UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

FELIPE MOREIRA DA SILVA

ESTRATÉGIAS E DESAFIOS NA CRIAÇÃO DE UM SMART CAMPUS: ANÁLISE E PERSPECTIVAS INICIAIS

TOLEDO

2025

FELIPE MOREIRA DA SILVA

ESTRATÉGIAS E DESAFIOS NA CRIAÇÃO DE UM SMART CAMPUS: ANÁLISE E PERSPECTIVAS INICIAIS

Strategies and Challenges in Creating a Smart Campus: Analysis and Initial Perspectives

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Ciência da Computação do Curso de Bacharelado em Ciência da Computação da Universidade Tecnológica Federal do Paraná.
Orientador(a): Dr. Tiago Piovesan Vendruscolo.

TOLEDO

2025

FELIPE MOREIRA DA SILVA

ESTRATÉGIAS E DESAFIOS NA CRIAÇÃO DE UM SMART CAMPUS: ANÁLISE E PERSPECTIVAS INICIAIS

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Ciência da Computação do Curso de Bacharelado em Ciência da Computação da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 14 / Fevereiro / 2025

Alvaro Ricieri Castro e Souza
Doutorado
Universidade Tecnológica federal do Paraná

Edson Tavares Camargo
Doutorado
Universidade Tecnológica federal do Paraná

Tiago Piovesan Vendruscolo
Doutorado
Universidade Tecnológica federal do Paraná

TOLEDO
2025

Dedico este trabalho aos meus pais, que empregaram anos de suas vidas para garantir minha educação formal e me ensinaram lições de vida valiosas.

AGRADECIMENTOS

Primeiramente, agradeço a Deus pela oportunidade e força para concluir essa jornada.

Sou muito grato aos meus pais e amigos, que sempre me apoiaram e incentivaram ao longo do caminho.

Também quero agradecer especialmente ao professor Dr. Tiago Piovesan Vendruscolo, que me guiou nessa reta final, e ao professor Dr. Fábio Engel, que esteve presente na primeira fase do trabalho. A dedicação e o conhecimento de ambos foram fundamentais para que eu pudesse chegar até aqui.

Por fim, deixo meu agradecimento a todos que, de alguma forma, contribuíram para a minha formação. Muito obrigado!

Eu denomino meu campo de Gestão do Conhecimento, mas você não pode gerenciar conhecimento. Ninguém pode. O que pode fazer - o que a empresa pode fazer - é gerenciar o ambiente que otimize o conhecimento. (PRUSAK, Laurence, 1997).

RESUMO

O *smart campus*, também conhecido como Campus Inteligente, é uma Integração emergente que utiliza o conceito da Internet das Coisas (IoT) em um ambiente universitário. Isso permite que as instituições de ensino forneçam serviços aprimorados e tomadas de decisão mais precisas. Neste trabalho de conclusão de curso, pretende-se realizar um estudo sobre a infraestrutura que pode ser utilizada para a implementação inicial de um Campus Inteligente, utilizando como exemplo, a Universidade Tecnológica Federal do Paraná, Campus Toledo. Por meio do uso de soluções de IoT, o objetivo é avaliar as tecnologias existentes e as soluções disponíveis no mercado. Como exemplo de aplicação, foi desenvolvido um dashboard de monitoramento de uma janela utilizando um sensor reed switch e sensor de chuva.

Palavras-chave: Campus Inteligente. Internet das Coisas. Automação.

ABSTRACT

The smart campus is an emerging integration that uses the Internet of Things (IoT) in a university environment. This allows educational institutions to provide enhanced services and make more precise decisions. This final project intends to conduct a study on the infrastructure that can be used for the initial implementation of an intelligent campus, using the Federal University of Technology – Paraná, Toledo Campus as an example. Through IoT solutions, the objective is to evaluate existing technologies and available solutions in the market. As an application example, a window monitoring dashboard was developed using a reed switch sensor and a rain sensor.

Keywords: Smart campus. Internet of Things. Automation.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BLE	*Bluetooth Low Energy*
CoAP	*Constrained Application Protocal*
HTTP	*Hypertext Transfer Protocol*
IEEE	*Institute of Electrical and Electrounics Engineers*
IoT	*Internet of Things*
IPv6	*Internet Protocol Version 6*
M2M	*Machine to Machine*
MQTT	*Message Queue Telemetry Transport*
NFC	*Near Field Communication*
RFID	*Radio Frequency Identification*
TWT	*Target Wake Time*
URI	*Uniform Resource Identifier*
UTFPR-TD	Universidade Tecnológica Federal do Paraná - Campus Toledo
WLAN	*Wireless Local Area Network*

SUMÁRIO

1 INTRODUÇÃO

A Internet das Coisas, ou *Internet of Things* (IoT) , é um paradigma de comunicação que presume que objetos do cotidiano podem possuir interfaces de comunicação. Estes objetos, como lâmpadas, interruptores, televisores e outros, quando dotados de uma interface de comunicação possibilitam a existência de uma grande quantidade de novos serviços (Alghamdi; Shetty, 2016). Estes serviços possibilitam diversas melhorias e facilidades em atividades do cotiano, que vão desde avisos sobre janelas abertas até alarmes de segurança que informam sobre a intrusão em um determinado perímetro.

As aplicações de IoT têm sido desenvolvidas em muitos domínios, incluindo, por exemplo, automação residencial e industrial (Abdulraheem *et al.*, 2020), aplicação no campo da medicina e nos cuidados da saúde (Selvaraj; Sundaravaradhan, 2020), controle de tráfego (Agarwal; Sharma; Agarwal, 2021), cidades inteligentes (Camero; Alba, 2019), entre outros. Contudo, este trabalho possui particular interesse em aplicações IoT voltadas para *smart campus*. O conceito de *smart campus*, ou campus inteligente, surge a partir da aplicação dos princípios das cidades inteligentes em um campus. De fato, um campus pode representar uma cidade em miniatura. A menor estrutura de um campus, comparada à de uma cidade, torna-o atrativo para que novas tecnologias sejam aplicadas e testadas. Estas mesmas tecnologias, se aprovadas, podem futuramente ser aplicadas em cidades inteligentes. Além disso, possibilitam automatizar diversos serviços e funcionalidades, fornecendo maior conforto aos usuários do campus.

O campus inteligente é uma indústria emergente, com inúmeras soluções já adotadas por diversas universidades em todo o mundo (Alyahya; Aljaber, 2023; Malatji, 2017; Nóbrega; Chim-miki; Castillo-palacio, 2022). Diferente de um campus tradicional, o *smart campus* é capaz de fornecer serviços em menor tempo, reduzir os esforços gastos e também diminuir os custos de operação. A adoção do *smart campus* implica que a instituição adota tecnologias para o controle e manutenção de suas instalações, oferecendo um melhor serviço à sua comunidade compostas por alunos, professores, servidores e visitantes.

A aplicação de serviços inteligentes em um *smart campus* vai além do âmbito acadêmico, afetando também a sociedade como um todo. Exemplos disso incluem edifícios inteligentes, uma rede elétrica inteligente (*smart grid*) e a gestão de resíduos e água (Alghamdi; Shetty, 2016). Os edifícios inteligentes representam uma inovação tecnológica em construções sustentáveis, tanto em novas estruturas quanto na adaptação de prédios antigos. Eles funcionam por meio da conectividade entre dispositivos IoT, como sensores e atuadores, e a nuvem, permitindo o monitoramento e controle remoto de sistemas como arrefecimento, iluminação e segurança. Já a *smart grid*, ou rede elétrica inteligente, utiliza a tecnologia da informação para tornar o sistema elétrico mais eficiente em termos econômicos, confiáveis e sustentáveis. Essa abordagem revolucionária oferece análise em tempo real da rede elétrica, detecção de problemas, isolamento e autocorreção dentro do contexto de um campus inteligente. A gestão de resíduos e água também é essencial em um campus, e o uso de dispositivos IoT para controle desses recursos tem o potencial de reduzir custos. Por exemplo, sensores podem identificar onde há

maior consumo de água e detectar vazamentos em estágios iniciais. Além disso, a utilização de sensores em lixeiras possibilita um mapeamento dos locais com maior geração de resíduos, oferecendo dados valiosos para aprimorar a coleta do lixo, bem como identificar áreas com maior concentração de alunos.

A automação por meio de sensores oferece uma ampla gama de benefícios em um campus universitário. Um exemplo é a aplicação de sensores em janelas e portas, que contribui tanto para a segurança quanto para evitar imprevistos, como deixar uma janela aberta durante uma chuva repentina. Utilizando sensores equipados com placas capazes de detectar a presença de chuva, é possível prevenir esses problemas. Além disso, com o auxílio de aplicativos, é viável receber alertas que evitam inconveniências relacionadas a esses aspectos. Essa simples automação proporciona tranquilidade e praticidade, garantindo o fechamento automático de janelas e portas durante períodos chuvosos. Além disso, as possibilidades de automação com sensores são vastas e podem ser aplicadas em diversas áreas do campus. Por exemplo, é possível instalar pequenos motores para abrir ou fechar janelas e portas, ou até mesmo realizar essas ações automaticamente em horários específicos ou em resposta a outros sensores externos (Bernardes, 2020) .

Ao aplicar a automação em um campus universitário, as possibilidades se estendem para além das janelas e portas. É possível automatizar salas de aula, laboratórios com computadores, salas de servidores de rede, estacionamentos e bibliotecas, entre outros espaços. No contexto acadêmico, é possível regular a umidade, controlar a temperatura, monitorar o consumo de energia e criar um ambiente mais agradável e confortável para os alunos, ajustando automaticamente o clima das salas de aula por meio do controle do ar-condicionado ou da abertura de janelas. Além disso, a aplicação dessas tecnologias permite o gerenciamento eficiente do campus, como a reserva de salas e o monitoramento da ocupação, contribuindo para uma rotina mais organizada e fornecendo relatórios detalhados para aprimorar a experiência de todos os envolvidos (Quiles, 2008) .

Com a implementação adequada dessas tecnologias, um *smart campus* vai além da automação de tarefas, proporcionando um ambiente mais eficiente, sustentável e seguro (Kayasima, 2024) . A integração de sensores em diferentes áreas do campus permite um monitoramento abrangente, melhorando a segurança e prevenindo incidentes. Essa abordagem transforma a experiência de todos que frequentam ou fazem parte do campus, oferecendo ambientes mais confortáveis e adaptáveis (Almeida *et al.*, 2024).

A implementação de um *smart campus* apresenta desafios significativos, especialmente devido à grande heterogeneidade de dispositivos e às dificuldades encontradas ao utilizar diferentes tecnologias de comunicação. A diversidade de dispositivos IoT disponíveis, cada um com suas próprias características e protocolos de comunicação, torna complexo o processo de integração e coordenação desses dispositivos em um sistema unificado. Além disso, a utilização de tecnologias de comunicação variadas, como Zigbee (Ergen, 2004), Wi-Fi (Khorov *et al.*, 2018), Bluetooth (Bluetooth, 2006) e outros, acrescenta uma camada adicional de dificuldade na interoperabilidade e na criação de uma infraestrutura de comunicação eficiente. Esses

desafios exigem soluções inovadoras para garantir a conectividade e a interoperabilidade dos dispositivos, a fim de obter um ambiente inteligente e integrado em um campus.

No entanto, existem soluções que podem auxiliar na superação desses desafios. Um exemplo é o Home Assistant[1], uma aplicação que facilita a implementação e o controle dessas tecnologias. Embora não resolva todos os problemas, ele oferece uma abordagem simplificada para gerenciar uma ou mais áreas e diversos grupos de dispositivos de comunicação. Com o Home Assistant, é possível ter um controle amplo ou específico sobre os sensores, como no exemplo anterior das lixeiras. Por exemplo, é possível monitorar a quantidade de lixo nas lixeiras 7 e 3 de um restaurante universitário, permitindo inferir os locais onde os alunos se posicionam durante as refeições. Essa é apenas uma das funcionalidades proporcionadas pelos nossos sensores (Rodrigues *et al.*, 2010) .

Considerando as informações apresentadas anteriormente, o objetivo principal deste trabalho é realizar um estudo abrangente sobre a implementação de um campus inteligente na Universidade Tecnológica Federal do Paraná - Campus Toledo (UTFPR-TD) , por meio da utilização de soluções baseadas em IoT. O propósito é avaliar as tecnologias existentes e as opções disponíveis no mercado, visando aprimorar a eficiência e a qualidade dos serviços oferecidos pela universidade. Vale ressaltar que a automação de um campus é uma tarefa complexa, demandando esforço, investimento e ações que devem ser autorizadas previamente pela administração. Portanto, este trabalho representa um esforço inicial para a construção de um campus inteligente, reconhecendo os desafios inerentes e estabelecendo uma base sólida para futuras iniciativas nessa área (Andrade, 2024) .

1.1 ORGANIZAÇÃO DO TRABALHO

Este documento apresenta uma abordagem detalhada sobre a implementação de um Campus Inteligente, explorando os desafios, objetivos e benefícios dessa iniciativa. Para isso, serão discutidos os seguintes tópicos: No capitulo 1 – São analisados os principais desafios enfrentados pela instituição e os fatores que contribuem para sua ocorrência, são definidas as metas e benefícios esperados com a adoção de tecnologias e estratégias inovadoras. Explica-se a escolha do tema, destacando sua relevância e impacto na modernização da instituição. No capitulo 2 – É apresentada a base conceitual da pesquisa, com embasamento teórico e explicações sobre o conceito de Campus Inteligente. No capitulo 3 – Detalham-se os recursos tecnológicos, infraestrutura necessária e metodologias aplicáveis para a implementação e gestão eficiente do campus. No capitulo 4 – É demonstrado como a adoção do Campus Inteligente pode otimizar a administração, melhorar a experiência acadêmica e aumentar a eficiência operacional da instituição. No capitulo 5 – É feita a conclusão do trabalho e também algumas ideias de trabalhos futuros.

[1] Disponível em: https://www.home-assistant.io/

1.2 PROBLEMAS E PREMISSAS

O tema da Internet das Coisas (IoT) tem suscitado confusão em tempos contemporâneos, uma vez que sua compreensão pode se mostrar complexa. Devido ao seu crescimento ao longo desta década, seus dispositivos têm se tornado cada vez mais versáteis. Inicialmente, havia apenas lâmpadas, as quais eram dispendiosas. Entretanto, nos dias atuais, encontram-se sensores acoplados a praticamente todos os objetos tecnológicos, tornando mais palpável a utilização desses equipamentos, uma vez que os custos foram reduzidos e a instalação se tornou mais acessível (Filho, 2016) .

No entanto, é importante considerar não apenas os aspectos positivos desse crescimento. O monitoramento desses dispositivos tornou-se mais complexo devido ao aumento da quantidade de equipamentos que precisam ser monitorados. Além disso, a heterogeneidade dos dispositivos, cada um com sua própria tecnologia e método de comunicação, adiciona complicações no planejamento de residências e, especialmente, em uma universidade. Felizmente, existem aplicativos que simplificam a coordenação dessa tecnologia, pois sem eles a logística seria muito mais desafiadora. No caso da UTFPR-TD, que possui diversos prédios, a situação se torna ainda mais complexa devido ao grande número de sensores envolvidos(Godoi; Araújo, 2019) .

A transformação do campus da UTFPR-TD em um campus inteligente apresenta desafios significativos. No entanto, pequenas modificações podem facilitar essa integração. O gerenciamento de dados é o maior obstáculo atual, exigindo atenção especial para assegurar a proteção dos dispositivos conectados, cuja vulnerabilidade aumenta com a interconectividade. Métodos eficazes de segurança serão necessários para mitigar esses riscos (Moreira; Aicos, 2020) .

Outro desafio importante é o investimento financeiro. Embora os custos dos sensores tenham diminuído em relação ao passado, a instalação de centenas deles ainda representa uma despesa considerável. Para minimizar riscos, testes em ambientes controlados podem avaliar a eficácia das soluções propostas antes de sua aplicação em larga escala. Com um planejamento financeiro adequado, será possível implementar um campus inteligente de forma mais segura e eficiente (Rosa, 2021).

1.3 OBJETIVOS

A seguir, são apresentados os objetivos deste trabalho, que abrangem o estudo da implementação de um sistema inteligente no campus da UTFPR-TD, com foco na criação de um ambiente de *smart campus* e na aplicação de padrões tecnológicos.

1.3.1 OBJETIVO GERAL

O objetivo geral deste trabalho consiste em apresentar um estudo sobre os padrões utilizados em aplicações de *smart campus* e iniciar a implementação de um sistema inteligente no campus da UTFPR-TD. Busca-se compreender as principais tecnologias e práticas adotadas nesse contexto, bem como suas aplicações e benefícios, visando promover a melhoria da eficiência e qualidade dos serviços oferecidos pela universidade.

1.3.2 OBJETIVOS ESPECÍFICOS

Para alcançar o objetivo geral, são estabelecidos os seguintes objetivos específicos:

- Realizar um estudo sobre as tecnologias comumente utilizadas em *smart campus*, compreendendo suas características, funcionalidades e aplicações específicas;
- Investigar os padrões de *smart campus* mais adotados, analisando suas diretrizes, boas práticas e recomendações para a implementação de sistemas inteligentes em ambientes acadêmicos;
- Projetar um dispositivo que tem como objetivo verificar o estado das janelas nos laboratórios, permitindo a detecção e registro de sua abertura ou fechamento. Esse *hardware* será um exemplo que sistema que poderia ser integrado ao sistema inteligente do campus, contribuindo para a coleta de dados e o monitoramento das condições ambientais;
- Desenvolver e configurar um *software* básico de gerenciamento do *smart campus*, que permita a integração de dispositivos, a coleta e análise de dados, bem como a implementação de automações e tomadas de decisão inteligentes. O software será selecionado levando em consideração as necessidades e requisitos específicos do campus da UTFPR-TD.

Por meio do cumprimento desses objetivos, espera-se obter um amplo conhecimento sobre os padrões e tecnologias aplicáveis a *smart campus*, assim facilitando futuros projetos de implementação de um sistema inteligente no campus da UTFPR Toledo, contribuindo para a modernização e aprimoramento das atividades acadêmicas e serviços prestados pela universidade.

1.4 JUSTIFICATIVA

Embora tenha havido significativo esforço dedicado à implementação de *smart campus*, ainda existem muitos desafios a serem superados para sua ampla adoção e efetividade. Um dos principais limitadores para a adoção em larga escala reside na grande heterogeneidade dos dispositivos de IoT presentes nos ambientes acadêmicos. Além disso, diversas barreiras técnicas

precisam ser consideradas, tais como segurança, privacidade, padronização, interoperabilidade e configuração (Alghamdi; Shetty, 2016).

A adoção de qualquer tecnologia em um ambiente acadêmico deve ser segura e garantir a privacidade de todos os usuários envolvidos. No entanto, atender aos requisitos de segurança e privacidade pode ser especialmente desafiador em um ambiente tão heterogêneo em termos de dispositivos e tecnologias de comunicação utilizadas por eles. A incorporação de dispositivos inteligentes em um campus resulta na concentração de dezenas ou até centenas de sensores e atuadores, o que pode representar uma carga significativa em relação à configuração e manutenção desses dispositivos. É fundamental, portanto, que existam mecanismos padronizados para a configuração, substituição ou expansão desses dispositivos, a fim de simplificar e agilizar esses processos.

A transformação de um campus convencional em um campus inteligente é uma tarefa árdua que requer o envolvimento e engajamento de toda a comunidade acadêmica. Este trabalho representa um esforço inicial para estabelecer uma base conceitual sólida sobre a implementação de um campus inteligente, combinando conhecimentos teóricos com a aplicação prática de um sistema capaz de gerenciar dispositivos de IoT. Por meio dessa iniciativa, pretende-se demonstrar os benefícios e as oportunidades proporcionados por um campus inteligente, além de identificar os desafios inerentes à implantação dessas soluções tecnológicas. Ao fornecer uma estrutura inicial e uma compreensão mais aprofundada dos aspectos envolvidos, este trabalho busca estabelecer as bases para futuras pesquisas e iniciativas na área de *smart campus*, contribuindo para o avanço da tecnologia e para a melhoria da qualidade de vida acadêmica.

2 REFERENCIAL TEÓRICO

O conceito de *smart campus* tem emergido como uma tecnologia promissora que combina os princípios da Internet das Coisas (IoT) com um ambiente universitário. O *smart campus* visa proporcionar melhorias significativas nos serviços e na tomada de decisões das instituições de ensino, por meio da aplicação de soluções tecnológicas inovadoras. Neste capítulo, serão apresentados os principais conceitos e fundamentos relacionados ao *smart campus*, fornecendo uma base teórica sólida para o estudo proposto (Sánchez-torres *et al.*, 2018) . A Seção 2.1 aborda as principais tecnologias de comunicação utilizadas no contexto do *smart campus*. Em seguida, na Seção 2.2, são apresentados os protocolos de comunicação relevantes para esse ambiente. Por fim, na Seção 2.3, são exploradas as principais plataformas de integração de dispositivos de IoT (Matos, 2021) .

2.1 Tecnologias de Comunicação sem Fio

No contexto de um *smart campus*, a comunicação sem fio desempenha um papel crucial na conectividade e interação entre dispositivos e sistemas distribuídos em todo o campus. As tecnologias de comunicação sem fio fornecem a base para a implementação de soluções de Internet das Coisas (IoT) e serviços inteligentes, permitindo a troca de dados, controle e coordenação entre os dispositivos e infraestruturas do campus.

Dentre as tecnologias mais relevantes utilizadas em um *smart campus*, destacam-se o Wi-Fi, Bluetooth, Zigbee, Thread, NFC, RFID e Z-Wave. Essas tecnologias oferecem diferentes características e capacidades de comunicação sem fio, tornando-as adequadas para casos de uso específicos no ambiente do campus inteligente. O restante desta seção apresenta mais informações sobre estas tecnologias (Saccol; Reinhard, 2007).

2.1.1 Wi-Fi

O Wi-Fi é uma tecnologia de comunicação sem fio que permite a conexão de computadores e dispositivos móveis à Internet, facilitando a troca de informações entre eles por meio de um ponto de acesso. Sua ampla utilização se deve à versatilidade que oferece, embora a transmissão de dados possa sofrer interferências externas, já que o trajeto das informações não é protegido (Deng *et al.*, 2020) .

As frequências mais comuns usadas pelo Wi-Fi são 2,4 GHz e 5 GHz. A frequência de 2,4 GHz, amplamente adotada devido à sua faixa não licenciada e de uso geral em muitos países, é vulnerável à interferência, já que também é utilizada por dispositivos como telefones sem fio, aparelhos Bluetooth e dispositivos de Internet das Coisas (IoT). Por essa razão, o Wi-Fi se tornou essencial para uma grande variedade de produtos que dependem dessa tecnologia para estabelecer suas conexões.

Nos dias atuais, é bastante comum que praticamente tudo esteja conectado à Internet, e o Wi-Fi facilitou imensamente essa tendência. Graças a essa tecnologia, tem-se uma ampla gama de dispositivos que podem ser controlados por meio dela. É possivel citar exemplos como campainhas, televisões, aspiradores de pó, lâmpadas, entre outros, conforme ilustrado na Figura 1.

Figura 1 – Rede Wi-fi.

Fonte: TNS (2023).

No âmbito do conceito de *smart campus*, essa tecnologia desempenha um papel de extrema relevância, uma vez que proporciona acesso aos dispositivos. Embora haja outros meios de conexão que serão abordados ao longo deste capítulo, o Wi-Fi se destaca como o principal, pois é capaz de reunir todos os dispositivos em uma rede para permitir sua manipulação. Isso se dá pelo fato de que todos esses dispositivos necessitam estar conectados à Internet, e o Wi-Fi se apresenta como a forma mais conveniente de alcançar essa conectividade. A partir do momento em que se está conectados à Internet, torna-se possível controlar tais dispositivos a partir de qualquer lugar (Perahia; Gong, 2011) .

Os padrões de protocolo mais utilizado hoje são o IEEE 802.11ac também chamado de Wi-Fi 5 e o IEEE 802.11ax também conhecido como Wi-Fi 6. O Wi-Fi 5 foi lançado em 2014 e tem o foco em oferecer altas taxas de dados, buscando suprir a alta demanda de serviços como televisão, *streaming* e interfaces de multimídia de alta definição. Diferente de suas versões anteriores essa versão teve o foco na frequência de 5 Ghz pois assim alcança uma melhor taxa de transmissão de dados.

Apesar de sua popularidade, o protocolo Wi-Fi convencional enfrentava limitações significativas diante do aumento na demanda por dispositivos de *Wireless Local Area Network* (WLAN) em ambientes de alta densidade, como estádios, *shoppings*, aeroportos e escritórios. A grande concentração de dispositivos gera interferências e congestionamentos nos canais de frequência, exigindo o uso de canais sobrepostos para manter a conectividade (Muñoz, 2014) .

Canais de sobreposição ocorrem quando diferentes redes Wi-Fi utilizam frequências próximas ou idênticas dentro do mesmo espectro, causando interferência mútua. Isso acontece

principalmente na faixa de 2,4 GHz, que possui apenas três canais não sobrepostos (1, 6 e 11). Quando mais redes são configuradas nesses intervalos limitados, suas transmissões se cruzam, reduzindo a qualidade do sinal e a eficiência da conexão (Lugli; Sobrinho, 2012) .

Para solucionar esses desafios e atender às necessidades crescentes de IoT, foi lançado em 2016 o Wi-Fi 6. Esse novo protocolo visa facilitar a adoção e o uso de dispositivos IoT, uma vez que permite a sobreposição de canais e a adaptação mais eficiente desses equipamentos. O Wi-Fi 7 é considerado o padrão mais avançado de Wi-Fi atualmente, desenvolvido com foco na otimização do desempenho e da eficiência em ambientes com alta concentração de dispositivos, o que é especialmente relevante para a implementação de IoT em um *smart campus* (Mozaffariahrar; Theoleyre; Menth, 2022) .

Uma das características essenciais do Wi-Fi 6 é a redução da latência, um fator crucial para o funcionamento adequado de aplicações de IoT em tempo real. Além disso, o protocolo apresenta recursos avançados, como o *Target Wake Time* (TWT) , que permite que dispositivos IoT programem quando devem permanecer ligados ou entrar em modo de economia de energia, aumentando a eficiência energética e reduzindo ainda mais a latência. Outro recurso importante é o OFDMA (*Orthogonal Frequency Division Multiple Access*), que divide os canais de frequência em subcanais menores, permitindo que múltiplos dispositivos transmitam dados simultaneamente. Isso melhora significativamente a eficiência da rede, reduz a concorrência pelo uso do canal e minimiza atrasos, especialmente em ambientes de alta densidade.

O Wi-Fi 6 oferece um ambiente de comunicação robusto e otimizado para atender à crescente demanda de dispositivos IoT, sendo ideal para implantações em *smart campus* ou qualquer cenário que exija alta densidade de dispositivos e baixa latência. Com suas capacidades avançadas de gerenciamento de canais, eficiência energética e redução de atrasos, o Wi-Fi 6 desempenha um papel fundamental na expansão e viabilização da Internet das Coisas (Zhang *et al.*, 2022) .

2.1.2 Bluetooth

O Bluetooth é uma tecnologia de baixo custo criada em 1989 pela empresa Ericsson, que buscava desenvolver uma solução de comunicação sem fio para seus dispositivos. O Bluetooth foi anunciado em 1998 e, a partir de 2000, começou a ser disponibilizado comercialmente. A tecnologia opera na frequência de 2,4 GHz (Brito, 2021).

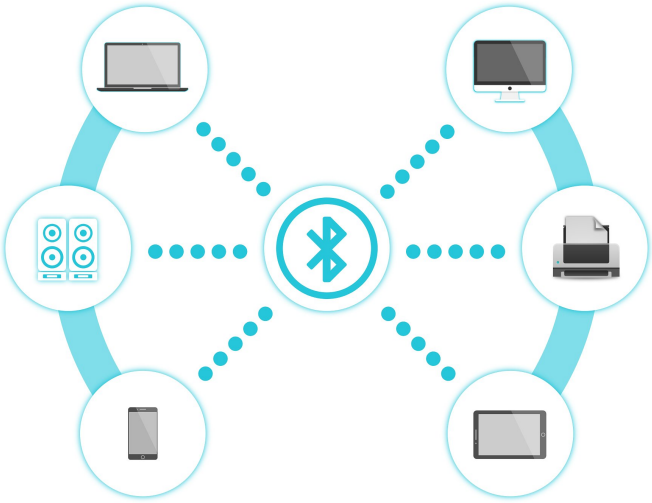
Essa faixa de frequência de 2,4 GHz é conhecida por sofrer alta interferência e poluição, similar ao que ocorre com o Wi-Fi na mesma frequência. Apesar desse desafio, o Bluetooth continua amplamente utilizado em dispositivos de pequeno porte, como *smartphones*, *tablets*, câmeras e outros dispositivos móveis (Tosi *et al.*, 2017) .

A distância de conexão do Bluetooth depende da classe de potência utilizada. Existem quatro classes de Bluetooth, sendo a segunda a mais comumente utilizada. Essa classe tem um alcance típico de cerca de 10 metros. No entanto, se for necessário um alcance maior, a

primeira classe pode ser empregada, sendo mais adequada para ambientes industriais e áreas de maior extensão, permitindo distâncias de até 100 metros.

É importante destacar que o Bluetooth não se limita a um único protocolo, mas possui sete protocolos distintos, cada um responsável por uma função específica dentro do sistema Bluetooth. Essa variedade de protocolos proporciona uma ampla gama de aplicações e usos para essa tecnologia de comunicação sem fio. No nosso dia a dia, é comum encontrarmos dispositivos que fazem uso do Bluetooth, como *smartwatches*, balanças, óculos inteligentes, monitores de batimentos cardíacos e muitos outros dispositivos que se beneficiam dessa tecnologia de conectividade sem fio. Na Figura 2 são apresentados exemplos de dispositivos que usam do Bluetooth para se conectar (Hallberg; Nilsson; Synnes, 2003).

Figura 2 – Aplicações para Bluetooth.



Fonte: 200degrees (2016).

No contexto da Internet das Coisas (IoT), o Bluetooth tem sido amplamente utilizado, muitas vezes sem que seja percebido. Um exemplo disso foi observado em shows de renomados artistas, como Taylor Swift e a banda Coldplay. Nesses eventos, os fãs receberam pulseiras de LED que eram controladas de acordo com a música, criando uma experiência imersiva e interativa. Esses dispositivos demonstram a versatilidade do Bluetooth, capaz de transformar um simples show em algo mais envolvente e tecnologicamente avançado.

Além disso, no contexto de um *smart campus*, o Bluetooth pode ser aplicado de diversas maneiras. Sensores de presença baseados nessa tecnologia podem ser utilizados para detectar a presença de pessoas em determinados locais, permitindo o monitoramento e controle inteligente de espaços. Além disso, a integração do Bluetooth com dispositivos como o Arduino, por meio de módulos Bluetooth dedicados, possibilita a automação de dispositivos e a criação de códigos personalizados para atribuições específicas, proporcionando maior flexibilidade e controle na implementação de soluções IoT.

Assim, o Bluetooth desempenha um papel fundamental no contexto da IoT, permitindo a conexão e comunicação entre dispositivos de forma eficiente e versátil. Seu uso em shows e

em um *smart campus* ilustra apenas algumas das muitas aplicações possíveis dessa tecnologia, que continua a evoluir e a impulsionar inovações em diversos campos (Melo, 2016).

2.1.3 Zigbee

A rede de comunicação Zigbee foi concebida em 2003 pelo *Institute of Electrical and Electrounics Engineers* (IEEE) em parceria com a Zigbee Alliance (Stoll, 2008). Sendo um padrão aberto (*open standard*), ganhou notoriedade devido ao seu baixo consumo de energia. Essa tecnologia foi desenvolvida para suprir algumas lacunas do Wi-Fi e do Bluetooth, uma vez que ambos operam em taxas de transmissão mais elevadas. No entanto, em muitas aplicações de IoT, não é necessário transmitir grandes volumes de dados, mas sim informações sucintas, como alguns bits que indiquem o status do dispositivo. Nesse contexto, o Zigbee surgiu para resolver essas limitações. Embora seja possível utilizar o Bluetooth e o Wi-Fi, fazê-lo seria um desperdício de recursos e energia, uma vez que os dispositivos Zigbee consomem menos energia.

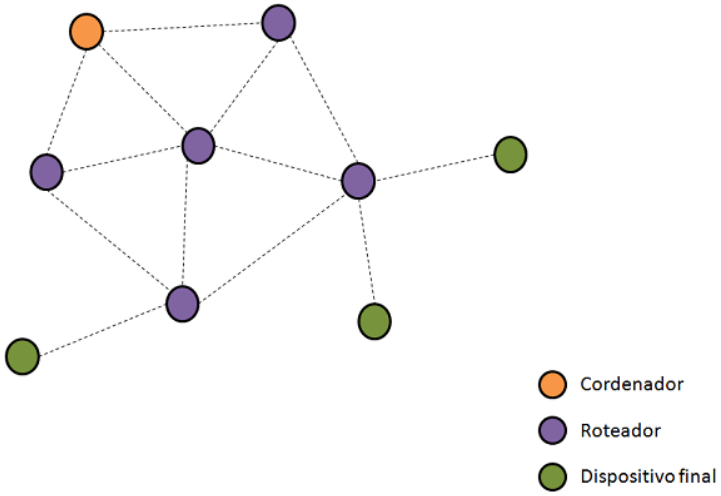
Uma das vantagens distintas dessa tecnologia é que os dispositivos Zigbee possuem o protocolo 802.15.4, que permite a comunicação entre dispositivos e encaminha o sinal de um aparelho para outro, possibilitando a descoberta de dispositivos de forma adequada e automática. Isso configura uma comunicação de ponto a ponto, baseada na capacidade dos equipamentos de ouvirem outros elementos da rede. No entanto, também existem desafios associados a essa tecnologia e diferentes tipos de dispositivos Zigbee (Monsignore, 2007) .

O componente básico é o dispositivo final Zigbee (ZED), que é capaz de se comunicar com os demais nós da rede. Em seguida, tem-se o roteador Zigbee (ZR), que atua como final e também pode ser usado como dispositivo intermediário de retransmissão. No topo da hierarquia, encontra-se o coordenador Zigbee (ZC), que controla os demais dispositivos Zigbee (Azevedo,) . Um aspecto dessa tecnologia é que, para utilizar um dispositivo Zigbee, é necessário um *hub*, que nesse caso seria o coordenador Zigbee, responsável pela coordenação dos outros dispositivos e pela comunicação entre eles. É por isso que essa tecnologia apresenta vantagens em relação ao Wi-Fi, já que não sobrecarrega a rede, permitindo a conexão de um maior número de dispositivos na mesma rede, considerando que apenas um dispositivo final é conectado ao Wi-Fi (Monsignore, 2007) . A Figura 3 mostra uma representação de uma rede Zigbee contendo dispositivos ZED, ZR e ZC.

Atualmente, a maioria dos dispositivos Zigbee são do tipo roteador (ZR). Isso significa que é possível usar esses dispositivos com maior probabilidade de sucesso, pois eles atuam como roteadores, estendendo o alcance do sinal e proporcionando uma resposta mais rápida. Comparados ao Wi-Fi e ao Bluetooth, os dispositivos Zigbee apresentam tempos de reação menores, o que significa que suas respostas são mais rápidas.

Em um ambiente de *smart campus*, esses dispositivos seriam uma escolha adequada. Além de consumirem pouca energia, o que resulta em maior eficiência energética, sua rede pode ser expandida conforme as necessidades, sem sobrecarregar a rede Wi-Fi existente. Isso

Figura 3 – Rede Mesh ZigBee.



Fonte: Stoll (2008).

torna os dispositivos Zigbee uma excelente opção, pois permitem a conexão de um grande número de dispositivos sem comprometer a capacidade da rede Wi-Fi. No entanto, vale destacar que a eficiência de Zigbee também depende da taxa de dados disponível, já que ele utiliza uma largura de banda mais limitada em comparação com outras tecnologias, o que pode impactar o desempenho em alguns cenários. (Monsignore, 2007) .

2.1.4 Thread

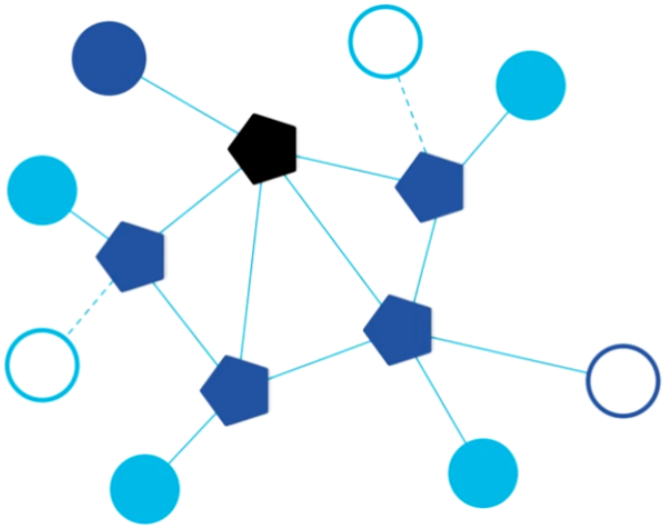
A comunicação em Thread representa uma inovadora tecnologia que adentrou o mercado recentemente. Possuindo um protocolo aberto e a utilização do IPv6, seu lançamento ocorreu em 2015, com a finalidade de atender especialmente os sistemas de casas inteligentes. Similar ao Zigbee, essa tecnologia opera em uma rede *mesh* IEEE 802.15.4 auto adaptável (Correa, 2018).

A rede Thread também engloba diferentes tipos de dispositivos e modos de operação, contudo, em contraste com o Zigbee, não requer especificamente um coordenador central. Isso se deve ao fato de que essa tecnologia está incorporada em alguns dispositivos, tais como a Apple TV, o HomePod Mini, a quarta geração do Amazon Echo e roteadores da Eero, que já utilizam essa tecnologia.

Portanto, é necessário ao menos um desses dispositivos mencionados, pois eles atuam como "*hubs*". No entanto, diferentemente do Zigbee, a tecnologia Thread é capaz de se adaptar automaticamente. Por exemplo, caso ocorra a desconexão de algum desses "*hubs*", os dispositivos intermediários se conectam a outro disponível. Em casos de instabilidade de conexão, o mesmo processo ocorre, direcionando a conexão para o dispositivo mais próximo, a fim de evitar interrupções. Vale ressaltar que a capacidade máxima suportada por uma rede Thread ultrapassa a marca de 250 dispositivos para cada dispositivo intermediário.

Dessa forma, uma vez que não exige um *hub* específico, torna-se necessário designar um dispositivo como líder, responsável pela comunicação com os demais aparelhos. A seguir, há um exemplo ilustrativo da adaptação das redes *mesh*, exibido nas imagens.

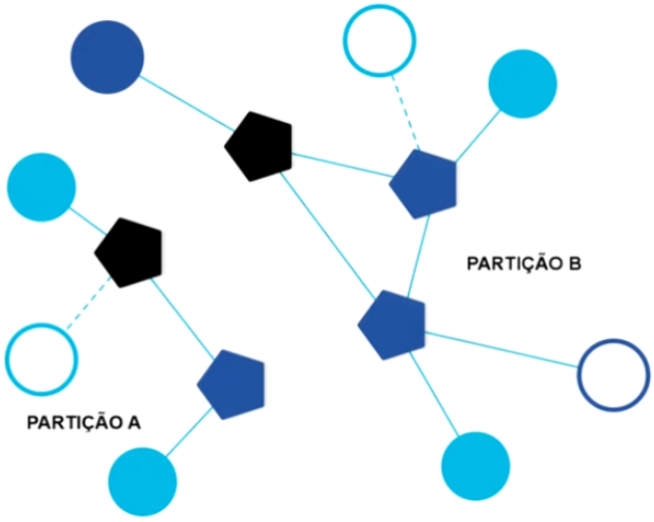
Figura 4 – Rede Mesh com uma malha.



Fonte: Texeira (2023).

Na Figura 4 é possivel observar uma malha única composta por um dispositivo líder, bem como roteadores e dispositivos finais. A rede Thread é projetada de modo a permitir uma adaptação eficiente caso um roteador não consiga estabelecer comunicação com outro nó. Assim, a malha Thread se ajusta de maneira adequada para evitar perdas na conexão.

Figura 5 – Rede Mesh adaptada.



Fonte: Texeira (2023).

A Figura 5 representa a malha Thread após sua divisão e adaptação automática da rede. Essa capacidade de ajuste automático é uma das características que torna esse modo de comunicação tão vantajoso em um contexto de *smart campus*. No entanto, como se trata de uma tecnologia relativamente nova, existem alguns obstáculos em relação à sua adoção,

especialmente no Brasil, onde ainda não é tão comum. Além disso, questões como os licenciamentos de banda e a compatibilidade com dispositivos existentes podem representar desafios para a implementação do Thread, pois é necessário garantir que a infraestrutura de rede esteja de acordo com as regulamentações locais e que os dispositivos compatíveis sejam amplamente acessíveis.

No entanto, à medida que o tempo passa, essa tecnologia tende a se tornar mais viável. A cada momento, novos sensores podem ser desenvolvidos e a comercialização desses dispositivos pode se expandir com o surgimento de mais empresas que adotam a tecnologia Thread. Diferentemente de outras redes sem fio, a Thread não apresenta problemas de compatibilidade entre marcas de dispositivos, permitindo uma integração mais flexível, sem a necessidade de adaptações complexas.

2.1.5 NFC

O *Near Field Communication* (NFC) é um sistema de identificação por radiofrequência que se baseia na proximidade física entre os dispositivos para estabelecer a comunicação. Ao contrário das tecnologias anteriores, que permitiam a comunicação a certa distância, o NFC requer o contato direto entre as partes envolvidas. Atualmente, essa tecnologia é amplamente utilizada em cartões de bancos, vales-transporte e até mesmo em cartões de visita, mas suas aplicações não se limitam a esses exemplos. Por exemplo, é possível encontrar o NFC sendo empregado em sistemas de segurança, como fechaduras eletrônicas.

O NFC divide-se em duas categorias principais: as etiquetas ou cartões que contêm as informações e as máquinas que facilitam a comunicação entre as etiquetas e os dispositivos. Em casos específicos, como nos *smartphones* atuais, essas duas funções são desempenhadas pelo mesmo dispositivo. Uma das grandes vantagens dessa tecnologia é que as etiquetas não requerem energia própria, pois o dispositivo que realiza a comunicação transmite uma pequena carga que ativa a etiqueta por alguns segundos, o tempo necessário para realizar a troca de informações. Além disso, o NFC possui baixa latência, o que resulta em um processo de comunicação com menos atraso (Rahul *et al.*, 2015)

Outro aspecto favorável ao NFC é o seu custo reduzido, o que facilita seu uso e aquisição. Essa característica torna o NFC especialmente adequado para ambientes de *smart campus*, onde pode ser implementado de maneira prática. Por exemplo, ao serem incorporadas aos crachás universitários, as etiquetas NFC carregam as informações dos alunos, evitando assim a necessidade de preencher fichas de acesso e economizando tempo. Basta encostar o crachá para registrar a identidade do usuário e controlar o acesso a determinados locais, como salas de aula e laboratórios, evitando inconvenientes e permitindo o monitoramento das entradas e saídas de alunos e funcionários. Além disso, devido ao seu tamanho reduzido e quase imperceptível, as etiquetas NFC podem ser facilmente integradas aos crachás universitários. A Figura 6 mostra um exemplo dos locais aos quais pode-se aplicar o NFC.

Figura 6 – Aplicação para NFC.

Fonte: Filosofia (2023).

Atualmente, é amplamente difundido o uso dessas etiquetas na automação residencial, onde desempenham o papel de um botão capaz de executar diversas ações simultaneamente. Essa aplicação proporciona uma solução elegante para evitar possíveis lapsos de memória humana, como esquecer de trancar uma porta ou fechar uma janela (Madlmayr *et al.*, 2008).

Devido aos benefícios mencionados, essa tecnologia tem experimentado um aumento significativo em seu uso, tornando-se cada vez mais acessível e popular.

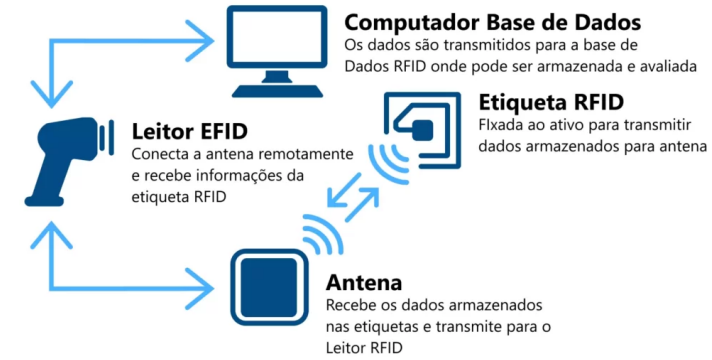
2.1.6 RFID

A tecnologia NFC é derivada da tecnologia *Radio Frequency Identification* (RFID) . Ao contrário do NFC, o RFID permite a comunicação em distâncias relativamente maiores. Essa característica torna o RFID adequado para aplicações que envolvem trânsito, como sistemas de pedágio com liberação automática. Os dispositivos RFID possuem componentes adicionais em relação ao NFC, incluindo *transponders*, transceptores (leitores), antenas e *middleware* (Yao; Chu; Li, 2010) .

Os *transponders* são as etiquetas RFID, que armazenam as informações relevantes. Os transceptores são os leitores RFID que captam as informações contidas nas etiquetas. As antenas desempenham um papel essencial na comunicação, permitindo a transmissão e recepção de sinais entre as etiquetas e os leitores. Por fim, o *middleware* é o software responsável pelo gerenciamento e fluxo de dados das etiquetas RFID. Essa distinção entre NFC e RFID reflete as diferentes necessidades e aplicações dessas tecnologias, sendo o RFID mais adequado para cenários que exigem comunicação em distâncias maiores e o NFC para interações próximas e de curto alcance. A Figura 7 mostra o ciclo de funcionamento do RFID.

As diferenças entre o RFID e o NFC são sutis, mas significativas. Uma delas é a distância de comunicação. Como mencionado anteriormente, o RFID possui um alcance maior, o que pode tornar a comunicação mais vulnerável em certos casos, como no uso de cartões de crédito.

Figura 7 – Esquema de funcionamento de um RFID



Fonte: cpcon (2023).

Por outro lado, o NFC é projetado para interações de curto alcance, o que aumenta a segurança nessas transmissões (Weinstein, 2005) .

Outra diferença importante é a disponibilidade de dispositivos. No caso do NFC, existem dispositivos que funcionam tanto como leitores quanto como etiquetas, como é o caso dos *smartphones*. Já o RFID não possui essa funcionalidade, sendo que há a distinção clara entre os leitores e as etiquetas.

Uma aplicação potencial do RFID seria no controle de acesso de veículos em uma universidade, por exemplo. Isso facilitaria o monitoramento e controle de acesso, tornando os estacionamentos mais seguros e dificultando roubos ou furtos (Narciso, 2008) .

2.1.7 Z-Wave

A tecnologia Z-wave foi introduzida em 2001 e, em termos gerais, apresenta semelhanças com outros protocolos conhecidos, como Zigbee e Thread. Todos eles utilizam a lógica de rede *mesh*, embora cada um possua suas peculiaridades. No caso do Z-wave, uma característica a ser considerada é que, dependendo da região em que é adquirido, ele pode operar em frequências diferentes. Portanto, é importante prestar atenção a esse aspecto ao realizar a compra.

Ao contrário de algumas outras tecnologias, o emparelhamento de dispositivos Z-wave possui uma camada adicional de segurança. Geralmente, envolve inserir um código ou escanear um QR *code* durante o processo de configuração. Além disso, assim como o Zigbee, o Z-wave possui três tipos principais de dispositivos: o *hub* (controlador central), os roteadores e os dispositivos finais (Yassein; Mardini; Khalil, 2016) .

A rede Z-wave tem capacidade para conectar até 232 dispositivos, o que a torna uma opção interessante para implantações em *smart campus* ou mesmo em ambientes empresariais. Além disso, o Z-wave oferece um nível de segurança superior em comparação a outros dispositivos (Badenhop *et al.*, 2017) .

Um aspecto vantajoso do Z-wave é que, até recentemente, era um protocolo fechado. Isso resulta em uma maior compatibilidade entre produtos de diferentes marcas, facilitando para os usuários a utilização de dispositivos Z-wave em suas configurações residenciais ou comerciais.

2.1.8 Considerações sobre as Tecnologias de Comunicação sem Fio

Após explorar os diversos tipos de redes sem fio, é possível concluir que cada uma delas apresenta aspectos positivos e negativos, bem como aplicações específicas. Por exemplo, o Wi-Fi possui um alcance longo e uma alta taxa de transferência de dados, mas consome uma quantidade significativa de energia. Essa dinâmica se repete com os outros dispositivos, cada um oferecendo vantagens em áreas específicas. É por isso que a combinação dessas tecnologias se torna tão interessante, exigindo o uso de uma plataforma de integração. A seguir, é apresenta na Tabela 1 uma comparação entre as tecnologias de comunicação sem fio (Saccol; Reinhard, 2007) .

Tabela 1 – Comparação entre tecnologias de comunicação sem fio.

Tecnologia	Alcance	Consumo de Energia (Dependendo do Modo)	Taxa de Transferência	Topologia de Rede	Segurança
Wi-Fi	Longo	Alto	Alta	Ponto a Ponto	Boa
Bluetooth	Curto	Baixo	Média	Ponto a Ponto	Moderada
Zigbee	Médio	Baixo	Baixa	Malha	Boa
NFC	Curto	Baixo	Baixa	Ponto a Ponto	Alta
Thread	Médio	Baixo	Média	Malha	Boa
RFID	Curto	Baixo	Baixa	Ponto a Ponto	Baixa
Z-wave	Médio	Baixo	Baixa	Malha	Boa

Fonte: Elaborado pelo autor (2023).

Essa tabela proporciona uma visão geral das características das tecnologias de comunicação sem fio abordadas. É importante destacar que as especificações podem variar dependendo das implementações específicas e do ambiente de implantação. A escolha da tecnologia mais adequada dependerá das necessidades e requisitos específicos de cada aplicação.

2.2 Protocolos e Padrões de Comunicação

A comunicação eficiente e confiável entre dispositivos de IoT desempenha um papel crucial no contexto de um *smart campus*, pois permite a interconexão e coordenação de uma ampla variedade de dispositivos distribuídos por todo o campus. Para viabilizar essa comunicação, são utilizados protocolos e padrões de comunicação específicos, estabelecendo diretrizes e regras para a troca de dados e informações entre os dispositivos conectados.

Dentre os protocolos de comunicação mais comuns em um *smart campus*, destacam-se o HTTP *(Hypertext Transfer Protocol)*, MQTT *(Message Queuing Telemetry Transport)*, CoAP *(Constrained Application Protocol)* e Bluetooth Low Energy (BLE). Além desses protocolos, é importante mencionar a expectativa em torno do protocolo Matter (anteriormente conhecido como Projeto CHIP - *Connected Home over IP*), que visa oferecer uma solução padrão e interoperável para dispositivos domésticos inteligentes. O Matter tem o potencial de simplificar a integração e a comunicação entre dispositivos IoT em um *smart campus.* Estes protocolos de comunicação desempenham um papel essencial na conectividade e interoperabilidade dos dispositivos, permitindo a troca eficiente de dados e informações entre diferentes sistemas. Cada protocolo possui suas características e benefícios únicos, o que os torna adequados para diferentes tipos de aplicações e cenários (Loureiro *et al.*, 2003) .

Além desses protocolos, existem também mecanismos de integração, como os *Webhooks*, que não são propriamente protocolos, mas representam padrões ou formas de comunicação entre sistemas. Os *Webhooks* são gatilhos que permitem a comunicação em tempo real entre diferentes sistemas, notificando eventos e desencadeando ações em resposta a eles. Essa integração facilita a troca de informações entre dispositivos heterogêneos presentes no *smart campus*, possibilitando a interoperabilidade e a automação de processos.

Esses protocolos e padrões desempenham um papel fundamental no estabelecimento de um ecossistema conectado e inteligente em um *smart campus*. Por meio dessas soluções, é possível integrar dispositivos de diferentes tipos e realizar a troca de informações de forma eficiente, promovendo a automação, o monitoramento em tempo real e a tomada de decisões baseada em dados, contribuindo assim para a eficiência operacional, a segurança e a qualidade dos serviços prestados pela instituição de ensino.

O restante desta seção apresenta, de maneira detalhada, protocolos e padrões de comunicação comumente utilizados em *smart campus*.

2.2.1 CoAP

O *Constrained Application Protocal* (CoAP) é um protocolo Machine-to-Machine (M2M) que se concentra na transferência de dados web para uso em nós restritos em redes de Internet das Coisas (IoT). Entre suas características, destacam-se a troca de mensagens assíncrona, o suporte a *Uniform Resource Identifier* (URI) , a baixa sobrecarga de cabeçalho e a baixa complexidade de análise. Com um armazenamento simples e a funcionalidade de *proxy* em *cache*, o CoAP é projetado para adaptar protocolos web genéricos aos requisitos especiais dos ambientes restritos. Além disso, ele possui a capacidade de interagir com o HTTP, promovendo assim a integração com a web.

O CoAP adota um modelo que se assemelha ao modelo cliente/servidor do HTTP. Suas interações *Machine to Machine* (M2M) permitem que os dispositivos atuem simultaneamente como cliente e servidor. Para garantir a confiabilidade, cada mensagem implementa um identificador, permitindo a identificação de mensagens duplicadas. Além disso, as mensagens pos-

suem um tempo limite padrão e utilizam o mecanismo de *backoff* exponencial para retransmissão (Khattak; Ruta; Sciascio, 2014) .

No contexto do modelo TCP/IP, o protocolo CoAP encontra-se entre a camada de aplicação e a camada de transporte, criando duas subcamadas: a camada de requisições/transporte e a camada de mensagens. Esse protocolo pode ser utilizado em dispositivos Zigbee, aproveitando assim suas capacidades de comunicação (Arvind; Narayanan, 2019) .

2.2.2 MQTT

O protocolo *Message Queue Telemetry Transport* (MQTT) é uma tecnologia que surgiu no final dos anos 1990 e foi desenvolvida com o objetivo de facilitar a conexão entre dispositivos remotos que possuem restrições de memória e banda de rede limitada. Com uma arquitetura baseada em padrões de publicação/assinatura, o MQTT envolve três entidades distintas: o *publisher*, o *broker* e o *subscriber* (Silveira; Gradvohl, 2021) .

Uma das principais diferenças entre o MQTT e o protocolo HTTP reside no fato de que, no MQTT, o cliente não precisa solicitar ativamente as informações necessárias. Em vez disso, ele realiza a assinatura de um recurso de interesse e, a partir desse momento, o *broker* assume a responsabilidade de enviar as informações atualizadas aos *subscribers* quando o *publisher* realizar atualizações.

O *broker* desempenha um papel central nesse protocolo, atuando como um dispositivo intermediário responsável por facilitar a comunicação entre as outras duas entidades mencionadas anteriormente. Essa arquitetura permite uma troca eficiente de informações em ambientes com restrições de recursos (Quincozes; Emilio; Kazienko, 2019) .

O protocolo MQTT é amplamente utilizado em diferentes tipos de tecnologias de comunicação, tais como redes Wi-Fi, Zigbee e até mesmo Bluetooth. Ele se adapta bem a essas tecnologias e possibilita a conexão de dispositivos em diversos ambientes, contribuindo para a expansão e a integração da Internet das Coisas.

Em resumo, o MQTT é um protocolo de comunicação desenvolvido para atender às necessidades de dispositivos remotos com restrições de memória e banda de rede. Com sua arquitetura de publicação/assinatura e a intermediação do *broker*, ele oferece uma solução eficiente para a troca de informações em redes Wi-Fi, Zigbee, Bluetooth e outras (Lugli; Sobrinho, 2012) .

2.2.3 HTTP

O protocolo *Hypertext Transfer Protocol* (HTTP) é um protocolo fundamentado no modelo TCP/IP, utilizado para a transferência de dados como arquivos HTML, imagens e strings de busca na *World Wide Web*. Utilizando a porta 80 na camada TCP, esse protocolo estabelece uma forma de comunicação padronizada entre dois *hosts*. Ele se baseia no modelo de requisição/resposta, no qual o cliente envia uma requisição ao servidor contendo um *link* de um

recurso, e o servidor responde informando se o *link* é válido ou não (Jaafar; Abdullah; Ismail, 2019) .

Dentre os métodos disponíveis no protocolo HTTP, os mais utilizados são *POST, GET, PUT e DELETE*. O método *POST* tem a finalidade de criar recursos dentro do servidor, enquanto o método *GET* é utilizado para buscar um recurso que já está armazenado no servidor. O método *PUT* permite a modificação e atualização de um recurso no servidor, e o DELETE é utilizado para remover um recurso do servidor.

Além disso, o protocolo HTTP também é empregado na implementação de *webhooks*, um método comumente utilizado em IoT. Os *webhooks* se baseiam no envio de requisições HTTP *POST* a partir de um aplicativo web, contendo uma URL predefinida. Essa comunicação depende da ocorrência de um evento, como no caso da tecnologia NFC. Quando um leitor se aproxima de uma *tag* contendo uma URL, esse evento desencadeia a ativação desse *link*. Por essa razão, o uso de *webhooks* é comum em IoT (Seyyar; Çatak; Gül, 2018).

Essa tecnologia utiliza a comunicação de API para API, permitindo uma ampla gama de integrações entre dispositivos. Essas integrações são possíveis graças à interoperabilidade proporcionada pelo protocolo HTTP, possibilitando a comunicação e intercâmbio de dados entre diferentes sistemas e dispositivos IoT (Biswas; Biswas, 2021) .

2.2.4 Bluetooth Low Energy (BLE)

O *Bluetooth Low Energy* (BLE) é um meio de comunicação de baixo custo e baixo consumo de energia. Muitos recursos do Bluetooth clássico foram herdados pelo BLE, porém essa tecnologia vem sendo amplamente aproveitada no contexto da Internet das Coisas. Seu baixo consumo de energia torna possível a utilização em diversos dispositivos, muitas vezes sem que se perceba que estão utilizando essa tecnologia (Mackensen; Lai; Wendt, 2012) .

Alguns exemplos de dispositivos que utilizam o BLE incluem relógios inteligentes, sensores de temperatura, sensores de umidade e aplicativos de saúde que necessitam enviar pequenos dados. Atualmente, o BLE possui dois protocolos principais: o iBeacon e o Eddystone. O iBeacon foi desenvolvido pela Apple e possui seu código fechado. Ele transmite apenas um pacote de publicidade (*advertising*) composto por um número de identificação, que é construído por três partes: a UUID, major e minor (Tosi *et al.*, 2017) .

Por outro lado, o Eddystone, desenvolvido pela Google e de código aberto, oferece três tipos diferentes de pacotes: o Eddystone-UID, que é semelhante ao iBeacon; o Eddystone-URL, que não requer a instalação prévia de um aplicativo desenvolvedor; e o Eddystone-TLM, que envia dados do sensor (Darroudi; Gomez, 2017) .

Essas características do BLE tornam-no uma escolha atrativa para diversos cenários de IoT, proporcionando uma comunicação eficiente e de baixo consumo de energia.

2.2.5 Matter

A tecnologia Matter, conhecida anteriormente como “Project CHIP” (*Connected Home over IP*), surge como uma promissora proposta para revolucionar o campo da Internet das Coisas. Seu principal objetivo é simplificar a comunicação entre dispositivos, reduzindo as complexidades associadas às instalações. Com um enfoque no protocolo de *Internet Protocol Version 6* (IPv6) , essa tecnologia conta com a participação de um grupo diversificado de mais de 200 empresas, incluindo gigantes como Apple, Google, Zigbee e Amazon.

A proposta do Matter é resolver o desafio da heterogeneidade presente nos dispositivos IoT, permitindo uma maior integração e interoperabilidade entre diferentes marcas e modelos. Essa abordagem é particularmente atrativa para usuários leigos que desejam adentrar no mundo da IoT, uma vez que a tecnologia promete simplificar as interações entre dispositivos.

O Matter utilizará as tecnologias de Wi-Fi e Thread para proporcionar uma infraestrutura de comunicação segura e confiável. Estamos entrando em uma nova era para a IoT, com soluções que superam os desafios de compatibilidade entre dispositivos e marcas. Com isso, diversas áreas serão impactadas, desde residências inteligentes até cidades inteligentes, permitindo uma integração mais eficiente e coesa de dispositivos de diferentes fabricantes (Riaz; Kim; Ahmed, 2009) .

Uma aplicação ideal para a tecnologia Matter seria em ambientes de *smart campus*, nos quais o uso da tecnologia Thread possibilitaria a conexão de um grande número de sensores, além de oferecer baixo consumo energético. No entanto, como se trata de uma tecnologia recente, sua viabilidade em termos de custos e adoção em larga escala ainda pode levar algum tempo para se concretizar.

2.3 Plataformas de Integração

As plataformas de integração, como SmartThings, Google Home, Amazon Alexa e Home Assistant , desempenham um papel fundamental na construção de um ecossistema conectado em um *smart campus*. Essas plataformas atuam como intermediárias entre os dispositivos e sistemas do campus, oferecendo uma interface unificada para gerenciamento, controle e automação.

Esse tipo de plataforma proporciona a integração de dispositivos heterogêneos, permitindo que diferentes tecnologias e protocolos de comunicação sejam harmonizados em uma única plataforma. Dessa forma, os usuários podem controlar e monitorar vários dispositivos, como iluminação, sistemas de segurança, climatização e entretenimento, por meio de uma única interface. Além disso, essas plataformas geralmente oferecem recursos avançados, como programação de cenas, criação de rotinas personalizadas e integração com assistentes de voz. Isso permite que os usuários configurem cenários automatizados e personalizados, adaptando o ambiente do *smart campus* às suas necessidades e preferências (Madakam, 2015) .

Essas plataformas também oferecem recursos de análise e monitoramento, permitindo que os usuários obtenham percepções sobre o uso de energia, segurança e eficiência dos dispositivos e sistemas do campus. Com base nesses dados, é possível tomar decisões informadas para otimizar o desempenho, reduzir os custos operacionais e melhorar a experiência dos usuários no ambiente do *smart campus* (Li *et al.*, 2017) .

De modo resumido, as plataformas de integração desempenham um papel central na construção de um *smart campus*, proporcionando a interoperabilidade entre dispositivos e sistemas diversos, facilitando o controle e a automação, e oferecendo recursos avançados de análise e monitoramento. Essas plataformas contribuem para a criação de um ambiente conectado e inteligente, que promove a eficiência operacional, a comodidade dos usuários e a melhoria geral da experiência no campus. A seguir, são apresentas algumas das plataformas mais comuns. (Kowalski *et al.*, 2019) .

2.3.1 SmartThings

O SmartThings foi lançado em 2012 por uma *startup*, que posteriormente, em 2014, vendeu seu aplicativo para a Samsung. Atualmente, esta plataforma está sendo aprimorada e desenvolvida pela Samsung, com o objetivo de facilitar a comunicação entre dispositivos, permitindo a integração de dispositivos Zigbee, Wi-Fi e Bluetooth (Stojmenovic, 2014) .

Essa plataforma de integração é capaz de se conectar a plataformas de assistência de voz, como o Google Home e a Amazon Alexa. Isso é especialmente relevante, uma vez que a tecnologia em questão possui várias limitações de compatibilidade, as quais o SmartThings busca solucionar. Dessa forma, é possível criar rotinas de aplicação mais eficientes, baseadas em sensores (Stojmenovic, 2014) .

Além disso, o SmartThings oferece uma interface de usuário de fácil navegação, o que proporciona simplicidade para os novos usuários. Sendo parte integrante da Samsung, a conexão com os dispositivos da marca é ainda mais simples.

Vale destacar que essa plataforma possui uma comunidade robusta, o que proporciona suporte adequado em caso de ocorrência de eventuais problemas e a necessidade de correções.

2.3.2 Home Assistant

O Home Assistant é atualmente uma das plataformas mais abrangentes disponíveis, oferecendo uma ampla gama de funcionalidades que outras plataformas não possuem. Pode ser considerado uma versão aprimorada do Samsung SmartThings, uma vez que algumas funcionalidades são semelhantes. No entanto, o Home Assistant proporciona um maior grau de liberdade no uso de dispositivos e permite a criação de automações que não seriam viáveis em outras plataformas (Yamazaki *et al.*, 2012) .

Essa plataforma de integração vai além do simples controle e estado dos dispositivos, permitindo a criação de rotinas complexas e apresentando modos de exibição mais simplificados. O Home Assistant pode ser executado em qualquer dispositivo, desde um notebook antigo até um Raspberry Pi. É possível utilizá-lo em um dispositivo móvel ou em uma máquina virtual em um computador convencional.

No entanto, um desafio encontrado nessa plataforma é a sua curva de aprendizado, que é considerada alta devido à sua complexidade e ao amplo conjunto de opções disponíveis. O Home Assistant oferece a liberdade de criar automações por meio de código e até mesmo por meio de diagramas de blocos. Essa abordagem pode não ser tão atraente para usuários que buscam automatizar tarefas simples, mas para aqueles que desejam transformar suas residências em casas inteligentes, o Home Assistant é a melhor opção, devido à sua capacidade de integração com uma ampla variedade de dispositivos.

É importante ressaltar que o Home Assistant possui a maior compatibilidade entre os sistemas de integração, permitindo a integração de dispositivos Wi-Fi, Bluetooth, Zigbee e até mesmo Z-Wave, que são os dispositivos mais comuns atualmente. No entanto, pode haver dificuldades na comunicação com assistentes de voz, como a Amazon Alexa e o Google Home, devido aos desafios iniciais encontrados ao conectar esses assistentes devido à curva de aprendizado exigida pela plataforma (Yassein; Mardini; Khalil, 2016) .

2.3.3 Amazon Alexa

A Amazon Alexa vai além de uma simples plataforma de integração, funcionando como uma assistente de voz com entonação mais humanizada. Isso resulta em respostas menos predefinidas em comparação à assistente presente no Google Home. No entanto, no que diz respeito à integração, a Alexa apresenta certas limitações que comprometem sua eficácia nesse aspecto (Bogdan *et al.*, 2021) .

Embora a Alexa possua um amplo espectro de habilidades e seja compatível com diversos dispositivos, sua integração com certos produtos é falha. Tal fato pode gerar frustração aos usuários, uma vez que uma variedade de dispositivos não se conecta de maneira eficiente à assistente. Por conseguinte, a Alexa é majoritariamente utilizada como uma assistente de voz e é comumente conectada a plataformas de integração mais robustas, como o Home Assistant ou o SmartThings.

Essas plataformas, por sua vez, proporcionam uma integração mais abrangente, permitindo que a Alexa interaja com uma maior diversidade de dispositivos e execute automações mais avançadas. Assim, a Alexa complementa e aprimora as funcionalidades dessas plataformas, expandindo as possibilidades de controle e automação no âmbito de um ambiente inteligente.

2.3.4 Google Home

Assim como a Amazon Alexa, o Google Home desempenha mais o papel de assistente de voz do que o de uma plataforma de integração. Sua voz tende a ser mais robotizada em comparação à Alexa, porém, caso o usuário seja adepto dos serviços Google, o Google Home pode oferecer respostas mais específicas. Assim como a Alexa, o Google Home também é compatível com uma variedade de dispositivos. Contudo, sua principal função é atuar como assistente de voz, e não como uma plataforma de integração para automação residencial (Meraj, 2021) .

Embora o Google Home possa ser útil em estágios iniciais, quando há poucos dispositivos, ele pode encontrar limitações ao lidar com uma quantidade maior de dispositivos ou ao tentar automatizar rotinas complexas. Nesse contexto, plataformas mais avançadas, como o Home Assistant e o SmartThings, se destacam, oferecendo recursos mais aprimorados para automação residencial.

Portanto, embora o Google Home seja capaz de interagir com dispositivos e auxiliar em tarefas básicas, sua capacidade como plataforma de integração para automação residencial é limitada em comparação com outras soluções mais especializadas. A escolha entre a Amazon Alexa e o Google Home dependerá das necessidades individuais do usuário e da complexidade das automações desejadas (Vishwakarma *et al.*, 2019) .

2.3.5 Considerações finais

Existem atualmente no mercado diversas plataformas de integração, sendo as mais destacadas para automação residencial o SmartThings e o Home Assistant. Essas plataformas oferecem um amplo espectro de possibilidades de automação. O SmartThings é especialmente indicado para usuários iniciantes, pois permite uma fácil integração com assistentes de voz. Já o Home Assistant, por sua vez, proporciona uma ampla gama de manipulações específicas de sensores, sendo mais adequado para usuários com maior experiência e conhecimento na área.

Cabe ressaltar que, embora a Amazon Alexa e o Google Home sejam assistentes de voz populares e possam ser utilizados como plataformas de integração, não oferecem todas as funcionalidades e automações disponíveis nas plataformas especializadas mencionadas anteriormente. Eles apresentam limitações em comparação com essas plataformas mais robustas.

A seguir, é apresenta a Tabela 2, que mostra uma comparação entre as plataformas de integração mencionadas. Lembrando que essa tabela é uma síntese geral das características e recursos de cada plataforma, e as informações podem variar conforme as atualizações e versões. A escolha entre essas plataformas dependerá das necessidades individuais de automação residencial, do nível de experiência técnica e das preferências pessoais. Recomenda-se avaliar com cuidado cada plataforma e considerar os recursos que são mais importantes para o contexto específico antes de tomar uma decisão.

Tabela 2 – Comparação entre plataformas de integração.

Recursos	Home Assistant	SmartThings	Amazon Alexa	Google Home
Integração com assistentes de voz	Sim	Sim	Sim	Sim
Personalização	Alta	Moderada	Limitada	Limitada
Suporte a automações complexas	Sim	Sim	Limitado	Limitado
Compatibilidade com dispositivos	Ampla	Ampla	Ampla	Ampla
Aprendizado inicial	Moderado	Fácil	Fácil	Fácil
Flexibilidade de personalização	Alta	Moderada	Restrita	Restrita
Preço	Gratuito	Gratuito	Varia	Varia

Fonte: Elaborado pelo autor (2023).

2.4 Implementações de *smart campus*

A implementação de um campus inteligente pressupõe a necessária diligência no que concerne à determinação do ponto de partida e à seleção do sensor inicial a ser empregado. Nesse contexto, a análise dos campi preexistentes que já incorporaram essa inovação desempenha um papel fundamental ao simplificar a viabilidade de sua adoção em novas instituições de ensino superior. A construção de uma sólida base conceitual outorga maior precisão a essa abordagem, direcionando a atenção para a resolução das potenciais adversidades que possam surgir ao longo do processo de implementação (Polin *et al.*, 2023) .

2.4.1 Aplicações

Diversas instituições de ensino superior, tanto nacionais como internacionais, têm adotado a implementação de smart campus. Na Universidade Federal do Pará, encontram-se em vigor várias aplicações notáveis, destacando-se, dentre elas, o mapeamento abrangente da instituição. Essa ferramenta proporciona uma visão panorâmica da totalidade da universidade, realçando os pontos de interesse para a comunidade estudantil. Além disso, ela viabiliza a utilização de uma funcionalidade de busca de locais e a visualização de rotas (Neves *et al.*, 2017).

Igualmente, podemos identificar exemplos notáveis de implementações em outras instituições de ensino, a exemplo da Universidade Estadual de Campinas (Unicamp), que apresenta uma série de aplicações altamente proveitosas tanto para seu corpo discente como para seus colaboradores. Dentre essas aplicações, destacam-se: o sistema de circulação interna, a gestão

de vagas de estacionamento, o controle das filas nos restaurantes, e até mesmo uma ferramenta de avaliação do volume de passageiros na circulação interna. Além disso, a Unicamp também demonstra compromisso com iniciativas futuras, envolvendo o monitoramento do desperdício de alimentos, a gestão eficiente de energia, o abastecimento hídrico, bem como a implementação de sistemas de irrigação, entre outras inovações (unicamp, 2023).

Pode-se citar também a Faculdade de Engenharia de Sorocaba (FACENS) como um exemplo de sucesso, uma vez que transformou seu campus em um laboratório vivo, permitindo a experimentação de soluções para cidades inteligentes. A instituição adota práticas de sustentabilidade e eficiência, reduzindo desperdícios e promovendo o uso responsável de recursos. Além disso, incentiva o envolvimento ativo dos estudantes, proporcionando aprendizado prático por meio da aplicação de novas tecnologias. Esse modelo demonstra como um Campus Inteligente pode otimizar a gestão acadêmica e servir de referência para outras instituições(Romano; Pinto; Pacheco, 2016).

A Universidade Federal Rural do Semi-Árido (UFERSA) enfrentou dificuldades na implementação do conceito de Campus Inteligente devido a três principais fatores: falta de infraestrutura tecnológica, recursos financeiros insuficientes e carência de planejamento estratégico. A ausência de dispositivos IoT e conectividade adequada comprometeu as soluções propostas, enquanto o orçamento limitado dificultou investimentos essenciais na modernização do campus. Além disso, a falta de um plano estruturado prejudicou a adaptação das iniciativas às necessidades específicas da instituição e da região. Esse caso destaca a importância do planejamento e dos investimentos para o sucesso de um Campus Inteligente (Santos, 2023).

3 MATERIAIS E MÉTODOS

Neste capítulo, serão abordados os métodos e materiais utilizados no desenvolvimento do projeto. Como mencionado, devido à diversidade de meios de comunicação sem fio disponíveis, os materiais selecionados podem variar. No entanto, os métodos adotados serão aplicáveis à maioria desses meios de comunicação.

Será necessário instalar a plataforma de integração que permitirá a conexão dos sensores. Para este projeto, optou-se pelo sensor de abertura de janelas e portas, além do sensor de chuva, levando em consideração o equilíbrio entre custo e benefício, bem como a facilidade de integração. O uso de sensores com alta complexidade seria problemático em uma escala maior, mas como o projeto será implantado em um ambiente de teste, a avaliação da melhor opção será feita durante o processo.

Após a conexão dos dispositivos à plataforma, serão realizadas análises individuais de cada sensor para compreender seu comportamento. Em seguida, será feita uma análise conjunta dos dispositivos, buscando alcançar a eficiência desejada para o projeto. Além disso, será implementado um *dashboard* para facilitar o controle e monitoramento dos dispositivos.

Por fim, a definição das rotinas a serem aplicadas será cuidadosamente planejada. Todas as rotinas serão testadas exaustivamente para identificar o caminho mais eficiente e confiável, minimizando a ocorrência de falhas humanas.

3.1 NodeMCU

Neste projeto, será utilizado o NodeMCU ESP8266 V3, um microcontrolador amplamente empregado na área de Internet das Coisas (IoT) devido à sua versatilidade e desempenho. Esse dispositivo conta com nove portas digitais e uma porta analógica (na versão utilizada no projeto), oferecendo uma ampla gama de possibilidades para conectividade e controle de dispositivos. Foram utilizados diversos componentes eletrônicos, tais como o reed switch, sensor de chuva e, para exemplificação, um motor servo. Esses dispositivos são acompanhados de módulos que facilitam a implementação utilizando portas analógicas, permitindo uma integração mais ágil e eficiente. (Team, 2014) .

A escolha do NodeMCU foi motivada por sua combinação vantajosa de características, incluindo a quantidade de portas digitais, seu tamanho compacto e seu custo-benefício. Esta combinação torna o NodeMCU uma das opções mais atrativas e economicamente viáveis do mercado para projetos de IoT. Inicialmente, a comunicação deste microcontrolador é realizada via cabo USB, mas ele também permite comunicação sem fio utilizando o chip Wi-Fi integrado. Esta flexibilidade é crucial para projetos que exigem conectividade dinâmica e confiável.

Para possibilitar a comunicação entre o NodeMCU e o Home Assistant, foi empregada a biblioteca ESPHome, que simplifica a interação entre o ESP e o próprio Home Assistant. No ESPHome, é necessário programar os dispositivos e suas funcionalidades, permitindo a atribuição de diversas automações de maneira intuitiva e eficaz. Este processo de programação

oferece uma gama de possibilidades para personalização e otimização do sistema, facilitando a implementação de soluções inteligentes.

A arquitetura utilizada pode ser comparada à rede Zigbee, que também permite a utilização de vários dispositivos diferentes. No entanto, há uma diferença significativa no custo, tornando a solução baseada no ESP8266 mais recomendada para automações com conexões próximas, pois a qualidade do sinal pode ser comprometida pela distância. Tal problema não ocorre com dispositivos Zigbee, que são especificamente projetados para manter uma rede sólida de comunicação entre os dispositivos, porém como este é um trabalho inicial e de baixo custo, implementar uma rede Zigbee ficaria fora do escopo do estudo inicial. Concluí-se que a escolha das tecnologias utilizadas foi adequada para um projeto em pequena escala. Devido à heterogeneidade dos dispositivos presentes na IoT, é possível combinar as duas tecnologias para obter uma qualidade superior, com cada dispositivo focado em sua função específica. Esta abordagem permite uma implementação mais robusta e eficiente, aproveitando as vantagens de cada tecnologia para criar um sistema de automação altamente funcional e adaptável. A integração dessas tecnologias oferece uma solução poderosa para o desenvolvimento de aplicações inteligentes, potencializando a eficiência e a interconectividade dos dispositivos em um ambiente IoT.

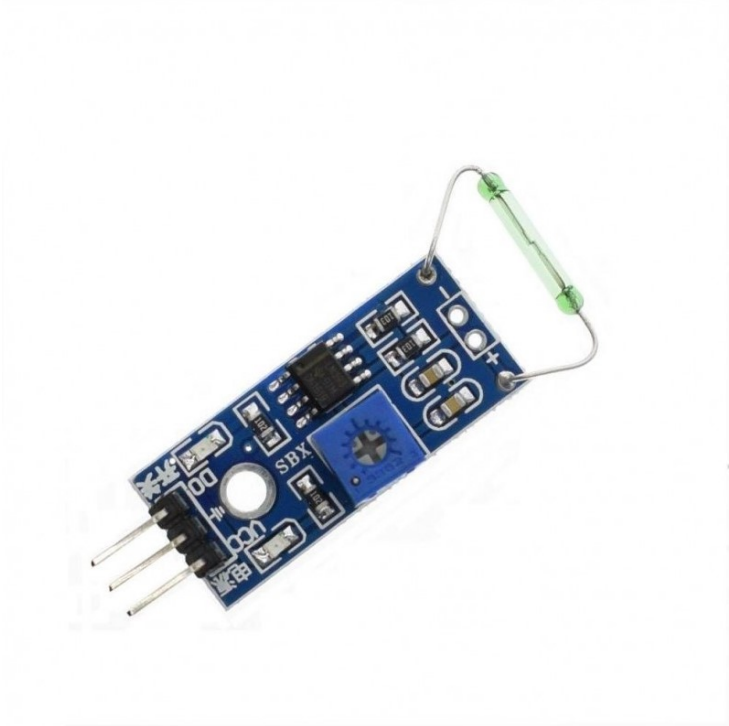
3.2 Dispositivos

A parte prática deste trabalho concentra-se, sobretudo, na utilização do sensor reed switch e do sensor de chuva, uma vez que esses dispositivos representam a base da ideia inicial do projeto. Ambos os sensores foram empregados em conjunto com módulos específicos, visando a simplificação do processo de implementação e configuração dos dispositivos. Esses módulos apresentam características relevantes, como a presença de um potenciômetro integrado, que possibilita ajustes precisos no funcionamento dos sensores, facilitando correções e calibragens quando necessário.

Embora o módulo utilizado possa ser substituído diretamente pelo próprio reed switch, sua inclusão no projeto visa ampliar a funcionalidade, já que permite identificar a passagem de corrente elétrica e sinalizá-la por meio de sua saída digital. O reed switch, em específico, possui a capacidade de detectar a aproximação de ímãs. Esse funcionamento se dá devido à presença de um filamento no interior de uma cápsula de vidro que, ao entrar no campo magnético de um ímã, fecha o circuito elétrico, permitindo a passagem da corrente, por esse motivo ele é muito usado para objetos de fim de curso como portão elétrico e elevadores, entre outros. A Figura 8 mostra o modulo utilizado no projeto. A escolha de sensor foi devido ao seu baixo custo, visando a economia, mas podemos ter dispositivo no mercado pronto para uso sem a utilização do nodeMcu para seu funcionamento.

No caso do sensor de chuva, o princípio de funcionamento é similar em termos de detecção de corrente, mas sua operação apresenta particularidades. Este sensor consiste em uma placa metálica com gravações conectadas a dois terminais. Quando gotas de água

Figura 8 – Modulo Reed Switch.



Fonte: sotudo (2025).

entram em contato com a superfície, a corrente é conduzida através da gota, estabelecendo a conexão entre os terminais. O módulo desempenha um papel ainda mais relevante nesse caso, pois possibilita regular a sensibilidade do sensor, determinando a intensidade mínima da chuva necessária para ativar o dispositivo. Para seu funcionamento ideal o sensor deve ser instalado de forma a ficar inclinado assim fazendo que quando seja atingido pela chuva as gotas de água consigam escorrer por ele assim não deixando água parada pois o sensor iria detectar a chuva mesmo não existindo. Esse é o único dispositivos que necessariamente precisa ser instalado do lado de fora, porem não tem a necessidade da instalação no mesmo nodeMcu que os outro dispositivos, Na Figura 9 é o modulo e a placa que foi utilizada no projeto. Para melhorar a qualidade e facilitar futuros trabalhos, seria interessante utilizar uma placa maior. Como este trabalho foi um estudo inicial, a placa menor atendeu bem aos testes realizados, mas pode não ser a melhor opção para um uso mais amplo. Por conta do tamanho reduzido, ela precisaria ser instalada em um local estratégico onde acumulasse mais água, o que poderia atrasar a detecção. Por isso, uma placa maior seria mais eficiente para um Smart Campus, garantindo uma resposta mais rápida e precisa.

Além desses sensores, também foi utilizado um motor servo, que foi integrado ao sistema para simular a automação de abertura e fechamento de janelas. Esse motor exemplifica como seria possível acoplar um mecanismo automatizado, proporcionando maior praticidade ao sistema. O motor utilizado, mostrado na Figura 10, e esse motor é muito versátil, porém tendo

Figura 9 – Modulo para sensor de chuva.

Fonte: autocore (2025).

como problema sua configuração no home assitant que é um pouco mais complicada do que sensores binários como o sensor reed switch e o sensor de chuva . É possível expandir o projeto para incluir sensores adicionais voltados ao bem-estar dos usuários, como sensores de luminosidade ou de velocidade do vento. Tais possibilidades demonstram que a automação apresenta aplicações diversas, deixando espaço para futuras expansões e inovações.

Figura 10 – Motor servo

Fonte: Byteflop (2025).

Todos os dispositivos foram conectados a um microcontrolador ESP8266, que, por sua vez, foi integrado ao sistema Home Assistant para programar e gerenciar suas funcionalidades. Para facilitar a configuração, utilizou-se a biblioteca ESPHome, que simplifica o desenvolvimento de aplicações baseadas em IoT, permitindo a comunicação e o controle eficiente dos sensores e atuadores empregados.

3.3 Home Assistant

O Home Assistant apresenta-se como uma ferramenta de grande relevância e alta eficiência para o desenvolvimento de automações, abrangendo desde casas inteligentes até campus inteligentes. Este sistema se destaca por sua capacidade de integrar dispositivos heterogêneos, possibilitando a comunicação entre eles, mesmo diante dos problemas gerado pela diversidade de protocolos e tecnologias.

Em um primeiro momento, para realizar os testes, utilizou-se uma máquina virtual para fazer a instalação do Home Assistant. Após a realizar as configurações iniciais, foi necessário conectar o microcontrolador ESP8266 ao sistema. Para tal, foram utilizados complementos disponibilizados pela própria plataforma, em especial o ESPHome, que facilitou a integração e a configuração dos dispositivos empregados no projeto. O Figura 11 mostra o código para fazer esta comunicação entre o ESP8266 e o home assitant. Esse código em si não é o que vai para o dispositivo pois este código é gerado automaticamente pelo esphome. Apos essa configuração primaria, deve-se escolher como vai ser o meio que o home assitant vai entrar em contado com o nodeMcu. A primeira compilação foi feito via cabo, apos isso todos os processos podem ser executados via wi-fi, mas para isso acontecer é necessario declarar a rede wi-fi e a senha no ESPHome, em seu canto superior na aba de secrets. A partir desse ponto, configura-se os dis-

Figura 11 – Codigo de comunicação

```
esphome:
  name: sensores
  friendly_name: sensores

esp8266:
  board: esp01_1m

# Enable logging
logger:

# Enable Home Assistant API
api:
  encryption:
    key: "elCwmvkAMOigz9elXA4Z9+OrTB+2f3ZD5Cd53waxY3s="

ota:
  - platform: esphome
    password: "a158e4384339c420b09f9da3bb631d33"

wifi:
  ssid: !secret wifi_ssid
  password: !secret wifi_password

  # Enable fallback hotspot (captive portal) in case wifi connection fails
  ap:
    ssid: "Sensores Fallback Hotspot"
    password: "uGOtWzaKurks"
```

Fonte: Elaborado pelo autor (2025).

positivos utilizados: o sensor reed switch, o sensor de chuva e o motor servo, conforme mostrado no Figura 12. Nesse código, tem-se as declarações dos sensores e do motor servo, sendo que este é o que tem uma complexidade maior comparado aos sensores de chuva e o reed switch. Esses sensores dentro do ESPHome são denominados de sensores binários, sendo mais fácil sua declaração e uso. Com isso, obtém-se as informações necessárias para o monitoramento e controle, embora ainda fosse necessário implementar as automações desejadas.

Figura 12 – Código de declaração

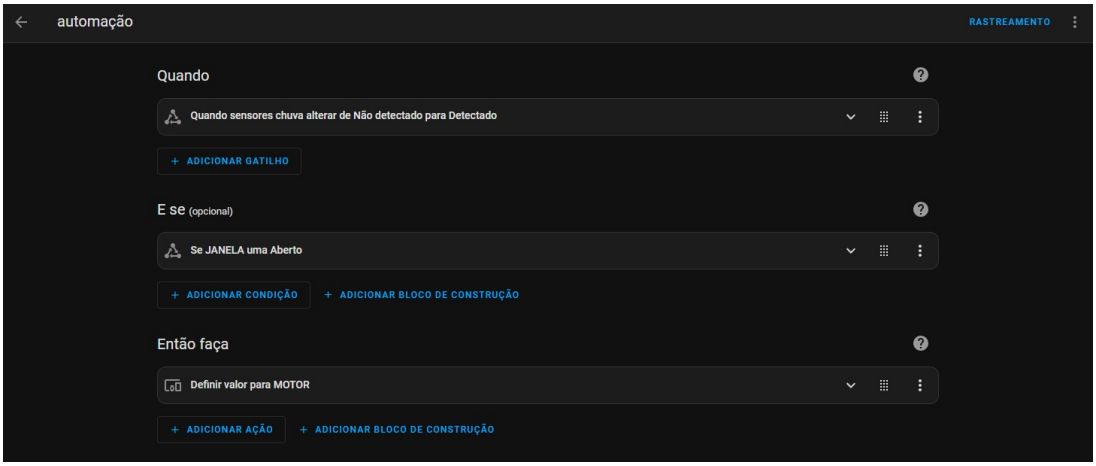
```
output:
  - platform: esp8266_pwm  # Use esp8266_pwm para ESP8266 ou ledc para ESP32
    id: pwm_servo
    pin: 2  # Pino GPIO ao qual o motor servo está conectado
    frequency: 50 Hz  # Frequência padrão para servos

# Configuração do motor servo
servo:
  - id: my_servo
    output: pwm_servo

# Controle do servo como uma entidade deslizante no Home Assistant
number:
  - platform: template
    name: "Posição do Servo"
    id: servo_position
    min_value: 0
    max_value: 180
    step: 1
    set_action:
      then:
        - servo.write:
            id: my_servo
            level: !lambda 'return x / 180.0;'
captive_portal:

binary_sensor:
  - platform: gpio
    pin:
      number: 16
      mode: INPUT
      inverted: False
    name: "janela"
    device_class: door

  - platform: gpio
    pin:
      number: 5
      mode: INPUT
      inverted: True
    name: "chuva"
    device_class: motion
```

Fonte: Elaborado pelo autor (2025).

As automações descritas acima podem parecer complexas, mas o seu desenvolvimento graças ao home assistant é facilitado. Como podemos ver na Figura 13, essa configuração é separada em três partes:

1. **Quando**: É o gatilho da automação, ou seja, o momento em que um sensor muda de estado.
    - No caso, utiliza-se o **sensor de chuva**. Assim que ele detecta chuva, a automação é ativada.
2. **E se**: Essa etapa verifica uma condição antes de executar a ação.
    - Aqui, utiliza-se o **sensor reed switch**, que identifica se a janela está aberta ou fechada.
3. **Então faça**: É a ação que será realizada caso a condição anterior seja atendida.
    - Se a janela estiver aberta, a automação pode realizar diversas ações, como enviar uma mensagem ou, no caso, **acionar o motor servo para fechá-la** automaticamente.

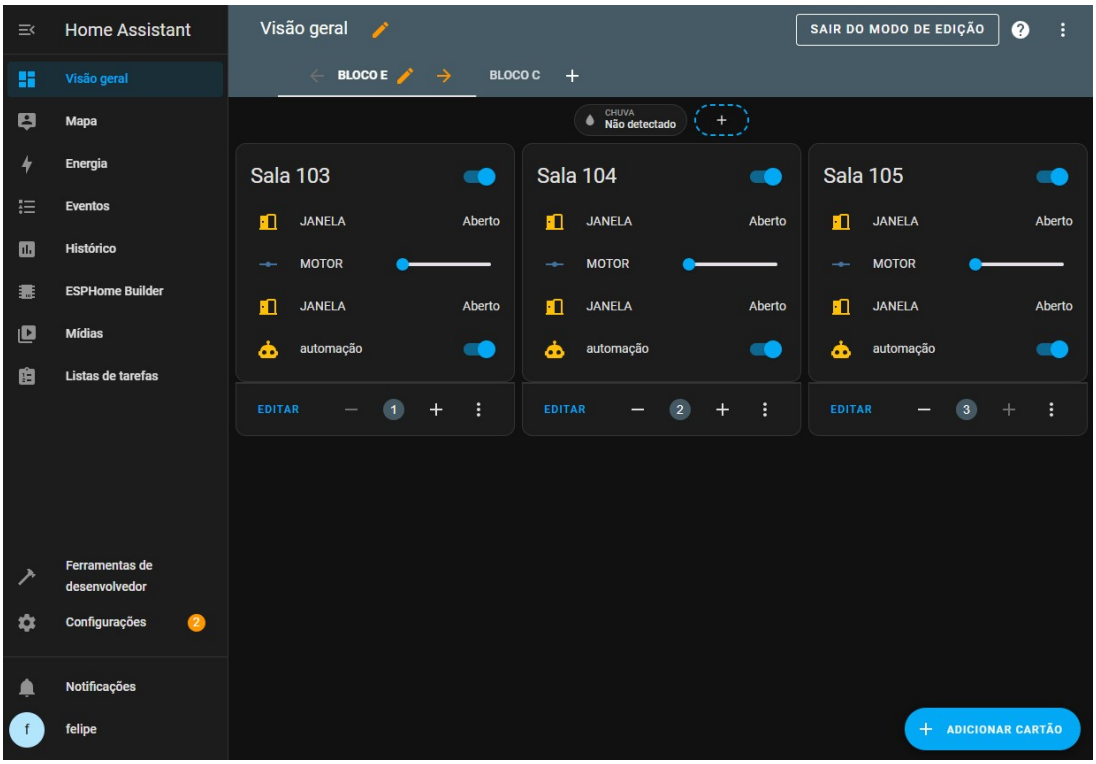
Figura 13 – Automação



Fonte: Elaborado pelo autor (2025).

O Home Assistant dispõe de uma interface gráfica intuitiva, desenvolvida para facilitar a criação de automações de maneira acessível e simplificada. Essa característica foi um dos principais fatores que motivaram a escolha desta ferramenta. Após as configurações iniciais, foi possível projetar e personalizar o dashboard do sistema, como demonstrado na Figura 14 e Figura 15 .

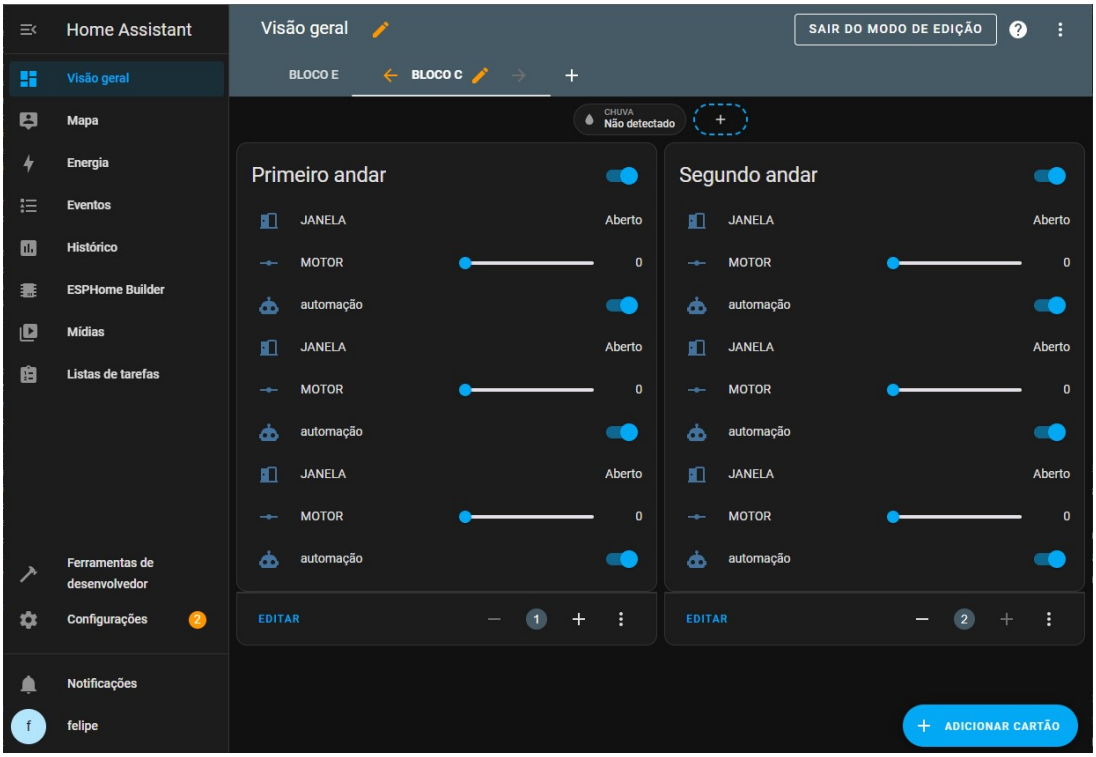
Figura 14 – Exemplo de Dashboard 1.



Fonte: Elaborado pelo autor (2025).

É possivel configurar os dashboards da maneira que se desejar. No caso, foram utilizados os cartões de entidades disponibilizados pelo próprio Home Assistant, como mostrado na Figura 16. Podem ser definidas várias configurações, como título, tema, entidades e até mesmo sua visibilidade. Para o exemplo, utilizou-se a base da Figura 14, simulando a existência de

Figura 15 – Exemplo de Dashboard 2.



Fonte: Elaborado pelo autor (2025).

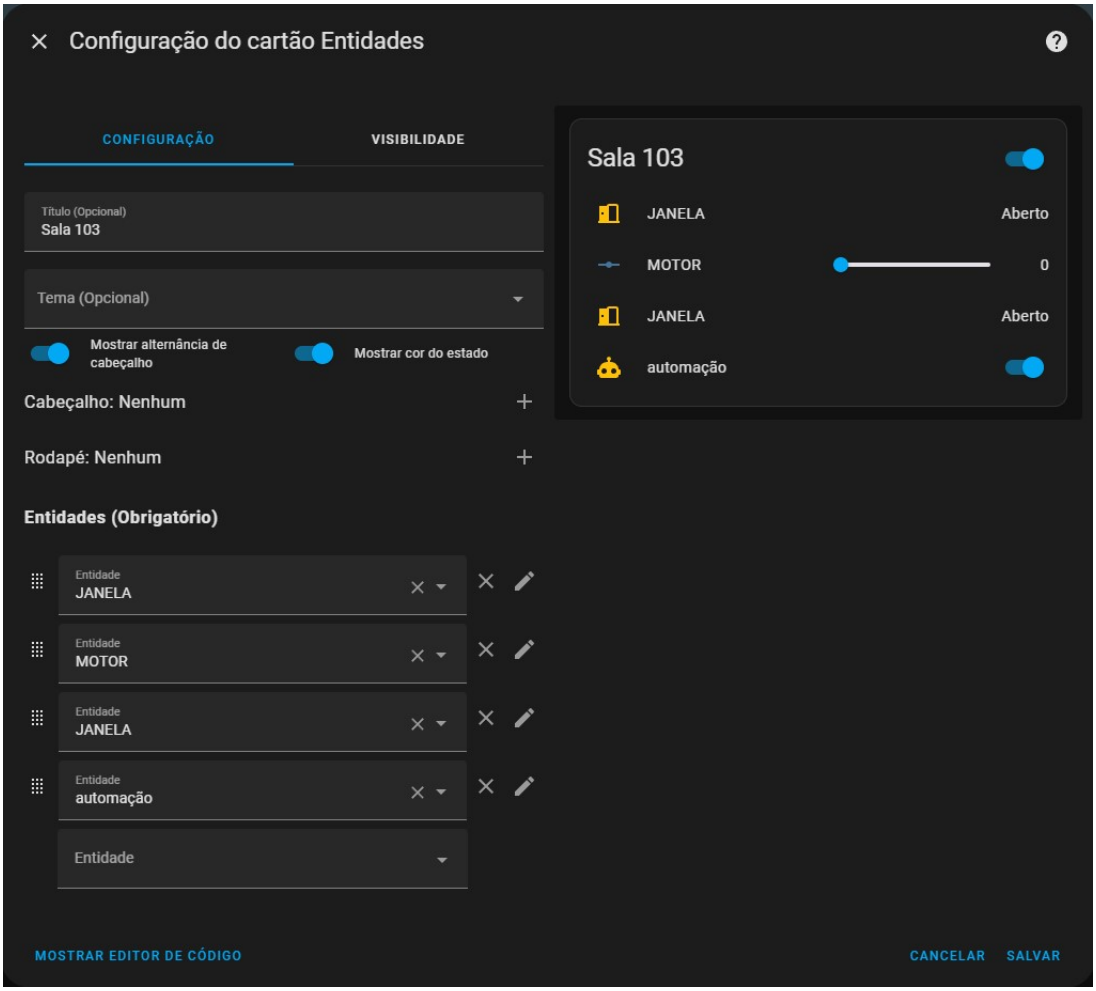
duas janelas, apenas um motor e a automação para que sejam fechadas em caso de chuva. No entanto, nesses cartões, é possível adicionar mais entidades, como demonstrado na Figura 15. Nos cartões desse segundo dashboard, foi adicionado o triplo de entidades em comparação com o primeiro exemplo. É possivel expandir essa configuração conforme a necessidade, seja para um andar, uma sala ou até mesmo um prédio inteiro.

Além disso, o sistema permite o constante aperfeiçoamento de funcionalidades, como a criação de automações específicas. Por exemplo, é possível programar o sistema para que, na ausência de chuva e com a janela fechada, o motor realize a abertura automática da mesma. Essa lógica pode ser facilmente adaptada para outros dispositivos, como cortinas ou aparelhos de ar-condicionado, ampliando as possibilidades de automação e conforto para os usuários.

Com base nos motivos expostos anteriormente, optou-se pela escolha do Home Assistant, visto que, nas questões das automações e interfaces interativas (dashboards), este se destaca como um dos softwares mais completos disponíveis. Porem, como mencionado em seções anteriores, sua curva de aprendizado pode ser considerada um pouco mais elevada. No entanto, ao dominar os conceitos básicos da plataforma, é possível implementar uma vasta gama de automações, tornando-se uma ferramenta extremamente versátil e poderosa.

Uma das grandes vantagens do Home Assistant é sua capacidade de integrar diferentes tecnologias e protocolos. Por exemplo, sensores que utilizam a tecnologia Zigbee podem se comunicar eficientemente com dispositivos conectados via ESP8266, Wi-Fi ou Bluetooth, possibilitando um leque praticamente ilimitado de configurações e interações. Essa característica amplia significativamente as possibilidades de automação, promovendo maior flexibilidade e escalabilidade no desenvolvimento de projetos inteligentes.

Figura 16 – Configuração do cartão de entidades



Fonte: Elaborado pelo autor (2025).

No que se refere aos requisitos para hospedar o Home Assistant em uma máquina virtual, destaca-se que não é necessário um computador de alto desempenho. Um exemplo disso é o Raspberry Pi 3, que oferece uma performance satisfatória para configurações domésticas ou de pequena escala. Entretanto, considerando que este trabalho está voltado à aplicação em um smart campus, recomenda-se a utilização de um computador com melhor desempenho e especificações mais modernas, a fim de atender às demandas específicas de maior complexidade e escala associadas a este tipo de projeto.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Neste capítulo, apresentam-se as conclusões obtidas a partir deste estudo, cujo principal objetivo foi a analise inicial da aplicação de tecnologias voltadas para Smart Campus na UTFPR Campus Toledo.

Inicialmente, os objetivos específicos relacionados ao estudo do conceito de campus inteligente foram plenamente atingidos, dedicando uma grande parte sobre as tecnologia de comunicações que possa ser utilizadas em seu desenvolvimento. Foram exploradas diferentes tecnologias aplicáveis em automações, descrevendo as principais soluções empregadas em casas e cidades inteligentes. No que se relaciona à implementação prática, a integração dos sensores de chuva e reed switch foi realizada com sucesso, sendo sua configuração a de maior facilidade, avançando com a adição de um motor servo para exemplificar seu funcionamento em um sistema automatizado mais robusto. Por fim, para o monitoramento dos sensores utilizados, foi realizada a instalação do Home Assistant, software escolhido por sua ampla gama de recursos, abrangendo desde a integração de dispositivos até a automação e a interface interativa com os usuários por meio de painéis personalizados (dashboards).

Na justificativa deste trabalho, foi destacada a complexidade da implementação do Smart Campus, evidenciando os desafios encontrados ao longo do desenvolvimento. A grande parte desses desafios são devido à diversidade de sensores e tecnologias disponíveis assim demonstrando a dificuldade desse tipo de projeto, exigindo que a segurança e a privacidade dos usuários sejam sempre priorizadas. Assim, estudos como este devem continuar sendo realizados com foco na melhoria da qualidade de vida dos estudantes, professores e demais colaboradores da instituição.

No que se refere ao referencial teórico, foram abordadas diversas tecnologias, com ênfase na comunicação sem fio e suas particularidades dentro de um ambiente acadêmico .Das tecnologia sem fios citadas utilizou-se apenas a comunicação via wi-fi pois seu baixo custo inicial foi mais atrativo o nosso estudo. Além disso, foram discutidos protocolos e padrões de comunicação, destacando suas diferenças e níveis de segurança. Também foram analisadas as principais plataformas de integração disponíveis no mercado, decidindo pelo uso do Home Assistant devido às suas características específicas e por sua vasta gama de atributos que facilitam muito a análise e as automações necessárias. Por fim, apresentamos algumas iniciativas de Smart Campus já implementadas em outras universidades, demonstrando o potencial dessas tecnologias.

Na seção de materiais e métodos, detalhada uma implementação prática do projeto, destacando o uso do NodeMCU ESP8266 como microcontrolador responsável pela conexão dos sensores ao Home Assistant. Foram descritos os sensores utilizados e como foi implementado assim como suas configurações e suas automações e, esboçando um dashboard que permite o monitoramento em tempo real do estado dos sensores a automação será deixada ligada ou desligada. Essa abordagem destaca a importância da automação para garantir segurança, eficiência e disponibilidade de informações em um ambiente acadêmico inteligente. Apensar de

minimizar erros humanos, é necessário monitoramento do sistema , realizando verificações de integridade e manutenção preventivas, além de correções de problema quando necessário.

5 CONCLUSÃO

Com este estudo, foi possível estabelecer uma base e um referencial de pesquisa sobre novas tecnologias aplicadas à área de Smart Campus, apresentando um panorama das soluções já disponíveis no mercado. Dessa forma, este trabalho pode servir como suporte para futuras pesquisas, otimizando o tempo de desenvolvimento de novos projetos relacionados ao tema.

Além disso, foram descritas as principais dificuldades referentes à implementação de um Smart Campus, especialmente no que se refere à complexidade do processamento das informações. Cabe ressaltar que este estudo teve caráter exploratório e inicial, abordando aplicações voltadas para a automação e integração de dispositivos. Com o avanço da tecnologia e o desenvolvimento de novos métodos, é esperado que soluções mais eficientes sejam criadas ao longo dos anos, embora a base teórica aqui discutida permaneça relevante para futuras implementações.

Por fim, pode-se concluir que a aplicação de tecnologias voltadas para campus inteligentes tem o potencial de facilitar a vida acadêmica, otimizando recursos e promovendo maior segurança patrimonial e individual para estudantes, professores e demais colaboradores da instituição.

5.1 Trabalhos Futuros

Nesta seção, são deixadas algumas sugestões de projetos futuros que podem se beneficiar deste trabalho e contribuir para a evolução do conceito de Smart Campus.

Para melhorar o sistema desenvolvido, uma das primeiras sugestões é substituir a placa do sensor de chuva por uma de tamanho maior, o que pode aumentar a precisão da detecção. Além disso, seria interessante adicionar um sensor de luminosidade para o controle automatizado das cortinas, otimizando a entrada de luz natural e reduzindo o consumo de energia.

Outra ideia é criar uma automação para o controle de temperatura dentro das salas, permitindo que os ares-condicionados sejam ligados automaticamente quando a temperatura externa atingir um certo nível, tornando o ambiente mais confortável.

Pensando na infraestrutura do campus, um estudo mais aprofundado sobre a tecnologia Zigbee pode ser uma ótima alternativa, já que a comunicação via Wi-Fi, utilizada neste trabalho, pode sobrecarregar a rede à medida que a quantidade de sensores cresce. Com o Zigbee, esse problema seria minimizado, permitindo a conexão de mais dispositivos de forma eficiente. Outras sugestões de expansão incluem monitoramento de estacionamentos, utilizando câmeras para identificar vagas disponíveis em tempo real, controle de vazão de água, ajudando a evitar desperdícios e melhorar a gestão do consumo, gestão inteligente de energia, permitindo um controle mais detalhado do uso de eletricidade no campus. Com essas melhorias, seria possível aprimorar ainda mais o controle e a automação do campus, tornando-o um ambiente mais eficiente, sustentável e tecnológico.

REFERÊNCIAS

200DEGREES. *Bluetooth, Conectividade, Sem fio*. [*S.l.*]: , 2016. Disponível em: <https://pixabay.com/pt/vectors/bluetooth-conectividade-sem-fio-1690677/>. Acesso em: 10 de junho de 2023.

ABDULRAHEEM, A. S. *et al.* Home automation system based on iot. **Technology Reports of Kansai University**, v. 62, n. 5„ 2020.

AGARWAL, V.; SHARMA, S.; AGARWAL, P. Iot based smart transport management and vehicle-to-vehicle communication system. *In*: **Computer Networks, Big Data and IoT**. [*S.l.*]: Springer 2021. p. 709–716.

ALGHAMDI, A.; SHETTY, S. Survey toward a smart campus using the internet of things. *In*: IEEE. 2016 IEEE 4TH INTERNATIONAL CONFERENCE ON FUTURE INTERNET OF THINGS AND CLOUD (FICLOUD). 2016. **Anais [...]** [*S.l.*], 2016. p. 235–239.

ALMEIDA, A. N. P. de *et al.* Aplicações de iot em automação residencial para idosos e pessoas com mobilidade reduzida. **BIUS-Boletim Informativo Unimotrisaúde em Sociogerontologia**, v. 47, n. 41, p. 1–14, 2024.

ALYAHYA, N.; ALJABER, B. Internet of things in saudi arabia universities: State of the art, future opportunities, and open challenges. **ICT with Intelligent Applications**, Springer„ p. 821–842, 2023.

ANDRADE, J. de G. **Estudo e projecto de transformação de uma casa tradicional numa casa inteligente, baseada em IoT**. 2024. Dissertação (Mestrado) — Universidade da Madeira (Portugal) 2024.

ARVIND, S.; NARAYANAN, V. A. An overview of security in coap: Attack and analysis. *In*: 2019 5TH INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING COMMUNICATION SYSTEMS (ICACCS). 2019. **Anais [...]** [*S.l.*: *s.n.*], 2019. p. 655–660.

AUTOCORE. **sensor de chuva**. [*S.l.*]: , 2025. Disponível em: https://www.autocorerobotica.com.br/modulo-sensor-de-chuva. Acesso em: 1 de fevereiro de 2025.

AZEVEDO, T. Roteamento zigbee. **Universidade Federal do Rio de Janeiro. Disponível em:< www. gta. ufrj. br/ensino/CPE825/2006/resumos/Trabal hoZigbee. pdf>. Acesso em**, v. 12„„.

BADENHOP, C. W. *et al.* The z-wave routing protocol and its security implications. **Computers & Security**, Elsevier v. 68„ p. 112–129, 2017.

BERNARDES, J. P. S. Automação residencial: Design universal e qualidade de vida-estado da arte., . Universidade Federal de Uberlândia„, 2020.

BISWAS, N.; BISWAS, N. Using webhooks at the site. **Advanced Gatsby Projects: Create Two Advanced Sites Using Technologies that Compliment Gatsby**, Springer„ p. 133–147, 2021.

BLUETOOTH, S. Bluetooth. **Go Faster. Go Further White Paper. Available online: https://www. bluetooth. com/wp-content/uploads/2019/03/Bluetooth_5-FINAL. pdf (accessed on 11 September 2021)**, „, 2006.

BOGDAN, R. *et al.* A practical experience on the amazon alexa integration in smart offices. **Sensors**, MDPI v. 21, n. 3, p. 734, 2021.

BRITO, I. B. Mapeamento sobre o uso das tecnologias wi-fi, bluetooth e iot no desenvolvimento de ações de entretenimento, . Universidade Federal de Uberlândia„, 2021.

BYTEFLOP. **servo motor**. [*S.l.*]: , 2025. Disponível em: https://www.byteflop.com.br/micro-servo-9g-sg90-towerpro. Acesso em: 1 de fevereiro de 2025.

CAMERO, A.; ALBA, E. Smart city and information technology: A review. **cities**, Elsevier v. 93„ p. 84–94, 2019.

CORREA, N. Comparativo de protocolos de iot para automação residencial: potenciais vulnerabilidades e sugestões de melhorias., . Universidade de Passo Fundo„, 2018.

CPCON. **ciclo RFID**. [*S.l.*]: , 2023. Disponível em: https://www.grupocpcon.com/rfid-para-inventarios/. Acesso em: 10 de junho de 2023.

DARROUDI, S. M.; GOMEZ, C. Bluetooth low energy mesh networks: A survey. **Sensors**, MDPI v. 17, n. 7, p. 1467, 2017.

DENG, C. *et al.* Ieee 802.11be wi-fi 7: New challenges and opportunities. **IEEE Communications Surveys Tutorials**, v. 22, n. 4, p. 2136–2166, 2020.

ERGEN, S. C. Zigbee/ieee 802.15. 4 summary. **UC Berkeley, September**, v. 10, n. 17, p. 11, 2004.

FILHO, M. F. Internet das coisas. **Unisul Virtual**, „, 2016.

FILOSOFIA, n. e. c. **NFC e a comunicação entre dispositivos**. [*S.l.*]: , 2023. Disponível em: https://marcosmucheroni.pro.br/blog/?p=6800. Acesso em: 10 de junho de 2023.

GODOI, M. G. D.; ARAÚJO, L. S. A internet das coisas: evolução, impactos e benefícios. **Revista interface tecnológica**, v. 16, n. 1, p. 19–30, 2019.

HALLBERG, J.; NILSSON, M.; SYNNES, K. Positioning with bluetooth. *In*: 10TH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS, 2003. ICT 2003. 2., 2003. **Anais [...]** [*S.l.*: *s.n.*], 2003. p. 954–958 vol.2.

JAAFAR, G. A.; ABDULLAH, S. M.; ISMAIL, S. Review of recent detection methods for http ddos attack. **Journal of Computer Networks and Communications**, Wiley Online Library v. 2019, n. 1, p. 1283472, 2019.

KAYASIMA, M. Telegestão e automação da iluminação pública: um estudo para a cidade de ilha solteira, . Universidade Estadual Paulista (Unesp)„, 2024.

KHATTAK, H. A.; RUTA, M.; SCIASCIO, E. E. D. Coap-based healthcare sensor networks: A survey. *In*: PROCEEDINGS OF 2014 11TH INTERNATIONAL BHURBAN CONFERENCE ON APPLIED SCIENCES TECHNOLOGY (IBCAST) ISLAMABAD, PAKISTAN, 14TH - 18TH JANUARY, 2014. 2014. **Anais [...]** [*S.l.*: *s.n.*], 2014. p. 499–503.

KHOROV, E. *et al.* A tutorial on ieee 802.11 ax high efficiency wlans. **IEEE Communications Surveys & Tutorials**, IEEE v. 21, n. 1, p. 197–216, 2018.

KOWALSKI, J. *et al.* Older adults and voice interaction: A pilot study with google home. *In*: EXTENDED ABSTRACTS OF THE 2019 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS. 2019. **Anais [...]** [*S.l.*: *s.n.*], 2019. p. 1–6.

LI, B. *et al.* Acoustic modeling for google home. *In*: INTERSPEECH. 2017. **Anais [...]** [*S.l.*: *s.n.*], 2017. p. 399–403.

LOUREIRO, A. F. *et al.* Comunicação sem fio e computação móvel: tecnologias, desafios e oportunidades. *In*: MINICURSO APRESENTADO NO CONGRESSO DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. CAMPINAS, SP. 78., 2003. **Anais [...]** [*S.l.*: *s.n.*], 2003.

LUGLI, A. B.; SOBRINHO, D. G. Tecnologias wireless para automação industrial: Wireless_hart, bluetooth, wisa, wi-fi, zigbee e sp-100. **Instituto Nacional de Telecomunicações Inatel**, „, 2012.

MACKENSEN, E.; LAI, M.; WENDT, T. M. Bluetooth low energy (ble) based wireless sensors. *In*: SENSORS, 2012 IEEE. 2012. **Anais [...]** [*S.l.*: *s.n.*], 2012. p. 1–4.

MADAKAM, S. Internet of things: smart things. **International journal of future computer and communication**, Citeseer v. 4, n. 4, p. 250, 2015.

MADLMAYR, G. *et al.* Nfc devices: Security and privacy. *In*: 2008 THIRD INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY. 2008. **Anais [...]** [*S.l.*: *s.n.*], 2008. p. 642–647.

MALATJI, E. M. The development of a smart campus-african universities point of view. *In*: IEEE. 2017 8TH INTERNATIONAL RENEWABLE ENERGY CONGRESS (IREC). 2017. **Anais [...]** [*S.l.*], 2017. p. 1–5.

MATOS, M. d. L. Relatório técnico de proposta de reestruturação da infraestrutura da universidade de brasília baseada no conceito de smart campus, „,. 2021.

MELO, E. C. A. d. Salas de aula inteligentes: utilização de arduino e bluetooth low energy como beacons para o mapeamento de salas de aula, „,. 2016.

MERAJ, S. Google assistant home automation. **Available at SSRN 3918333**, „, 2021.

MONSIGNORE, F. Sensoriamento de ambiente utilizando o padrao zigbee. **São Carlos**, „, 2007.

MOREIRA, W.; AICOS, F. P. Implantaçao de múltiplos gateways iot definido por software e virtualizado para campus inteligente. **Revista de Sistemas de Informaçao da FSMA**, , n. 25, p. 2–18, 2020.

MOZAFFARIAHRAR, E.; THEOLEYRE, F.; MENTH, M. A survey of wi-fi 6: Technologies, advances, and challenges. **Future Internet**, MDPI v. 14, n. 10, p. 293, 2022.

MUÑOZ, H. A. A. Avaliação da interferência de redes sem fio wi-fi e bluetooth sobre uma rede bacnet/ieee 802.15. 4, „,. 2014.

NARCISO, M. G. Aplicação da tecnologia de identificação por radiofreqüência (rfid) para controle de bens patrimoniais pela web., . Global Science and Technology, v. 1, n. 7, p. 50-59, dez./mar. 2008.„, 2008.

NEVES, A. R. d. M. *et al.* Iniciativa smart campus: um estudo de caso em progresso na universidade federal do pará. *In*: SBC. ANAIS DO I WORKSHOP DE COMPUTAÇÃO URBANA. 2017. **Anais [...]** [*S.l.*], 2017.

NÓBREGA, P. I. Silva-da; CHIM-MIKI, A. F.; CASTILLO-PALACIO, M. A smart campus framework: Challenges and opportunities for education based on the sustainable development goals. **Sustainability**, MDPI v. 14, n. 15, p. 9640, 2022.

PERAHIA, E.; GONG, M. X. Gigabit wireless lans: an overview of ieee 802.11 ac and 802.11 ad. **ACM SIGMOBILE mobile computing and communications review**, ACM New York, NY, USA v. 15, n. 3, p. 23–33, 2011.

POLIN, K. *et al.* The making of smart campus: A review and conceptual framework. **Buildings**, MDPI v. 13, n. 4, p. 891, 2023.

QUILES, C. N. S. As salas de tecnologias educacionais: modos de “ensinar” e de “aprender” como traduções de cultura escolar, „,. 2008.

QUINCOZES, S.; EMILIO, T.; KAZIENKO, J. Mqtt protocol: Fundamentals, tools and future directions. **IEEE Latin America Transactions**, v. 17, n. 09, p. 1439–1448, 2019.

RAHUL, A. *et al.* Near field communication (nfc) technology: a survey. **International Journal on Cybernetics & Informatics (IJCI)**, AIRCC Publishing Corporation v. 4, n. 2, p. 133, 2015.

RIAZ, R.; KIM, K.-H.; AHMED, H. F. Security analysis survey and framework design for ip connected lowpans. *In*: 2009 INTERNATIONAL SYMPOSIUM ON AUTONOMOUS DECENTRALIZED SYSTEMS. 2009. **Anais [...]** [*S.l.*: *s.n.*], 2009. p. 1–6.

RODRIGUES, D. D. *et al.* Um modelo de assistente reflexivo para suporte à educação continuada em ambiente organizacional, . Universidade Católica de Brasília„, 2010.

ROMANO, R. R.; PINTO, L. G. P.; PACHECO, S. C. P. Smart campus facens–construindo uma cidade inteligente em um campus universitário utilizando-se do fablab. **Disponível http://fablearn. org/wp-content/uploads/2016/09/FLBrazil_2016_paper_150. pdf**, „, 2016.

ROSA, J. P. G. Mecanismos de segurança iot. **Universidade de Nova Lisboa, Portugal**, „, 2021.

SACCOL, A. Z.; REINHARD, N. Tecnologias de informação móveis, sem fio e ubíquas: definições, estado-da-arte e oportunidades de pesquisa. **Revista de administração contemporânea**, SciELO Brasil v. 11„ p. 175–198, 2007.

SÁNCHEZ-TORRES, B. *et al.* Smart campus: Trends in cybersecurity and future development. **Revista Facultad de Ingeniería**, Universidad Pedagógica y Tecnológica de Colombia v. 27, n. 47, p. 104–112, 2018.

SANTOS, S. M. Análise da viabilidade de implementação de um smart campus na ufersa-pau dos ferros, „,. 2023.

SELVARAJ, S.; SUNDARAVARADHAN, S. Challenges and opportunities in iot healthcare systems: a systematic review. **SN Applied Sciences**, Springer v. 2, n. 1, p. 1–8, 2020.

SEYYAR, M. B.; ÇATAK, F. Ö.; GÜL, E. Detection of attack-targeted scans from the apache http server access logs. **Applied computing and informatics**, Elsevier v. 14, n. 1, p. 28–36, 2018.

SILVEIRA, M. F.; GRADVOHL, A. L. Security analysis of the message queuing telemetry transport protocol. **Revista Brasileira de Computação Aplicada**, v. 13, n. 2, p. 83–95, 2021.

SOTUDO. **sensor reed switch**. [*S.l.*]: , 2025. Disponível em: https://www.sotudo.com.br/produto/modulo-sensor-magnetico-reed-switch. Acesso em: 1 de fevereiro de 2025.

STOJMENOVIC, I. Fog computing: A cloud to the ground support for smart things and machine-to-machine networks. *In*: 2014 AUSTRALASIAN TELECOMMUNICATION NETWORKS AND APPLICATIONS CONFERENCE (ATNAC). 2014. **Anais [...]** [*S.l.*: *s.n.*], 2014. p. 117–122.

STOLL, G. R. O que é este tal do zigbee. **UTC Journal-Smart Utilities Networks, Special Issue**, „, 2008.

TEAM, N. Nodemcu: A lua-based firmware for the esp8266 wifi soc. **GitHub Repository**, „, 2014. Disponível em: https://github.com/nodemcu/nodemcu-firmware.

TEXEIRA, P. **ENTENDENDO O THREAD NA PRÁTICA**. [*S.l.*]: , 2023. Disponível em: https://www.youtube.com/watch?v=ugaW_Mrcj7Y&t=705s&ab_channel=PatrickTeixeira-PatteTech. Acesso em: 10 de junho de 2023.

TNS. **IoT: Como implementar um projeto na sua empresa**. [*S.l.*]: , 2023. Disponível em: https://blog.tnsi.com.br/iot-como-implementar-um-projeto-na-sua-empresa. Acesso em: 09 de junho de 2023.

TOSI, J. *et al.* Performance evaluation of bluetooth low energy: A systematic review. **Sensors**, MDPI v. 17, n. 12, p. 2898, 2017.

UNICAMP. **exemplos de aplicações no campus da unicamp**. [*S.l.*]: , 2023. Disponível em: https://smartcampus.prefeitura.unicamp.br/. Acesso em: 23 de outubro de 2023.

VISHWAKARMA, S. K. *et al.* Smart energy efficient home automation system using iot. *In*: 2019 4TH INTERNATIONAL CONFERENCE ON INTERNET OF THINGS: SMART INNOVATION AND USAGES (IOT-SIU). 2019. **Anais [...]** [*S.l.*: *s.n.*], 2019. p. 1–4.

WEINSTEIN, R. Rfid: a technical overview and its application to the enterprise. **IT Professional**, v. 7, n. 3, p. 27–33, 2005.

YAMAZAKI, K. *et al.* Home-assistant robot for an aging society. **Proceedings of the IEEE**, v. 100, n. 8, p. 2429–2441, 2012.

YAO, W.; CHU, C.-H.; LI, Z. The use of rfid in healthcare: Benefits and barriers. *In*: 2010 IEEE INTERNATIONAL CONFERENCE ON RFID-TECHNOLOGY AND APPLICATIONS. 2010. **Anais [...]** [*S.l.*: *s.n.*], 2010. p. 128–134.

YASSEIN, M. B.; MARDINI, W.; KHALIL, A. Smart homes automation using z-wave protocol. *In*: 2016 INTERNATIONAL CONFERENCE ON ENGINEERING MIS (ICEMIS). 2016. **Anais [...]** [*S.l.*: *s.n.*], 2016. p. 1–6.

ZHANG, W. *et al.* A two-port microstrip antenna with high isolation for wi-fi 6 and wi-fi 6e applications. **IEEE Transactions on Antennas and Propagation**, v. 70, n. 7, p. 5227–5234, 2022.