Aplicativo Móvel Para Auxiliar no Monitoramento de Rondas da Equipe de Vigilância do IFSC/Lages

Matheus de Figueiredo Lopes[1], **Vinicius Carvalho Santos**[1], **Robson Costa**[1]

[1]Instituto Federal de Santa Catarina (IFSC)
R. Heitor Villa Lobos, 225 - São Francisco, Lages - SC, 88506-400

{matheus.fl14, vinicius.cs02}@aluno.ifsc.edu.br

robson.costa@ifsc.edu.br

Abstract. *The Internet of Things (IoT) has been a major growth field in computing, bringing technology to all areas of society, increasing efficiency, productivity and security in everyday processes. This paper presents a proposal for its application in the context of property security, namely to the problems faced by the IFSC Lages Campus with regard to monitoring guard patrols. The solution integrates the use of smartphones, mobile applications, geopositioning systems and data management and visualization software. The results, obtained from its use in the field by the surveillance team, showed a significant improvement in the process of patrols and their monitoring by managers.*

Resumo. *A Internet das Coisas (IoT) tem sido um campo de grande crescimento na computação, trazendo tecnologia para todas as áreas da sociedade, aumentando a eficiência, a produtividade e a segurança em processos habituais. Este trabalho apresenta uma proposta de sua aplicação no contexto de segurança patrimonial, nomeadamente para os problemas enfrentados pelo Câmpus Lages do IFSC, no que diz respeito ao monitoramento de rondas de vigilantes. A solução integra o uso de smartphones, aplicativos móveis, sistemas de geoposicionamento, e software de gestão e visualização de dados. Os resultados, obtidos a partir do seu uso em campo pela equipe de vigilância, demonstraram uma significativa melhoria no processo de rondas e do monitoramento das mesmas pelos gestores.*

1. Introdução

Nos dias de hoje, percebe-se um crescente uso de tecnologia no cotidiano da sociedade, com número de dispositivos conectados à Internet das Coisas (IoT – *Internet of Things*) próximo à 12 bilhões e com expectativa de aumento para 27 bilhões até o ano de 2025, sem incluir computadores, telefones fixos, celulares e *tablets* (Mano and Marcolino, 2022). Neste contexto de computação ubíqua[1], soluções baseadas em IoT emergem como candidatas para expressar este tipo de tecnologia (Zainab et al., 2015). Sua utilização em diversas áreas está trazendo grandes evoluções e renovando a forma de realizar tarefas de forma geral.

Dentre as aplicações de IoT, pode-se citar a segurança, com proteção de câmeras e sensores conectados à Internet e o uso no dia a dia, com a assistente virtual Alexa, por

[1]Termo usado para definir a integração da tecnologia no cotidiano humano, sendo usada de maneira natural pelas pessoas (PontoTel, 2022).

exemplo, que pode marcar agendas, despertadores, criar listas de supermercado, entre outros. A IoT também está presente em aplicativos de locomoção urbana, conectando usuário e motorista e trocando dados entre estes; em fábricas, com máquinas conectadas à Internet, na saúde, com a telemedicina[2], entre diversas outras aplicações.

No âmbito de segurança patrimonial, soluções com IoT podem fazer uso de sensores de presença acoplados em portas e janelas, para detectar possíveis invasões, como demonstrado por (Gimawa, 2019). Outro exemplo são câmeras inteligentes, as quais visam a redução da incidência de crimes, permitindo que sejam mais rapidamente resolvidos (Lima, 2021).

O Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC) - Câmpus Lages é uma instituição pública de ensino, que necessita de fiscalização para manter a plena preservação, tanto de seus bens, como de sua estrutura. Neste contexto, existe um contrato de terceirização da vigilância no qual a empresa contemplada é responsável pela segurança do câmpus.

Devido às recentes experiências deste contrato, utilizando sensores RFID[3] para marcar o ponto das rondas da equipe de vigilância, notou-se a necessidade de melhorar o método utilizado, pois este não estava sendo eficiente e assertivo. O sistema tinha custos com manutenção dos *hardwares* necessários e problemas frequentes, pois não se mostrava resistente de acordo com seu tempo de uso. Utilizava-se uma caneta com a etiqueta, que era lida por pequenos sensores para marcar a ronda, os quais apresentaram problema técnico e, ao tentar utilizar a marcação do ponto, a equipe de vigilância notou que a detecção não estava funcionando.

Após o sensor parar de funcionar, como meio temporário de sanar o problema, *selfies*[4] passaram a ser feitas durante as rondas e enviadas através de um aplicativo próprio da empresa de segurança. Porém, trata-se de uma forma provisória de solução, visto que a mesma é realizada durante as rondas do trabalho da vigilância. *Selfies* não garantem a localização exata ou o horário em que foram feitas, por exemplo. Além disso, os vigilantes precisavam parar seu trabalho para realizar as *selfies*, perdendo a atenção ao ambiente, podendo comprometer a segurança do patrimônio e pessoal do vigilante.

Neste contexto, o objetivo geral deste trabalho é propor a criação de um aplicativo para *smartphones*, que auxilie e simplifique o processo de realização de rondas pelos vigilantes que atuam na instituição, permitindo assim, que estes se concentrem na observação e monitoramento das instalações e não no processo de registro da ronda em si.

Os objetivos específicos deste Trabalho de Conclusão de Curso (TCC) foram:

- Entender o procedimento e rotina de rondas dos vigilantes e levantar requisitos;
- Buscar artigos e trabalhos relacionados ao tema, para composição do referencial teórico;
- Identificar *frameworks* e bibliotecas para criação do aplicativo móvel;
- Desenvolver e testar a aplicação com os objetivos e necessidades exigidos.

[2] A telemedicina está relacionada ao uso de tecnologias para consultas médicas à distância.

[3] É um método de identificação automática através de sinais de rádio, recuperando e armazenando dados remotamente através de dispositivos denominados etiquetas RFID.

[4] A palavra "*selfie*" está relacionada ao ato de tirar fotos de si mesmo, ou seja, corresponde ao termo auto retrato.

A metodologia utilizada neste trabalho, lançou mão de um estudo transversal, exploratório e descritivo, com uma abordagem qualitativa, dividida em 4 (quatro) etapas (Fortin et al., 2009). Na primeira etapa foi realizada uma pesquisa do procedimento de rondas dos vigilantes, para que se obtivesse o entendimento do trabalho realizado para fiscalização do IFSC e dos requisitos necessários para o desenvolvimento de um sistema de monitoramento (baseado em IoT). A segunda etapa consistiu na elaboração do material teórico, onde foram pesquisados artigos e trabalhos relacionados ao tema, para compor o TCC com os objetivos e necessidades que o projeto em questão visa atingir. A terceira etapa consistiu no desenvolvimento da solução, passando pela instalação e configuração de uma plataforma de gestão IoT para a centralização dos dados, bem como o desenvolvimento de um aplicativo móvel para a coleta de dados e interação com o sistema. Por fim, a quarta e última etapa, consistiu na realização de testes e eventuais ajustes, que se fizeram necessários no levantamento de resultados qualitativos, bem como na análise, comparação e compreensão dos resultados obtidos.

Este documento está organizado com a seguinte estrutura: na seção 2 é apresentado o referencial teórico, na seção 3 é descrita a solução proposta; na seção 4 são descritos os testes e resultados obtidos; ao final, na seção 5 são apresentadas as conclusões e propostas de trabalhos futuros.

2. Referencial Teórico

Esta seção é dedicada à apresentação e entendimento de tecnologias utilizadas para o desenvolvimento de soluções IoT e seu uso em segurança patrimonial.

2.1. *Internet of Things* (IoT)

Com o avanço da tecnologia, a sociedade está sendo direcionada a uma realidade onde tudo e todos estarão conectados. O paradigma da IoT caracteriza-se por permitir a conexão e troca autônoma e segura de dados entre dispositivos e aplicativos do mundo real, dessa forma, conectando tarefas físicas do mundo real com o mundo virtual.

A quantidade de dispositivos conectados à Internet está aumentando rapidamente, dentre eles os *smartphones*, *tablets*, computadores pessoais, entre outros dispositivos utilizados diariamente. A IoT concede a conexão entre bilhões de coisas no mundo todo, diversos dispositivos com finalidades, tamanhos e capacidades computacionais diferentes, podem ser utilizados para detectar grandezas físicas, pessoas e objetos, realizar cálculos, tomar decisões inteligentes e transmitir informações pela Internet. Essa gama de dispositivos e aplicativos que atuam e geram diferentes dados, podem dar origem a serviços e aplicativos que podem trazer benefícios pessoais, profissionais e econômicos de forma significativa.

Neste contexto, a pilha TCP/IP[5] define o conjunto de protocolos padrão utilizados na Internet para a comunicação entre os *hosts*[6] da rede. Porém, a IoT conecta bilhões de coisas, criando um tráfego significativamente maior para os parâmetros da Internet comum, além de se encontrar muitos desafios relacionados à privacidade e segurança dos dados e dispositivos conectados. Portanto, tendo em vista a grande quantidade de

[5]Conjunto de protocolos de comunicação entre computadores em rede.

[6]Qualquer dispositivo conectado a uma rede, podendo oferecer informações, recursos, serviços e aplicações aos usuários ou outros nós na rede.

dispositivos conectados, viu-se a necessidade de abordar fatores como escalabilidade, interoperabilidade, confiabilidade e diversos outros. Considerando essas características, o desenvolvimento da IoT depende da evolução da tecnologia e do design de novos aplicativos e modelos de negócios (Khan et al., 2012).

2.2. Indústria 4.0

O termo Indústria 4.0 refere-se à Quarta Revolução Industrial (Figura 1), onde as companhias melhoram a produção e distribuição integrando novas tecnologias. Dentre as tecnologias inovadoras deste novo modelo de indústria, pode-se destacar a IoT, computação e análise em nuvem[7], inteligência artificial com aprendizado de máquina[8] e desenvolvimento de aplicativos.

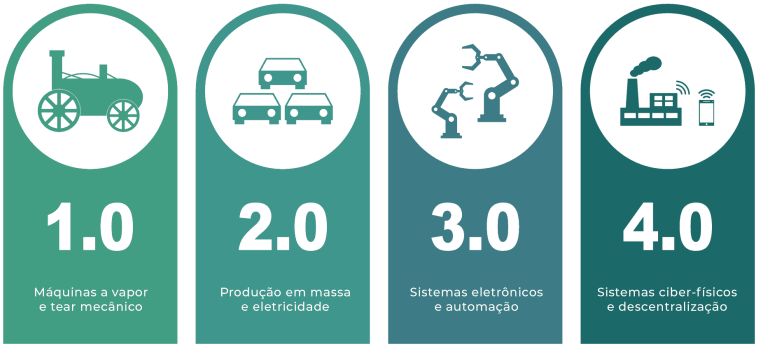

Figura 1. As quatro revoluções industriais (Azevedo, 2019).

Estas tecnologias digitais levam a uma maior automação, permitindo manutenção preventiva, auto-otimização de processos e melhorias, e, principalmente, um novo nível de eficiência previamente inacessível.

A Primeira Revolução Industrial data do final do século XVIII, iniciou na Grã-Bretanha e marcou a transição da produção manufatureira para a maquinofatureira. Neste momento, a humanidade começou a substituir a força puramente humana ou animal, pelo uso de maquinário à vapor e carvão mineral para, por exemplo, geração de energia (Sousa, 2023).

A Segunda Revolução Industrial teve início no final do século XIX, momento em que houve a adoção de novas fontes de energia com custo reduzido, permitindo maior incorporação das máquinas nas fábricas e dando início à automatização do processo de produção. Teve como principais fontes de energia o petróleo e a energia elétrica, que permitiu a iluminação urbana e invenções como o telégrafo[9] (Silva, 2023).

A Terceira Revolução Industrial teve início em meados do século XX, em consequência do avanço tecnológico ocorrido neste período. Pode-se destacar a criação de

[7]Conjunto de servidores, os quais disponibilizam recursos de computação sob demanda na internet. Elimina a necessidade de gerenciamento, aquisição e configuração de infraestrutura para utilizadores, que pagarão somente pelo que utilizarem (Cloud, 2023).

[8]Ramo da inteligência artificial, no qual máquinas podem aprender com dados, tomar decisões e identificar padrões (SAS, 2023).

[9]Dispositivo inventado por Samuel Morse, para envio de mensagens codificadas através de pulsos de corrente elétrica.

computadores e *softwares* com foco na criação de processos industriais controlados por sistemas computadorizados.

A Quarta Revolução Industrial, a qual ocorre nos dias atuais, caracteriza-se pelo uso de inteligência artificial, computação em nuvem e IoT, por exemplo, como meios de buscar desenvolvimento e produtividade para os meios de produção. Nota-se que ao longo da história, o ser humano busca constantemente por desenvolvimento. É possível observar na Figura 1 a principal mudança de cada revolução industrial, como o uso de vapor, carvão mineral e energia elétrica, sendo alguns dos destaques das revoluções industriais anteriores, enquanto a atual revolução industrial, busca o desenvolvimento através de dispositivos conectados à internet, por exemplo.

O uso de IoT em fábricas inteligentes, pode levar à maior produtividade e qualidade. Com investimento na indústria 4.0, o indivíduo encarregado pelo controle de qualidade, pode utilizar um celular conectado à nuvem, por exemplo, para monitorar todo o processo de produção, através de percepções feitas por dispositivos conectados à Internet e que fazem uso de inteligência artificial (IBM, 2020).

2.3. Fluxos de dados IoT

O fluxo de dados no contexto da IoT refere-se ao envio contínuo e bidirecional de informações entre dispositivos conectados à Internet e ocorre quando sensores e dispositivos inteligentes realizam a coleta, processamento, transmissão e recebimento de dados.

Esse fluxo geralmente inicia-se pelos dispositivos IoT que realizam a coleta dos dados, em seguida esses dispositivos processam os dados coletados ou os enviam para a nuvem ou servidores intermediários, onde esses dados são armazenados e processados de maneira mais robusta. Assim que processados, os dados podem ser enviados para outros dispositivos conectados à rede IoT ou para sistemas externos, como aplicativos móveis, *dashboards* de um sistema de gerenciamento e usuários finais. Com esses dados sendo fornecidos em tempo real é possível gerar alertas, acionar funções automatizadas ou fornecer *insights* para tomadas de decisões de um negócio.

2.3.1. Computação em nuvem

A computação em nuvem (*Cloud Computing*) é uma tecnologia que foi introduzida como a próxima geração de serviços sob demanda pela Internet. Esse novo paradigma de arquitetura usa os conceitos de virtualização, conectividade, poder de processamento e compartilhamento para armazenar recursos e compartilhá-los pela Internet.

A definição mais aceitável de computação em nuvem foi introduzida pelo *National Institute of Standards and Technology* (NIST), descrito da seguinte forma: "A computação em nuvem é um modelo para permitir acesso onipresente, conveniente e sob demanda à rede para um conjunto compartilhado de recursos de computação configuráveis, como redes, servidores, armazenamento, aplicativos, e serviços, que podem ser rapidamente provisionados e liberados com o mínimo esforço de gerenciamento ou interação com o provedor de serviços."

Com esta definição podemos observar aspectos importantes para a computação em nuvem como:

- Virtualização;
- Poder de processamento;
- Armazenamento;
- Conectividade;
- Compartilhamento;
- Serviços sob demanda;
- Isolamento;
- Distribuição.

A arquitetura de *Cloud computing* é dividida em 5 (cinco) camadas principais: Infraestrutura física, infraestrutura virtual, plataforma, aplicação e rede. Como demonstrado a seguir (Figura 2):

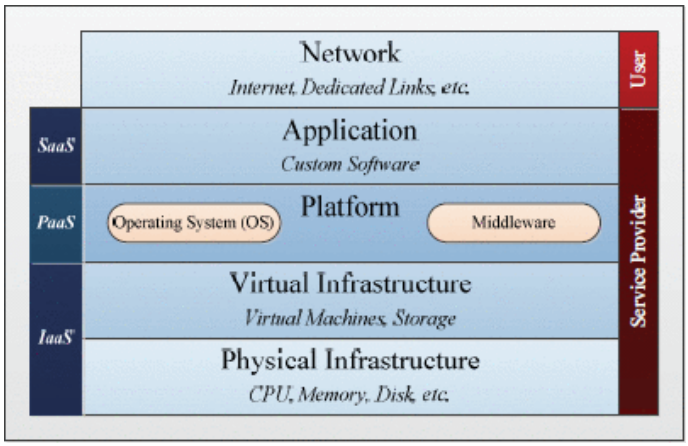

Figura 2. *Cloud Models* (Fatemi Moghaddam et al., 2015).

Em resumo, essas camadas permitem que as empresas implementem modelos de serviço em nuvem, como *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS) e *Software-as-a-Service* (SaaS), que oferecem flexibilidade, escalabilidade e eficiência para as operações de negócios. Com a crescente demanda por soluções em nuvem, a arquitetura de *Cloud computing* tornou-se uma das áreas em constante evolução no setor de tecnologia. (Fatemi Moghaddam et al., 2015)

2.3.2. *Fog computing*

Fog computing promove uma camada de infraestrutura intermediária que conecta as fontes de dados e a nuvem. Esta camada pode ser alocada em qualquer lugar entre os dispositivos finais (*end devices*[10]) e a nuvem, portanto, nem sempre são diretamente conectados aos dispositivos finais.

Além disso, o *Fog computing* não se concentra somente no lado dos dispositivos IoT, mas também fornece seus serviços para a nuvem, desta forma observa-se que o *Fog computing* não serve apenas como uma extensão ou substituição do *Cloud computing*, mas sim uma camada adicional para promover a interação entre nuvem e IoT.

[10]Dispositivos finais que se conectam a uma rede e são capazes de enviar e receber informações através da rede

A *Fog computing* tem dois modelos de arquitetura, sendo elas a *Three-Layer Architecture* (Arquitetura de Três Camadas) demonstrada na Figura 3 e a *OpenFog N-Tier Architecture*, que pode ser considerada como um refinamento da Arquitetura de Três Camadas, mas que não será abordada neste documento.

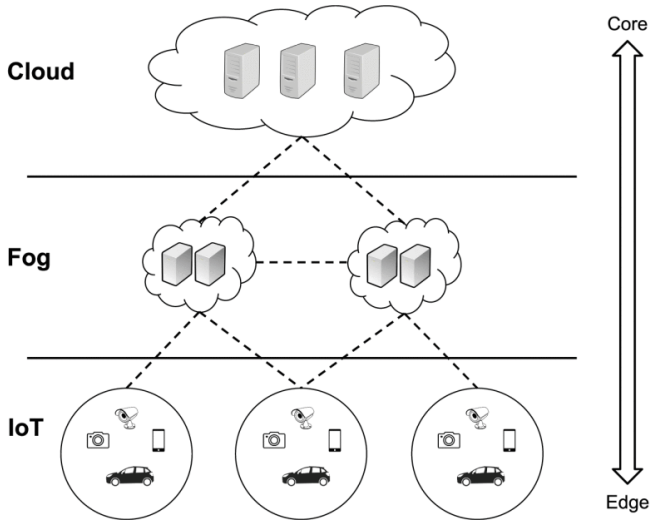

Figura 3. *Cloud Models* (De Donno et al., 2019).

A *Three-Layer Architecture* surgiu da ideia da *Fog computing* ser uma entidade intermediária entre a nuvem e os *end devices*, as três camadas que compõem esta arquitetura são basicamente: a camada IoT (*IoT layer*), composta pelos dispositivos IoT, que enviam os dados para a camada da névoa *Fog layer* a camada que é o núcleo de *Fog computing*, composta por diversos nós-névoa (*Fog nodes*) que são capazes de computar, transmitir e armazenar temporariamente os dados recebidos pelos dispositivos IoT ou pela nuvem; e por fim, a camada nuvem (*Cloud layer*), composta majoritariamente com diversos servidores com alto poder computacional e de armazenamento, podendo oferecer diferentes serviços à *Fog*.

2.3.3. *Edge computing*

Edge computing é um paradigma que surgiu pela necessidade da computação em dispositivos nas bordas da rede, por isso o termo: computação de borda. Este termo acabou por ganhar maior notoriedade com a evolução e popularização da IoT.

De acordo com Shi et al. (2016), em tradução livre, a definição de *Edge computing* é dada da seguinte forma: "*Edge computing* refere-se às tecnologias que permitem a realização de computação na borda da rede, tanto em dados no fluxo *downstream*[11] em relação aos serviços em nuvem, quanto em dados no fluxo *upstream*[12] em relação aos serviços de IoT". Portanto, a ideia é estender a computação em nuvem para a rede de borda com o intuito de aproximar a computação nas fontes de dados, como dispositivos IoT, por exemplo.

[11]Fluxo de dados que se move do servidor para o dispositivo de destino ou para o usuário final
[12]Fluxo de dados que se move do dispositivo de origem ou do usuário final para o servidor

Na prática, isso significa que, ao invés de todos os dados serem processados na nuvem, a computação será realizada em dispositivos na borda da rede, próximos às fontes de dados, podendo reduzir a latência e o congestionamento da rede.

2.4. Padrões para soluções IoT

No segmento de padrões para soluções IoT não há padrões definitivos estabelecidos para a construção das mesmas, porém, foram criados alguns documentos e iniciativas que fornecem padronização e diretrizes para a organização das soluções.

Existem várias organizações e fóruns, que estão trabalhando ativamente no desenvolvimento de padrões para soluções IoT, tais como o IEEE[13], o IETF[14], o ISO/IEC[15], o W3C[16] e a OCF[17], entre outros. Essas entidades estão envolvidas na definição de padrões para aspectos-chave, como comunicação entre dispositivos, segurança, gerenciamento de identidade, interoperabilidade e arquitetura de sistemas.

Esses documentos, embora não constituam um padrão definitivo, fornecem orientações valiosas para a arquitetura de soluções IoT, auxiliando a estabelecer uma base comum e que promova a interoperabilidade entre dispositivos e sistemas. Contudo vale ressaltar que devido a natureza diversificada e em constante evolução da IoT, é improvável que um único padrão de arquitetura possa atender a todas as necessidades específicas de uma solução sem necessitar de adaptações.

Citando brevemente os documentos utilizados para embasamento deste projeto foram: o RFC-7452, intitulado "*Architectural Considerations in Smart Object Networking*", que descreve uma arquitetura de referência para a IoT, identificando os principais componentes e suas interações. E o IEEE P2413, um padrão em desenvolvimento intitulado "*Standard for an Architectural Framework for the Internet of Things*", que procura fornecer um modelo arquitetônico de alto nível e um conjunto de práticas recomendadas para o desenvolvimento de soluções IoT.

2.4.1. RFC 7452

RFC's (*Request for Comments*) são documentos técnicos publicados pela *Internet Engineering Task Force* (IETF) que descrevem especificações técnicas, protocolos, procedimentos e conceitos relacionados à Internet, portanto, são amplamente utilizadas para estabelecer padrões de comunicação e interoperabilidade entre sistemas e dispositivos conectados à Internet (Tschofenig et al., 2015).

[13]Instituto de Engenheiros Eletricistas e Eletrônicos, a maior organização profissional do mundo dedicada ao avanço da tecnologia em benefício da humanidade, tendo criado diversos padrões de implementações.

[14]Internet Engineering Task Force, um grupo internacional aberto, composto de técnicos, agências, fabricantes, fornecedores e pesquisadores, que se ocupa do desenvolvimento e promoção de padrões para a internet

[15]Organização Internacional de Normalização, uma entidade que congrega os grêmios de padronização/normalização de 162 países.

[16]World Wide Web Consortium, a principal organização de padronização da World Wide Web.

[17]Open Connectivity Foundation, uma organização do setor para desenvolver padrões, promover um conjunto de diretrizes de interoperabilidade e fornecer um programa de certificação para dispositivos envolvidos na Internet das coisas.

A RFC 7452 publicada em março de 2015, intitulada de "*Architectural Considerations in Smart Object Networking*", descreve as considerações arquiteturais que devem ser consideradas para a projeção de redes de objetos inteligentes (*smart objects*). *Smart objects* são definidos como um dispositivo com recursos limitados de processamento, memória e energia, que é capaz de se comunicar com outros dispositivos através de uma rede.

Esta RFC também apresenta uma arquitetura de rede para objetos inteligentes, que inclui várias camadas, sendo elas: a de aplicação, de rede e de enlace, além de descrever como as funções de segurança, gerenciamento de recursos e comunicação devem ser distribuídas entre essas camadas para garantir um desempenho adequado e uma operação segura da rede.

Sendo assim, considerando os aspectos de segurança, a RFC 7452 reforça a sugestão de abordagens diferentes para a segurança de cada infraestrutura, pois uma rede doméstica pode possuir uma implantação de segurança com necessidades distintas de ambientes industriais mais robustos, por exemplo. Dessa forma, é importante considerar a relação entre a arquitetura de rede e a arquitetura de computação, ao projetar e implementar sistemas de objetos inteligentes.

2.4.2. IEEE P2413

O IEEE P2413 é um projeto de padrão desenvolvido pelo *Institute of Electrical and Electronics Engineers* (IEEE) que se concentra na arquitetura de sistemas para a Internet das Coisas. É tido como objetivo principal desse padrão fornecer um modelo arquitetônico de alto nível e práticas recomendadas para o desenvolvimento de soluções IoT.

Este padrão é fundamentado na ideia de que a interoperabilidade é um elemento essencial para a IoT, portanto, visa estabelecer uma estrutura que permita a integração de diferentes dispositivos, redes e sistemas em soluções IoT, independentemente de fabricante, tecnologia ou aplicação específica.

A estrutura arquitetural irá propor definições de abstrações de domínio e identificação de características comuns entre diferentes domínios da IoT, além de fornecer um direcionamento que auxilie os desenvolvedores a projetar soluções IoT escaláveis, interoperáveis e seguras, oferecendo diretrizes sobre como organizar e estruturar os componentes de uma solução IoT, de modo a facilitar a comunicação entre eles.

Por fim, também promove a reutilização de componentes e a interoperabilidade entre diferentes soluções IoT. Ele fornece um conjunto de práticas recomendadas para padronizar interfaces, protocolos e formatos de dados, facilitando a integração de dispositivos e sistemas de diferentes fornecedores.

2.5. Arquitetura de soluções IoT

No contexto das arquiteturas de soluções IoT, é importante destacar que não existe um padrão único e universalmente aceito para as arquiteturas IoT. A arquitetura pode variar em termos do número de camadas e dos procedimentos utilizados. Geralmente, são mencionadas três, quatro e cinco camadas como opções comuns, mas é importante ressaltar

que a escolha da arquitetura de pilha depende das necessidades e requisitos específicos de cada aplicação IoT.

Mas vemos que a solução proposta por Khan et al. (2012), conforme exibido na Figura 4, é a que melhor se adéqua à solução proposta, portanto, é a que será descrita a seguir:

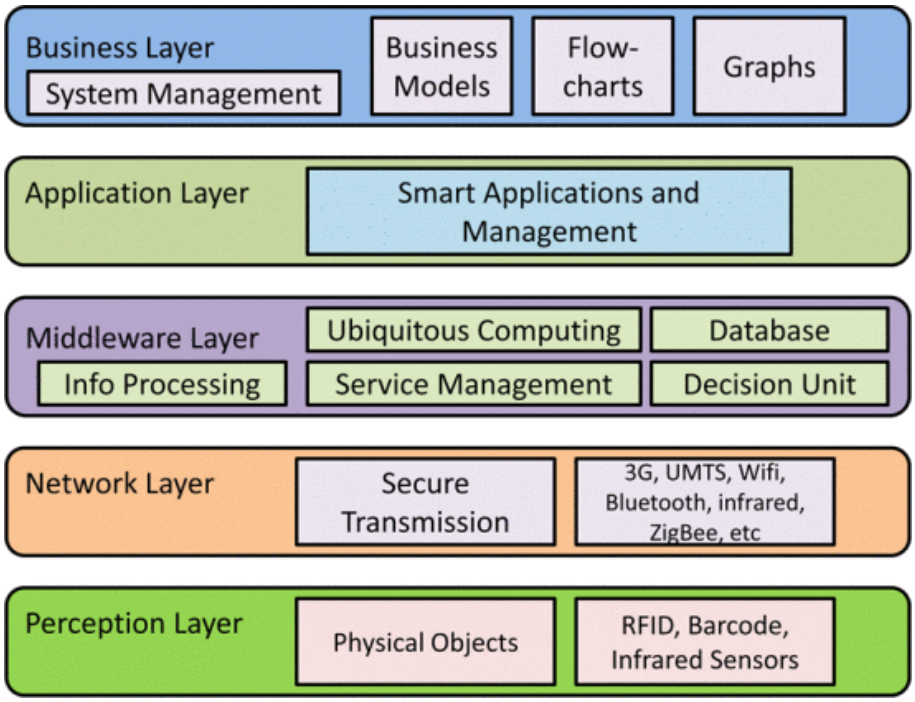

Figura 4. A Arquitetura IoT (Khan et al., 2012).

A camada inferior (Camada de Percepção) centraliza-se nos objetos físicos e nos dispositivos sensores de forma geral. Os sensores podem ser diversos, como RFID, sensores infravermelho, sensores de umidade, entre outros, dependendo da necessidade do projeto. Esta camada é responsável pela identificação e coleta de informações específicas dos dispositivos sensores. Considerando o tipo de sensor, as informações podem ser sobre temperatura, movimento, localização, umidade, aceleração, entre outros. Estas informações são coletadas e enviadas para a próxima camada, a camada de rede, efetuando a sua transmissão de forma segura para as camadas seguintes.

A Camada de Rede (também conhecida como Camada de Transmissão), por sua vez, transfere com segurança os dados obtidos pelos dispositivos sensores, para o sistema de processamento de informações. A forma de transmitir esses dados pode variar, podendo ser por comunicação com ou sem fio, utilizando 3G/4G, Wi-Fi[18], Bluetooth[19], infravermelho, ZigBee[20], entre outras. A decisão pela tecnologia mais adequada nesta camada deve estar em consonância com os requisitos funcionais da solução IoT em desenvolvimento.

[18]Rede de área local sem fio, para conexão com a internet através de ondas de rádio, definida pelo padrão IEEE 802.11.

[19]Bluetooth é um padrão para troca de dados entre dispositivos de curto alcance, sem uso de fio.

[20]Protocolo de comunicação sem fio destinado a aparelhos IoT.

A camada de rede realiza a transmissão das informações entre a camada de percepção e a camada *middleware*. Esta última, por sua vez, garante a integração de dispositivos heterogêneos (no âmbito de arquiteturas, formato de dados e sistemas de comunicação), fornecendo diferentes tipos de serviço. Um *middleware* tem como funcionalidade principal abstrair as complexidades do sistema em questão, complexidades essas que podem estar relacionadas à aspectos de comunicação ou cálculos em geral, integrando dispositivos heterogêneos de computação e comunicação, suportando a interoperabilidade entre os diversos aplicativos e serviços executados nesses dispositivos, além de possibilitar o gerenciamento e persistência dos dados processados (Razzaque et al., 2016).

A camada de aplicação proporciona o gerenciamento por completo da aplicação, com base nas informações recebidas pela camada *middleware*, sendo responsável, portanto, por realizar a entrega do serviço para os clientes. Esta possui diversos protocolos que podem ser usados como COAP (*Constrained Application Protocol*), DDS (*Data Distribution Service*), MQTT (*Message Queue Telemetry Transport*), HTTP (*Hypertext Transfer Protocol*), entre outros.

A última camada desta arquitetura, a camada de negócio, é utilizada para o gerenciamento do sistema IoT de forma geral, incluindo as aplicações e serviços que serão disponibilizados. Nela são criados modelos de negócios, fluxogramas, gráficos, entre outros, utilizando os dados recebidos pela camada de aplicação. Com esses dados é possível determinar as futuras ações e estratégias que serão tomadas, graças à camada de negócios.

2.6. Soluções IoT para Segurança Patrimonial

O uso de IoT por aparelhos e serviços é diversificado e tem se mostrado muito eficiente em comparação com métodos usados pela humanidade anteriormente, por isso se tornando cada vez mais presente no cotidiano da sociedade. Sistemas de segurança IoT também vêm sendo implementados, fazendo uso de sistemas de tecnologias de comunicação sem fio para transferência de dados, como Wi-Fi.

2.6.1. Casas com uso de IoT para segurança

Casas podem ser equipadas com sensores de presença, fechaduras inteligentes, câmeras, entre outros, como demonstrado na Figura 5. Estes dispositivos, podem ser acessados ou enviar informações com uso de Internet, como as câmeras, que podem disponibilizar transmissão ao vivo mesmo quando o proprietário estiver longe do local ou sensores, que podem enviar notificações sobre percepção de movimentos nas proximidades do patrimônio, entre outros dispositivos.

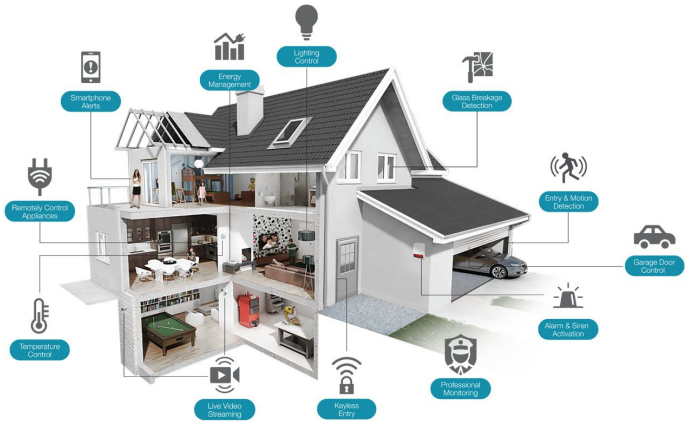

Figura 5. Casa inteligente com dispositivos IoT (Smarthomeworks, 2018).

2.6.2. Benefícios de uma propriedade com segurança inteligente

Propriedades inteligentes têm o objetivo de tornar a vida mais fácil e conveniente e, neste caso, mais segura também. Quando se está trabalhando ou mesmo quando uma propriedade como uma universidade, ou uma empresa não estão em horário de expediente, sistemas de segurança podem ser criados para enviar alertas, reportes (se uma ronda foi cumprida, por exemplo) ou mesmo ligar para um número de emergência em caso de detecção de incêndio e desbloquear as portas para os bombeiros nestes casos.

Tecnologias para propriedades inteligentes, podem ser muito eficientes para pessoas que moram sozinhas, podendo alertar o hospital em caso de necessidades médicas, além de, no quesito segurança, alertar a pessoa sobre possíveis aproximações de sua propriedade em horários não convencionais, permitindo-a agir de maneira preventiva. Sistemas com controle simplificado através de aplicativos podem permitir que os sistemas sejam ligados, desligados e ajustados de acordo com a necessidade do usuário, reduzindo o raio de alerta de sensores de movimentos, por exemplo.

Casas com proteção inteligente contra incêndio oferecem maior proteção do que os sistemas de alarme típicos. Os sensores podem ser espalhados, para detectar a presença de monóxido de carbono em todas as partes da propriedade. Em caso de incêndio, o proprietário pode ser alertado e o corpo de bombeiros acionado. Com uso de inteligência artificial, pode-se ainda mapear o local específico do incêndio e o nível da emergência ao corpo de bombeiros.

Códigos de segurança, cartões de acesso, leitores biométricos e câmeras de monitoramento, podem identificar os residentes ou trabalhadores da propriedade, sejam eles visitantes ou possíveis intrusos, através de dispositivos conectados à internet. Sistemas com inteligência artificial para segurança, podem identificar e alertar os proprietários sobre algum indivíduo não identificado tentando acessar o local, utilizando, por exemplo, técnicas de reconhecimento de padrão biométrico.

Em caso de detecção de indivíduo suspeito, o sistema pode prover vídeo e imagens para o proprietário. Através de configurações, pode-se bloquear alertas para dias de visitas ou ligar para a polícia automaticamente após arrombamento (Rosslin and Tai-hoon, 2010).

2.7. Soluções para auxílio de ronda

Conforme citado, o IFSC Lages já tentou utilizar outras soluções, sendo estes marcação de ponto com tecnologia de RFID e aplicativo de *selfies* no local da ronda. Além destas, outras possibilidades existem no mercado de proteção patrimonial.

2.7.1. Etiquetas RFID Afixcode

Este sistema da empresa Afixcode, utiliza etiquetas com tecnologia de radiofrequência como apresentada na Figura 6, espalhadas pelo local de uso, que servem para ler dados. Quando aplicada no contexto de segurança patrimonial, são usadas para a marcação de ponto sem necessidade de autenticação biométrica. O sistema conta com um objeto portado pelo funcionário, como cartão ou caneta, utilizados para aproximação dos pontos de controle, que marcam o ponto nas rondas do vigilante ao passar pelo local. Os sensores RFID são compostos por um chip e antena e podem ser acoplados dentro de outros objetos (Afixcode, 2023).

Figura 6. Etiqueta RFID da empresa Afixcode (Afixcode, 2023).

2.7.2. Aplicativo móvel para controle de rondas utilizando *selfies*

Este sistema emprega *selfies* para validar a localização do vigilante durante suas rondas. O aplicativo móvel dispõe de uma tela de registro que apresenta os locais pelos quais o vigilante deve passar, e a partir dela, ele pode registrar sua presença com uma *selfie* para assegurar sua localização atual. Este sistema exige que o usuário abra a aplicação e procure por uma boa posição para a foto, mostrando o ponto da ronda e necessitando de boa iluminação, o que pode deixar o vigilante vulnerável. Este aplicativo é o que o IFSC/Lages utilizava anteriormente, o qual não se demonstrou efetivo para as necessidades do câmpus.

2.7.3. Sistema com controle por GPS para dispositivos móveis

Outro sistema existente, utiliza um aplicativo para dispositivos móveis com sistema operacional Android 4.0, com necessidade de possuir GPS, para fazer o mapeamento e controle das rondas e conexão com a internet. Neste sistema, o aplicativo faz contato com um *web service*[21] para enviar os dados coletados pelo GPS. Este possui semelhanças com a solução proposta, mas possui pendências e não está disponível no mercado (Silva, 2013).

[21] Solução utilizada para integração e comunicação entre aplicações diferentes.

2.7.4. Sistema de posicionamento utilizando sensor acoplado ao calçado, *smartphones* e código QR

O sistema utiliza um sensor acoplado ao calçado do vigilante, que envia por bluetooth estimativas de posicionamento em tempo real ao celular, como demonstrado na Figura 7. Quando o vigilante chega em pontos pré-determinados da ronda, onde estão localizados códigos QR[22], deve utilizar o celular para lê-los. O código QR contém as coordenadas tridimensionais da localização, que são obtidas pelo aplicativo, quando lido pela câmera do celular. Então, o algoritmo fará uma fusão dos dados obtidos pelo sensor de posicionamento na bota e as coordenadas obtidas pelo código QR, para validar a real posição do vigilante. Para suportar o aplicativo, o celular deverá ter sistema operacional Android, GPS e Bluetooth (Liu et al., 2021).

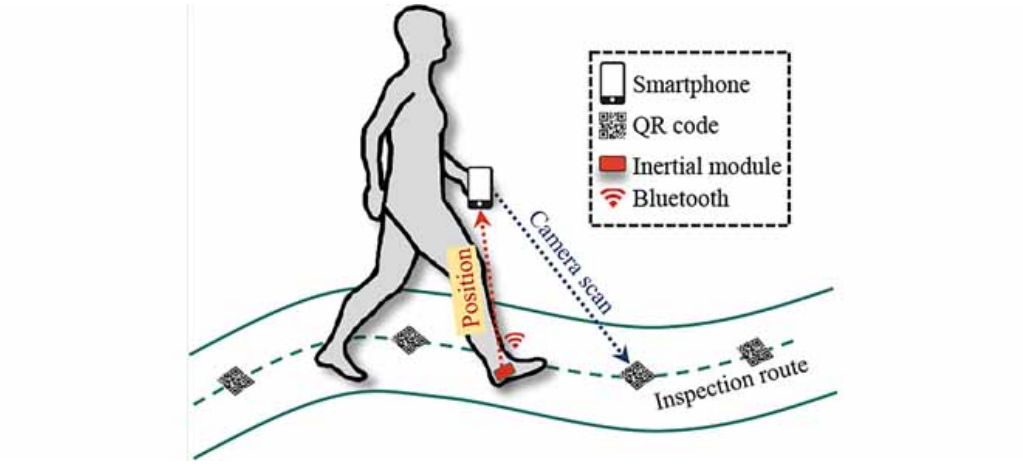

Figura 7. Sistema de posicionamento utilizando sensor acoplado ao calçado, *smartphones* e código QR (Liu et al., 2021).

2.7.5. ATMobile ActiveTrack

É um aplicativo móvel desenvolvido pela EBS Brasil[23] para garantir a segurança e a eficiência dos serviços de vigilância e monitoramento em diversos setores, como empresas, condomínios, escolas, hospitais, entre outros. Por meio do aplicativo móvel, é possível registrar a localização atual do vigilante por meio de *selfies*, garantindo que ele esteja cumprindo sua rota de ronda e aumentando a confiabilidade do serviço prestado.

O aplicativo apresenta uma tela de registro que delimita os locais de ronda em que o vigilante deve passar, permitindo que ele realize a marcação utilizando a câmera do *smartphone* para capturar uma imagem e confirmar sua presença no local. Além disso, o aplicativo permite que os usuários consultem relatórios de atividades e verifiquem o histórico de rondas realizadas pelos vigilantes. O ATMobile ActiveTrack também dispõe de uma série de funcionalidades para garantir a segurança e a eficiência do serviço de monitoramento, uma delas seria o botão de pânico, que permite que o vigilante informe

[22]Código QR é um código de barras, que podem ser escaneados utilizando a câmera de um *smartphone*.
[23]`https://www.ebsbr.com/atmobile`

emergências em tempo real, o registro de ocorrências, que possibilita que os usuários registrem eventos relevantes durante a ronda, entre outras.

2.7.6. Mobitraxx

A empresa Mobitraxx oferece uma solução, com diversas utilidades unidas em um único aplicativo, sendo elas: controle de rondas, registro de ocorrências, botão de pânico, criação de listas de checagem, registro de pontos e controle de tempos para locomoção e realização de serviços para o administrador. O aplicativo é feito para que os vigilantes o utilizem no celular e, conforme demonstrado na Figura 8, possui suas funcionalidades dispostas em uma tela principal. A solução também conta com uma aplicação web[24], para controle dos administradores sobre os relatórios gerados durante os trabalhos dos vigilantes.

Figura 8. Aplicativo para monitoramento de rondas Mobitraxx (Mobitraxx, 2023).

2.7.7. Quadro comparativo entre soluções

O quadro 1 realiza comparações entre diferentes soluções apresentadas neste projeto. Como pode-se notar, nenhum é gratuito, ficando de fora de uma das necessidades básicas do IFSC/Lages. Além disso, alguns fazem parte de projetos desenvolvidos para apresentação de artigos e não estão disponíveis para uso no mercado. As etiquetas RFID e o controle por meio de *selfies*, são soluções que já foram testadas pelo IFSC, e não se demonstraram efetivas para a instituição. Quatro das soluções precisam de intervenção

[24] Aplicação web é o tipo de *software* que se executa no navegador de computadores e celulares.

do vigilante durante as rondas, o que se torna um problema para os funcionários, que precisam manter a atenção constante no ambiente. Três soluções possuem interface para controle das rondas pelo administrador, porém, como estas não possuem outros requisitos apresentados no quadro, não cumprem as necessidades do câmpus.

Quadro 1: Relação comparativa entre as soluções.

Solução	Gratuito	Disponível	Se demonstrou efetivo ao IFSC/Lages	Precisa de intervenção do vigilante durante as rondas	Possui interface para controle de rondas
Etiquetas RFID Afixcode	Não	Sim	Não	Sim	Não
Controle com *Selfies*	Não	Sim	Não	Sim	Não
Sistema com controle por GPS	Não	Não	Não	Não	Sim
Sistema com sensor acoplado ao calçado	Não	Não	Não	Sim	Não
ATMobile ActiveTrack	Não	Sim	Não	Sim	Sim
Mobitraxx	Não	Sim	Não	Não	Sim
Solução proposta	Sim	Sim	Sim	Não	Sim

3. Solução Proposta

O aplicativo proposto pelos autores, possui como requisitos principais: ser gratuito, de fácil utilização e permitir que o usuário (vigilante) foque a sua atenção no ambiente ao qual está monitorando, e não em operações no aplicativo. Sendo assim, o mesmo possui apenas uma tela onde estarão concentradas as principais funções, como o botão para início e término de ronda e o botão de pânico. Após iniciar uma ronda, a localização do dispositivo é enviada com uma periodicidade pré-determinada para um sistema de armazenamento e visualização de dados. Este sistema permite aos administradores que visualizem em tempo real a posição atual do vigilante, bem como mantém um histórico da sua movimentação dentro do câmpus. Um fluxograma é apresentado na Figura 9.

Para tal, o aplicativo utiliza o receptor GPS (*Global Positioning System*[25]), bem como outros sensores disponíveis no dispositivo móvel. Os trajetos e horários das rondas realizadas, podem ser monitorados pelos administradores da instituição e pela empresa terceirizada.

Como meio de organização para as atividades relacionadas ao desenvolvimento do projeto, um *backlog*[26] foi utilizado, através da plataforma Github. O quadro foi dividido

[25] *Global Positioning System* - Sistema de navegação e aquisição de medidas de localização geográfica.

[26] *Backlog* refere-se a um quadro de atividades divididas em diferentes raias, onde os itens são organizados por status e prioridade em um determinado período de tempo.

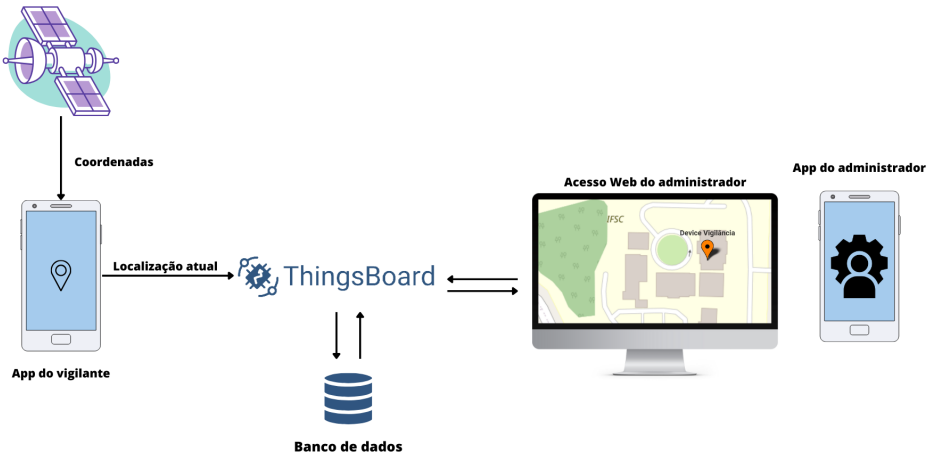

Figura 9. Esquema de uso da solução.

em 5 diferentes raias, sendo elas: *todo* (atividades aguardando para serem iniciadas), *in progress* (atividades em andamento), *test* (atividades em fase de teste), *done* (atividades já concluídas) e *documents* (atividades relacionadas à elaboração deste documento teórico), sendo elas exibidas na Figura 10. Com o objetivo de melhor detalhar a solução proposta, utilizou-se como referência a arquitetura apresentada na subseção 2.5.

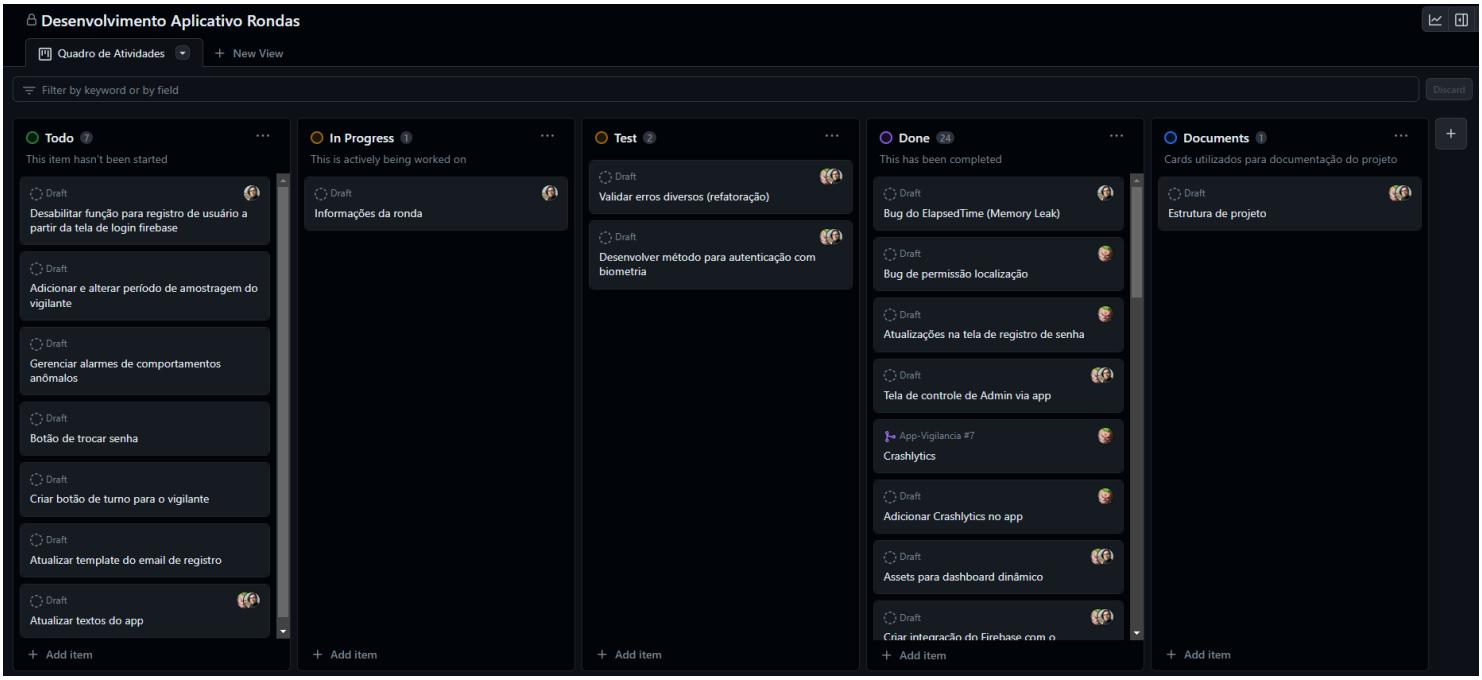

Figura 10. Quadro de atividades (*backlog*) relacionadas ao desenvolvimento do sistema em questão.

3.1. Camada de Percepção

Os requisitos do *smartphone* já são contemplados pela maioria dos dispositivos móveis atualmente disponíveis no mercado. Sendo necessário um receptor de GPS e o sistema operacional Android na versão 4.1 ou superior, pois o Flutter[27], que foi usado para desenvolvimento da aplicação, tem suporte mínimo para a versão citada. Também é necessário que o dispositivo possua autenticação biométrica, para garantir a identidade do funcionário (vigilante) que vier a efetuar a ronda.

3.2. Camada de Comunicação

Para realizar o envio e recebimento dos dados coletados, é utilizada a interface de rede móvel do dispositivo (4G/5G) ou a interface IEEE 802.11 (Wi-Fi). A escolha destas opções se dá por conta do dispositivo móvel comumente ter estes componentes em seu *hardware* e possuir uma bateria com autonomia suficiente para a utilização destes recursos. A escolha da opção adequada dependerá de fatores como a velocidade da rede, a qualidade do sinal e a disponibilidade da rede.

Além disso, o Android oferece a funcionalidade "Wi-Fi Adaptativo" a partir de versões como o Android 10 e posteriores, que aprimora ainda mais essa escolha de conectividade. Com o Wi-Fi Adaptativo, o dispositivo pode alternar automaticamente entre redes Wi-Fi e redes móveis com base em preferências do usuário, priorização de sinal Wi-Fi forte e economia de energia, assegurando uma experiência de conectividade otimizada em todas as situações. Essa abordagem híbrida combina as duas opções de conectividade de forma inteligente, garantindo a transferência rápida e confiável dos dados na maioria das circunstâncias e economizando energia quando a conexão Wi-Fi não é necessária.

3.3. Camada de *Middleware*

O *middleware* faz a conexão entre a interface acessada pelo usuário e o servidor[28] (Figura 11), atuando como intermediário entre as camadas de comunicação e de aplicação. A camada de *middleware* tem funções essenciais, como gerenciamento de informações e de dispositivos, controle de acesso, segurança e privacidade e filtragem de dados (Schenfeld et al., 2016).

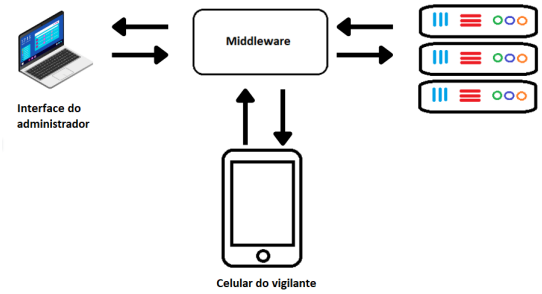

Figura 11. Exemplificação de *middleware*.

[27] Kit de desenvolvimento de interface de usuário, baseado na linguagem de programação Dart, que possibilita a criação de aplicativos compilados nativamente, para os sistemas operacionais mais utilizados.

[28] Um servidor é um computador com foco em capacidade de armazenamento, que conecta computadores distintos em uma rede.

Na perspectiva da computação, o *middleware* faz um *link* entre o *software* e o *hardware*, recebendo os dados coletados pelos sensores IoT (neste caso os dados do GPS) e sendo responsável, por exemplo, pelo gerenciamento e persistência dos dados, trabalhando em mais alto nível quando comparado aos sensores. Na proposta em questão, para persistência e gerenciamento dos dados coletados, foi utilizada a plataforma Thingsboard e, para atualizações, análise de uso e autenticação de usuários, foi utilizado o Firebase.

O celular do vigilante se conecta ao Thingsboard[29] e ao Firebase[30], com os quais faz envio e recebimento de dados coletados pelo GPS e autenticação de usuários, respectivamente, enquanto o administrador poderá visualizar os dados coletados em um mapa, que será exibido na própria plataforma do Thingsboard e, ao realizar seu acesso no aplicativo, também terá a funcionalidade de cadastrar um novo vigilante.

3.3.1. Thingsboard

O Thingsboard é uma plataforma de código aberto para coleta, visualização, processamento, persistência e gerenciamento de dados obtidos por sensores. Uma das características marcantes do Thingsboard é o suporte a uma ampla gama de protocolos de comunicação, o que o torna uma escolha ideal para projetos IoT. Entre os protocolos suportados, destacam-se o HTTP (*Hypertext Transfer Protocol*) e o MQTT (*Message Queuing Telemetry Transport*). O suporte a esses protocolos permite que dispositivos IoT se comuniquem eficientemente com a plataforma, seja por meio de conexões HTTP tradicionais ou de mensagens MQTT leves e eficazes.

Esta também permite a fácil personalização de certas funcionalidades e comportamentos, para atender às necessidades específicas de seus projetos. Isso inclui a capacidade de criar painéis de controle personalizados, criar regras de automação avançadas (*Rule Chains*) e integrar o Thingsboard com outros sistemas e aplicativos. O Thingsboard também será utilizado por oferecer uma modalidade de serviço gratuita, apesar de ter suas versões comerciais pagas.

3.3.2. Firebase

O Firebase é um conjunto de serviços de computação em nuvem oferecido pela Google, sendo os principais apresentados na Figura 12. Seus serviços incluem bancos de dados, modelos de autenticação, gerenciamento de *crashs*[31], entre outros.

No aplicativo proposto, o Firebase foi utilizado para a autenticação dos vigilantes e administradores que vierem a utilizar o aplicativo, com sistema de usuário e senha, mas é notável que a capacidade de autenticação do Firebase é robusta, suportando além da autenticação via email/senha, também autenticação social (como o acesso com o Google ou Facebook), via número de telefone, e métodos de autenticação personalizados, oferecendo flexibilidade e segurança para o gerenciamento de identidades de usuários. O uso

[29] `https://thingsboard.io`

[30] `https://firebase.google.com`

[31] Falhas apresentadas pelo aplicativo, geralmente causadas por uma exceção, como esgotamento de recursos.

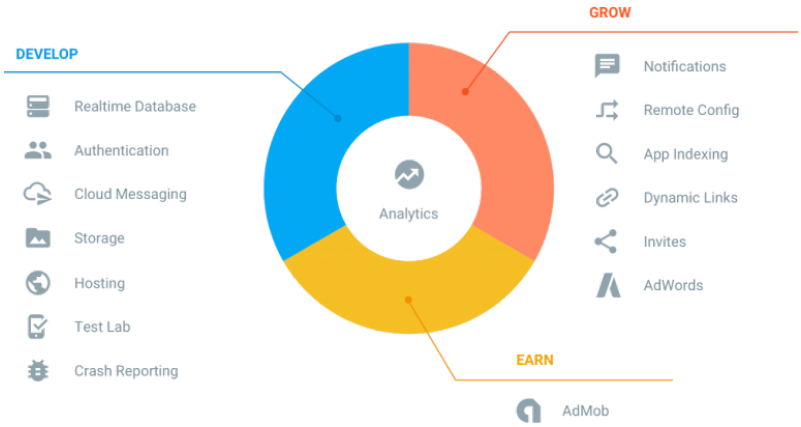

Figura 12. Principais serviços oferecidos no Firebase (Turasm, 2017).

do Firebase Authentication garante que apenas vigilantes e administradores autorizados possam acessar o aplicativo, aumentando a segurança da plataforma.

Além disso, o Firebase App Distribution simplifica o processo de lançamento de novas versões, permitindo a distribuição eficiente de atualizações para os usuários. O Firebase também disponibiliza um serviço de coleta de dados de uso do aplicativo, como reportes de *crash* com o Crashlytics (Figura 13), que também foi utilizado no aplicativo móvel, para monitoramento de falhas. Com a capacidade de oferecer esses serviços de maneira gratuita, o Firebase se destaca como uma escolha econômica e poderosa para o desenvolvimento do aplicativo, fornecendo uma base sólida para as funcionalidades propostas.

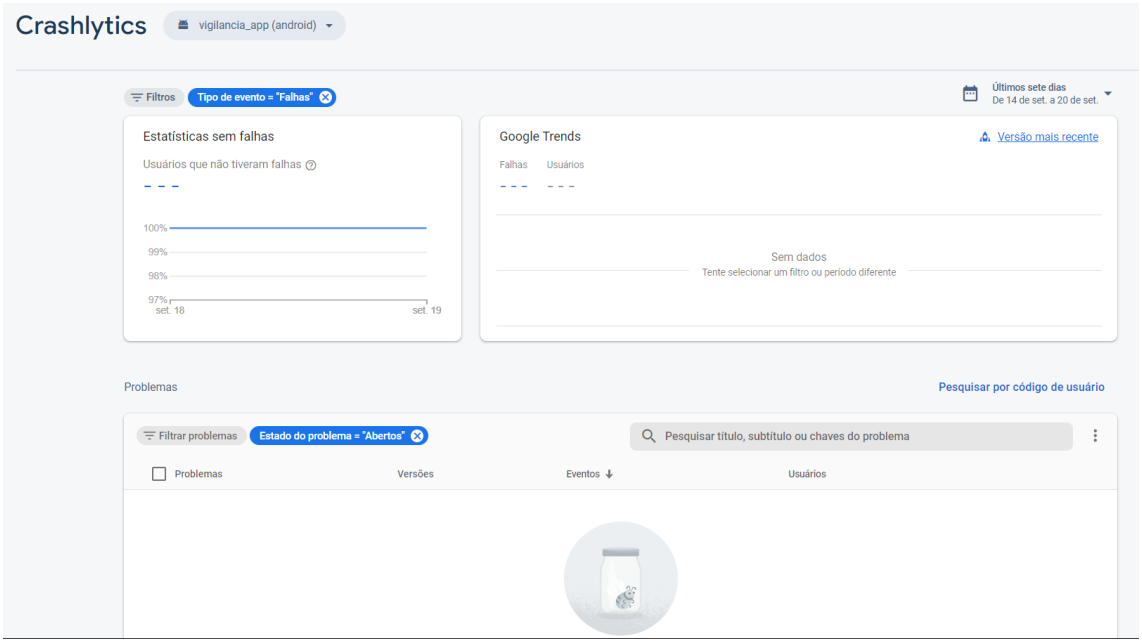

Figura 13. Visualização dos reportes de *crashs* e erros no aplicativo.

3.4. Camada de Aplicação

Esta camada está relacionada à entrega dos serviços aos clientes. Em um sistema IoT é responsável pela recepção e interpretação dos dados recebidos da camada de *middleware* e, posteriormente, pelo envio à camada de negócios, onde serão apresentados na interface de usuário (Bitencourt et al., 2021). Na solução proposta, a camada de aplicação é responsável por encaminhar os dados coletados pelo GPS à camada de *middleware*, para ter as localizações exibidas em um mapa, para os administradores das rondas (Figura 14).

```
try {
  await http.post(url, headers: headers, body: body);
} catch (e, stackTrace) {
  FirebaseCrashlytics.instance.recordError(
    e,
    stackTrace,
    reason: 'Ocorreu um erro durante o POST na API do Thingsboard',
  );
  Logger().e("Ocorreu um erro durante o POST na API do Thingsboard",
      error: e.toString());
}
```

Figura 14. Lógica utilizada para envio da localização do dispositivo ao Thingsboard.

A conexão para transmissão dos dados é feita através do protocolo HTTP, que tem por característica o uso de uma URL[32] para conexão com o servidor, permitindo envio e recepção de dados, conforme pode ser observado na Figura 15.

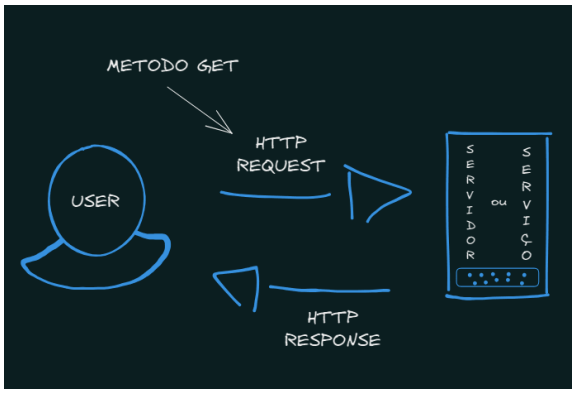

Figura 15. Funcionamento do protocolo HTTP (Mascarenhas, 2023).

Tendo isso em mente, por ser um protocolo simples de se trabalhar e já haver conhecimento prévio por parte dos autores, o HTTP foi utilizado no aplicativo para realizar o envio dos dados de localização do vigilante para o Thingsboard, para realização do acesso ao sistema, tanto para vigilantes como para administradores, além de também ser utilizado para cadastrar novos vigilantes. E, por fim, no painel de controle do Thingsboard, o administrador tem acesso às coordenadas dos vigilantes, que serão enviadas previamente através do mesmo protocolo HTTP.

[32]Endereços utilizados para acessar sites na internet.

3.5. Camada de Negócios

No aplicativo móvel, os vigilantes têm a função básica de realizar o login no aplicativo, através da tela que pode ser observada na Figura 16, iniciar e finalizar a ronda e gerar um alarme de pânico.

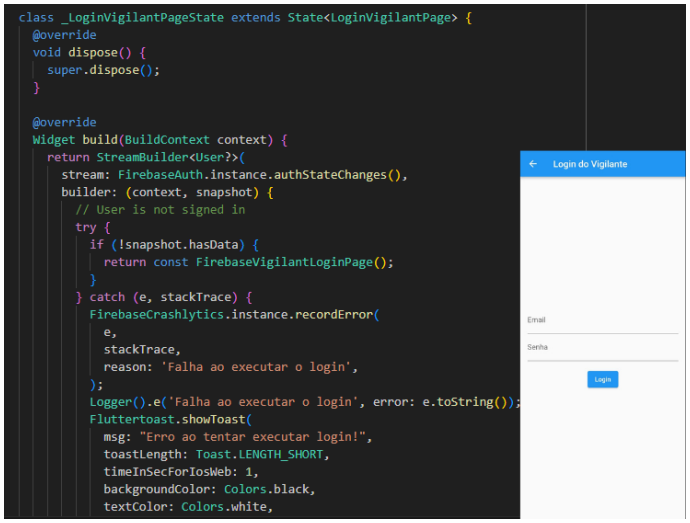

Figura 16. Implementação e exibição da tela de login do usuário vigilante.

É possível iniciar uma ronda de forma prática e intuitiva, pois após realizar a autenticação biométrica utilizando a digital, com apenas alguns cliques, os usuários podem definir o início da ronda e começar seu serviço sem complicações e, assim que finalizado, encerrar a ronda clicando no respectivo botão (Figura 17).

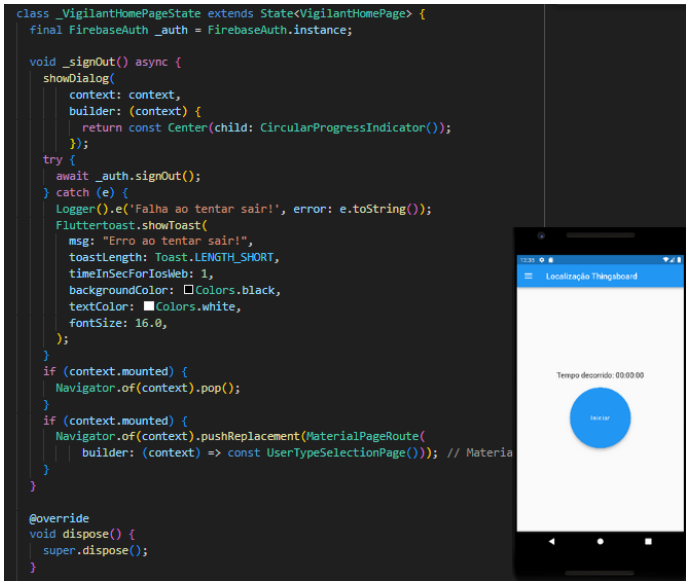

Figura 17. Implementação e exibição da tela principal do usuário vigilante.

Para iniciar o processo de ronda, os usuários precisam, anteriormente, realizar a autenticação por reconhecimento de digital, conforme pode ser observado na Figura 18.

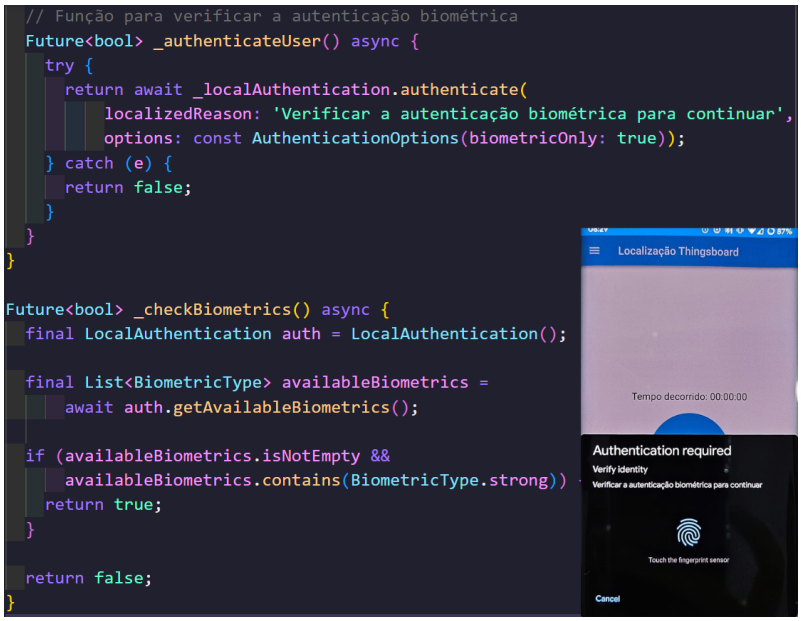

Figura 18. Implementação e demonstração da tela onde a leitura de digital é requisitada.

Também está presente a função de disparar um alarme de pânico, clicando no botão representado na Figura 19, onde os administradores são avisados, caso algum imprevisto tenha ocorrido durante a ronda. O alarme de pânico será disparado, caso o vigilante clique no respectivo botão ou fique parado por mais de 5 minutos, durante a ronda, avisando aos administradores que algo fora do esperado ocorreu, como uma abordagem ou outro comportamento inesperado dentro do câmpus.

Figura 19. Ícone do botão de pânico.

O usuário administrador pode cadastrar novos vigilantes no aplicativo móvel e, ao cadastrar um novo vigilante, um dispositivo que representará as rondas do vigilante cadastrado será criado no Thingsboard (Figura 20).

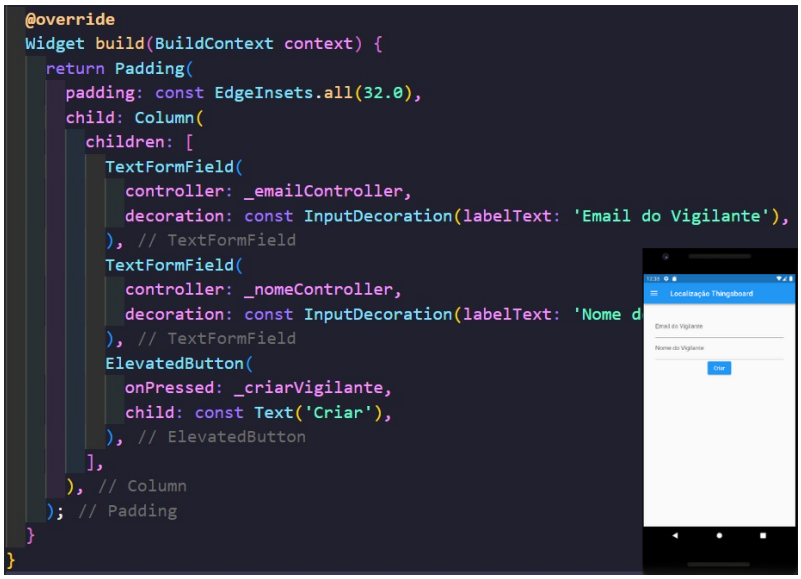

Figura 20. Implementação e demonstração da tela de cadastro de vigilantes, disponível para o usuário administrador, no aplicativo móvel.

Além disso, possui a capacidade de visualizar o histórico das rondas já realizadas pelos vigilantes, observando o caminho feito pelo vigilante durante a ronda (Figura 21), acessando uma visão completa das atividades de segurança.

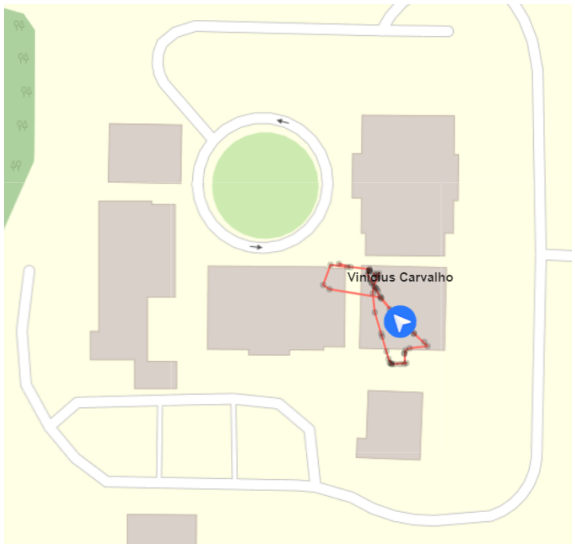

Figura 21. Mapa com a rota realizada pelo vigilante e pontos de amostragem.

Também é permitido que o administrador defina o intervalo de tempo que deseja filtrar no mapa e visualize os dispositivos dos vigilantes, que já foram cadastrados. Todas estas funcionalidades estão disponíveis no Thingsboard (Figura 22), onde o administrador tem acesso aos dispositivos conectados ou desconectados, aos vigilantes em atividade e

ao histórico de rondas, onde pode selecionar o período que deseja visualizar ou a exibição em tempo real.

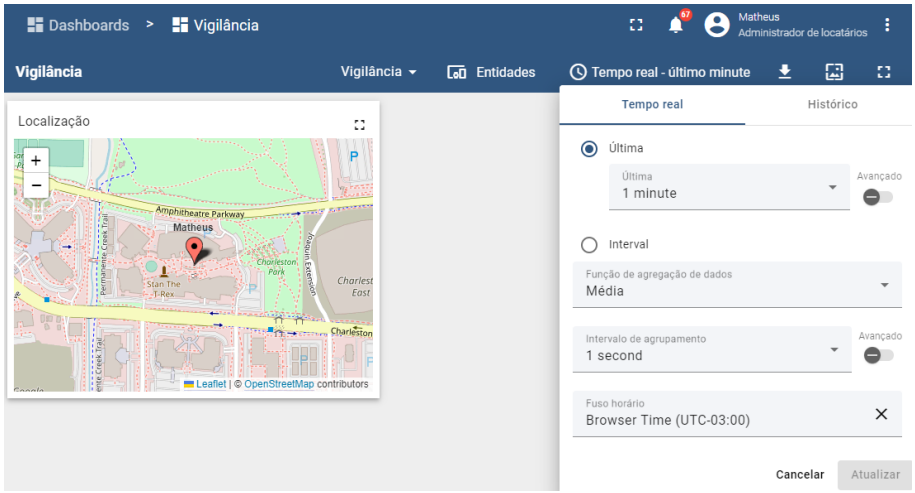

Figura 22. Quadro e configurações que podem ser controlados pelo administrador, para visualização das rondas dos vigilantes.

Uma funcionalidade adicional importante é a possibilidade de acompanhar a localização dos vigilantes em tempo real durante seus turnos. Isso permite ao Administrador ter uma visão atualizada da posição dos vigilantes, o que é especialmente útil em situações onde se trata de segurança de forma geral. O administrador também pode ser informado quando um alarme de pânico vier a ser disparado e visualizar os possíveis alarmes gerados.

Para facilitar o entendimento das funcionalidades do aplicativo, fez-se necessária a criação de Diagramas de Casos de Uso, apresentando as funcionalidades para os usuários vigilantes e administradores, exibidos nas Figuras 23 e 24, respectivamente. Além destes, também foi criado um diagrama de atividades para os vigilantes, na Figura 25.

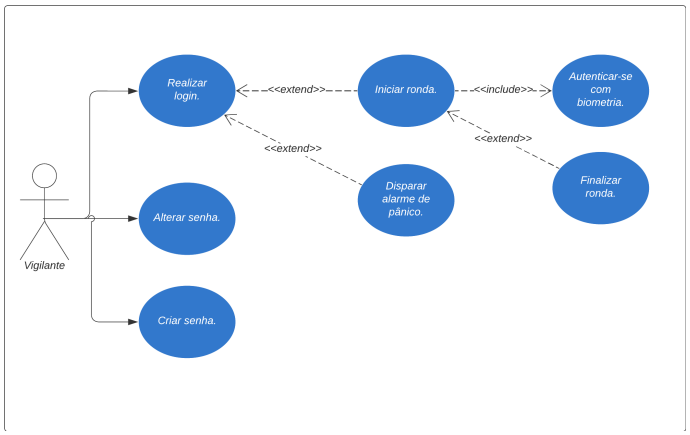

Figura 23. Diagrama de casos de uso do vigilante.

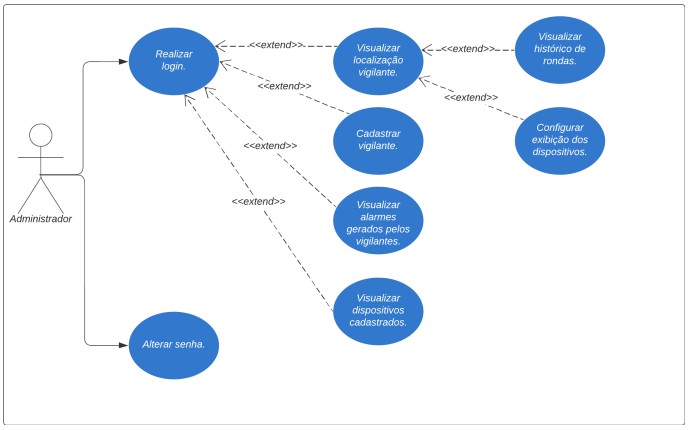

Figura 24. Diagrama de casos de uso do administrador.

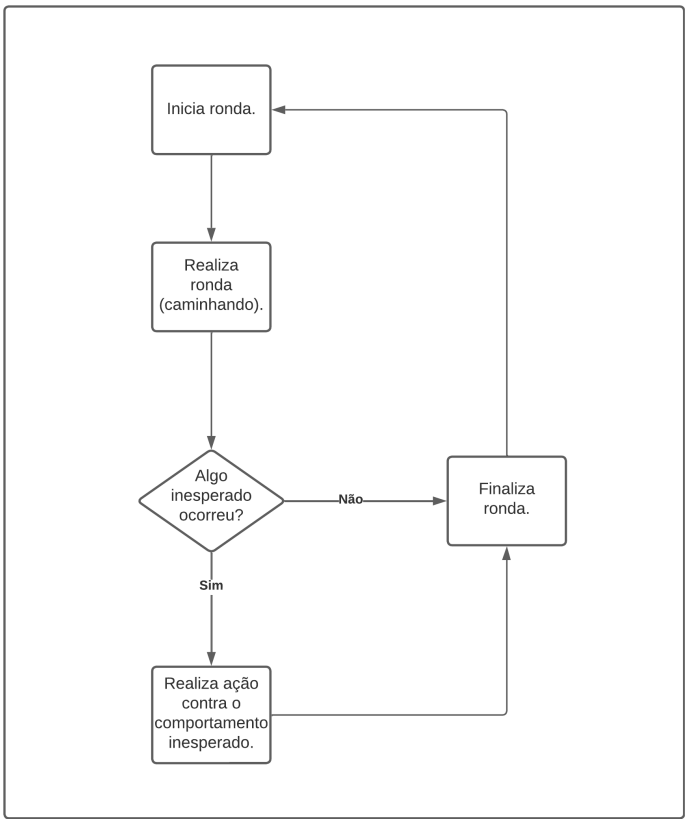

Figura 25. Diagrama de Atividades do vigilante.

4. Teste e Resultados

Uma das grandes vantagens para os administradores do sistema em questão, é a versatilidade na customização de painéis de controle que o Thingsboard oferece, permitindo a visão geral do estado dos dispositivos. Por padrão é exibido um mapa contendo a última localização registrada que aquele dispositivo recebeu, um mapa de rotas realizadas em um determinado tempo selecionável e um mapa que permite visualizar de forma interativa o percurso e a velocidade em que uma ronda foi realizada, respectivamente demonstrados na Figura 26.

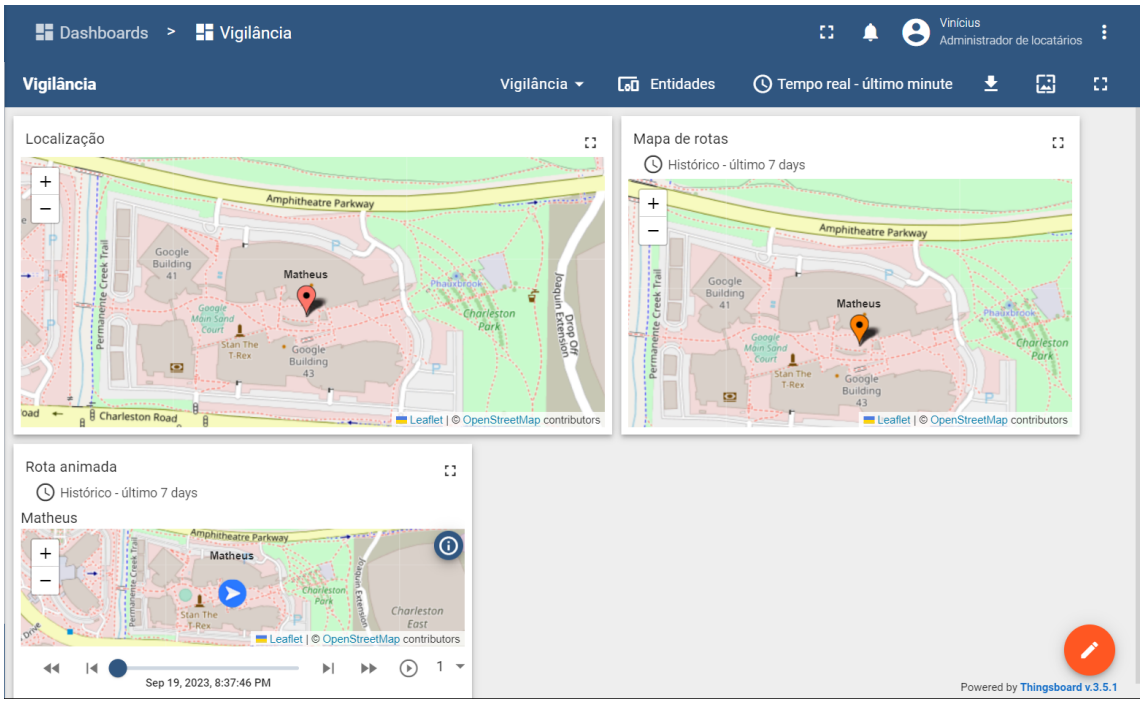

Figura 26. Mapa com a última localização registrada de um vigilante (Thingsboard, 2023).

Com o objetivo de coletar as opiniões do público adotado como alvo, realizou-se uma entrevista como forma de descobrir a opinião do usuário, permitindo possíveis ajustes no sistema e validar se o objetivo do projeto foi alcançado. Além disso, pôde-se ter uma experimentação prática do uso da solução.

4.1. Coleta dos Dados

Nos primeiros testes, notou-se que, em certos momentos, as amostras estavam inconsistentes, isso se dá pela perda de sinal com os satélites momentaneamente, gerando dados de latitude e longitude fora do escopo ideal para a ronda no câmpus, como pode ser observado na Figura 27.

Figura 27. Mapa de ronda exibindo as amostras com incoerências.

Para corrigir as amostras incoerentes, uma validação dos dados antes de seu envio foi implementada, realizando uma apuração, para que o dispositivo esteja necessariamente com uma acurácia alta na localização, assim a amostra seguinte não estará extremamente distante das últimas amostras. Uma amostra gerada após o ajuste, pode ser observado na Figura 28.

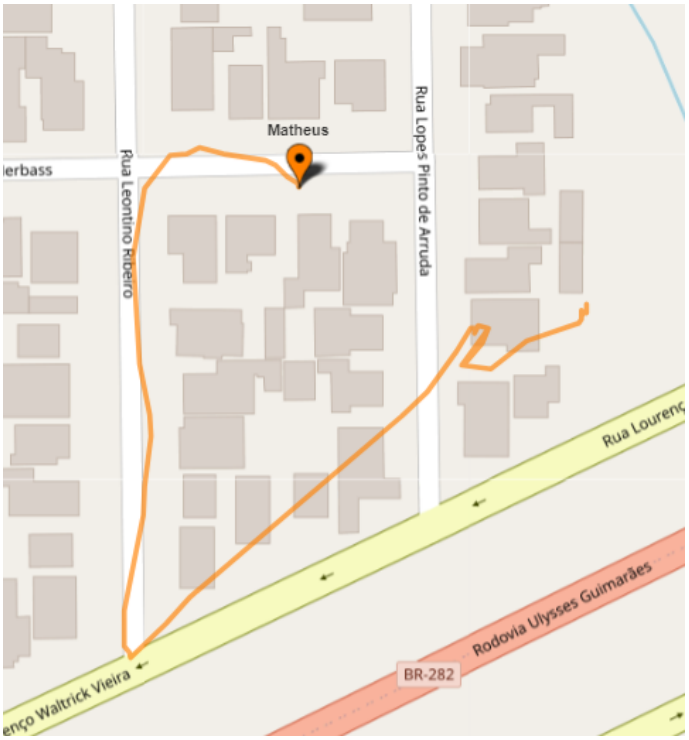

Figura 28. Mapa de ronda exibindo as amostras geradas após ajustes.

4.2. Entrevista

Foram realizadas conversas com o vigilante que utilizou o aplicativo, para análise de sua experiência com o sistema, essa conversa foi realizada após uma semana de uso do aplicativo. O retorno foi positivo, pois o usuário, durante a entrevista, expressou que o aplicativo está simples de se utilizar, intuitivo e responsivo, além de dizer que a solução não incomoda durante a ronda e que se sente muito mais confortável com o uso do novo sistema quando comparado aos anteriormente utilizados. Um destaque foi a importância da funcionalidade do alarme, pois segundo o usuário, transmite maior segurança em casos de emergência, já que os sistemas anteriores utilizados pelo IFSC/Lages não possuem este tipo de precaução para os vigilantes. Tal entrevista foi realizada no câmpus, no dia 1 de novembro de 2023, durante o trabalho do vigilante, que conseguiu um pequeno momento para responder às perguntas, após a semana de testes, que ocorreu entre 23 (vinte e três) e 27 (vinte e sete) de outubro de 2023.

Os pontos negativos foram com problemas na leitura da biometria, porém isso se deve ao leitor do dispositivo móvel não estar totalmente funcional, não sendo um problema da solução disponibilizada, mas sim do dispositivo utilizado para o teste, visto que este possuía um sensor de baixa qualidade. Sendo assim, o sistema se mostrou eficiente e mais adequado em comparação com as soluções anteriores que o IFSC/Lages utilizou e ainda utiliza. Também não haverá custos para a instituição, bem como a implantação (instalação do sistema) foi realizada e está pronta para uso. Tudo isso demonstra que o objetivo da solução foi alcançado, permitindo um controle de rondas com qualidade e aumentando a satisfação dos usuários.

5. Conclusões e Trabalhos Futuros

A partir dos resultados obtidos, através dos testes realizados e das amostras de localizações de GPS coletadas durante o uso do aplicativo, nota-se que o sistema funcionou de maneira estável e manteve-se funcionando durante todo o trajeto, demonstrando-se útil para o monitoramento de rondas. Através da entrevista, também observou-se que o objetivo qualitativo foi alcançado, pois o vigilante demonstrou gostar do sistema e de suas funcionalidades e ter interesse em utilizá-lo nos seus dias de serviço. A gratuidade de implantação e uso da solução também foi mantida, para assim suprir as necessidades do IFSC/Lages.

Sendo assim, os objetivos mencionados no início deste trabalho foram alcançados, mesmo que que com desafios durante o desenvolvimento da solução, como integrar certas operações do Thingsboard ao aplicativo móvel, devido a falta de documentação para alguns casos, manter o envio constante de localização em segundo plano e desenvolver a funcionalidade do alarme após determinado tempo de permanência do dispositivo no mesmo local.

Para trabalhos futuros, identificou-se melhorias e novas funcionalidades para o sistema. Uma destas é permitir a alteração do tempo de amostragem, de forma que o controle dos tempos em que as localizações serão enviadas, sejam personalizáveis para cada dispositivo cadastrado. Também é recomendado adicionar uma notificação fixa, que exiba o tempo de ronda atual, fazendo com que o vigilante possa verificar o tempo atual de sua ronda, sem precisar desbloquear o dispositivo, já que esta notificação será visível na tela de bloqueio. Também poderá ser adicionada uma lógica de cerca virtual, como

uma medida extra de segurança, para que caso o dispositivo seja detectado fora da área de cobertura do câmpus, um alarme seja emitido. Além destes pontos, o lançamento oficial do aplicativo na Play Store, fornecerá maior visibilidade e disponibilidade para os futuros usuários.

Referências

Afixcode (2023). Etiquetas rfid para patrimônio. Disponível em: https://www.afixcode.com.br/identificacao/etiquetas-rfid-patrimonio/. Acesso em: 17 de abr de 2023.

Azevedo, B. (2019). Entenda o que é a Quarta Revolução Industrial e como ela afeta o trabalho dos advogados. Disponível em: https://bernardodeazevedo.com/conteudos/entenda-o-que-e-a-quarta-revolucao-industrial-e-como-ela-afeta-os-advogados/. Acesso em: 20 de abr de 2023.

Bitencourt, E., Costa, R., and Anjos, W. (2021). Estudo comparativo entre plataformas iot para um contexto de smart campus: Estudo de caso de uma mini estação meteorológica. page 6.

Cloud, G. (2023). O que é a computação em nuvem? Disponível em: https://cloud.google.com/learn/what-is-cloud-computing. Acesso em: 29 de maio de 2023.

De Donno, M., Tange, K., and Dragoni, N. (2019). Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog. *IEEE Access*, 7:150936–150948.

Fatemi Moghaddam, F., Rohani, M. B., Ahmadi, M., Khodadadi, T., and Madadipouya, K. (2015). Cloud computing: Vision, architecture and characteristics. In *2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC)*, pages 1–6.

Fortin, M. F., Côté, J., and Filion, F. (2009). *Fundamentos e Etapas do Processo de Investigação*. Lusodidacta.

Gimawa (2019). Como os sensores de presença funcionam e onde utilizar? Disponível em: https://www.gimawa.com.br/single-post/2019/02/07/como-funcionam-os-sensores-de-presenca-e-onde-utilizar. Acesso em: 16 de mar de 2023.

IBM (2020). How Industry 4.0 technologies are changing manufacturing. Disponível em: https://www.ibm.com/topics/industry-4-0. Acesso em: 30 de mar de 2023.

Khan, R., Khan, S. U., Zaheer, R., and Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *2012 10th International Conference on Frontiers of Information Technology*, pages 257–260.

Lima, R. (2021). Câmeras inteligentes: como funcionam e quais comprar? Disponível em: https://www.tecmundo.com.br/produto/225041-cameras-inteligentes-funcionam-comprar.htm. Acesso em: 16 de mar de 2023.

Liu, T., Kuang, J., Ge, W., Zhang, P., and Niu, X. (2021). A simple positioning system for large-scale indoor patrol inspection using foot-mounted ins, qr code control points, and smartphone. *IEEE Sensors Journal*, 21(4):4938–4948.

Mano, J. and Marcolino, A. (2022). Dispositivos IoT devem chegar a 27 bilhões até 2025. Disponível em: https://www.poder360.com.br/brasil/dispositivos-iot-devem-chegar-a-27-bilhoes-ate-2025/. Acesso em: 20 de abr de 2023.

Mascarenhas, J. (2023). Protocolo HTTP – Como funciona? Disponível em: https://simplificandoredes.com/protocolo-http-como-funciona/. Acesso em: 15 de maio de 2023.

Mobitraxx (2023). Mobitraxx. Disponível em: https://www.mobitraxx.com.br/. Acesso em: 28 de abr de 2023.

PontoTel, R. (2022). Computação ubíqua: conheça a origem do conceito, características, recursos e suas vantagens! Disponível em: https://www.pontotel.com.br/computacao-ubiqua. Acesso em: 15 de mar de 2023.

Razzaque, M. A., Milojevic-Jevric, M., Palade, A., and Clarke, S. (2016). Middleware for internet of things: A survey. *IEEE Internet of Things Journal*, 3(1):70–95.

Rosslin, R. and Tai-hoon, K. (2010). International Journal of Advanced Science and Technology. *International Journal of Computer Applications*.

SAS (2023). Computação em nuvem. Disponível em: $https : //www.sas.com/pt_br/insights/analytics/machine - learning.html$. Acesso em: 5 de abr de 2023.

Schenfeld, M., Amaral, L., de Matos, E., and Hessel, F. (2016). Arquitetura para fog computing em sistemas de middleware para internet das coisas. In *Anais do XLIII Seminário Integrado de Software e Hardware*, pages 1819–1829, Porto Alegre, RS, Brasil. SBC.

Shi, W., Cao, J., Zhang, Q., Li, Y., and Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5):637–646.

Silva, D. N. (2023). Telégrafo. Disponível em: https://brasilescola.uol.com.br/geografia/primeira-revolucao-industrial.htm. Acesso em: 10 de abr de 2023.

Silva, L. F. (2013). Sistema Móvel Para Controle de Rondas. Disponível em: https://repositorio.ufsc.br/handle/123456789/184639. Acesso em: 18 de abr de 2023.

Smarthomeworks (2018). Smart Home Security for Beginers. Disponível em: https://smarthomeworks.com.au/2018/03/05/smart-home-security-for-beginners/. Acesso em: 15 de maio de 2023.

Sousa, R. (2023). Primeira revolução industrial. Disponível em: https://brasilescola.uol.com.br/geografia/primeira-revolucao-industrial.htm. Acesso em: 17 de abr de 2023.

Thingsboard (2023). Thingsboard. Disponível em: https://thingsboard.io/. Acesso em: 15 de maio de 2023.

Tschofenig, H., Arkko, J., Thaler, D., and McPherson, D. R. (2015). Architectural Considerations in Smart Object Networking. RFC 7452.

Turasm (2017). Firebase: O Que é e Como Funciona. Disponível em: https://micreiros.com/firebase-o-que-e-e-como-funciona/. Acesso em: 15 de maio de 2023.

Zainab, H., Mahmoud, B., and Hashan, A. (2015). Internet of Things (IoT): Definitions, Challenges and Recent Research Directions. *International Journal of Computer Applications*.