DANIELA YASSUDA
GABRIELA MELO
HUGO POSSANI
VICTOR TAKASHI

HEDWIG - CASA CONECTADA

São Paulo
2017

DANIELA YASSUDA
GABRIELA MELO
HUGO POSSANI
VICTOR TAKASHI

HEDWIG - CASA CONECTADA

Trabalho apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Engenheiro Eletricista com ênfase em Computação.

São Paulo
2017

DANIELA YASSUDA
GABRIELA MELO
HUGO POSSANI
VICTOR TAKASHI

HEDWIG - CASA CONECTADA

Trabalho apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Engenheiro Eletricista com ênfase em Computação.

Área de Concentração:
Engenharia de Computação

Orientador:
Prof. Dr. Reginaldo Arakaki

Co-orientador:
Eng. Marcelo Pita

São Paulo
2017

RESUMO

resumo

Palavras-Chave –

ABSTRACT

abstract

Palavras-Chave –

LISTA DE FIGURAS

1 Projeto Hedwig 18

2 Diagrama ilustrativo do módulo de Acesso ao Portão 20

3 Camadas da arquitetura usada no Projeto HomeSky. As camadas em verde correspondem às bibliotecas desenvolvidas no trabalho. 25

4 Tabela de requisitos por nível de conectividade 29

5 Primeira versão da arquitetura do projeto Hedwig 31

6 Segunda versão da arquitetura do projeto Hedwig 32

7 Rotina de multiplexação de procedimentos no tempo 35

8 Tratamento de indisponibilidade de recursos 36

9 Tratamento de ataque de DoS Local 37

10 Diagrama PCB do Módulo Base 38

11 Diagrama PCB do Módulo Base 39

12 Entradas Em A0 40

13 Funcionamento do Circuito de Antitravamento 41

14 Tópicos MQTT 46

15 Comparação entre uma aplicação monolítica (esquerda) e com microsserviços (direita) 48

16 53

LISTA DE TABELAS

LISTA DE SIGLAS

SUMÁRIO

1 Introdução **17**

1.1 Motivação 17

1.2 Projeto Hedwig 17

1.2.1 Objetivo 17

1.2.2 Nome do Projeto 18

1.3 Aplicações 19

1.3.1 Aplicações de Machine Learning 19

1.3.2 Módulo de Acesso 20

2 Projetos Relacionados **23**

2.1 Sistemas Existentes no Mercado 23

2.1.1 Sistemas Comerciais 23

2.1.2 Sistemas Open Source 24

2.2 Projeto HomeSky 24

3 Especificação **26**

3.1 Componentes 26

3.2 Stakeholders 26

3.3 Requisitos 27

3.3.1 Requisitos Funcionais 27

3.3.2 Requisitos Não-Funcionais 28

3.3.3 Requisitos por Nível de Conectividade 29

4 Arquitetura **30**

4.1 Visão geral 30

4.2 Evolução arquitetural 30
4.3 Módulos 33
4.3.1 Módulos Base 34
4.3.1.1 ESP8266 34
4.3.1.2 Multiplexação no tempo 35
4.3.1.3 Tratamento de indisponibilidade 35
4.3.1.4 DoS Local (Evil Twin) 36
4.3.1.5 Diagrama 37
4.3.1.6 Montagem 42
4.3.2 Módulo de Interface com Sistema de Alarmes 42
4.3.2.1 Especificação 42
4.3.2.2 Montagem 42
4.3.3 Módulo de Acesso 42
4.3.3.1 Especificação 42
4.3.3.2 Montagem 42
4.3.4 Módulo de Quarto 42
4.3.4.1 Especificação 42
4.3.4.2 Montagem 42
4.3.5 Módulo de Aquário 42
4.3.5.1 Especificação 42
4.3.5.2 Montagem 42
4.3.6 Módulo de Cozinha 42
4.3.6.1 Especificação 42
4.3.6.2 Montagem 42
4.4 Controlador Local 42
4.4.1 Requisitos funcionais 43

4.4.2 Formato dos Tópicos MQTT . . . 43
4.4.3 Regras de Negócio . . . 43
4.4.4 Definição de Interfaces . . . 44
4.4.5 Definição das Mensagens . . . 44
4.4.5.1 Configuração (configuration) . . . 44
4.4.5.2 Requisição de ação (action_request) . . . 44
4.4.5.3 Confirmação (confirmation) . . . 44
4.4.5.4 Transmissão de dados (data_transmission) . . . 45
4.4.5.5 Requisição de dados (data_request) . . . 45
4.4.6 Raspberry Pi . . . 46
4.5 Servidor na Nuvem . . . 46
4.5.1 Arquitetura de Microsserviços . . . 47
4.5.1.1 Características . . . 47
4.5.1.2 Casos de uso . . . 50
4.5.1.3 Microsserviços e Internet das Coisas . . . 50
4.6 Cliente Web . . . 50
4.7 App Backup . . . 51
4.7.1 Interface . . . 51
4.7.2 Setup . . . 51
4.7.3 Abertura de porta do roteador . . . 51
4.7.4 Configurações . . . 51
4.7.5 Serviços essenciais . . . 51
4.8 Comunicação . . . 51
4.8.1 Entre módulos e controlador local . . . 53
4.8.2 Entre controlador local e nuvem . . . 53
4.8.3 Entre cliente web e nuvem . . . 53

4.8.4 Entre app backup e módulos 53

5 Metodologia **54**

5.1 Gerência do projeto 54

5.1.1 Gerência de Escopo Tempo 54

5.1.2 Gerência de Partes Interessadas Aquisição 54

5.1.3 Gerência de Processos de Software 54

5.1.4 Gerência de Partes Interessadas 55

5.1.5 Gerência de Comunicação 55

5.1.6 Gerência de Escopo 55

5.1.7 Gerência de Riscos 55

5.2 Pesquisa bibliográfica 55

5.3 Ferramentas e tecnologias 55

6 Implementação **56**

6.1 Morpheus 56

6.1.1 Descrição 56

6.1.2 Plataforma 56

6.1.3 Requisitos 57

6.1.3.1 Requisitos Funcionais 57

6.1.3.2 Requisitos Não Funcionais 58

6.1.4 Especificações 58

6.1.4.1 Tópicos 58

6.1.4.2 Regras de negócio 59

6.1.4.3 Definição de interfaces 59

6.1.4.4 Definição das mensagens 60

6.1.4.5 Testes realizados da comunicação Morpheus e módulos: . . . 66

6.1.5 Comunicação entre Morpheus e Nuvem 70

6.1.6 Websocket 71
6.1.6.1 Morpheus 71
6.1.6.2 Nuvem 71
6.1.7 Configurações 72
6.1.7.1 MQTT Mosquitto broker - Configuração 72
6.1.7.2 Estratégia 73
6.1.7.3 Guia de instalação (Testado no Ubuntu 16,10 x64) 73
6.1.7.4 Criação dos certificados 73
6.1.7.5 Comandos úteis 74
6.1.7.6 Senhas 74
6.1.7.7 Casos de teste para Controle de Acesso nos Tópicos MQTT entre módulos e nuvem 74
6.1.7.8 Restrição de Tópicos s2m (Server to Module) 75

7 Aprendizado de Máqina **76**
7.1 Coleta de Dados 76
7.1.1 Conexões 76
7.1.2 Uso 76

8 Conclusões **78**

Anexo A – Códigos das aplicações desenvolvidas **79**

1 INTRODUÇÃO

1.1 Motivação

Há uma expectativa de que o número de casas inteligentes aumente cerca de 17% nos Estados Unidos no ano de 2017 (**??**), onde já se tem investimentos de grandes empresas, como Google, Amazon e Apple, mostrando a relevância do tema no momento atual. O interesse nessa área é tamanho que a Google investiu cerca de 5 milhões de dólares em um comercial de seu produto Google Home no Super Bowl 2017 (final de futebol americano nos EUA) (**??**).

Assim, as oportunidades trazidas pelo conceito de Internet das Coisas à área de automação residencial são uma grande motivação para esse projeto. Também destacam-se as possibilidades de trazer tais tecnologias de casas inteligentes ao mercado nacional, personalizando produtos e adequando-as às necessidades dos potenciais consumidores brasileiros. Mesmo nos Estados Unidos, ainda é necessário algum tempo até que a casa conectada se consolide, de modo que há grandes oportunidade de pioneirismo no mercado brasileiro, com o lançamento de produtos de casa conectada a preços acessíveis e focando nas necessidades dos consumidores locais.

1.2 Projeto Hedwig

1.2.1 Objetivo

A contribuição do projeto será um sistema baseado em arquitetura local modularizada, com funcionalidades local e em nuvem, e provedor de uma API que permita seu acesso por diversos clientes - como *websites* ou aplicativos para *smartphones* - e que seja capaz de monitorar e agir em diversos módulos presentes na residência do usuário final do sistema. Ainda irá dispor de *Machine Learning*, inicialmente alimentado com dados reais de quatro módulos exemplo, armazenados em nuvem, o que irá permitir adaptabilidade do sistema à utilização por cada um de seus usuários.

Desta forma, os principais pontos do projeto são:

- **Robustez**

  3 níveis de funcionamento: Online, Local e Offline, para garantir a disponibilidade mesmo com problemas (queda do servidor, internet indisponível, falha no roteador), com medidas como tentativa automática de reconexão, monitoramento e manutenções preventivas e corretivas do sistema.

- **Modularidade**

  Garante a independência de funcionamento dos módulos que atendem às várias necessidades, contribuindo para a robustez. Diminui o custo e personaliza o produto, de acordo com as necessidades do cliente.

- **Machine Learning**

  Levantamento de rotinas para gerar conhecimento, que se mostra como notificações, alertas e acionamentos automáticos de funções para o cliente.

- **Segurança**

  Autenticação dos usuários e proteção contra ataques de DoS ((**??**)) Local.

Figura 1: Projeto Hedwig

1.2.2 Nome do Projeto

O nome do projeto foi escolhido em homenagem a Hedy Lamarr. Nascida Hedwig Eva Maria Kiesler (**??**), a atriz e inventora desenvolveu, durante a Segunda Guerra Mundial, um aparelho de interferência em rádio para despistar radares nazistas, cujos princípios estão incorporados nas tecnologias atuais de Wi-fi, CDMA e Bluetooth (**??**). Baseado nessa ideia de um sistema de comunicação seguro, e como reconhecimento de seu trabalho, foi dado esse nome ao projeto aqui descrito.

1.3 Aplicações

Como aplicações do projeto Hedwig, destacam-se a automação de eletrodomésticos e iluminação, segurança no acesso à casa, economia nas contas de água e energia elétrica, além de um monitoramento remoto de pessoas que moram sozinhas (como é o caso de idosos), garantindo a tranquilidade de seus familiares e mantendo a segurança do indivíduo.

Exemplos de módulos que podem ser incluídos no sistema são: quarto (despertador, iluminação, monitoramento de temperatura e umidade); cozinha (timer, iluminação, monitoramento de presença e gás); acesso (controle de abertura, monitoramento de estado); externo (monitoramento de temperatura, umidade, energia elétrica e consumo de água); corredor (monitoramento de presença, iluminação), chuveiro (controle de temperatura/potência a partir do perfil de usuário e temperatura externa) e ar condicionado (controle da potência a partir do monitoramento das temperaturas interna e externa da casa).

1.3.1 Aplicações de Machine Learning

Como possíveis perguntas a serem respondidas pelo módulo de Machine Learning do projeto e os dados a serem coletados (em diferentes lugares da casa), temos:

- Quando notificar a chegada de pessoas ou falta dela? - presença e sensor de abertura do portão
- Quando enviar alertas de atividade suspeita? - presença
- Quanto o sistema é usado? (Por funcionalidade) - sensor de abertura e log de aberturas pelo módulo
- Quando notificar condições insalubres, como temperatura e umidade altas persistentes? - temperatura e umidade
- Quando notificar falta de atividades rotineiras (como acordar, almoçar) - presença
- Melhor horário para despertar? - presença
- Notificar mudança brusca de temperatura, principalmente esfriamento? - temperaturas interna e externa, umidade (para sensação térmica)
- Quanto o sistema está indisponível na instalação do cliente? - log de qualquer dado periódico

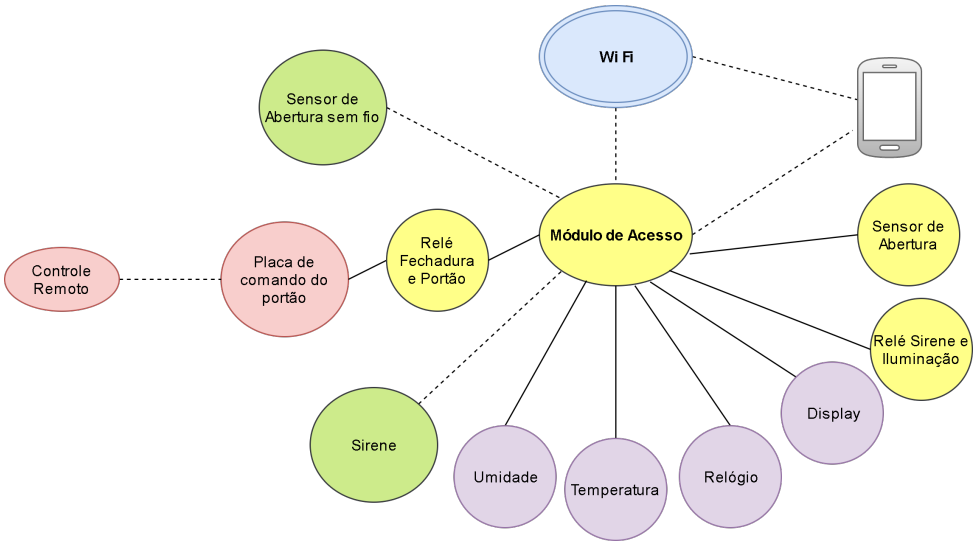
- Quando acender ou apagar a luz? - presença, acionamento manual (horário e módulo)
- Quantas vezes notificar? Prioridades? - respostas do cliente (log), para notificar o mínimo necessário, e classificação de notificações (email, somente quando usuário abre o aplicativo, notificação no celular e até módulo de painel externo com buzzer, no caso de comunicação de situação de perigo entre residências fisicamente separadas).

Respondendo a essas perguntas, esperamos contribuir para a construção de um sistema autônomo, que aprende com feedbacks do usuário seja pelo monitoramento por módulos ou respostas dadas pelo aplicativo, atuando em segurança (safety), saúde e A automação da residência do cliente.

1.3.2 Módulo de Acesso

Buscando garantir mais segurança e comodidade para o acesso à residência, além de um controle de liberação, o módulo de acesso atua em paralelo com uma fechadura eletrônica, que é acionada por meio de um controle por ondas de rádio, para que, mesmo com falha total do sistema, o usuário possa abrir o portão (ou que ele possa optar por usar o antigo sistema exclusivamente).

Figura 2: Diagrama ilustrativo do módulo de Acesso ao Portão



O diagrama ilustra o sistema já existente (em vermelho), sensor e sirene sem fio adicionais em verde (dispositivos externos ao módulo, que se comunicam por rádio), o próprio módulo de acesso, com um buzzer embutido, e sua conexão com a rede local Wi-Fi ou sua conexão direta com o celular (quando o módulo opera como um ponto de acesso de rede) em amarelo, além de funcionalidades adicionais em roxo.

A comodidade está em abrir o portão por meio do celular, por um aplicativo ou página web local, sem a necessidade de carregar uma chave ou controle. Além disso, pode prover maior praticidade (enquanto o celular está com o usuário na maioria do tempo, chave e controle podem estar na mochila). Para usuários que fazem passeios a pé, em sua maioria curtos, ou que vão à academia perto de suas casas, carregar chaves/controles é particularmente incômodo.

Por outro lado, é desejável realizar esse controle de forma segura. Por isso, o acesso é apenas local (o usuário deve estar com o celular conectado à rede local para acessar a página local, por exemplo), e um algoritmo de rotação de teclas é realizado, para evitar que pessoas mal intencionadas possam (1) olhar e copiar a senha que o usuário digita em seu celular e (2) copiar os dados de abertura e usá-los mais tarde ("middle man"). Na última alternativa, a cada acesso de um usuário, um novo mapeamento de teclas é gerado e enviado ao usuário. Mesmo que haja cópia, ela não funcionará devido ao mapeamento ter mudado. Observe ainda que a fechadura eletrônica por si só já estava vulnerável a isso (há inclusive dispositivos copiadores de senhas).

Outro aspecto de segurança é a preocupação dos usuários com o estado do portão. Muitas vezes, pode haver esquecimento ou falha e o portão ficar aberto. Para mitigar esse perigo, o módulo deve monitorar, por meio de um sensor, o estado da porta (aberto/fechado), e alertar localmente (por meio de "buzzer") e remotamente (por email ou notificação no *smartphone*, por exemplo) o usuário a abertura em horários . Essa e outras configurações (como de rede) são acessadas por meio de uma senha diferente daquela de abertura, para que a interface básica seja simples para uso.

Para o caso de falha de envio de email (servidor falha, ou algum outro problema), há um algoritmo de novas tentativas com tempos progressivamente maiores conforme as falhas ocorrerem, que busca deixar o módulo disponível para outras funções enquanto o serviço de e-mail não está disponível. No caso de indisponibilidade da internet, temos um procedimento análogo.

Para o caso de falta de conexão à internet, o módulo não seria controlável pela API, e as atualizações de dados como estado do portão seriam armazenadas para serem enviadas ao servidor em momento posterior, quando houvesse conexão à internet novamente. Caso o usuário esteja conectado à mesma rede local que o módulo, o mesmo continuaria funcionando normalmente.

Já no caso de falha da rede local, ou desconexão do módulo da rede local por problema de autenticação ou outros, o módulo de acesso ativa o *Access Point*, e possibilita ao usuário acessar a rede do módulo e abrir o portão.

Para evitar o travamento, um sinal de "keep alive" é monitorado, e um circuito anti travamento deve ativar um "hard reset" (reset por hardware), ou então uma rotina de "soft reset" deve ser acionada. No entanto, observe que a segunda alternativa é a mais fácil de implementar, mas a menos robusta, já que ainda pode não funcionar em casos de loop infinito.

Outra situação que poderia gerar indisponibilidade do sistema é um ataque de DoS local ("Evil Twin"), no qual uma rede mal intencionada usa o mesmo SSID (*Service Set Identifier*, o nome associado à rede WLAN) da rede original, tentando obter a senha na ocasião de reconexão de módulos. Muitas vezes, é também acompanhado de rádio interferência e outros procedimentos para fazer os módulos se desconectarem. Para mitigar o risco, cada módulo tenta inicialmente se conectar usando uma senha falsa no SSID fornecido. Caso obtenha sucesso (se a rede for aberta, como é o caso na maioria desses ataques), ele executa algoritmo análogo ao envio de emails (observe que enquanto não está conectado à rede o módulo atua como ponto de acesso e disponibiliza funcionalidades básicas). Caso ele não obtenha sucesso usando a senha errada (portanto, não detectou a situação de "evil twin"), o módulo envia a senha correta. Para proteger a rede, um controlador local do sistema pode atuar junto ao roteador e desligar a conexão sem fio enquanto a situação se manter.

O controle de acesso pode ser implementado por meio de persistência de dados de login e senha, e o uso de diversas senhas para uma residência (uma para cada morador - isso torna possível o conhecimento dos usuários que abriram o portão sem a necessidade de login prévio, facilitando o uso). O log destes acessos pode ser analisado (utilizando técnicas de Machine Learning) para determinar perfis de acesso, e evoluir até o sistema saber quando houver um acesso em horário inesperado e notificar o usuário remotamente. O aprendizado de máquina é fundamental aqui para descobrir comportamentos que podem ser entendidos como suspeitos. Para um usuário que costuma chegar em um horário aproximado todos os dias, e acionar funções semelhantes da casa, uma tentativa de acesso que não se enquadre em tais padrões pode ser produto de atividade criminosa, a qual pode ser informada pela casa para uma central, que acionará a polícia caso não seja um falso positivo.

2 PROJETOS RELACIONADOS

2.1 Sistemas Existentes no Mercado

2.1.1 Sistemas Comerciais

Atualmente, já percebe-se a existência de alguns sistemas comerciais de automação residencial - a maioria deles atuando de maneira mais forte do mercado Norte-Americano. Alguns dos sistemas mais populares nessa linha são o Amazon Echo e o Google Home.

O Amazon Echo[1] consiste em um *smart speaker* (alto falante inteligente) conectado ao assistente pessoal Alexa, também da empresa Amazon, que é capaz de entender comandos de voz. Inicialmente, funcionava como uma maneira de encomendar produtos por voz. Atualmente, além de funcionar como assistente pessoal, também é capaz de controlar diversos *smart devices* da casa, funcionando como um *hub* de automação residencial. Uma limitação deste produto é que funciona apenas com uma conexão *wireless* de Internet, não sendo capaz de operar em nenhum nível sem a mesma.

Algumas características interessantes do Alexa são que desenvolvedores são capazes de adicionar novas *skills* (habilidades) por meio de documentação da API que está pública e disponibilizada *online*. Dessa forma, seu *skillset* é passível de grande expansão e personalização. Além disso, o serviço de voz desse sistema, conhecido como Alexa Voice Service, pode ser utilizado por qualquer dispositivo que contenha microfone e alto falante e consiga conectar-se a ele pela Internet.

O Google Home[2] é similar ao Amazon Echo em alguns aspectos, sendo também um *smart speaker*, que surgiu como expansão do aplicativo para *smartphones* Google Now (um assistente pessoal). Atualmente existe também como aplicativo para *smartphones*. Não é possível o desenvolvimento de módulos e expansões ao Google Home por desenvolvedores desvinculados à Google, porém ela trabalha diretamente com outras marcas e produtos para o

[1] http://www.amazon.com/oc/echo/
[2] https://madeby.google.com/home/

estabelecimento de parcerias que permitam integração com eles, de forma que o Google Home também consiga funcionar como *hub* de automação residencial.

2.1.2 Sistemas Open Source

Também existem diversos projetos *open source* sobre o tema, cujas documentações estão disponíveis publicamente online. Alguns desses projetos analisados para o desenvolvimento do nosso projeto Hedwig foram o OpenHAB e o Home Assistant.

O OpenHAB[3] possui como objetivo principal o estabelecimento de uma plataforma em software de integração que seja capaz de solucionar o problema atual de que os diversos *devices* de uma residência não são capazes de se comunicar devido à falta de uma linguagem comum com a qual eles possam estabelecer tal comunicação. Por ser independente de hardware específico, é extremamente flexível e personalizável, porém isso implica em certa complexidade para o usuário, no momento de sua instalação. Apresenta interface para o usuário em cliente web e aplicativos nativo para iOS e Android.

O Home Assistant[4] é uma plataforma de automação residencial capaz de controlar e monitorar os diversos devices em uma casa, oferecendo uma plataforma web para o controle do sistema pelo usuário. O controlador local é implementado em Python, e recomenda-se instalá-lo em um Raspberry Pi. Possui diversas integrações já estabelecidas, com sistemas e serviços como o próprio Amazon Echo, Google Cast, IFTTT, Digital Ocean, entre outros, mas possibilita também a criação de novos componentes pelos próprios usuários. A personalização pelos usuários é feita por meio de um arquivo de configuração, no formato YAML.

Os dois projetos apresentam a dificuldade de que é necessário que o usuário possua conhecimentos técnicos para utilizá-los.

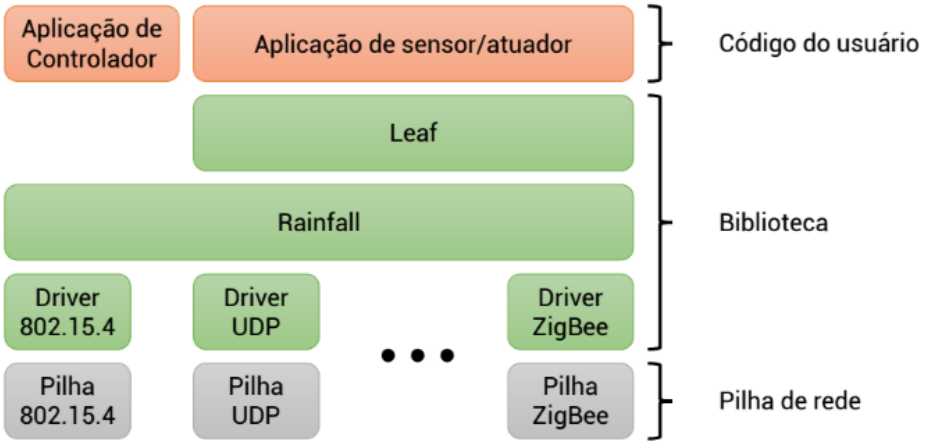
2.2 Projeto HomeSky

O Projeto HomeSky (**??**) é um Trabalho de Conclusão de Curso desenvolvido por alunos de Engenharia de Computação na Escola Politécnica da Universidade de São Paulo. Com o objetivo de fomentar iniciativas de desenvolvimento na área de casas inteligentes, o trabalho focou-se na criação do protocolo Rainfall, um protocolo em código aberto a nível de aplicação para ser usado na coordenação de uma rede de sensores. Isso permitiria aos desenvolvedores ter uma maior flexibilidade em seus projetos, visto que muitas das soluções existentes são

[3] http://www.openhab.org/
[4] https://github.com/home-assistant/home-assistant

proprietárias. Por fim, também foi realizada a implementação de um algoritmo de aprendizado de máquina capaz de controlar a iluminação.

Figura 3: Camadas da arquitetura usada no Projeto HomeSky. As camadas em verde correspondem às bibliotecas desenvolvidas no trabalho.



No desenvolvimento do protocolo Rainfall, foram consideradas algumas hipóteses simplificadoras a respeito da conectividade e da segurança. O protocolo não trata de forma especial a fase de conexão à rede, considerando que todos os nós já estão conectados a ela, e também considera que todos os protocolos adjacentes são confiáveis, deixando possíveis implementações de mecanismos de reconhecimento de entrega e retransmissão a cargo do desenvolvedor. Quanto à segurança, assume-se que a infraestrutura seja segura e que nenhum nó conectado à rede tenha comportamento mal intencionado, como por exemplo espionar mensagens destinadas a outros nós ou fingir ser o controlador.

O sistema Hedwig será uma evolução natural do Projeto HomeSky, buscando aperfeiçoar seu protocolo e arquitetura quanto à robustez e expandir a aplicação de aprendizado de máquina, além de viabilizar seu conceito, desenvolvendo soluções voltadas ao mercado brasileiro.

3 ESPECIFICAÇÃO

3.1 Componentes

3.2 Stakeholders

Com as funcionalidades e os módulos apresentados, podemos destacar os seguintes grupos dentre os potenciais consumidores:

- Pessoas que moram sozinhas e suas famílias, que podem estar interessadas em monitoramento;
- Pessoas que desejam comodidade de controlar seus aparelhos numa interface única, pelo celular, e/ou conforto maior em casa;
- Pessoas preocupadas com o consumo de água e energia elétrica.

Considerando o Censo de 2010 (**??**), podemos estimar grosseiramente as classes de consumidores, para a cidade de São Paulo:

- Considerando que 1/10 da população com mais de 60 anos more sozinha e que 1/4 deles adquiriria o produto, temos uma estimativa de 33 mil consumidores. Como essa população está envelhecendo em taxas cada vez maiores (8,96% em 2000 contra 13,6% em 2016) (**??**), a tendência é que essa classe aumente;
- Considerando que 1/100 dos domicílios ocupados tenha uma pessoa com esse perfil, temos uma estimativa de 35 mil consumidores em potencial;
- Considerando que cerca de 70% das residências reduziram o consumo com campanhas de redução de uso de água em 2015 (**??**), supondo que 5% ficariam preocupados/interessados ao nível de se tornarem consumidores, temos uma estimativa de 71 mil consumidores em potencial.

3.3 Requisitos

O levantamento de requisitos não-funcionais foi realizado com base na norma ISO25010:2011 (**??**).

3.3.1 Requisitos Funcionais

- O sistema deve permitir o monitoramento de aparelhos do dia a dia, dentro de uma residência, em módulos independentes;
- O sistema deve ser capaz de enviar notificações aos usuários, seja por meio de um serviço no cliente utilizado pelo usuário (web ou mobile app);
- O sistema deve poder ser personalizável pelo usuário, o qual pode adquirir novos módulos ou retirar algum já existente;
- O sistema deve ser capaz de aprender a respeito de cada usuário, utilizando conceitos de Machine Learning. O aprendizado de máquina é responsável por detectar padrões no comportamento do usuário, os quais podem ser utilizados para a segurança da casa. Assim, se o usuário, por padrão, chega em casa em uma janela de horário constante, e interage com certos módulos, caso haja uma atividade que não se enquadra no padrão, o comportamento pode ser considerado suspeito, e providências tomadas (como notificações para outros usuários, como alguém da família);
- O sistema deve manter backup de dados do controlador local na nuvem;
- O sistema deve permitir ao usuário o seu cadastro na plataforma, pela plataforma que melhor lhe convier;
- O usuário poderá cadastrar sua casa na plataforma, podendo ter uma ou mais casas cadastradas;
- O usuário poderá cadastrar os módulos dentro de uma casa, sendo que uma casa pode ter vários módulos, e cada módulo só poderá existir em uma casa;
- O usuário pode efetuar as operações de remoção e modificação nos seus módulos e casas;
- O sistema deve possuir uma função de reset de fácil utilização.

3.3.2 Requisitos Não-Funcionais

- Os módulos que compõem o sistema dentro de uma residência devem ser independentes entre si, devendo obedecer a uma interface comum de integração com o core do projeto, para que seja facilitada a ampliação e a inserção de novos módulos, com outras funcionalidades. Haverá validação com o desligamento de um módulo e verificação do comportamento dos demais;

- O sistema deve garantir segurança dos dados por meio de protocolo de comunicação seguro, tanto para o controle de acesso à API por usuários autenticados quanto para impedir que dados sejam interceptados em sua transmissão;

- O banco de dados deve possuir acesso restrito e estar hospedado em servidor de alta segurança;

- O sistema deve ser robusto, de modo a continuar operando, mesmo com menor nível de funcionalidades, quando da ocorrência de falhas na comunicação com a nuvem (indisponibilidade parcial devido a problemas com os servidores remotos, ou total com perda da conexão com a internet) ou falhas na rede local (indisponibilidade da conexão com a rede local). Também deve se recuperar em caso de travamento total do módulo e continuar funcionando em caso de DoS Local. Para validação, haverão testes de indisponibilidade de servidor, conexão com a internet, rede local e DoS local, e observação da continuidade de serviço de atuação na iluminação da casa e abertura do portão em menos de 10 minutos;

- O sistema deve apresentar disponibilidade de 99,9% (cerca de 8 horas de indisponibilidade por ano, não levando em consideração problemas com a conexão de internet da residência);

- O sistema deve ser escalável a até 10 mil usuários, sem perdas de desempenho consideráveis, ou aumento na latência para as requisições serem atendidas;

- O sistema deve estar preparado para inclusão de novos módulos no sistema pelo usuário e ser de instalação intuitiva e simplificada.

O levantamento de requisitos não funcionais foi realizado com base na norma ISO25010:2011 (**??**).

3.3.3 Requisitos por Nível de Conectividade

Figura 4: Tabela de requisitos por nível de conectividade

#	Requisito	Medição	Descrição	Online	Local (App-Controlador)	Offline (App-Módulo; direto no módulo)
1	Automação Residencial	Demonstração das funcionalidades listadas	Controle por App ou no módulo	Usar parâmetros para controle inteligente de lâmpada e despertador (Quarto)	Configurar lâmpada automática (Quarto) - App Configurar despertador (Quarto) - App	Ligar e desligar lâmpada (Quarto) - Módulo Desativar despertador (Quarto) - Módulo Destravar porta (Acesso) - App
2	Monitoramento Residencial	Demonstração das funcionalidades listadas	Monitoramento no App e displays dos módulos	Estado do portão (Acesso) Temperatura, Umidade (Todos) Presença (Quarto)	Estado do portão (Acesso) Temperatura, Umidade (Todos) Presença (Quarto)	Temperatura, Umidade (Todos) - Módulo Presença (Quarto) - Módulo
3	Modularidade	Funcionamento de módulo "stand-alone"	Soluções modulares		Inserção automática/reconhecimento (Todos)	
4	Escalabilidade para n residências	Testes de carga, acessos simultâneos	Suporta carga, acessos simultâneos			
5	Machine Learning	Tratamento de séries de dados reais	Análise dos dados para levantamento de rotinas e reconhecimento de padrões	Derivações de Regras Perfil Esperado de Comportamento	Alerta de Portão Aberto (Acesso)	Alerta de Portão Aberto (Acesso) - Módulo
6	Backup de dados	Funcionalidade de Backup de dados no controlador local		Redundância na nuvem	Armazenamento de dados temporariamente num cartão SD, no controlador local	
7	Tolerância a falhas	Estatísticas de keep alive, ping local, ping internet de módulo base com e sem as melhorias	Manter funcionalidade Online, Local e Offline		Notificações e alertas no App (Monitoramento estado módulos)	Circuito "Keep Alive" - Hard Reset e Soft Reset
8	Segurança da informação	Protocolos seguros, controle de acesso	Protocolos seguros, controle de acesso	Autenticação para as funcionalidades descritas nesta coluna	Autenticação para as funcionalidades descritas nesta coluna	Autenticação para as funcionalidades descritas nesta coluna - Módulo

4 ARQUITETURA

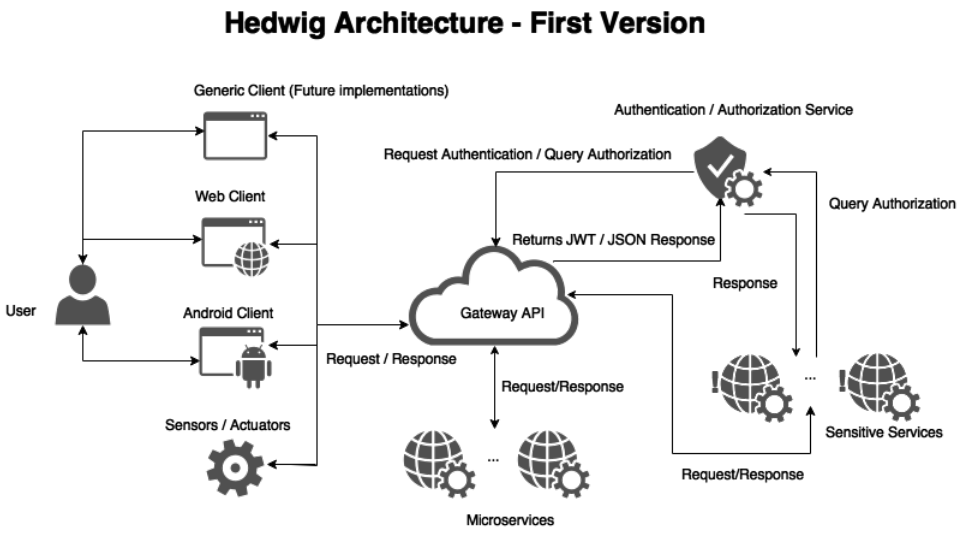
4.1 Visão geral

4.2 Evolução arquitetural

O processo de escolha para a arquitetura utilizada foi iterativo, e foram analisados os pontos fracos e as vantagens de cada nova sugestão.

A primeira versão proposta baseava-se unicamente em microsserviços, responsáveis por toda a inteligência do projeto, o que a fazia interessante do ponto de vista da escalabilidade, para um número muito grande de casas. Com uma arquitetura fundamentalmente desenvolvida assim, também é possível utilizar quantas tecnologias forem necessárias ou desejáveis para cada um dos serviços, sem efeitos colaterais nos outros, transparentemente.. Por outro lado, cria-se grande complexidade na integração entre todos os serviços disponíveis, mas que pode ser gerenciada por técnicas conhecidas, e também explicadas aqui (como a coreografia e a orquestração). O overhead para a comunicação, no entanto, é aumentado, e os serviços necessitam de um meio rápido e robusto, que implemente qualidade de serviço para padrões diferentes de mensagens. Foi proposto um gateway para os serviços da nuvem, onde passaria toda a comunicação com a casa. A inserção do gateway, no entanto, cria um ponto único de falha.

Figura 5: Primeira versão da arquitetura do projeto Hedwig

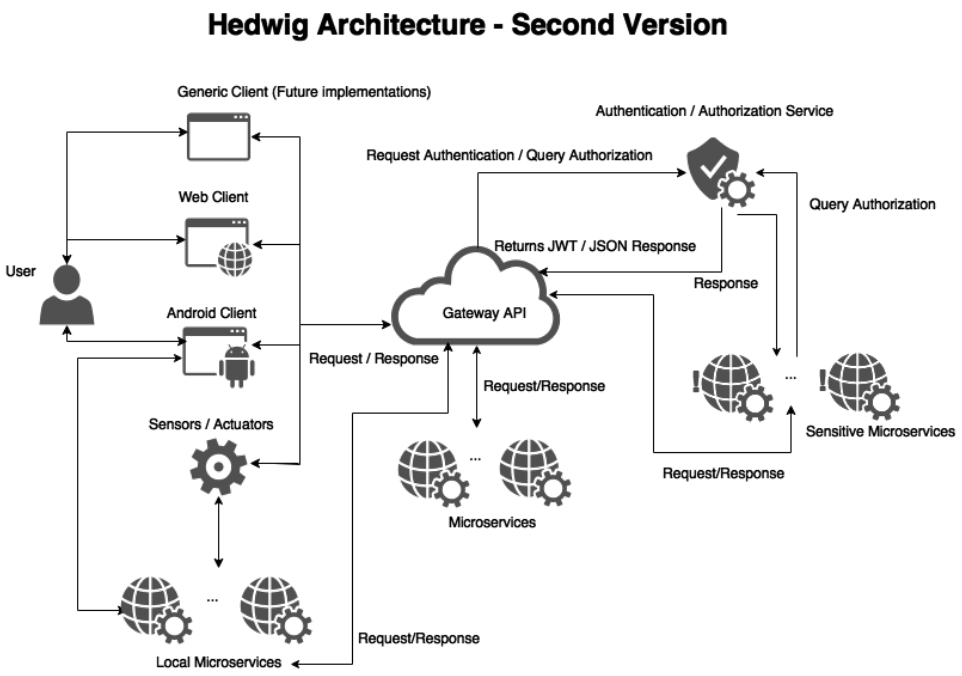


É possível observar que alguns microsserviços são classificados como sensitivos, os quais dependem de nova consulta ao serviço de autenticação e autorização, para garantir a segurança. Esses serviços são todos aqueles responsáveis por tomar uma ação em relação à casa que envolva riscos. Os microsserviços não sensitivos utilizam a autenticação já realizada pelo gateway, na chegada do request.

Quando uma requisição chega à nuvem, ela deve ser autenticada, e caso passe nos critérios de autenticação e autorização, é retornado um JWT (JSON Web Token), necessário para os passos seguintes. O token JWT é discutido aqui, na seção MARCAR SEÇÃO AQUI.

De extrema importância, e não cobertos pela arquitetura anterior, são os requisitos de disponibilidade do projeto. Se o gateway estiver inacessível em determinado momento, a casa não terá mais nenhuma forma de comunicação com os meios externos, mesmo para os serviços mais básicos. Para resolver este problema, foi proposta uma segunda versão, conforme ilustra a imagem seguinte.

Figura 6: Segunda versão da arquitetura do projeto Hedwig



Nesta versão, serviços essenciais seriam duplicados dentro da casa, e no caso de haver qualquer forma de impedimento na comunicação com a nuvem, esses serviços seriam responsáveis por controlar diretamente os atuadores desejados. Entretanto, cria-se mais uma complexidade, ao manter serviços duplicados na casa, e no caso destes serviços não estarem online no momento necessário, também não seriam alcançados requisitos mais fortes de disponibilidade. Contudo, é uma versão que chega mais próximo de obedecer às necessidades do projeto.

Essa arquitetura provê módulos sem inteligência, e todo o controle é feito pelo serviço correspondente. Ao mesmo tempo que essa escolha tem benefícios, como a escalabilidade, a manutenção (já que é muito mais simples atualizar o software de um ponto único, sempre que necessário), para correções ou possíveis aumentos de funcionalidade. Porém, não ficaríamos livres, mais uma vez, do ponto único de falha. Também, alguns módulos ficariam em lugares de difícil acesso, ou mesmo fora da casa, onde a comunicação poderia ser perdida, ou ser intermitente. Assim, em caso de falha de comunicação, um atuador não receberia os sinais necessários do serviço, acarretando em sérios problemas de segurança. No caso de uma garagem, por exemplo, o portão permaneceria aberto indeterminadamente, ou poderia não ser aberto o morador chegasse em csa.

Assim, começamos o desenvolvimento de um modelo arquitetural modularizado, onde cada módulo teria inteligência para realizar as tarefas necessárias e, ao mesmo tempo, podendo

enviar dados à nuvem, e ser avisado quando deve realizar uma tarefa. Com isso, em um aspecto também comercial, módulos inteiros poderiam ser vendidos, substituídos e aumentados.

A arquitetura escolhida, também faz uso de microsserviços, no lado da nuvem, e no lado da casa os componentes de hardware passam a ser agrupados em módulos independentes, com responsabilidades bem estabelecidas, inteligência para fazer todas as atividades necessárias, e com comunicação a um servidor local, que realizará, por último, a comunicação direta com os serviços não locais. Esse servidor se comunicaria com módulos por meio de mensagens, enviadas em tópicos, as quais seriam interpretadas e enviadas aos servidores remotos. Se a casa perder comunicação com a nuvem, o servidor local armazenará as mensagens, que serão enviadas posteriormente. Essas mensagens, no caso, seriam de dados, advindas de sensores em módulos. Como não há urgência para o processamento de tais dados, os quais serão utilizados para análise de comportamento e machine learning, não há prejuízo com o eventual envio tardio.

Quando a comunicação entre o servidor local e a nuvem for perdida, os aplicativos web ou mobile, poderão se comunicar diretamente com o servidor local da casa, para acessar uma quantidade mais restrita e essencial de ações (como liberação de acesso, por exemplo). Além disso, no caso de perda de comunicação com o servidor local também, os aplicativos poderão se comunicar diretamente com os módulos para terem acesso aos serviços de extrema importância.

Por ser escolhida, essa arquitetura será extensivamente detalhada e discutida aqui, com seus benefícios e limitações.

4.3 Módulos

Para a criação dos módulos de hardware, foram escolhidos componentes de IoT comerciais, que possuem preços acessíveis, ampla documentação disponível e uma comunidade de desenvolvedores crescente.

A interconexão dos componentes, bem como a comunicação com o mundo externo pela internet será intermediada por um servidor local, que rodará na plataforma Raspberry Pi, rodando um sistema operacional Linux (Raspbian), baseado em Debian, e que dispõe da interface de hardware necessária para conexão com a rede.

Os sensores e atuadores devem ser conectados fisicamente com um módulo controlador, de modo que, para contornarmos essa limitação, utilizaremos módulos ESP8266 para transmissão sem fio por meio do WiFi. Esses módulos serão responsáveis pela transmissão das informações

recebidas para o servidor local. Toda a arquitetura para essa transmissão será detalhada mais à frente. Os outros módulos a serem utilizados, como sensores DHT11, LM555, etc, podem ser vistos no anexo, em uma lista completa.

Em geral, esses módulos consistem do microcontrolador, relés, sensores e fontes/conversores de tensão a depender do módulo, além de um circuito para manutenção corretiva baseado no astável 555, conectados à rede WiFi e/ou trabalhando como pontos de acesso. Para casos de falha de conexão, há um algoritmo de novas tentativas com tempos progressivamente maiores conforme as falhas ocorrerem, que busca deixar o módulo disponível para outras funções enquanto o serviço não está disponível. Para evitar o travamento, um sinal de "keep alive" é monitorado, e um circuito anti travamento deve ativar um "hard reset" (reset por hardware), ou então uma rotina de "soft reset" deve ser acionada. No entanto, observe que a segunda alternativa é a mais fácil de implementar, mas a menos robusta, já que ainda pode não funcionar em casos de loop infinito.

4.3.1 Módulos Base

4.3.1.1 ESP8266

O ESP8266 é um microprocessador com baixo consumo e conexão WiFi 802.11 integrada (**??**). Pode ser programado usando a Arduino IDE, já muito utilizada (**??**). Opera com uma tensão de 3.3 V, suporta WPA e possui modo de interrupção somente por software. É amplamente usado como shield para conexão WiFi de placas de desenvolvimento da plataforma Arduino; contudo, no projeto Hedwig, o utilizaremos em modo StandAlone como principal processador e responsável pela conexão dos diferentes módulos de automação. Suas duas principais plataformas de desenvolvimento são Wemos[1] e NodeMCU[2]. O projeto utilizará o Wemos D1 Mini, versão compacta da Wemos D1 R2.

Possui um modo de operação de baixa potência (sleep mode), em que o nível de funcionalidades fica limitado, contudo o consumo de bateria fica muito menor. Podemos usar 7 portas de E/S digitais e uma porta de entrada analógica. Duas portas são inutilizáveis, pois são usadas para programação e outras tarefas do sistema integrado do ESP8266. Uma alternativa para extensão de portas é utilizar, por exemplo, três níveis de sinal análogico para detectar três tipos de acionamento (através de um circuito dedicado, com priorização de entrada), interface I2C (como o usado para o display) e uso de Radio Frequência, através de um par receptor-transmissor integrado no módulo, controles, atuadores e sensores sem fio.

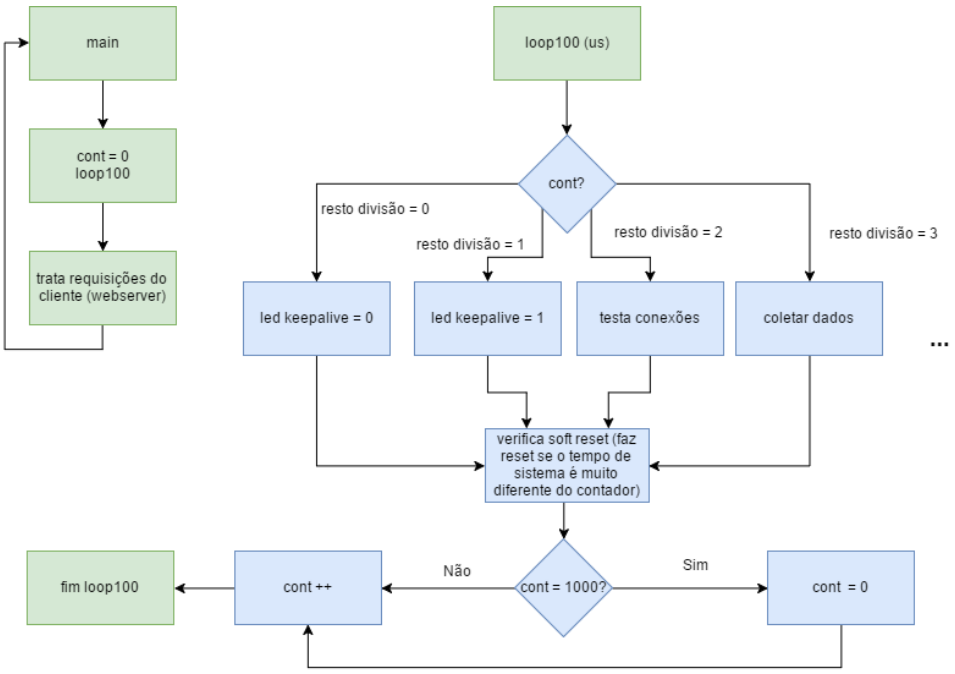
[1]Plataforma Wemos: https://www.wemos.cc/
[2]Plataforma NodeMCU: http://nodemcu.com/

Dentre os materiais adquiridos, destacam-se como exemplos o controle RF e sensor de abertura de portão sem fio - observe que a fechadura eletrônica já existe na residência teste, logo é utilizada nesse projeto, contudo não está na lista de materiais para aquisição.

4.3.1.2 Multiplexação no tempo

Para tratar indisponibilidade dos módulos devido a tentativas de reconexão e conexão e requisições não gerenciadas e aumentar a disponibilidade, além do circuito antitravamento e hard reset, as diversas rotinas (desde configuração inicial, reconfigurações, coletas de dados, atuar por meio de relés, até conexão, desconexão, reconexão e envio de dados) foram multiplexadas no tempo da seguinte forma:

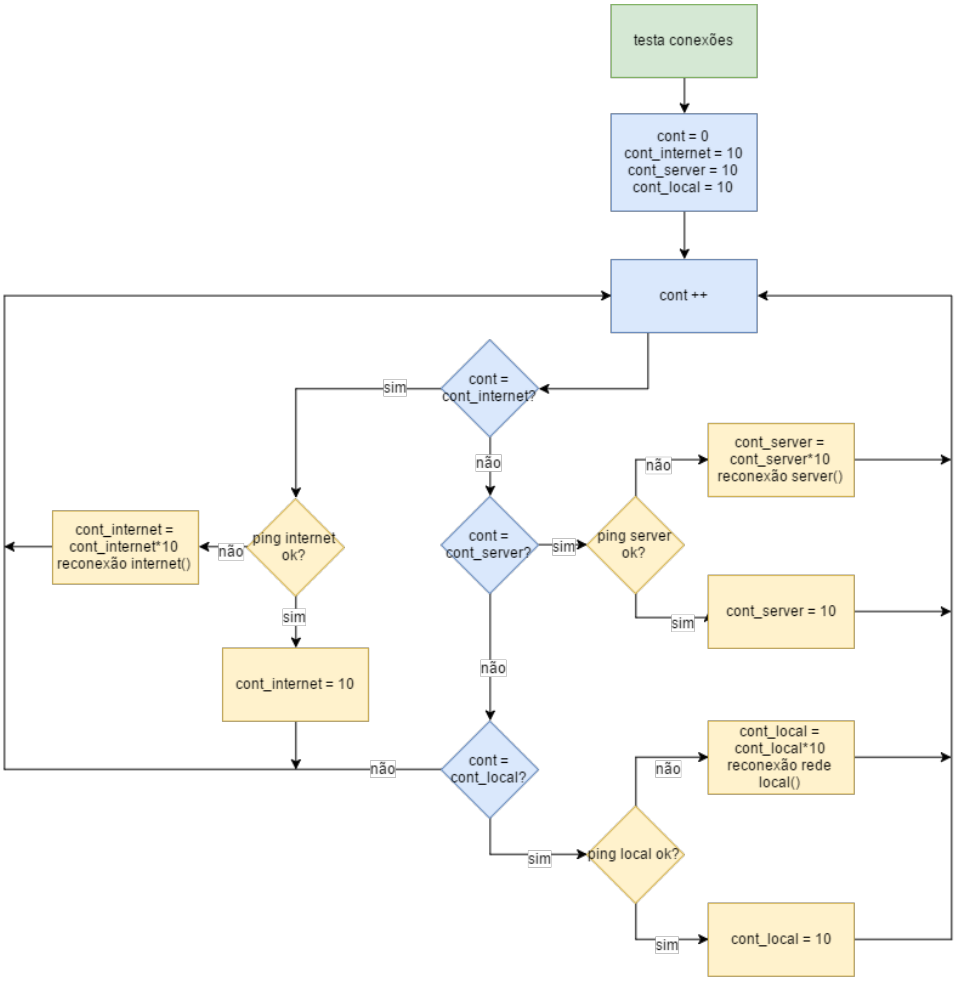
Figura 7: Rotina de multiplexação de procedimentos no tempo



4.3.1.3 Tratamento de indisponibilidade

Nos casos de indisponibilidade de internet, servidor ou rede local, o seguinte procedimento foi adotado: (observe que a indisponibilidade do próprio módulo é tratada pelo circuito antitravamento).

Figura 8: Tratamento de indisponibilidade de recursos



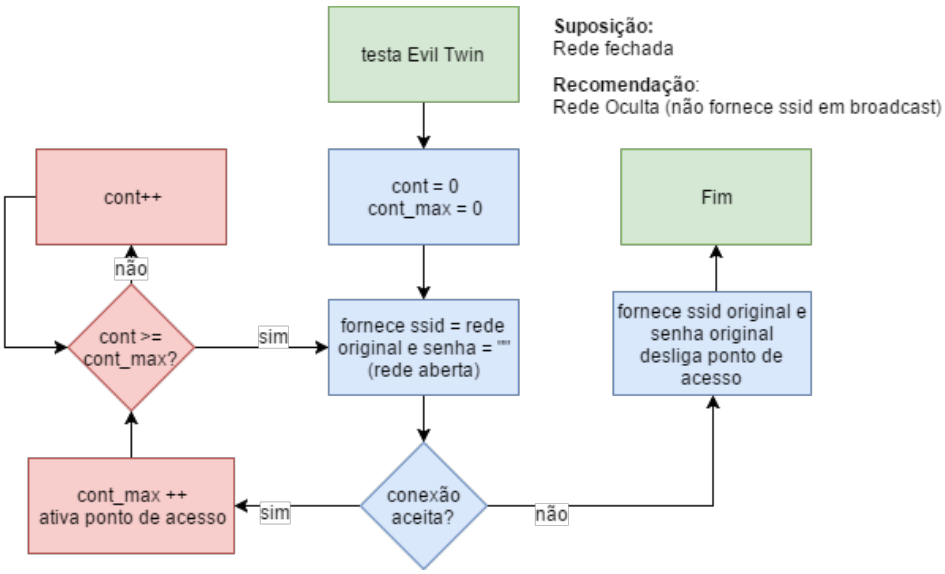
Com esse procedimento, as tentativas de reconexão à internet, servidor e rede local estão segregadas e com tentativas realizadas em intervalos de tempo sucessivamente maiores. Desta forma, conseguimos gerenciar esses procedimentos, já que o nível de processamento é baixo.

4.3.1.4 DoS Local (Evil Twin)

No caso de ataque de Evil Twin, no qual uma rede mal intencionada, usualmente aberta, usa o mesmo ssid da rede original, com o objetivo de obter a senha, o sistema pode ficar indisponível até ao nível local. Módulos podem se conectar à rede mal intencionada e ficarem somente com as funcionalidades offline (como acionamento de lâmpada por botão física acoplado ao módulo). Outro problema é a queda da rede por interferência de radio frequência ou outro mecanismo utilizado pelo usuário mal intencionado para que os clientes se desconectem, tentem reconexão e forneçam a senha da rede.

Para mitigar esses riscos, os módulos executam o seguinte procedimento:

Figura 9: Tratamento de ataque de DoS Local

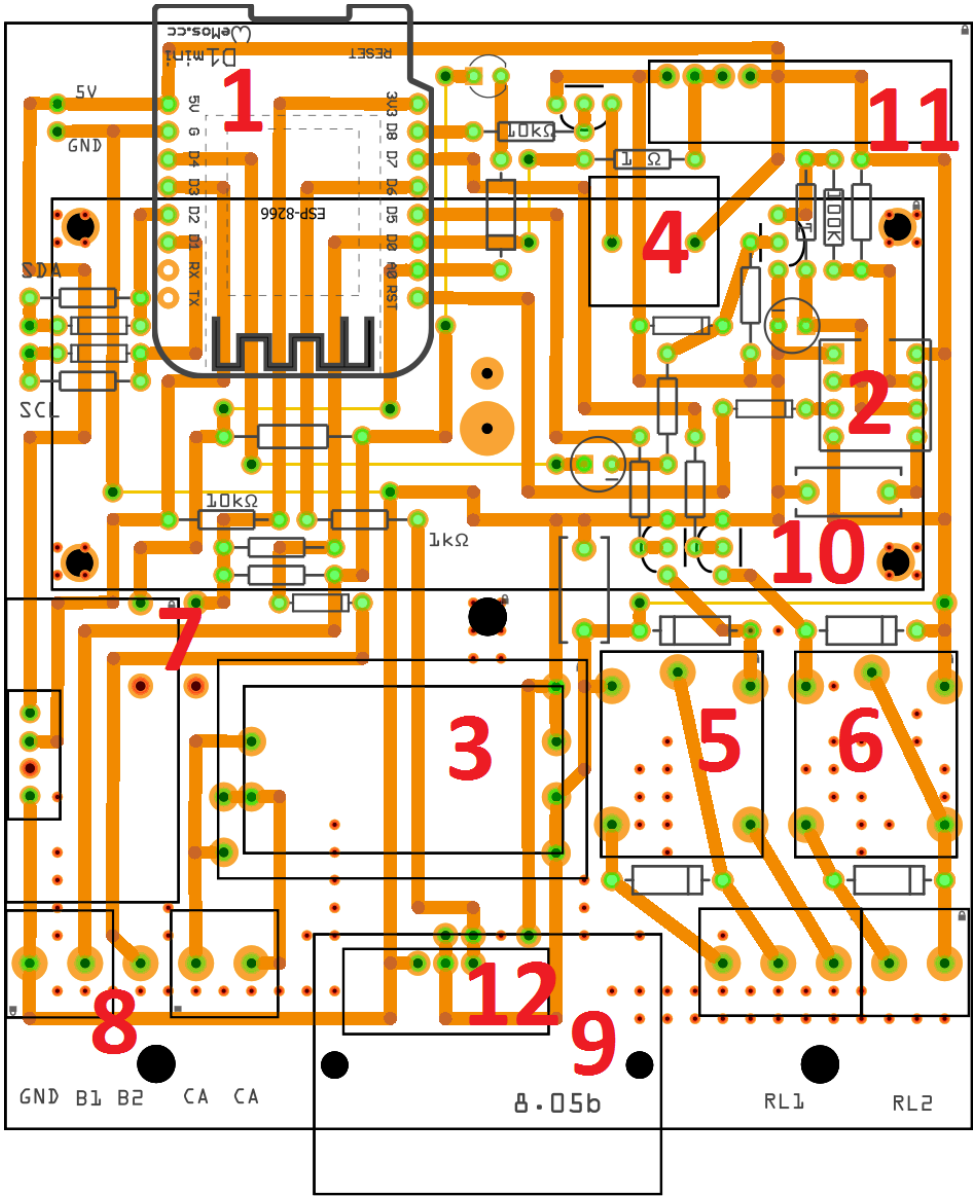


4.3.1.5 Diagrama

Segue diagrama do circuito impresso (PCB) feito em conjunto com o Projeto Katz-House[3]. Funcionalidade, componentes e arquitetura foram responsabilidade do Projeto Hedwig, enquanto a disposição física, se atentando para problemas de interferência e mantendo um módulo menor possível foi responsabilidade do Projeto Katz-House.

[3]Katz-House, Fabio Hayashi. Projeto Pessoal, 2017.

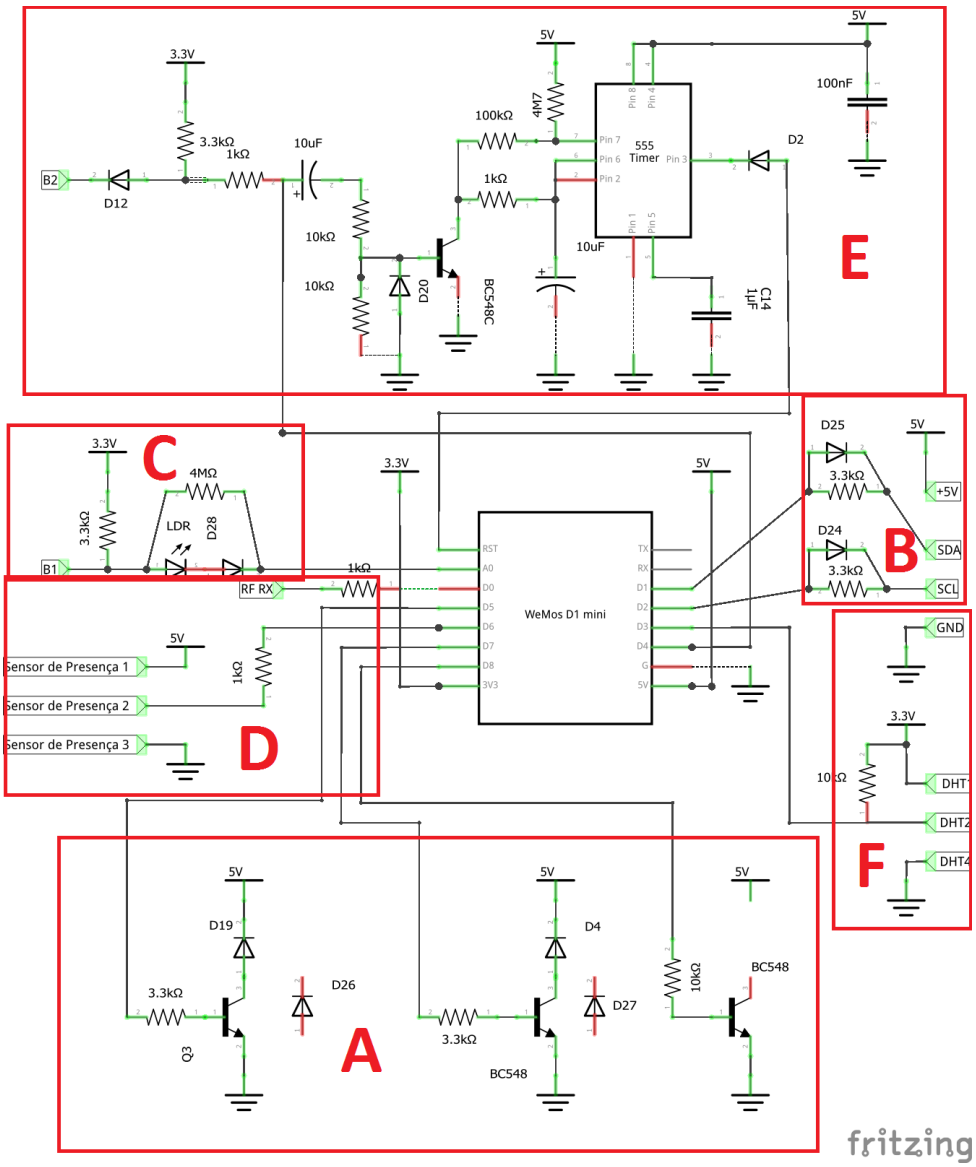
Figura 10: Diagrama PCB do Módulo Base



1. Wemos D1 mini
2. Astável 555
3. Fonte 5V 3W
4. Buzzer
5. Relé 1
6. Relé 2
7. Hard Reset

8. Botões
9. Presença
10. RF-RX
11. RF-TX

Figura 11: Diagrama PCB do Módulo Base

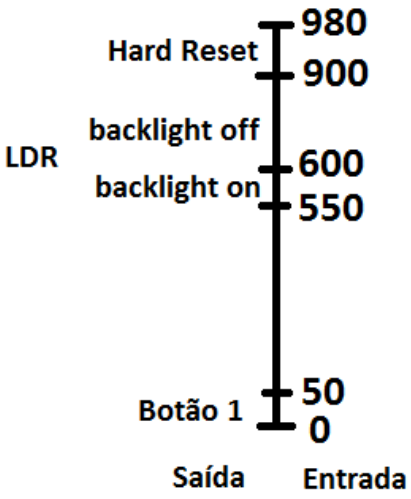


A - Saídas Circuitos simples de transistor para acionamento de relés (para lâmpadas) e buzzer.

Proteção 3V3 5V Como o display trabalha com tensão de 5V, há proteções com diodos para não danificar as entradas digitais do Wemos D1 mini, que trabalha com tensão de 3V3.

3 Entradas em A0 O circuito tem como entradas um botão (para acionamento do relé 1), o LDR (para chaveamento do backlight do display), e um outro botão para hard reset do dispositivo, todos numa entrada analógica, cujo mapeamento E/S é da seguinte forma:

Figura 12: Entradas Em A0



Presença ou RF-TX A entrada digital D6 é usada exclusivamente como entrada do sensor de presença PIR ou receptor RF.

Astável 555 para Hard Reset e Botão A porta D6 é usada como LED "keep alive" do módulo. Sua demora ao piscar indica que o módulo está travado ou demorando muito para processar algo (o que não deveria acontecer, uma vez que os procedimentos estão multiplexados no tempo, de acordo com seus tempos limite). Dessa forma, conectamos essa saída a um circuito antitravamento, que executa o reset caso nos casos mencionados, de travamento ou "timeout".

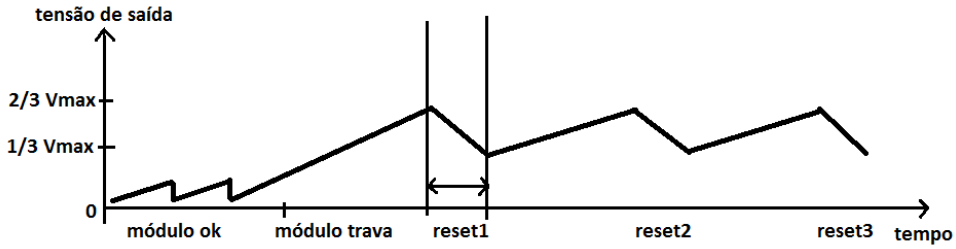
O primeiro capacitor tem como objetivo desacoplamento DC, de forma que a entrada do circuito envolvendo o astável 555 seja somente AC. Assim, travamentos em 0 ou 1 indicam travamento.

Enquanto o led pisca em intervalos esperados (regularmente), o transistor conduz e mantém uma saída dente de serra muito próxima de 0. Quando o módulo trava, o transistor não conduz mais, e a saída passa a oscilar entre 1/3 e 2/3 da tensão total (observe que o carregamento é feito pelo resistor de 4M7, muito maior que o resistor de 100k, fazendo com que o tempo de carga seja muito maior que o tempo de descarga, uma vez que esses tempos são diretamente proporcionais à constante de tempo dos circuitos RC, que é dada pelo produto do R*C). Durante a descarga, o reset da placa é realizado. Observe que os tempos foram ajustados pelos valores dos componentes

discretos, para que o tempo entre resets sucessivos seja menor que o tempo necessário para o módulo voltar a funcionar após um reset.

Segue abaixo uma ilustração sobre o funcionamento do circuito.

Figura 13: Funcionamento do Circuito de Antitravamento



DHT11 Entrada D3 é ligada a uma montagem básica para leitura de umidade e temperatura através do periférico DHT11.

4.3.1.6 Montagem

4.3.2 Módulo de Interface com Sistema de Alarmes

4.3.2.1 Especificação

4.3.2.2 Montagem

4.3.3 Módulo de Acesso

4.3.3.1 Especificação

4.3.3.2 Montagem

4.3.4 Módulo de Quarto

4.3.4.1 Especificação

4.3.4.2 Montagem

4.3.5 Módulo de Aquário

4.3.5.1 Especificação

4.3.5.2 Montagem

4.3.6 Módulo de Cozinha

4.3.6.1 Especificação

4.3.6.2 Montagem

4.4 Controlador Local

Para a intercomunicação entre os módulos e a nuvem, há a presença do servidor local Morpheus, responsável por introduzir mais uma camada de segurança, na autenticação das mensagens e garantir que as autorizações necessárias para os procedimentos existam. Para isso, foi desenvolvido um sistema de mensageria, com a definição de um protocolo de comunicação entre os serviços de nuvem e os módulos, e dos módulos para os serviços. Assim, quando um usuário desejar realizar determinada operação por meio do cliente web, uma mensagem é enviada, a qual será interpretada pelo servidor local, e em seguida encaminhada para o destino, por meio do protocolo MQTT, com o broker Mosquitto.

4.4.1 Requisitos funcionais

- Configuração dos módulos, de acordo com as regras e interfaces estabelecidas. Irá enviar para os módulos os novos parâmetros (vindos da nuvem) para se adaptar, de acordo com as necessidades do usuário;
- Autenticação local do usuário;
- Envio dos dados vindos do módulo para a nuvem, para que sejam tratados. É necessário estabelecer interface para a comunicação e formato dos dados;
- Persistência de dados. Quando não houver conexão, o servidor deverá armazenar os dados localmente, e depois enviar para a nuvem;
- Envio de pedidos de tomadas de ação para os módulos.

4.4.2 Formato dos Tópicos MQTT

hw<nome_do_modulo>s2m (Server to Module - o módulo deve ser subscriber desse tópico. O servidor deve ser publisher desse tópico).

hw<nome_do_modulo>m2s (Module to Server - o servidor deve ser subscriber desse tópico. O módulo deve ser publisher desse tópico).

4.4.3 Regras de Negócio

- Após a compra de cada módulo, o usuário deverá registrar online a aquisição. O servidor da nuvem enviará para o servidor local, da casa, a requisição para configurar o módulo;
- Cada módulo enviará mensagens para o servidor local com o seus dados, por meio do MQTT. A interface de comunicação deve ser estabelecida;
- Troca de senha do wifi: O usuário cadastra no site a nova senha. O servidor na nuvem faz a requisição para o servidor local, o qual enviará um arquivo de configuração com a nova senha para cada um dos módulos registrados. Após a configuração de todos os módulos, o servidor local envia resposta de sucesso para a nuvem, a qual indica ao usuário que a troca de senha já pode ser feita com sucesso;
- Todo módulo sai de fábrica configurado com o tópico que deve se inscrever e publicar;
- Cada módulo terá um certificado digital. O broker MQTT somente deixará alguém ser publisher/subscriber de um tópico caso tenha esse certificado.

4.4.4 Definição de Interfaces

- Dois tipos de mensagens do servidor para os módulos: Configuração (configuration) e Requisição de Ação (action_request);
- Três tipos de mensagens dos módulos para o servidor: Confirmação (confirmation), Envio de Dados (data_transmission) e Data Request (data_request).

4.4.5 Definição das Mensagens

4.4.5.1 Configuração (configuration)

- Sentido: Servidor para módulo
- Protocolo: MQTT
- Uso: Envio dos parâmetros para se adaptar ao comportamento do usuário (Machine Learning). Isso ocorre quando o algoritmo de ML, na nuvem, identifica a necessidade de modificar um comportamento do módulo. O servidor da nuvem envia uma mensagem para o servidor local, com a identificação de cada módulo e quais variáveis devem ser modificadas em cada um deles.
- Definição do formato: #configuration $ts:<timestamp>$ty:<tipo da configuracao>@ <dados a serem interpretados pelo módulo>@

4.4.5.2 Requisição de ação (action_request)

- Sentido: Servidor para módulo
- Protocolo: MQTT
- Uso: Quando um usuário faz a requisição de uma ação por meio do aplicativo. Por exemplo, quando deseja-se acender uma luz, o aplicativo envia uma requisição para o servidor local, o qual enviará uma mensagem de action_request para o módulo correspondente.
- Definição do formato: #action_request $ts:<timestamp>$ty:<tipo da ação>@ <dados a serem interpretados pelo módulo>@

4.4.5.3 Confirmação (confirmation)

- Sentido: Do módulo para o servidor

- Protocolo: MQTT
- Uso: Confirmação de uma configuração, patch ou requisição de ação, vindas do servidor.
- Definição do formato: #confirmation $ts:<timestamp>$ty:<tipo da confirmação>@ <dados a serem interpretados pelo servidor>@

4.4.5.4 Transmissão de dados (data_transmission)

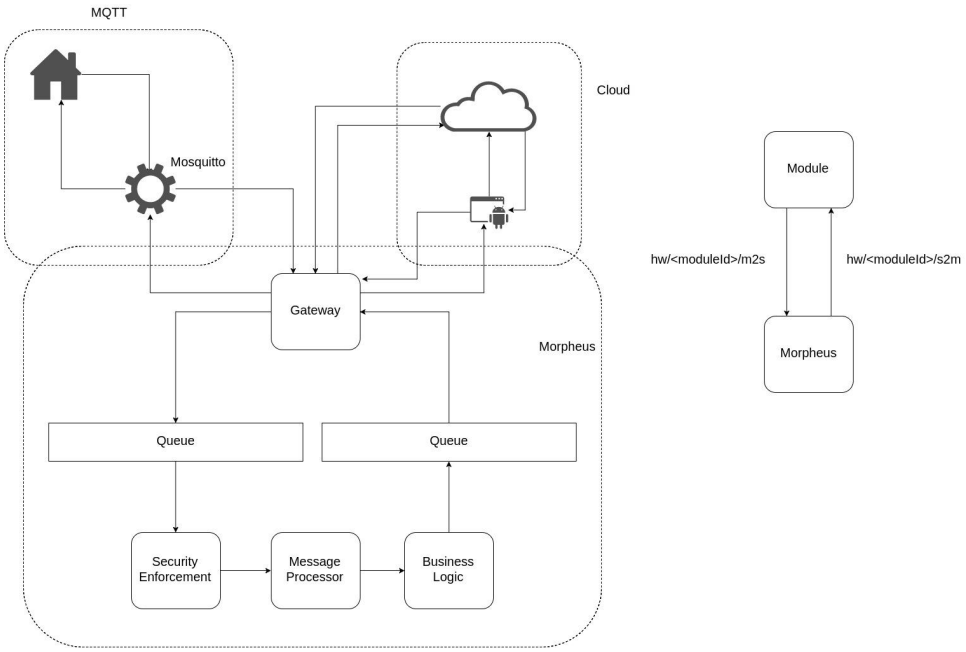
- Sentido: Do módulo para o servidor
- Protocolo: MQTT
- Uso: Envio de dados de sensores para o servidor
- Definição do formato: #data_transmission $ts:<timestamp>

  $ty:<tipo de dados>@ * sn:<sensor name>vl:<value>* * sn:<sensor name>vl:<value>* * sn:<sensor name>vl:<value>* @

4.4.5.5 Requisição de dados (data_request)

- Sentido: Do módulo para o servidor
- Protocolo: MQTT
- Uso: Requisição de alguma informação do servidor. Ex.: Atualização de hora
- Definição do formato: #data_request $ts:<timestamp>$ty:<request_type>

Figura 14: Tópicos MQTT



4.4.6 Raspberry Pi

O Raspberry Pi é um computador integrado num único chip, do tamanho de um cartão de crédito. Foi desenvolvido com o objetivo de promover o ensino de computação básica, que possui funcionalidades tais como um computador desktop: navegação na internet, reprodução de video, processamento de texto, dentre outros. No projeto, será utilizado como servidor local (gerenciador de módulos local da casa), exatamente pelas funcionalidades compatíveis com a de um computador desktop.

A versão 3 possui uma CPU 1.2 Ghz 64-bit quad-core ARMv8, conexão 802.11n Wireless LAN, Bluetooth 4.1, suporte a Bluetooth Low Energy (BLE), 1GB RAM, 4 portas USB, 40 pinos GPIO, porta HDMI, porta Ethernet, interface para câmera, display e cartão SD. Para projetos que necessitem de baixo consumo energético, os modelos mais indicados são Pi Zero ou A+ (**??**).

4.5 Servidor na Nuvem

Como foi escolhida uma arquitetura baseada microsserviços para construção do projeto, módulos diferentes podem ser escritos em linguagens de programação diferentes, o que promove uma maior flexibilidade não só durante o desenvolvimento dos módulos de mostrados nesse trabalho, mas também daqueles projetados futuramente como extensões do sistema

Hedwig.

Para o desenvolvimento dos módulos definidos na especificação do projeto, utilizamos tecnologias atuais que são utilizadas em grandes empresas de tecnologia do mundo e possuem vasta documentação, referências e fontes de conhecimento como tutoriais e exemplos. Para o desenvolvimento da parte de software, utilizaremos tecnologias atuais, que são também utilizadas nas maiores empresas de tecnologia do mundo. De acordo com o planejamento, utilizaremos uma arquitetura de microsserviços para construção do projeto. Com esta técnica, módulos diferentes poderiam ser escritos em, inclusive, linguagens de programação diferentes, o que promove uma maior flexibilidade durante o desenvolvimento. Para o desenvolvimento da API, responsável pelos módulos sendo executados na nuvem e comunicação com banco de dados, utilizaremos Node.js (interpretador de código JavaScript do lado do servidor), com a utilização de alguns frameworks como é o caso do Express. O banco de dados com a qual ela se conecta é do tipo MongoDB (banco de dados orientado a documentos). Tais decisões foram baseadas no fato de bancos de dados em MongoDB serem altamente escaláveis e flexíveis, assim como Node.js, que, por sua arquitetura movida a eventos de E/S que não bloqueiam o servidor, provê ao mesmo uma altíssima escalabilidade, ao permitir milhares de conexões simultâneas, sem impacto na performance do servidor. Além disso, o fato de que os dados provindos do banco já estão organizados em objetos, e dessa forma, podem ser recebidos prontamente como objetos JavaScript no código em Node.Js geram facilidade e fluidez para o desenvolvimento do código.

4.5.1 Arquitetura de Microsserviços

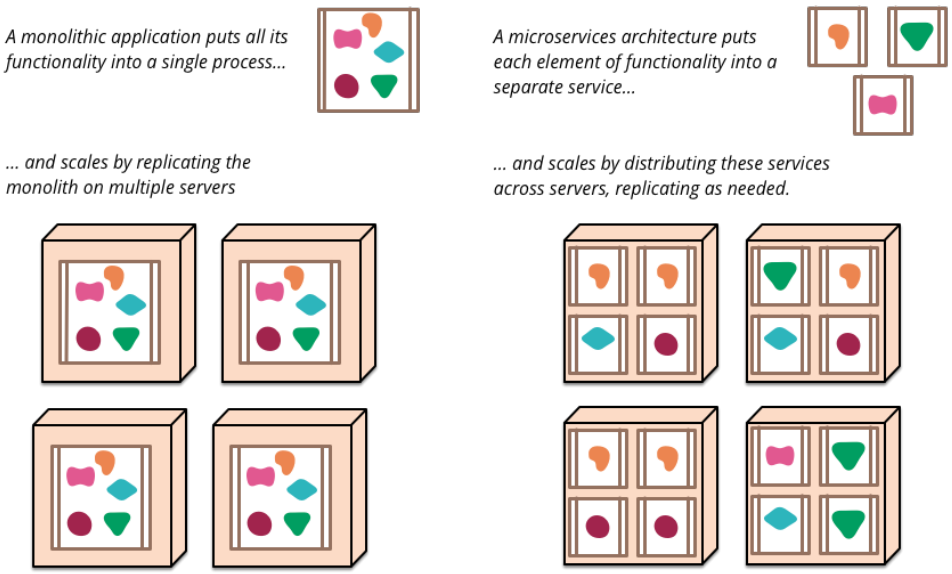
4.5.1.1 Características

A arquitetura de microsserviços é um estilo que compreende a estruturação de uma aplicação em um conjunto de serviços com baixo grau de acoplamento que se comunicam por meio de protocolos de comunicação leves.

Para melhor compreender essa arquitetura, podemos compará-la à arquitetura monolítica. Uma aplicação monolítica está contida em uma única unidade, que geralmente é dividida em camadas de funcionalidade tecnológica como interface web, camada de negócios server-side e camada de persistência de dados. A escalabilidade desse modelo é dada por meio do aumento do número de servidores, máquinas virtuais ou contêineres juntamente a um load balancer - é a chamada escalabilidade horizontal. Uma alteração em uma pequena parte da aplicação significa que toda a aplicação deverá passar por um processo de build e deploy. Já a arquitetura de microsserviços divide as funcionalidades em serviços autônomos, muitas vezes

usando as regras de negócios para realizar essa divisão. Cada serviço tem seu próprio ciclo de desenvolvimento e pode ser atualizado independentemente. A escalabilidade também é tratada serviço a serviço.

Figura 15: Comparação entre uma aplicação monolítica (esquerda) e com microsserviços (direita)



É difícil delimitar uma definição formal para arquitetura de microsserviços, pois não existe consenso a respeito de sua definição formal. Contudo, existe uma série de características que projetos usando essa arquitetura compartilham. Detalhamos a seguir alguns atributos e aspectos dos microsserviços. Nem todos os projetos possuem rigorosamente todas as características, mas a maioria deles possui um perfil similar ao descrito aqui.

- **Serviços são processos.** Pode-se fazer um mapeamento de um processo para um serviço, porém isso é apenas uma aproximação, podendo um serviço ser constituído por uma aplicação de múltiplos processos.
- **Serviços comunicam-se por protocolos leves.** Geralmente, são usados protocolos como o HTTP.
- **Serviços implementam capabilidades do negócio.** Isto é, a divisão de serviços é baseada nas regras de negócio e nas funcionalidades que o produto deverá suprir.
- **Serviços são facilmente substituíveis.**
- **Cada serviço tem um ciclo de vida independente.** Isso inclui o desenvolvimento e os processos de deploy. Um microsserviço pode ser implementado e atualizado independentemente dos outros.

As vantagens da arquitetura de microsserviços giram em torno da modularidade e autonomia dos serviços que é natural à sua estrutura. Com isso, pode-se ter uma heterogeneidade de tecnologias, isto é, cada serviço pode ser desenvolvido usando diferentes linguagens, frameworks e ferramentas de acordo com seus requisitos. A independência entre serviços também possibilita o deploy automatizado e o uso de práticas de integração contínua. Também há benefícios de aspecto gerencial: como cada serviço tem como escopo uma capabilidade do negócio que envolve interfaces de interação com usuário, código em várias camadas que implementa as funcionalidades necessárias e persistência em bancos de dados, é possível criar pequenas equipes multidisciplinares para cada microsserviço.

Building for failure

Existem trade-offs que devem ser considerados ao decidir pela arquitetura de microsserviços. A comunicação entre serviços por meio de uma rede possui maior latência e exige maior processamento do que mensagens trocadas a nível de processos. Por isso, é muito importante analisar as fronteiras dos serviços e a alocação de responsabilidades durante do projeto. A descentralização de dados entre microsserviços traz também a necessidade de métodos para manter a consistência das informações. Outro ponto crítico são sistemas com alta granularidade de microsserviços, causando overhead tanto de comunicação como de código além de uma fragmentação lógica que causa mais impactos negativos na complexidade e performance do que benefícios - tal caso de antipadrão foi chamado de nanosserviço (**??**).

Os microsserviços podem ser vistos como um estilo específico de arquitetura orientada a serviços (Service-oriented architecture - SOA), visto que existem várias características compartilhadas entre os dois. Contudo, o termo arquitetura orientada a serviços é muito amplo, e muitas de suas implementações podem não seguir certos pontos apresentados como aspectos dos microsserviços, como por exemplo, o uso de grande inteligência no mecanismo de comunicação de dados ao invés de delegar tal complexidade aos endpoints do serviço (**??**). Esse e outros problemas conhecidos das experiências passadas de sistemas estruturados em SOA fazem com que muitos encarem os microsserviços como uma modernização da arquitetura orientada a serviços.

Apesar do termo microsserviço ter surgido por volta de 2011 (**??**), as ideias por trás desse estilo arquitetural não são recentes. O aumento da discussão em torno dos microsserviços nos últimos anos pode ser creditada a avanços tecnológicos tais como a disseminação dos serviços de nuvem, o crescimento de ferramentas de automatização de deployment, a consolidação dos conceitos de DevOps, entre outros.

4.5.1.2 Casos de uso

4.5.1.3 Microsserviços e Internet das Coisas

4.6 Cliente Web

Para criar aplicações web que demonstrem as funcionalidades dos módulos de automação da casa, foi escolhida a biblioteca de JavaScript React, que permite o fácil desenvolvimento de aplicações single-page, renderizadas do lado do cliente, e que permitem a atualização dinâmica da página, de forma fluida, rápida, o que acaba enriquecendo a experiência do usuário na aplicação (UI e UX). Esse cliente irá se comunicar com a API, por meio do protocolo HTTP, e utilizando autenticação de usuário por meio de tokens do tipo JSON Web Token. JSON Web Tokens são tokens gerados no cadastro ou login do usuário, e são enviados ao browser, onde são armazenados na Localstorage do mesmo.

A partir desse momento, todas as requisições ao back end conterão tal token no campo de Authentication do cabeçalho dos métodos HTTP (GET, PUT, POST, DELETE). Somente requisições contendo tal token, e cujo token seja válido, são aceitas.

Outro ponto interessante para a utilização da biblioteca React é que, com a biblioteca React Native - uma extensão da biblioteca React - é possível a geração de aplicativos nativos para iOS e Android, que podem vir a ser desenvolvidos no desenrolar do projeto. Isso diminui a necessidade de retrabalho e dispensa a necessidade de estudo aprofundado das linguagens e ambientes de desenvolvimento tradicionais de projeto de aplicativos nativos.

4.7 App Backup

4.7.1 Interface

4.7.2 Setup

4.7.3 Abertura de porta do roteador

4.7.4 Configurações

4.7.5 Serviços essenciais

4.8 Comunicação

Conforme explicado anteriormente, neste projeto utilizamos tanto protocolos de comunicação próprios quanto os elaborados comercialmente. A arquitetura desenvolvida aqui busca viabilizar a robustez do sistema, trabalhando em um nível local e outro nível remoto, onde o usuário terá o controle de sua casa por meio do Smartphone ou computador pessoal.

Teremos um serviço de nuvem (que será descrito na seção de software) que receberá as requisições do usuário, por meio de um cliente web ou nativo. Esse servidor processará as requisições, aplicando os filtros de segurança necessário, de modo a consultar a autenticidade do pedido, e se aquele usuário possui as permissões necessárias para o serviço que deseja operar. Os serviços da nuvem se comunicarão com o servidor local, da casa requisitada, o qual também aplicará os filtros de segurança necessários, e realizará a comunicação com os atuadores.

A infraestrutura de comunicação entre a nuvem e o servidor local, e o servidor local e os sensores e atuadores utilizará o protocolo de aplicação MQTT, referência em aplicações IoT no mundo. O protocolo MQTT é estabelecido em cima dos protocolos TCP/IP (nas camadas inferiores) e é orientado é orientado à sessão, diferentemente do protocolo HTTP, de mesma camada.

O protocolo MQTT é do tipo Pub/Sub (de publisher/subscriber) e é estritamente orientado à tópicos. Assim, um subscriber deve se inscrever a um tópico de seu interesse, e receberá todas as publicações que um publisher realizar. Os tópicos são organizados com estrutura semelhante a de um sistema de arquivos Unix, com níveis hierárquicos, separados por barras, de modo que o subscriber pode se inscrever para tópicos utilizando wildcards (* e $+$, os quais são válidos para mais de um nível e um único nível, respectivamente).

Para interconectar os tópicos, com publishers e subscribers, é necessário um agente que realiza a transmissão das mensagens, e que garante a segurança e confiabilidade. Esse agente é conhecido como Broker (em versões anteriores) ou Server (na versão atual, V3.1.1). O broker irá permitir ou negar a subscrição a determinado tópico, ou a publicação.

A segurança da troca de mensagens é realizada por meio do protocolo TLS (Transport Layer Security) que encripta os segmentos na camada de transporte. Toda a parte de segurança e criptografia será detalhada no momento oportuno, bem como a organização dos tópicos implementados.

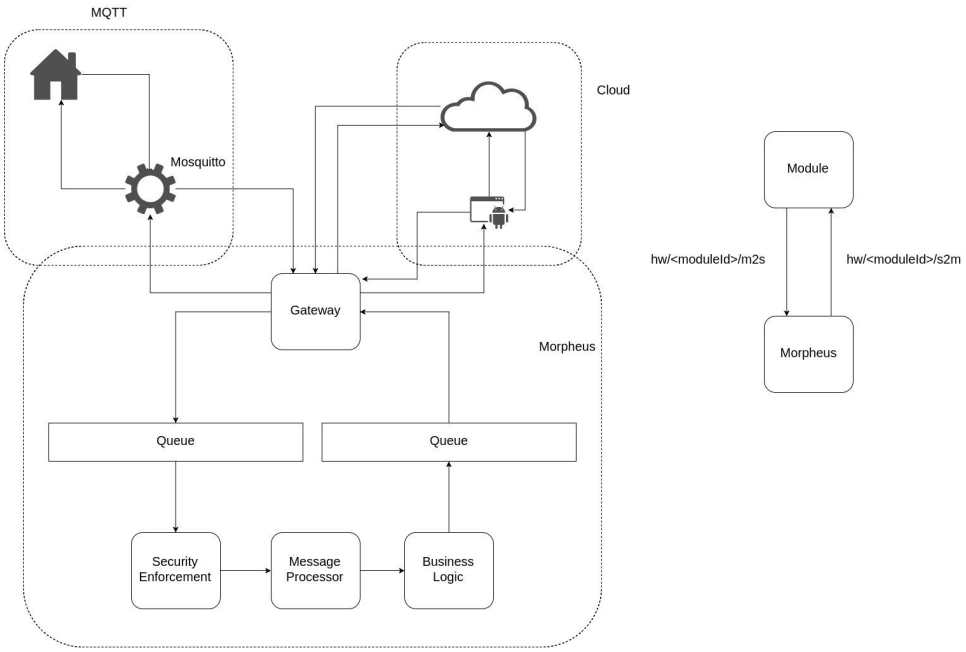
Além disso, o protocolo MQTT oferece três tipos de QoS (Quality of Service), possibilitando: diminuir o overhead ao máximo, enviando a mensagem uma única vez, na configuração mais simples; garantir que a mensagem seja entregue no mínimo uma vez, na configuração de segundo nível; garantir que a mensagem seja entregue exatamente uma vez, no terceiro nível, o que aumenta o overhead, consequentemente.

As mensagens são transmitidas em texto puro, e é necessário estabelecer um protocolo para a sua utilização. Utilizaremos aqui o protocolo que define a configurações das mensagens, desenvolvido no projeto HomeSky.

O broker Mosquitto será utilizado, e foi escolhido por ser amplamente adotado em projetos de IoT, além de ser open source e com licença abrangente (MIT). Entretanto, há diversas possibilidades, como o HiveMQ, adotado no projeto HomeSky, e com grande uso em aplicações enterprise.

A arquitetura de comunicação é representada pelo diagrama abaixo, com um alto nível de abstração, cujos detalhes serão vistos no momento oportuno, com granularidade menor.

Figura 16



4.8.1 Entre módulos e controlador local

4.8.2 Entre controlador local e nuvem

4.8.3 Entre cliente web e nuvem

4.8.4 Entre app backup e módulos

5 METODOLOGIA

5.1 Gerência do projeto

Para realizar a gerência do projeto Hedwig, foram usadas as diretrizes do Guia PMBOK (**??**) e da norma ISO/IEC 12207 (**??**) como referência para coordenar os processos.

Para gerenciar as tarefas, estudos e pesquisas necessárias para a realização do projeto, foi utilizado o Trello[1] - sistema online para organização de ideias e projetos, que permite listagem e acompanhamento de tarefas a serem realizadas, com deadlines, responsáveis e categorização em diversos tipos de tarefas.

5.1.1 Gerência de Escopo Tempo

5.1.2 Gerência de Partes Interessadas Aquisição

5.1.3 Gerência de Processos de Software

Para gerenciar o código-fonte e permitir o trabalho da equipe em múltiplas partes do projeto ao mesmo tempo, foi utilizado o Git, um sistema de controle de versão distribuído. Para publicação do código, foi escolhido o GitHub, onde está a organização do projeto Hedwig[2] e os repositórios de código dos módulos associados ao sistema. A preferência pelo GitHub se deu pelas suas funcionalidades de gerenciamento e colaboração como a notificação de bugs, acompanhamento do progresso de tarefas e criação de wikis, além de ser uma plataforma conhecida por abrigar grandes projetos open-source que chegam a ter centenas ou milhares de contribuidores (**??**).

Para o fluxo de trabalho nesses repositórios, foi utilizado o fluxo conhecido como Feature Branch Workflow (**??**), caracterizado pela criação de branches (ramificações) para o desenvolvimento de cada nova funcionalidade. Ao final do desenvolvimento de cada funcionalidade, é

[1] Pode ser acessado gratuitamente em https://trello.com/
[2] https://github.com/hedwig-project

feito um pedido para mesclar o código desenvolvido em tal ramificação com o da ramificação principal (master branch).

5.1.4 Gerência de Partes Interessadas

5.1.5 Gerência de Comunicação

5.1.6 Gerência de Escopo

5.1.7 Gerência de Riscos

5.2 Pesquisa bibliográfica

O estudo dos tópicos relacionados a aprendizagem de máquina foi realizado com auxílio do curso Aprendizagem Automática do Professor Andrew Ng[3], oferecido pela Universidade de Stanford e disponibilizado no Coursera, uma plataforma de MOOCs (Massive Open Online Courses) que oferece cursos abertos e especializações.

Os cursos da especialização em Data Science da Universidade Johns Hopkins[4], também disponíveis no Coursera, foram usados como referência e treinamento para realizar a coleta de dados de maneira metódica. Por esse motivo, foi dada maior atenção ao curso Getting and Cleaning Data. Contudo, também foi aproveitado conteúdo do curso Practical Machine Learning.

5.3 Ferramentas e tecnologias

Para aprender a utilizar a biblioteca React para o desenvolvimento do front-end, foi usada como referência a documentação oficial[5] oferecida pelo Facebook e o curso React for Beginners de Wes Bos[6]. O aprendizado de Redux foi auxiliado pelo curso Learn Redux[7], do mesmo autor.

[3] https://www.coursera.org/learn/machine-learning
[4] https://www.coursera.org/specializations/jhu-data-science
[5] https://facebook.github.io/react/docs/hello-world.html
[6] https://reactforbeginners.com/
[7] https://learnredux.com

6 IMPLEMENTAÇÃO

6.1 Morpheus

6.1.1 Descrição

Morpheus é o servidor local responsável pela interconexão da casa inteligente com os serviços de nuvem. O nome tem sua origem na mitologia grega, onde o Deus dos sonhos, Morpheus, era responsável pelo envio de mensagens entre dois mundos diferentes, os dos deuses, e os dos mortais [add source]. Sua principal atribuição é garantir que a troca de mensagem entre os módulos e a nuvem seja realizada com segurança e confiabilidade, munindo-se de soluções robustas para desempenhar o seu papel.

6.1.2 Plataforma

O Morpheus tem seu desenvolvimento realizado em Java. Tal escolha foi realizada com base na portabilidade que a máquina virtual Java (JVM) oferece, bem como na disponibilidade de bibliotecas e serviços largamente utilizados em aplicações comerciais. O servidor foi construído utilizando-se o Spring Boot Framework, com a utilização de seu container de Inversão de Controle (IoC - Inversion of Control), para injeção de dependências. Essa técnica diminui o acoplamento entre classes, e permite a evolução e implementação de novas funcionalidades de maneira mais facilitada.

Para se comunicar com os módulos, o Morpheus utiliza-se da conexão com um broker MQTT, o qual utilizamos o Mosquitto, por ser uma solução Open Source largamente utilizada em projetos de Internet of Things. Conforme detalhado a frente, configurações de segurança específicas para nosso projeto foram registradas no broker. Para a conexão com os serviços na nuvem, é utilizado um canal Websocket, aberto pelo Morpheus (cliente) e aceito pela nuvem (servidor). Esta solução veio a partir de uma discussão em relação à segurança, a qual está documentada aqui.

6.1.3 Requisitos

Para a concepção do servidor local, foram discutidos os seus requisitos funcionais e não funcionais, bem com suas prioridades na implementação.

6.1.3.1 Requisitos Funcionais

- Configuração dos módulos: De acordo com as regras e interfaces estabelecidas, documentadas aqui, os módulos podem ser configurados por meio de mensagens. Os serviços da nuvem enviarão os parâmetros de configuração de cada módulo ao Morpheus, que os transmitirão ao módulo.
- Conexão de emergência: Quando não há conexão da casa com a nuvem, deverá haver um canal para comunicação local entre o aplicativo e alguns dos módulos, com funcionalidades limitadas, apenas para serviços essenciais.
- Envio de dados para a nuvem: Dados provenientes de sensores são enviados para a nuvem, para que sejam tratados de acordo com as regras de Business Intelligence, por meio de Machine Learning.
- Persistência de dados. Quando não houver conexão, o servidor deverá armazenar os dados localmente e, quando solicitado, enviá-los à nuvem.
- Tentativas de reenvio: Quando uma mensagem não é enviada com sucesso à nuvem, o Morpheus deverá tentar novamente, um número configurável de vezes, em um curto espaço de tempo. Isso ocorre pois, se determinada mensagem não pode ser enviada em uma janela temporal, ela perde o seu sentido, mesmo por questões de segurança.
- Envio de e-mail: Se o Morpheus estiver desconectado da nuvem por um período, configurável, deverá avisar o usuário, por meio de uma mensagem de e-mail.
- Verificação do time-stamp: Quando uma nova mensagem chegar, seu timestamp deverá ser verificado, e a mensagem tomará curso somente se não for obsoleta.
- Tomadas de ação: Quando o usuário requisitar uma tomada de ação, esta deverá ser enviada por meio de uma mensagem ao Morpheus, o qual a transmitirá ao módulo.
- Configuração em arquivo: As configurações básicas do Morpheus devem ser registradas em um arquivo YAML, que será lido durante a inicialização.
- Listeners para diferentes tipos de mensagens: Deverão haver listeners para todos os tipos de mensagens, definidos aqui, que serão recebidos da nuvem e dos módulos.

6.1.3.2 Requisitos Não Funcionais

- Processamento concorrente: Toda a infraestrutura do Morpheus deverá permitir o processamento de mensagens de maneira concorrente. Não deve ser permitido esperar o processamento completo de uma mensagem para que outra comece a ser processada.
- Utilização de criptografia na troca de mensagens com a nuvem: Os dados que trafegam entre a nuvem e o servidor local não devem ser codificados em texto puro. Devem estar protegidos contra sniffers.
- Conversão de mensagens : As mensagens enviadas à nuvem devem estar em formato JSON, e não no protocolo definido aqui, para troca de mensagens entre os módulos e o Morpheus.
- Serialização das configurações: O servidor deverá serializar e persistir as configurações relativas aos módulos que foram configurados, e carregá-las em sua inicialização.
- Destruição de pools de threads: Ao ser desligado, todos os pools de threads criados devem ser destruídos.

6.1.4 Especificações

6.1.4.1 Tópicos

Todos os tópicos devem seguir o formato especificado abaixo. Com essa formatação, é possível garantir que:

1. Somente o Morpheus conseguirá publicar em qualquer tópico, ou ser um subscriber de qualquer tópico.
2. Cada módulo somente consiga publicar no tópico determinado para ele, que será garantido com as credenciais (usuário e senha) fornecidos pelo tópico.
3. Caso um módulo malicioso seja implantado, com o roubo das credenciais de um módulo legítimo, o impacto será unicamente concentrado naquele tópico, não atingindo outros módulos.

Temos as seguintes regras:

hw/<ID do módulo>/s2m (Server to Module - o módulo deve ser subscriber desse tópico. O servidor deve ser publisher desse tópico).

hw/<ID do módulo>/m2s (Module to Server - o servidor deve ser subscriber desse tópico. O módulo deve ser publisher desse tópico).

6.1.4.2 Regras de negócio

O servidor foi desenvolvido com base nas regras de negócio seguintes.

- Após a compra de cada módulo, o usuário deverá registrar online a aquisição. O servidor da nuvem enviará para o servidor local, da casa, a requisição para configurar o módulo.
- Cada módulo enviará mensagens para o servidor local com o seus dados, por meio do MQTT.
- Troca de senha do wifi: O usuário cadastra no site a nova senha. O servidor na nuvem faz a requisição para o servidor local, o qual enviará um arquivo de configuração com a nova senha para cada um dos módulos registrados. Após a configuração de todos os módulos, o servidor local envia resposta de sucesso para a nuvem, a qual indica ao usuário que a troca de senha já pode ser feita com sucesso.
- Todo módulo sai de fábrica configurado com o tópico que deve se inscrever e publicar, com base no seu ID, o qual será o seu usuário, e também haverá a senha para se autenticar junto ao broker MQTT.

6.1.4.3 Definição de interfaces

- Há três tipos de mensagens que vão do Morpheus para os módulos:
  - Configuração (configuration)
  - Requisição de Ação (action_request)
  - Requisição de dados (data_transmission)
- Há três tipos de mensagens que chegam dos módulos:
  - Confirmação (confirmation)
  - Envio de Dados (data_transmission)
  - Data Request (data_request)

6.1.4.4 Definição das mensagens

Configuração (configuration)

- Sentido: Morpheus para módulo
- Uso: Envio de parâmetros para configuração dos módulos.

Configuração de hora:

#configuration

$ts:<timestamp>

$ty:time_config

@

updated_ntp: <segundos desde 0h de 1 de Janeiro de 1970, 64 bits >

@

Configuração de nome:

#configuration

$ts:<timestamp>

$ty:name_config

@

new_name: <string do nome>

new_rele1name: <string do nome—"">

new_rele2name: <string do nome—"">

@

Configuração de comunicação:

#configuration

$ts:<timestamp>

$ty:comunication_config

@

new_ssid: <novo ssid>

new_password: <nova senha>

ip_local: <novo ip local fixo>

ap_mod: <"sempre ativo" ou "automatico">

ap_name: <nome do ap para acesso direto>

ap_password: <senha do ap para acesso direto>

@

Configuração de RF:

#configuration

$ts:<timestamp>

$ty:rf_config

@

*

<nome do sensor/controle/função>: <store—clear—keep>

*

@

Configuração de display:

#configuration

$ts:<timestamp>

$ty:display_config

@

displaytype: <1—2—3>

backlight: <0 para desligar, 1 para ligar>

@

Requisição de ação (action_request)

- Sentido: Servidor para módulo
- Uso: Quando um usuário faz a requisição de uma ação por meio do aplicativo. Por exem-

plo, quando deseja-se acender uma luz, o aplicativo envia uma requisição para o servidor local, o qual enviará uma mensagem de action_request para o módulo correspondente.

Requisição de acionamento:

#action_request

$ts:<timestamp>

$ty:rele1_action

@

rele1: <0 para desligar, 1 para ligar>

@

#action_request

$ts:<timestamp>

$ty:rele2_action

@

rele2: <0 para desligar, 1 para ligar>

@

Requisição de SW Restart:

#action_request

$ts:<timestamp>

$ty:sw_reset

@

swreset: <0 para não—1 para sim>

@

Requisição de Teste de Auto Reset:

#action_request

$ts:<timestamp>

$ty: autoreset_test

@

autoreset: <0 para não—1 para sim>

@

Confirmação (confirmation)

- Sentido: Do módulo para o servidor
- Uso: Confirmação de uma configuração, patch ou requisição de ação, vindas do servidor.

Confirmação de hora

#confirmation

$ts:<timestamp>

$ty:time_confirm

@

ntp: <segundos desde 0h de 1 de Janeiro de 1970, 64 bits >

@

Confirmação de nome

#confirmation

$ts:<timestamp>

$ty:name_confirm

@

name: <string do nome>

rele1name: <string do nome—"">

rele2name: <string do nome—"">

@

Confirmação de comunicação

#confirmation

$ts:<timestamp>

$ty:communication_confirm

@

ssid: <novo ssid>

password: <nova senha>

ip_local: <novo ip local fixo>

ap_mod: <"sempre ativo" ou "automatico">

ap_name: <nome do ap para acesso direto>

ap_password: <senha do ap para acesso direto>

@

Confirmação de RF:

#confirmation

$ts:<timestamp>

$ty:rf_confirm

@

*

<nome do sensor/controle/função>: <valor gravado>

*

@

Configuração de Display:

#confirmation

$ts:<timestamp>

$ty:display_confirm

@

displaytype: <1—2—3>

backlight: <0—1>

@

Confirmação de SW Restart:

#confirmation

$ts:<timestamp>

$ty:sw_reset_confirm

@

swreset

@

Confirmação de Teste de Auto Reset:

#confirmation

$ts:<timestamp>

$ty: autoreset_test_confirm

@

autoreset

@

Transmissão de dados (data_transmission)

- Sentido: Do módulo para o servidor
- Uso: Envio de dados de sensores para o servidor

Transmissão de Umidade, Temperatura, Presença e Reles

#data_transmission

$ts:<timestamp>

$ty:temp_umi_pres

@

s1:umidade

vl1:<value>

s2:temperatura

vl2:<value>

s3:presenca

vl3:<value>

s4:rl1

vl4:<value>

s5:rl2

vl5:<value>

@

Requisição de dados (data_request)

- Sentido: Do módulo para o servidor
- Protocolo: MQTT
- Uso: Requisição de alguma informação do servidor. Ex.: Atualização de hora

Requisição de atualização da hora

#data_request

$ts:<timestamp>

$ty:time_update

6.1.4.5 Testes realizados da comunicação Morpheus e módulos:

Para que fosse simulado o envio de mensagens, o aplicativo MQTT Fx foi utilizado. Com o uso deste software, é possível se inscrever em determinado tópico (enviando as credenciais para o broker, tanto em forma de usuário e senha, quando em forma de certificados), bem como publicar no tópico desejado.

Requisição de acionamento 1:

#action_request

$ts:<timestamp>

$ty:rele1_action

@

rele1: 0

@

Esperado: 0 no serial do Arduino, indicando recebimento

Resultado: De acordo

Requisição de acionamento 2:

#action_request

$ts:<timestamp>

$ty:rele2_action

@

rele2: 1

@

Esperado: 1 no serial do Arduino, indicando recebimento

Resultado: De acordo

Requisição e confirmação de SW Restart:

#action_request

$ts:<timestamp>

$ty:sw_reset

@

swreset: 1

@

Esperado: Confirmação de SW Restart no tópico MQTT m2s

Resultado: De acordo

Requisição e confirmação de Teste de Auto Reset:

#action_request

$ts:<timestamp>

$ty: autoreset_test

@

autoreset: 1

@

Esperado: Confirmação no tópico MQTT m2s

Resultado: De acordo

Configuração e confirmação de hora:

#configuration

$ts:293029

$ty:time_config

@

updated_ntp: 293029

@

Esperado: Confirmação no tópico MQTT m2s

Resultado: De acordo

Configuração e confirmação de nome:

#configuration

$ts:432524

$ty:name_config

@

new_name: NovoNome

new_rele1name: Portal1

new_rele2name: Portal2

@

Esperado: Confirmação no tópico MQTT m2s

Resultado: De acordo

Configuração e confirmação de comunicação:

#configuration

$ts:5349545

$ty:comunication_config

@

new_ssid: Novossid

new_password: novaSenha

ip_local: 192.168.0.32

ap_mod: automatico

ap_name: AcessoDiretoAP

ap_password: 1234

@

Esperado: Confirmação no tópico MQTT m2s

Resultado: De acordo

Configuração e confirmação de RF:

#configuration

$ts:4839434

$ty:rf_config

@

Janela4: 01234

@

Esperado: Confirmação no tópico MQTT m2s

Resultado: De acordo

Configuração e confirmação de display:

#configuration

$ts:543242

$ty:display_config

@

displaytype: 3

backlight: 1

@

Esperado: Confirmação no tópico MQTT m2s

Resultado: De acordo

Transmissão de Umidade Temperatura e Presença e Reles

messageToSend = UmiTempPresReles(0,80,25,1,1,0);

//UmiTempPresReles(unsigned long ts, int umidade, float temp, bool pres, bool rele1, bool rele2)

Esperado: Mensagem no Tópico MQTT m2s Resultado: De acordo

6.1.5 Comunicação entre Morpheus e Nuvem

Inicialmente, foi proposto um modelo arquitetural onde, para a comunicação com a nuvem, haveriam endpoints tanto do lado da casa quanto do lado da nuvem. Assim, quando o Morpheus precisasse enviar uma mensagem, seria necessário que fosse realizada uma chamada ao endpoint correspondente. Neste sentido (Morpheus para nuvem), não há nenhum problema, pois é possível garantir configurações avançadas de segurança, bem como a utilização de load balancers e servidores terceiros (como Akamai), para lidar com ataques do tipo DoS (Denial of Service).

O problema, no entanto, está em garantir a segurança e usabilidade do lado da casa. Primeiramente, os IPs residenciais não são fixos, e são trocados a cada nova conexão. Assim, se a conexão com a internet for perdida, por exemplo, um novo IP será atribuído àquela residência. Dessa forma, após essa troca, a não ser que o Morpheus atualize a nuvem, não será possível receber as mensagens que chegariam dos serviços remotos. Esta questão, no entanto, é contornável, por meio de um serviço de watchdog, que seria responsável por analisar o IP e notificar a nuvem sobre a troca, sempre que esta ocorrer. Há, ainda, um problema mais grave e mais difícil de ser contornado. Com essa arquitetura, o Morpheus também será um servidor, do ponto de vista da nuvem, e qualquer dispositivo pode tentar fazer uma requisição em um dos endpoints disponíveis. Mesmo que forem checados os dados da requisição, para garantir que esta é válida, temos ainda uma grave ameaça de segurança, em relação à negação de serviço. Para que este risco fosse minimizado, seria necessária configurações avançadas no roteador local, e mesmo assim, este não seria suficiente para processar um grande número de

requisições, deixando a casa vulnerável.

Foi discutida, então, uma mudança arquitetural na forma de comunicação entre a nuvem e a casa. A solução para o problema se encontra no uso de websockets. Assim, o Morpheus se comporta como um cliente em relação à nuvem, e é sempre ele que abre uma conexão. Assim, já não há mais a vulnerabilidade local, de estar exposto às negativas de serviço. Além disso, a conexão se mantém aberta, e forma um caminho full duplex, de modo que é possível receber as mensagens da nuvem a qualquer momento também. Com essa arquitetura, os desafios relativos à segurança recaem aos servidores, e não mais à casa, de modo que é possível gerenciar esses riscos, como o fazem grandes empresas, de forma transparente ao cliente final.

Por fim, somente restou um endpoint no Morpheus, que seria o de emergência. Este endpoint somente aceita requisições vindas do localhost, e não mais de fora.

6.1.6 Websocket

Com a utilização do canal de comunicação por websocket, foram utilizados eventos, que são recebidos e enviados, para a comunicação. São eles descritos abaixo.

6.1.6.1 Morpheus

O Morpheus ouvirá os seguintes eventos, vindos da nuvem.

- configurationMessage
- actionRequest
- dataTransmission (Requisitar informações sobre módulo, e.g. se portão está aberto ou não).

6.1.6.2 Nuvem

A nuvem ouvirá os seguintes eventos, vindos do Morpheus.

- confirmation
- configuration
- data

Definição de Mensagens Entre Nuvem e Morpheus configuration configurationId: <configurationId>, timestamp: <timestamp>, morpheusConfiguration: <morpheusConfiguration>, modulesConfiguration: <modulesConfiguration>

<morpheusConfiguration>= register: [<eachModuleRegistration>], requestSendingPersistedMessages: <true — false>

<eachModuleRegistration>= moduleId: <moduleId>, moduleName: <moduleName>, moduleTopic: <moduleTopic>, receiveMessagesAtMostEvery: <time>, qos: <qosLevel>

Requisitos:

O campo receiveMessagesAtMostEvery deve estar no formato"<time>:<unit>" A unidade deve ser "s" para segundos, "m" para minutos ou "h" para horas. O valor padrão é 60 segundos.

Ex: Requisição de mensagens persistidas e configuração do Morpheus

Module configuration

A seção de configuração de módulo será um objeto com duas partes. A primeira identifica o módulo dentro do Morpheus e, a segunda, envia as mensagens que serão interpretadas pelo módulo.

"moduleId": <moduleId>, "moduleName": <moduleName>, "moduleTopic": <moduleTopic>, "unregister": <true—false>messages: [<message>]

<message>"controlParameters": parameter: <name>, value: <value> "payload": <key>: <value>.... Ex.: Unregister a module and configure another

Action Request Messages As mensagens de action_request seguem o mesmo protocolo de mensagens, estabelecido anteriormente.

Data Transmission Messages As mensagens de data_transmission também seguem o mesmo protocolo de mensagens, estabelecido anteriormente.

6.1.7 Configurações

6.1.7.1 MQTT Mosquitto broker - Configuração

1. Para efeitos de desenvolvimento e testes, criamos uma instância na nuvem do MQTT Broker Mosquitto. Para um cenário real, essa instância rodará localmente, e somente aceitará conexões vinda da localhost.

2. Configurar restrição de tópicos na instância. Exemplo em: http://www.steves-internet-guide.com/topic-restriction-mosquitto-configuration/

3. Os tópicos que finalizam com s2m devem ser exclusivamente restritos para o Morpheus. Ninguém mais consegue publicar nestes tópicos. Morpheus pode publicar e ouvir todos os tópicos.

6.1.7.2 Estratégia

1. Usar a porta padrão 1883 para os módulos se conectarem. Essa porta não exige criptografia, deve exigir somente usuário e senha (que estarão vulneráveis).

2. O Morpheus será obrigado a se conectar por SSL na porta 8883, passando suas credenciais. Assim, suas credenciais serão protegidas.

3. Configurar a proteção de tópicos.

6.1.7.3 Guia de instalação (Testado no Ubuntu 16,10 x64)

Instalação

1. sudo apt-get update

2. sudo apt-get install mosquitto mosquitto-clients

3. sudo systemctl enable mosquitto

4. Create a .conf file in /etc/mosquitto/conf.d

Listener

listener 8883

6.1.7.4 Criação dos certificados

1. Criação da autoridade certificadora (key e certificado). Para a versão atual, a senha é hedwig123

   openssl req -new -x509 -extensions v3_ca -keyout ca.key -out ca.crt

2. Mosquitto Key e Certificado. Foi adicionado o IP do servidor. O Common Name deve ser o IP do servidor

openssl genrsa -out mosquitto.key 2048 openssl req -new -key mosquitto.key -out mosquitto.csr openssl x509 -req -in mosquitto.csr -CA ../ca.crt -CAkey ../ca.key -CAcreateserial -out mosquitto.crt -days 3650 -sha256

3. Morpheus Key e Certificado. Common Name será localhost

   openssl genrsa -out morpheus.key 2048 openssl req -new -key morpheus.key -out morpheus.csr openssl x509 -req -in morpheus.csr -CA ../ca.crt -CAkey ../ca.key -CAcreateserial -out morpheus.crt -days 3650 -sha256 -addtrust clientAuth openssl x509 -in morpheus.crt -outform der -out morpheus.der

6.1.7.5 Comandos úteis

Inicia na manualmente o mosquitto com as configurações do arquivo. Útil para checar se há algum erro no .conf. mosquitto -c /etc/mosquitto/conf.d/mosquitto.conf -d

6.1.7.6 Senhas

1. Criar o arquivo de senha no formato usuario:senha e usar sudo mosquitto_passwd -U passwd para gerar o hash da senha

2. No mosquiito.conf, insira: allow_anonymous false password_file c:\mosquitto\passwords.txt # Windows machine Tutorial:http://www.steves-internet-guide.com/mqtt-username-password-example/

6.1.7.7 Casos de teste para Controle de Acesso nos Tópicos MQTT entre módulos e nuvem

1. Conectar na porta 1883 sem usuário e senha.

   Esperado: Falha de conexão

   Resultado: Bem sucedido.

2. Conectar na porta 1883 com usuário e senha corretos.

   Esperado: Permissão de conexão

   Resultado: Bem sucedido.

3. Conectar com credenciais corretas e tentar publicar em tópico que não pertence ao seu usuário

   Esperado: Não publicação

Resultado: Bem sucedido.

4. Conectar com credenciais corretas e tentar publicar em tópico que pertence ao seu usuário

   Esperado: Publicação

   Resultado: Bem sucedido.

5. Conectar com credenciais corretas e tentar ouvir de um tópico que não pertence ao seu usuário

   Esperado: Não receber dados

   Resultado: Bem sucedido.

6. Conectar com credenciais corretas e tentar ouvir de um tópico que pertence ao seu usuário

   Esperado: Receber dados

   Resultado: Bem sucedido.

7. Conectar com credenciais referentes ao Morpheus e tentar publicar ou ouvir qualquer tópico começando com hw.

   Esperado: Publicação ou subscrição com sucesso

   Resultado: Bem sucedido.

6.1.7.8 Restrição de Tópicos s2m (Server to Module)

1. Morpheus consegue em todos que comecem com hw pubsub
2. Módulos conseguem pub em hw/username/m2s
3. Módulos conseguem sub em hw/username/s2m

Tutorial:http://www.steves-internet-guide.com/topic-restriction-mosquitto-configuration/

Sobre Segurança no Mosquitto: http://www.steves-internet-guide.com/mqtt-security-mechanisms/

Biblioteca do Arduino para o Client: https://pubsubclient.knolleary.net/index.html

7 APRENDIZADO DE MÁQINA

Para o desenvolvimento de funcionalidades de aprendizado de máquina, será utilizada a linguagem Python, que possui diversos pacotes que facilitam sua utilização para implementar algoritmos de aprendizado, e funcionalidades para tratamento de dados. Além disso, é usada em vários outros âmbitos como cursos acadêmicos voltados ao ensino de programação e aplicações web, o que facilita a familiarização com o desenvolvimento nela.

7.1 Coleta de Dados

Um dos processos mais críticos para o sucesso do diferencial do projeto (aplicações de Machine Learning) e para monitoramento da disponibilidade é a coleta de dados. Para cada módulo, os seguintes parâmetros serão monitorados:

7.1.1 Conexões

Para melhor diagnóstico do estado de disponibilidade de conexão dos módulos, o seguinte vetor de parâmetros é monitorado ao longo do tempo, para cada módulo instalado:

bit 0: 1 se houve reinicialização do módulo, 0 se não; bit 1: 1 se houve reconexão de wifi, 0 se não; bit 2: 1 em caso de reconexão ao broker MQTT, 0 se não; bit 3: 1 em caso de reconexão a servidor para persistência de dados, 0 se não;

Desta forma, podemos acompanhar a relação entre problemas de conexão para posterior análise e tratamento.

7.1.2 Uso

Para monitorar o uso das funcionalidades dos produtos, há o seu monitoramento. Dessa forma, funcionalidades mais usadas podem ser melhoradas e funcionalidades não utilizadas podem ser excluídas, gerando um melhor retorno aos usuários.

Por exemplo, para um uso de automação da iluminação, temos: bit 0: acionamento manual por botão físico no módulo; bit 1: acionamento manual por aplicativo de celular; bit 2: acionamento manual por página web; bit 3: acionamento automático.

8 CONCLUSÕES

ANEXO A – CÓDIGOS DAS APLICAÇÕES DESENVOLVIDAS

Todos os códigos das aplicações desenvolvidas neste projeto estão disponíveis em: ⟨https://github.com/hedwig-project/⟩.