforma, através de comunicações bidirecionais eficientes. Com isso, os recursos definidos no modelo do dispositivo

passam a ficarem disponíveis para acesso em tempo real a partir dos *endpoints* REST gerados automaticamente.

Essa abordagem é diferente de outras soluções encontradas de IoT, principalmente quando baseadas em HTTP, onde os dispositivos apenas enviam os dados para a nuvem e um cliente externo recebe essas informações (BUSTAMANTE *et al*, 2019). Neste cenário não há nenhuma interação em tempo real entre cliente externo e dispositivo, uma vez que é limitado pelos períodos de sincronização *push* ou *poll* configurados no dispositivo.

4.1.5. Tokens de acesso

O acesso ao servidor *back-end* para qualquer projeto se dá através do uso do REST API, feito isso, todos os recursos da plataforma *Thinger.io* ficam disponíveis para serem acessados. Nesse sentido, o console é apenas um cliente REST Angular que interage com a API para gerenciar os dispositivos, *buckets*, *endpoints*, painéis, entre outros. O REST faz uso da separação de responsabilidades que ocorre no estilo cliente servidor sem o problema da escalabilidade (FIELDING, 2000).

Cada solicitação da API REST deve ser autenticada, sendo assim, o cliente precisa fornecer um código de autorização em cada chamada. Nesse contexto, os tokens de acesso servem para fornecer autorização a serviços ou aplicativos de terceiros para fazer a solicitação de API, sem a necessidade de compartilhar o nome de usuário e a senha.

O token de acesso é um token JWT que é obtido através das credenciais do usuário, de um token de atualização ou de um token de acesso definido pelo usuário, ele é usado para conceder acesso a solicitações de API, devendo ser incluído no cabeçalho de autorização HTTP, ou como um parâmetro de URL na solicitação HTTP (THINGER.IO, 2022). Quando esse token é obtido das credencias do usuário ou de um token de atualização, ele possui validade de 2 horas, sendo necessário ser atualizado periodicamente.

Já o token de atualização não pode fornecer acesso aos recursos do usuário, porém pode ser usado para obter um novo token de acesso caso eles expirem. Portanto, o objetivo da autenticação é que você precise usar as credenciais do usuário para obter um token de acesso, assim como um token de atualização. Isso permite que você possa mandar o token de atualização em um local seguro e usar o token de

acesso para acessar os recursos do usuário.

Por fim, os tokens definidos pelo usuário podem ser usados como qualquer outro token de acesso para autenticar a solicitação. Entretanto, diferente dos tokens obtidos das credenciais do usuário, esses tokens não expiram por padrão, bem como, permite que o usuário possa definir o nível de acesso sobre os recursos da conta. Com isso, o usuário pode definir um token para acessar um único dispositivo ou para gravar em um *bucket* de dados sem que sejam incluídos outros recursos da conta.

4.1.6. Over-The-Air update (OTA)

Com o crescimento da Internet das Coisas se faz necessário pensar em soluções que garantam a manutenção das funcionalidades das aplicações e dos dispositivos que estarão conectados à Internet. Nesse sentido, é importante que a plataforma ofereça uma forma de atualização de *Software*, principalmente no que quesito segurança. De acordo com a norma ISO/IEC 27002 (2005), a possibilidade de um dispositivo estar sujeito a vulnerabilidades e incidentes podem comprometer um sistema como um todo.

Pensando nisso, surge como solução as OTA (*Over-The-Air-Updates*), que são atualizações utilizadas por sistemas distribuídos que visam garantir a disseminação de atualizações de patches de segurança e melhorias de código de forma escalável através dos dispositivos que fazem parte do sistema. Esse recurso é implementado nas bibliotecas de cliente do *Thinger.io*.

O processo de atualização via OTA é feito por meio de uma extensão do Visual Studio Code que faz parte dos recursos que se integram a plataforma *Thinger.io*, sendo uma ferramenta essencial para manutenção de dispositivos IoT. Uma vez dentro da IDE, basta compilar e fazer o upload como se o dispositivo estivesse conectado ao computador.

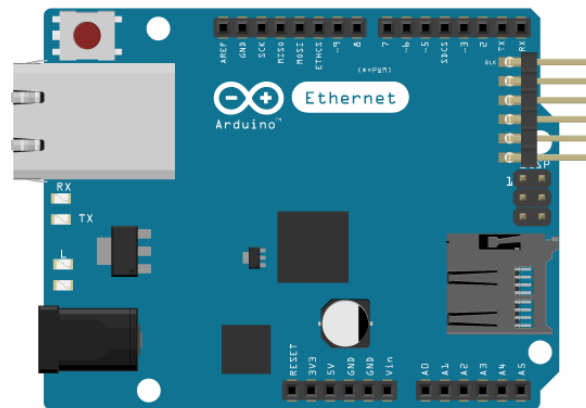
4.2. Compatibilidade com Arduino

O avanço tecnológico que estamos presenciando nos últimos anos é fascinante, hoje é possível ter várias funções ou *gadgets* em apenas 1 dispositivo e em muitos casos esses dispositivos muito menores que os tradicionais. É nesse contexto que as placas Arduino estão inseridas, pois elas possibilitam diversas

soluções em um curto espaço.

A Figura 6 mostra um Arduino com *Ethernet* que é uma ótima opção para conectar a placa Arduino à Internet em poucos minutos. Essa placa fornece conexão rápida e confiável para dispositivos IoT, o que a torna uma ótima opção para começar um projeto que necessite de conexão com a Internet.

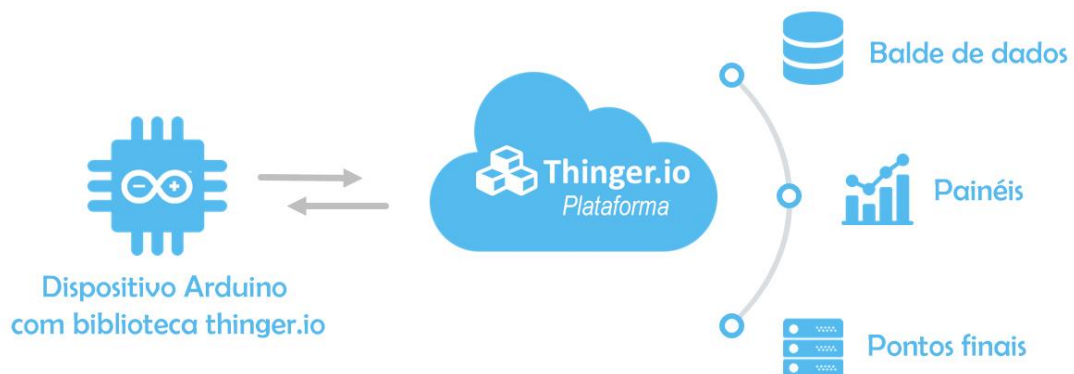
Figura 6 - Arduino com Ethernet Shield



Fonte: *Thingier.io* (2022, com Adaptações)

Para Mcroberts (2010), o Arduino é uma placa composta por um microcontrolador com sistema embarcado, essa placa suporta entrada e saída embutida e tem sua linguagem de programação padrão baseada em C e C++, podendo ser usada de maneira independente para controlar diversos equipamentos ou para criar novos equipamentos. A Figura 7 ilustra o Arduino usando a biblioteca do *Thingier.io*.

Figura 7 - Dispositivo Arduino com biblioteca *Thingier.io*



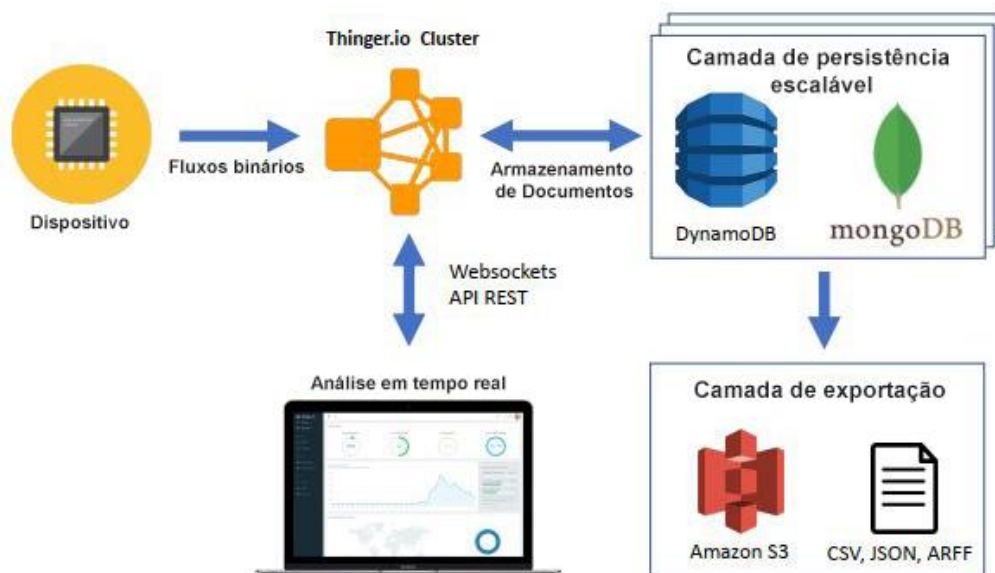
Fonte: *Thingier.io* (2022, com Adaptações)

De acordo com a documentação da plataforma, o *Thingier.io* possui uma biblioteca para o ecossistema Arduino IDE e foi projetada para dar suporte a praticamente qualquer microcontrolador ou dispositivo com recurso de comunicação, independente se é *Ethernet*, *Wifi* ou *GSM*. Sendo assim, possibilita que você possa escolher o *Hardware* que prefere conectar e isso é bastante relevante ao iniciar um projeto de IoT.

4.3. Gerenciamento de armazenamento

Quando falamos em gestão de armazenamento um dos recursos disponíveis na plataforma que está relacionado com essa funcionalidade se chama *Data Bucket* ou “Balde de Dados”. Um *bucket* é um recurso de nuvem que serve para armazenar dados de séries temporais, onde os dispositivos podem enviar informações quando necessário (BUSTAMANTE *et al*, 2019). Como podemos ver na Figura 8, essas informações são armazenadas na nuvem usando soluções seguras, eficientes e escaláveis como *DynamoDB* da *Amazon Web Service*.

Figura 8 - Visão geral do armazenamento de Big Data do *Thingier.io*.



Fonte: *Thingier.io* (2022, com Adaptações)

As informações armazenadas em um *bucket* podem ser exibidas através de um painel dentro da interface do console, outra forma é usando o *Amazon S3* (*Amazon*

Simple Storage Service) para exportar em armazenamento escalável em ARFF, JSON ou CSV para análise offline. O *Thinger.io* divide o armazenamento de informações em uma infraestrutura de nuvem escalável nos seguintes passos:

- Modelagem de recursos de dados no dispositivo, possibilitando que um dispositivo possa expor um conjunto de recursos, como temperatura ou umidade. Esses recursos não são vinculados a nenhuma estrutura de dados, já que são gerenciados como documentos não estruturados como o formato JSON.
- Conexão do dispositivo à infraestrutura do *Thinger.io*, onde o dispositivo expõe os recursos disponíveis para alimentar painéis em tempo real ou armazená-los em *data bucket*.
- Configuração de *bucket* no console, quando o dispositivo é conectado à plataforma permite que seja definido um novo *bucket* de dados. É nesse momento que o usuário seleciona o intervalo de amostragem necessário e o dispositivo passa a transmitir as informações na frequência necessária.

Portanto, desde que haja coletores para essas informações como um painel ou um *bucket* de dados, a infraestrutura de nuvem do *Thinger.io* inscreve os recursos do dispositivo automaticamente no intervalo necessário. Além do mais, a plataforma suporta o uso de diferentes armazenamentos de documentos como DynamoDB ou MongoDB que são alternativas que fornecem recursos altamente escaláveis no que tange armazenamento de dados na nuvem.

5. RESULTADOS

Com base na literatura e em todas as análises que foram realizadas no capítulo 4, tem-se através deste tópico, fazer uma junção dos resultados que foram obtidos e constatar se os objetivos propostos no início deste trabalho foram alcançados. Assim sendo, a ideia principal que objetivou a execução dessa pesquisa foi a de estudar e avaliar a veracidade de algumas funcionalidades de segurança da informação implementadas por uma plataforma de IoT de código livre denominada *Thinger.io*. A relevância desse estudo se dá devido ao enorme crescimento do paradigma da Internet das Coisas. Ademais, através desse estudo pretendeu-se contribuir com soluções de problemas e algumas diversidades que acompanham o desenvolvimento desta área em pleno crescimento.

Iniciando a avaliação, mais precisamente na seção 4.1, foi realizada uma análise conceitual sobre a arquitetura que é um dos fatores de destaque dessa plataforma, pois ela oferece um serviço de nuvem que em poucos minutos é possível conectar dispositivos à Internet e utilizar qualquer sensoriamento remoto. Além disso, a compatibilidade com dispositivos como Arduino, Raspberry Pi, Sigfox, ARM entre outros, faz com que qualquer dispositivo com Internet se conecte a plataforma. Essa compatibilidade facilita o acesso à plataforma e os seus recursos por dispositivos de terceiros através do uso de APIs REST, que também é responsável por possibilitar a comunicação bidirecional entre os dispositivos em tempo real, e com isso trazendo mais eficiência na largura de banda quando precisa se comunicar com a nuvem.

Quanto ao protocolo de comunicação, percebeu-se que essa plataforma utiliza protocolos HTTP que são usados em grande parte das plataformas de IoT e acaba sendo ineficiente. No entanto, diante do grande volume de dados que são gerados pelos dispositivos e a busca por soluções para melhorar a eficiência na transmissão desses dados, a solução encontrada foi a utilização do MQTT e o PSON para melhorar a eficiência e transmissão desses dados. Dessa forma, a latência no envio de informações para a nuvem diminui, assim como reduz o consumo de memória nos dispositivos.

Em relação ao protocolo de segurança, a comunicação entre os dispositivos e a *Thinger.io* são protegidos por meio do protocolo TLS SSL, permitindo que se possa equilibrar entre desempenho e compatibilidade. Quanto a interoperabilidade, a plataforma permite que qualquer dispositivo seja acessível independente do seu

propósito, seja para atuação ou sensoriamento. Nesse sentido, quando um dispositivo é conectado a nuvem, as definições do modelo do dispositivo são extraídas dinamicamente, permitindo que qualquer outro dispositivo possa acessar em tempo real através dos terminais REST. Finalizando a análise de arquitetura identificou-se que a plataforma oferece suporte para OTA (Over-The-Air-Updates) que é uma tendência necessária para o futuro da Internet das Coisas, pois esse recurso é muito importante para atualizações em grandes escalas, principalmente quando falamos de segurança.

Seguindo com a análise, na seção 4.2 foi feita uma breve descrição sobre Arduino e a biblioteca para ecossistemas Arduino IDE disponíveis na plataforma, onde foi possível ver via documentação que praticamente qualquer microcontrolador pode ser conectado a ela e isso é um ponto muito positivo, pois permite que o utilizador possa escolher o *Hardware* com base no custo ou recursos disponíveis. Na última análise, sob a perspectiva de gerenciamento de armazenamento foi possível identificar que a plataforma usa soluções eficientes e escaláveis como DynamoDB e MongoDB para armazenamento de dados na nuvem.

Assim sendo, percebeu-se que a plataforma *Thinger.io* mostrou-se ser uma boa alternativa de *Software* livre, tanto para aprendizado quanto para desenvolvimento de aplicações relacionadas à Internet das Coisas. Por outro lado, foi possível verificar a deficiência da documentação da plataforma, no que tange a detalhes mais aprofundados sobre algumas funcionalidades e recursos. No entanto, não afeta a sua usabilidade já que em contrapartida se mostra bastante satisfatória na questão de configurações e instalações de dispositivos. Sob a perspectiva da segurança e privacidade, conclui-se que a plataforma possui funcionalidades e recursos adequados para um uso satisfatório.

6. CONSIDERAÇÕES FINAIS

Em constante expansão, a Internet das Coisas surgiu com o propósito de contribuir de forma significativa para a evolução e modernização de diversos setores. Nesse sentido, a realização de pesquisas sobre assuntos relacionados à Internet das Coisas é bastante importante, uma vez que como tecnologia relativamente nova é notável a necessidade de mais trabalhos científicos relacionados à área.

A pesquisa possibilitou avaliar a plataforma de Internet das Coisas *Thingier.io*, do ponto de vista dos protocolos e configurações de segurança da informação e privacidade dos dados. Com base na totalidade da avaliação realizada foi possível afirmar que a plataforma contém tecnologias de segurança satisfatórias na sua construção.

Notou-se a necessidade de boas práticas da parte dos usuários desenvolvedores. Além do mais, foi possível validar a veracidade das informações contidas na documentação oficial da plataforma e assegurar que a *Thingier.io* é uma boa alternativa de plataforma de código aberto para o desenvolvimento de aplicações para a Internet das Coisas.

Por fim, espera-se que com as análises aqui demonstradas, possa contribuir em novas pesquisas relacionadas a área e conseqüentemente ajudar no crescimento desse paradigma. Sugiro a realização de trabalhos futuros de forma mais aprofundada a respeito de outras funcionalidades da plataforma, bem como um estudo para comparar a *Thingier.io* com outra plataforma de Internet das Coisas de código aberto, visando mostrar funcionalidades, vantagens e limites para facilitar na escolha dos usuários de qual se adequa melhor a seu projeto.

REFERÊNCIAS

- ASHTON, Kevin. **That ‘Internet of Things’ thing**. Publicado no RFID Journal, 2009. Disponível em: <https://www.rfidjournal.com/that-internet-of-Things-thing>. Acesso em: 04 set. 2021.
- ATZORI, L., IERA, A., and MORABITO, G. (2010). **The Internet of Things: A survey**. Computer Networks vol. 54, no. 15, pp. 2787-2805.
- BANDYOPADHYAY, S., SENGUPTA, M., MAITI, S., & DUTTA, S. (2011). **Role of middleware for internet of Things: A study**. International Journal of Computer Science & Engineering Survey, vol. 2, no. 3, pp. 94-105
- BERNSTEIN, P. A. (1996). **Middleware: a model for distributed system services**. Communications of the ACM, vol. 39, no. 2, 86-98.
- BELLAVISTA, P.; ZANNI, A. **Towards better scalability for iot-cloud interactions via combined exploitation of mqtt and coap**. In: 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI). [s.n.], 2016. p. 1U6. Disponível em: <https://doi.org/10.1109/RTSI.2016.7740614>. Acesso em: 10 fev. 2022.
- BROSTOFF, Alexander. **Improving password system effectiveness**. 2004. Tese (Doutorado) – Londres. Disponível em: <http://discovery.ucl.ac.uk/1445330/1/U592650%20Redacted.PDF>. Acesso em: 03 out. 2021.
- BUSTAMANTE A. L., Patricio M. A., Molina J. M. **Thinger.io: An Open Source Platform for Deploying Data Fusion Applications in IoT Environments**. Sensors (Basel). 2019;19(5):1044. Sensors (Basel, Switzerland), 19.
- CHABRIDON, Sophie et al, **A survey on addressing privacy together with quality of context for context management in the Internet of Things**. annals of telecommunications-Annales des télécommunications, v. 69, n. 1-2, p. 47-62, 2014.
- CLOUTIER, R., MULLER, G., VERMA, D., NILCHIANI, R., HOLE, E., BONE, M. (2010). **The concept of reference architectures**. Systems Engineering, vol. 13, no. 1, pp. 14-27.
- DOMINGOS, Dulce; MARTINS, Francisco; CÂNDIDO, Carlos. **Internet of Things Aware WS-BPEL Business Process**. Proceedings of the 15th International Conference on Enterprise Information Systems (ICEIS), 2013
- EVANS, D. **A Internet das Coisas: Como a próxima evolução da Internet está mudando tudo**. White paper: Cisco Internet Business Solutions Group (IBSG), 2011. p.1–11. Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_Things_iiot_ibsg_0411final.pdf. Acesso em: 27 ago. 2021.
- FERREIRA, Pedro; MARTINHO, Ricardo; DOMINGOS, Dulce. **IoT-aware business processes for logistics - limitations of current approaches**, Proc. of Inforum –

simpósio de informática, pp 611-622, Universidade do Minho, Braga, Portugal. 9 e 10 de set. 2010.

FIELDING, Roy Thomas. **Architectural Styles and the Design of Network-based Software Architectures**. Dissertação de Doutorado - University of California, Irvine, 2000. Disponível em http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm. Acesso em: 19 fev 2022.

FLEISCH, Elgar (2010) **What is the Internet of Things?: An Economic Perspective**. Economics, Management, and Financial Markets, 5 (2). 125-157. ISSN 1842-3191.

HALVORSEN, Hans-petter et al, **Case Studies in IoT -Smart-Home Solutions Pedagogical Perspective with Industrial Applications and some latest Developments**. In: EAEEIE ANNUAL CONFERENCE, 27., 2017, Grenoble, France. HAL. Grenoble, França: Hal, 2017. v. 1, p. 1 - 9. Disponível em: <https://hal.archives-ouvertes.fr/hal-01658856>. Acesso em: 02 out. 2021.

HAN, B., Gopalakrishnan, V., Ji, L., and Lee, S. (2015). **Network function virtualization: Challenges and opportunities for innovations**. IEEE Communications Magazine, 53(2): 90–97.

I-SCOOP. **LPWA network technologies and low-power standards**. Disponível em: https://www.i-scoop.eu/internet-of-things-iot/lpwan/#Making_choices_in_the_confusing_LPWA_landscape. Acesso em: 05 de dez. de 2021.

ISO/IEC 27002 (2005): Information technology - Security techniques - Code of practice for information security management - Redesignation of ISO/IEC 17799:2005.

KIM, D.; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação**. Rio de Janeiro: LTC, 2014. 385 p. ISBN 978-0-7637-9025-7.

LIKOTIKO, E.; PETROV, D.; MWANGOKA, J.; HILLERINGMANN, U. **Real Time Solid Waste Monitoring Using Cloud and Sensors Technologies**. Tosjat 2018, 8, 106–116.

MACHADO, José. **Implementação de uma fog computing para fornecer StaaS a dispositivos IoT utilizando sistemas embarcados**. 2018. 147 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Sergipe, São Cristóvão, SE, 2018.

MCEWEN, Adrian; CASSIMALLY, Hakim. **Designing the Internet of Things**. Chichester (UK): Wiley, 2013. 336 p.

MCROBERTS, Michael. **Beggining Arduino**. Apress. Nova Iorque: 2010.

MENDES, A. J. B.; PAULICENA, E. H.; SOUZA, W. A. R. **Criptografia Quântica: Uma Abordagem Direta**. Revista de Sistemas de Informação da FSMA, v. 7, n. 39-48, p. 9, 2011. Disponível em: http://www.fsma.edu.br/si/edicao7/FSMA_SI_2011_1_Tutorial_1.pdf

MIORANDI, Daniele et al, **Internet of Things: Vision, applications and research challenges**. Ad Hoc Networks, v. 10, n. 7, p. 1497-1516, 2012.

NAKAGAWA, E. Y., ANTONINO, P. O., BECKER, M. (2011). **Reference architecture and product line architecture: A subtle but critical difference**. In: Crnkovic, I., Gruhn, V., Book, M., eds. Proceedings of the 5th European Conference on Software Architecture. Lecture Notes in Computer Science, vol. 6903. Germany, Springer Berlin Heidelberg, pp. 207-211.

OLIVEIRA, Sergio. **Internet das Coisas com ESP8266, Arduino e Raspberry Pi**. São Paulo: Novatec, 2017.

PIRES, P. F. et al, **Plataformas para a Internet das Coisas**. In: XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Vitória: SBC, 2015. p. 110–169. Disponível em: <http://sbrc2015.ufes.br/wp-content/uploads/Ch3.pdf>. Acesso em: 03 fev. 2022.

RAJ, P.; RAMAN, A. C. The Internet of Things: Enabling Technologies, Platforms, and Use Cases. Boca Ratón: CRC Press, 2017. Disponível em: <https://books.google.com.br/books?id=cLI0DgAAQBAJ>. Acesso em: 15 set. 2019.

SHELBY e BORMANN (2011). 6LoWPAN: **The wireless embedded Internet**, volume 43. John Wiley & Sons.

SILVA, D. R. P. da; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano. Ciências e Cognição, Rio de Janeiro, v. 10, p. 46–53, 2007. Disponível em: <http://www.cienciasecognicao.org/pdf/v10/m346130.pdf>. Acesso em: 10 mar. 2019.

SOLDATOS, J., SERRANO, M., HAUSWIRTH, M. (2012). **Convergence of Utility Computing with the Internet-of-Things**. Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. USA, IEEE, pp. 874-879.

SUNDMAEKER et al, 2010, SUNDMAEKER, H., GUILLEMIN, P., FRIESS, P., and WOELFFLÉ, S. (2010). **Vision and challenges for realising the Internet of Things**, volume 20. EUR-OP.

TEIXEIRA, T., HACHEM, S., ISSARNY, V., GEORGANTAS, N. (2011). **Service oriented middleware for the Internet of Things: A perspective**. In: Abramowicz, W., Llorente, I. M., Surridge, M., Zisman, A., Vayssière, J., eds. Proceedings of the 4th European Conference on Towards a Service-Based Internet. Lecture Notes in Computer Science, vol. 6994. Germany, Springer Berlin Heidelberg, pp. 220-229.

THINGER.IO. **Thinger.io** [S.l.: s.n.], 2022. Disponível em: <https://thinger.io/>. Acesso em: 02 fev. 2022.

YASUMOTO, K.; YAMAGUCHI, H.; SHIGENO, H. **Survey of real-time processing technologies of iot data streams**. J. Inf. Process. 2016, 24, 195–202.

YOKOTANI, T.; SASAKI, Y. **Comparison with HTTP and MQTT on required network resources for IoT**. In Proceedings of the IEEE International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, Indonesia, 13–15 September 2016; pp. 1–6.

ZANELLA, A., Bui, N., CASTELLANI, A., VANGELISTA, L., Zorzi, M. (2014) **Internet of Things for smart cities**, IEEE Internet of Things Journal, vol. 1, pp. 22-32.