risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 01/03/2024
Aceitação/Acceptance: 09/06/2024

Segurança Universitária Reforçada: Uma solução de IoT para Proteção de Alunos em Campus

Anna Carolina Ferreira Rosa[1], Leonardo de Oliveira Almeida[1], Hugo Silva Vasconcelos[1], Mateus Romani[1], Fábio Lúcio Lopes de Mendonça[1], Francisco Lopes de Caldas Filho[1]

annacarolinafr36@gmail.com; leoengunb@gmail.com; hugo.svasc@gmail.com; mateusfromani@gmail.com; fabio.mendonca@redes.unb.br; francisco.lopes@uiot.org

[1] Departamento de Engenharia Elétrica, Universidade de Brasília, Campus Universitário Darcy Ribeiro Asa Norte, CEP 70910-900, Brasília/DF, Brasil

Pages: 228-242

Resumo: O aumento alarmante da violência contra mulheres, com 2.423 casos registrados em 2022, tem destacado a importância da tecnologia na segurança pessoal. Este artigo apresenta uma solução inovadora que integra botões de pânico em dispositivos móveis, combinando a praticidade dos smartphones com a robustez de dispositivos físicos dedicados. Isso proporciona uma maneira confiável e rápida de solicitar ajuda em situações de risco, promovendo a segurança pessoal dos alunos e funcionários na universidade..

Palavras-chave: Segurança, Situações de Risco, Aplicativo e Botão de Pânico.

Enhanced Campus Security: An IoT Solution for Student Protection

Abstract: The alarming rise in violence against women, with 2,423 cases reported in 2022, has highlighted the importance of technology in personal safety. This article presents an innovative solution that integrates panic buttons into mobile devices, combining the convenience of smartphones with the robustness of dedicated physical devices. This provides a reliable and quick way to request help in dangerous situations, promoting the personal safety of students and staff on campus.

Keywords: Security, High-Risk Situations, App, and Panic Button.

1. Introdução

A violência contra as mulheres é um problema social que vem apresentando números alarmantes. Em 2022 foram registrados 2.423 casos de violência contra a mulher (Agência Brasil, 2023). Esse cenário tem atribuído às soluções de tecnologia um papel importante no aumento da segurança para o público feminino. Tecnologia como a Internet das Coisas agregada às soluções de segurança pessoal, dispositivos vestíveis com sensores de detecção e botões de pânico, têm sido utilizados para prevenir e ajudar a combater situações de risco, como a mencionada (Biradar et al., 2020, pp. 688–691).

A Internet das Coisas (IoT) é uma tecnologia inovadora que trata da conexão de objetos físicos à Internet. Esses objetos são equipados com sensores e dispositivos de comunicação que lhes permitem coletar e trocar dados de forma autônoma. Essa tecnologia vem sendo empregada em soluções com o intuito de melhorar a segurança das mulheres, pesquisas como a de pulseiras inteligentes, que se comunicam com smartphones, o qual enviam a localização quando o usuário se encontra em situação de perigo vem sendo adotadas, pela facilidade de acionamento (Thamaraiselvi et al., 2019, pp. 1093–1096).

O botão de pânico é uma ferramenta eficaz e versátil que gera mais segurança para os usuários. Seus principais benefícios são: a facilidade de uso, integração com sistemas de segurança, geolocalização, rastreamento e facilidade de resposta em casos de emergência. Soluções de botão de pânico integradas com centrais policiais e contatos familiares cadastrados para o envio de mensagens de socorro, geram segurança por enviar mensagens para vários contatos e possibilita múltiplas tomadas de decisões contra cenários de violência (Swathi et al., 2022, pp. 5337–5342) e (Nasir et al., 2022, pp. 445–470).

Este artigo científico apresenta uma solução inovadora para melhorar a segurança pessoal através da integração de um botão de pânico em dispositivos móveis, complementado por um painel de controle para monitoramento e resposta eficaz às emergências. A abordagem combina a praticidade do uso de smartphones com a robustez de um dispositivo físico dedicado, proporcionando um meio confiável e rápido para solicitar auxílio em situações de risco.

Além desta introdução, o presente artigo encontra-se organizado da seguinte forma: na Seção 2, estão os trabalhos relacionados. Na Seção 3, será apresentada a metodologia, a qual contém a arquitetura proposta pelo projeto. Na Seção 4, serão descritos os testes e os resultados. Por fim, na Seção 5, serão apresentadas as conclusões e melhorias a serem desenvolvidas em trabalhos futuros.

2. Trabalhos Relacionados

O botão de pânico é uma ferramenta cada vez mais popular para a segurança pessoal, especialmente em emergências. Desde a sua introdução, muitos projetos de pesquisa e desenvolvimento têm sido realizados para aprimorar sua eficiência e acessibilidade.

O objetivo do artigo (Awodeyi et al., 2018, pp. 649–652) é construir um botão de pânico utilizando o Arduino Uno com módulos GPS para localização do usuário e o módulo Wi-Fi ESP8266 para comunicação. Quando o usuário pressiona o botão, a chamada é enviada para uma interface de controle e monitoramento. Para visualizar e rastrear os incidentes em tempo real, a plataforma do Google Maps é diretamente utilizada. Um problema identificado neste trabalho é a dependência exclusiva da comunicação via Wi-Fi, o que limita sua utilização em áreas onde esse tipo de comunicação não está disponível. Com base nessa limitação, nosso artigo propõe o desenvolvimento de um sistema alternativo que utiliza a comunicação de rede 4G e 5G para garantir a funcionalidade em áreas sem cobertura de Wi-Fi.

O botão de pânico também é utilizado no contexto das Cidades Inteligentes. O artigo (Prayogo et al., 2019) apresenta a criação de um sistema físico de botão de pânico para

uso residencial, utilizando o controlador ESP8266 para gerar alertas em emergências, como roubo, incêndio e acidentes. Uma diferença significativa neste artigo é a escolha da comunicação através do protocolo MQTT (Message Queuing Telemetry Transport). O artigo (Damayanti et al., 2019, pp. 1–5) descreve o projeto Bali Smart Island, desenvolvido na ilha de Bali, Indonésia, que implementa um dispositivo físico de botão de pânico de baixo custo e longa duração de bateria, utilizando a tecnologia de frequência de rádio LoRa.

Embora existam muitos artigos que abordem botões de pânico físicos devido à sua conveniência, é importante observar que também existem aplicações digitais de botões de pânico igualmente importantes. O artigo (Azman et al., 2018, pp. 37–41) apresenta uma aplicação chamada My Guardian, que tem como objetivo notificar contatos pré-definidos quando um usuário está em uma emergência. A comunicação é feita através de mensagens de texto, nas quais a localização fixa do usuário é enviada. Além disso, há um botão específico que pode ser usado para acionar serviços de emergência, como a polícia. No entanto, é importante destacar que este trabalho não inclui instalações físicas de um centro de comando e controle para monitorar casos de alerta.

Diversos aplicativos têm como alvo a prevenção da violência doméstica e a segurança das mulheres, incluindo os projetos (Azman et al., 2018, pp. 37–41) e (Srinivas et al., 2021, pp. 378–386). A pesquisa (Sumra et al., 2023) realiza uma interessante revisão de literatura sobre aplicativos que combatem a violência doméstica. A maioria desses aplicativos prioriza emergências, mas podem gerar custos com mensagens de texto ou chamadas enviadas para contatos de emergência cadastrados, o que pode ser um dificultador de uso para possíveis vítimas. Em contrapartida, nosso aplicativo oferece uma solução abrangente, que não necessita de envio de mensagens de texto ou chamadas telefônicas, pois existe uma central de comando e controle, dedicado ao recebimento das chamadas de emergência, proporcionando assistência rápida e segura, sem custos adicionais.

Existem aplicativos como o Red Panic Button (U. C. S. Ltd, n.d.) e o Rave Panic Button (Rave panic button, 2021), que podem ser facilmente encontrados nas lojas de aplicativos para Android e iOS. No entanto, as grandes empresas têm reconhecido a importância das funções de emergência e implementaram esses recursos nativamente nos smartphones modernos (Apple Support, 2023), (Motorola Mobility, n.d.) e (Samsung NZ, 2022). A implementação dessas funções nativas reflete a compreensão das empresas de tecnologia sobre a importância das funções de emergência, onde os usuários podem ativá-las rapidamente, mesmo em situações estresse ou pânico.

As soluções, entretanto, não mencionam os requisitos para transitar dados pessoais dos usuários de aplicativos e botões de pânico, de forma segura, por meio da Internet.

Nossa proposta de sistema, chamada AMORIS, oferece uma solução abrangente, pois possui tanto um botão de pânico físico quanto um botão de pânico digital para smartphones. Além disso, foi desenvolvido uma central de comando e controle, para receber e centralizar os pedidos de emergência, garantindo que ações para a segurança da vítima sejam tomadas rapidamente, transitando de forma criptografada, os dados dos usuários do sistema pela Internet.

Para construir o botão de pânico físico, utilizou-se um microcontrolador ESP32 com GPS integrado, a fim de se obter a localização em tempo real da vítima quando o botão é pressionado. Além disso, um módulo GSM foi empregado para enviar solicitações de ajuda em tempo real, semelhante aos dispositivos construídos nos projetos de botão de pânico (Sunehra et al., 2020, pp. 1–5) e (Yaswanth et al., 2020, pp. 87–92). Para garantir conectividade mesmo em áreas sem acesso Wi-Fi, é utilizado um cartão SIM pré-pago com um plano ativado, permitindo o uso das redes 4G e 5G.

Foi desenvolvido um aplicativo móvel utilizando o framework React Native (React Native, n.d.), para a criação de um botão de pânico digital, compatível com os sistemas operacionais Android e iOS. Este aplicativo permite que os usuários pressionem um botão dentro da interface para solicitar assistência de segurança quando se sentirem ameaçados.

A central de comando e controle desempenha um papel crucial na arquitetura, permitindo que a equipe de segurança receba chamadas de socorro e tenha acesso à localização da vítima e informações relevantes. A Tabela 1 apresenta uma comparação entre nossa solução abrangente e as soluções mencionadas anteriormente.

Referência	Botão de Pânico Físico	Botão de Pânico Digital	Central de Comando e Controle
(Awodeyi et al., 2018, pp. 649–652)	Sim	Não	Sim
(Prayogo et al., 2019)	Sim	Não	Não
(Damayanti et al., 2019, pp. 1–5)	Sim	Não	Sim
(Azman et al., 2018, pp. 37–41)	Sim	Sim	Não
(Srinivas et al., 2021, pp. 378–386)	Não	Sim	Não
(Sunehra et al., 2020, pp. 1–5)	Sim	Não	Não
(Yaswanth et al., 2020, pp. 87–92)	Sim	Não	Não
Projeto Amoris	Sim	Sim	Sim

Tabela 1 – Comparação das Características dos Trabalhos Relacionados

3. Metodologia

3.1. Arquitetura Proposta

Garantir a segurança e proteção dos seus alunos e funcionários é uma das principais prioridades da Universidade de Brasília. Para alcançar esse objetivo, a universidade desenvolveu o projeto AMORIS, um sistema abrangente que engloba um aplicativo móvel, uma nuvem IoT, um botão de pânico físico e um painel de comando e controle

para a equipe de segurança, como mostra a Figura 1. Essa proposta assegura que os tempos de resposta a um pedido de socorro em emergências sejam rápidos e confiáveis.

A nuvem IoT é o alicerce do projeto, sendo o principal canal de comunicação entre o aplicativo móvel, o botão de pânico e o painel de controle utilizado pela equipe de segurança. Todos os pedidos de socorro e registros de usuários são transmitidos para a nuvem IoT que possui uma API de serviço e um banco de dados relacional, onde todos os pedidos de socorro serão armazenados de forma segura em um banco de dados. Isso permite que a universidade tenha um registro completo de todos os incidentes, e possa tomar medidas proativas para prevenir ocorrências futuras.

Um dos componentes do projeto AMORIS é o aplicativo móvel, que proporciona uma interface fluida entre os usuários e os serviços de segurança da universidade. O design elegante e a interface intuitiva do aplicativo facilitam o acesso dos usuários aos serviços de emergência, com apenas um toque de botão. O aplicativo também possui capacidade de compartilhamento de localização do usuário, permitindo que a equipe de segurança possa chegar à vítima com precisão. Já o botão de pânico físico é um componente de hardware com o mesmo objetivo. A distinção entre o botão de pânico físico e o digital é que o primeiro não depende de um smartphone para funcionar, mas sim de um dispositivo físico independente.

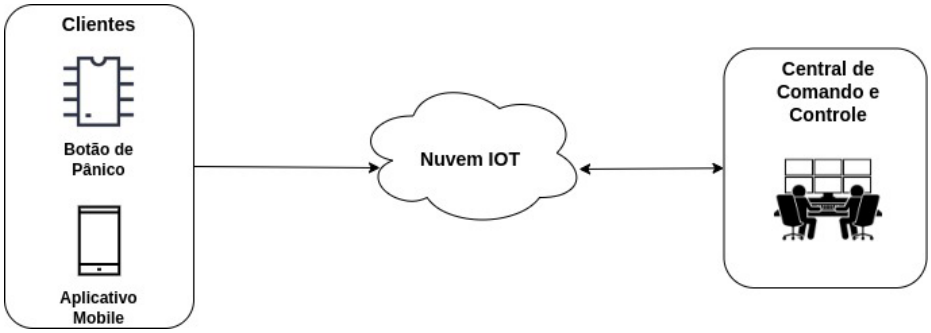

Figura 1 – Arquitetura Proposta

3.2. Nuvem IOT

A arquitetura proposta nesse trabalho é a cliente-servidor e foi elaborada para promover uma comunicação fluida entre os diferentes dispositivos, na qual os servidores fornecem os serviços de dados e os clientes os consomem. Para isso, um banco de dados relacional armazena os dados transitados pela API Restful ou Middleware, os quais atuam como o servidor, enquanto o botão de pânico, aplicativo móvel e painel de controle consomem e enviam dados a API.

A ferramenta NodeJS foi utilizada para implementar a API, por ser um software de código aberto que utiliza a linguagem de programação JavaScript, altamente presente em ambiente web.

Para facilitar a comunicação entre o cliente e o servidor, o cliente envia requisições HTTP para as rotas do servidor. Essas rotas utilizam o conceito de especialização para retornar os dados solicitados. Dentro desta arquitetura proposta, três rotas são de vital importância: as rotas de Usuário, Sessão e SOS.

A rota de Usuário atua como ponto de contato para todas as operações, regras de negócio e dados de usuário no sistema. Ela possui um conjunto de quatro rotas diferentes, responsáveis pelo registro de novos usuários, atualização de dados de usuário, listagem de todos os usuários registrados e fornecimento de informações específicas de um usuário.

A autenticação entre o cliente e o servidor é facilitada através da rota de Sessão, que utiliza o JSON Web Token (JWT) para realizar essa tarefa. O token JWT utiliza criptografia SHA-256 e é transmitido como um objeto JSON, auxiliando na autenticação das requisições web.

Para concluir, a rota de SOS oferece um meio para os usuários solicitarem ajuda da segurança da universidade. Ela possui um conjunto de três rotas diferentes, permitindo aos usuários registrarem uma nova solicitação de ajuda, alterar o status da solicitação e acessar todas as solicitações de ajuda registradas. No entanto, a arquitetura proposta tem uma limitação, pois requer conectividade Wi-Fi ou de rede móvel para utilizar o serviço.

3.3. Aplicativo Móvel

O aplicativo móvel foi desenvolvido utilizando a biblioteca React Native, para ser compatível tanto com sistema operacional iOS quanto Android, a fim de atingir o maior número de membros da comunidade acadêmica.

Para que possam acessar as funções do aplicativo, os usuários devem se cadastrar e fornecer dados pessoais, em especial o e-mail institucional. Esse processo de verificação auxilia a prevenir contas falsas de usarem os serviços. Uma vez registrados, usuários podem facilmente utilizar as funções disponíveis.

A principal função do aplicativo móvel é solicitar serviço de ajuda, de forma acessível, por meio do acionamento de um botão virtual na tela principal. Essa funcionalidade imediatamente envia alertas para a segurança universitária. Entretanto é essencial assegurar que o usuário esteja logado e tenha concedido permissão para que o aplicativo possa coletar seus dados de localização. A Figura 2 ilustra o processo de envio do pedido de ajuda dentro do aplicativo.

Apesar das vantagens, o aplicativo exige que o dispositivo tenha acesso à Internet, seja por redes móveis ou Wi-Fi, fazendo com que não seja tão efetivo em áreas com pouca ou nenhuma cobertura de rede. Essa limitação pode se tornar relevante em emergências, nas quais a conectividade esteja comprometida. Contudo, o aplicativo móvel é uma ferramenta para reforço da segurança do campus e promoção de um ambiente de estudo e trabalho mais seguros.

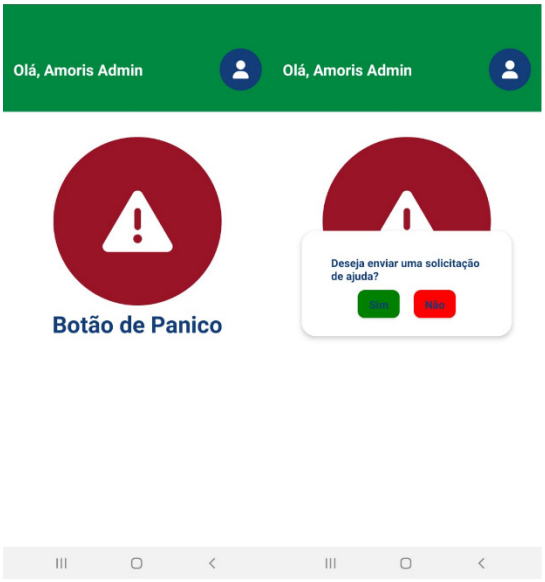

Figura 2 – Botão SOS Digital

3.4. Botão de Pânico

O desenvolvimento do botão de pânico exigiu diferentes estágios, como seleção apropriada do microcontrolador para o projeto. Nessa etapa foi escolhido o ESP32, pelo seu baixo custo e consumo de energia, além de já ser um dispositivo que provou ser uma ótima escolha para projetos IoT.

O ESP32 é equipado com processador de 32 bits, módulo Wi-Fi integrado e compatibilidade com Bluetooth, o que o fez um candidato ideal para um contexto em que seja necessária conectividade com a internet e comunicação com outros dispositivos. Essas funcionalidades facilitam a implementação de soluções de conectividade para o botão de pânico.

Além das funções de conectividade, a capacidade de processamento do ESP32 também foi um fator significativo para sua escolha. Esse microcontrolador é capaz de gerenciar tarefas complexas como leitura de sensores, envio e recebimento de dados em tempo real para servidores, fazendo-o uma excelente escolha para o projeto do botão de pânico.

Por fim, a baixa demanda por energia do ESP32 foi um fator crucial na sua escolha para o projeto. com uma única carga de bateria, o botão de pânico é capaz de funcionar por um longo período, o que é essencial para dispositivos que precisem estar sempre prontos para emergências.

A Figura 3 mostra a arquitetura proposta para o botão de pânico físico e a Figura 4 ilustra o projeto final do botão de pânico, que demandou a fabricação de um case impresso em 3D, usando material plástico ABS.

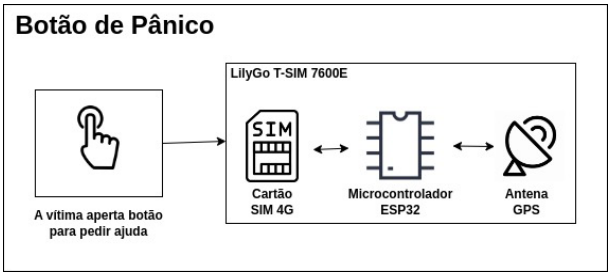

Figura 3 – Arquitetura do Botão de Pânico

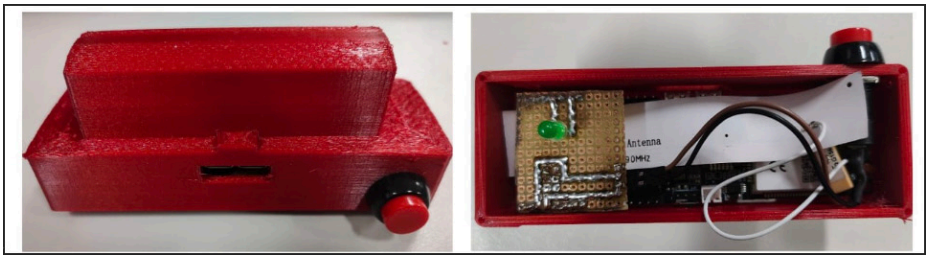

Figura 4 – Solução Completa. Dimensões 12x4 cm

3.5. Central de Comando e Controle

O desenvolvimento de um painel de controle foi um passo vital na gestão da segurança da Universidade de Brasília. O sistema foi criado para servir como mecanismo confiável e eficiente para estudantes e funcionários fazerem pedidos de socorro quando necessário. Esse objetivo foi alcançado como uso da biblioteca ReactJS, que permite a criação de aplicações web dinâmicas e altamente responsivas.

O painel de controle foi projetado para ser amigável ao usuário, os seguranças do campus, enquanto fornece notificações de chamados em tempo real, enquanto a localização, nome e número de telefone do solicitante são disponibilizados para contato. Essa funcionalidade permite que os profissionais de segurança possam rapidamente identificar a localização do pedido, e tomar medidas e ações apropriadas.

Um dos benefícios do painel de controle para a equipe de segurança, é a capacidade de gerenciar elevada carga de solicitações de socorro, assegurando que todos os pedidos sejam endereçados ao longo do tempo. Além disso, o painel de controle é otimizado para perplexidade, permitindo que a segurança acesse informações críticas de forma eficiente.

3.5. Monitoramento Inteligente do Estado da Vítima

A importância de conhecer a posição da vítima não pode ser exagerada, especialmente em emergências envolvendo crimes. O artigo (Yoon et al., 2016) esclarece a importância da localização da vítima em alguns cenários.

De acordo com o artigo, a informação precisa do local e estado físico da vítima dentro de instalações é altamente importante para respostas de emergência durante desastres. Esse conceito se estende para situações além de desastres naturais e calamidades, incluindo casos criminais em que a vítima esteja sob perigo imediato.

O sistema iRescue, como descrito no artigo, apresenta uma solução que vence esse desafio. Ele alavanca a tecnologia dos aparelhos móveis para ajudar equipes de emergência a localizar e acessar vítimas após calamidades. Um dos componentes chaves do sistema iRescue é seu sistema de posicionamento da vítima (VPS), o qual utiliza sinais de Wi-Fi para estabelecer uma trilha de sinais no mapa da edificação. Por essa abordagem, o sistema é capaz de determinar a localização das vítimas com elevada precisão.

O entendimento da localização da vítima, no contexto do aplicativo móvel de botão de pânico, em casos criminais, também se torna de grande importância. Pela incorporação de princípios e técnicas mencionados no artigo, o aplicativo móvel pode fornecer imediata e precisa localização e estado da vítima para equipes de segurança.

A combinação da tecnologia de localização da vítima e o aplicativo do botão de pânico em casos criminais, detêm grande potencial, aumentando a capacidade de resposta das equipes de emergência, provendo recursos informacionais, para que a eficiência e efetividade de operações de emergência possam ser melhoradas substancialmente.

Por isso, propusemos o uso de modelo de aprendizado de (Malekzadeh et al., 2018, pp. 2:1–2:6), treinado a partir de bases de dados de movimentações (Motionsense), com o objetivo de inferir informações sobre o estado da vítima a partir da dinâmica de seus dados de localização.

A base de dados de inclui séries temporais, dados de acelerômetros e giroscópios, gravidade, aceleração e rotação do usuário. Os dados foram coletados utilizando-se um dispositivo Apple Iphone 6S, no bolso frontal de participantes, juntamente com o framework SensingKit, o qual captura informações do processador de movimento de dispositivos iOS.

Com os dados de 24 participantes de diferentes gêneros, idades, pesos e alturas, a base de dados abrange seis atividades (descer escadas, subir escadas, caminhar, correr, sentar e parar em pé), conduzidas em condições similares entre todos.

O objetivo é descobrir diferentes padrões nos dados dos sensores que correspondam a atributos individuas, como gênero ou personalidade. Esses padrões de atributos pré especificados podem ser usados para inferir atividades e outros atributos.

Treinando o algoritmo de aprendizado de máquina com essa base de dados, podemos identificar padrões e classificar os estados do usuário em tempo real. Analisando os dados dos sensores, o modelo é capaz de forma inteligente, habilitar ou desabilitar a função GPS. Dessa forma, a economia de energia pode ser significativa, enquanto a capacidade de manter a localização é mantida.

Por fim, a aplicação proposta envolve o uso de modelos treinados com a base Motionsense para prever o estado do usuário e otimizar a energia gasta durante o uso do GPS. Essa abordagem economizaria energia e acrescentaria o reconhecimento e inferência de atributos pessoais da vítima.

4. Testes e Resultados

4.1. Nuvem IOT

A Nuvem de IoT desempenha um papel crucial na arquitetura, atuando como o elo de comunicação entre clientes e servidores. Portanto, garantir a sua disponibilidade contínua para receber requisições, provenientes tanto do aplicativo móvel quanto do botão de pânico, é de extrema importância. Isso é essencial para assegurar o registro preciso e a transmissão eficiente de todas as solicitações de socorro para a central de comando e controle.

A fim de testar a resiliência do ambiente, foram realizados testes de estresse na API localizada dentro da Nuvem de IoT para garantir que, mesmo sob alto acesso e volumes substanciais de solicitações de SOS concorrentes, o serviço suportaria essa carga.

O teste inicial realizado teve uma duração de aproximadamente 6 minutos e objetivou aumentar progressivamente o número de usuários enviando solicitações simultaneamente. O número total de solicitações enviadas durante o experimento foi de 11.131. O teste iniciou com um único usuário e finalizou com seis usuários. Os resultados obtidos nos testes podem ser observados na Figura 5, enquanto a Figura 6 ilustra os gráficos para “Total de Solicitações por Segundo”, “Tempo de Resposta (ms)” e “Número de Usuários”, respectivamente.

Método	Nome	# Requisições	# Falhas	Média (ms)	Min (ms)	Max (ms)	Tamanho médio (bytes)	RPS	Falhas/s
POST	/sos	11131	0	112	47	938	88	30.7	0.0
	Agragado	**11131**	**0**	**112**	**47**	**938**	**88**	**30.7**	**0.0**

Figura 5 – Resultado do primeiro teste de requisições

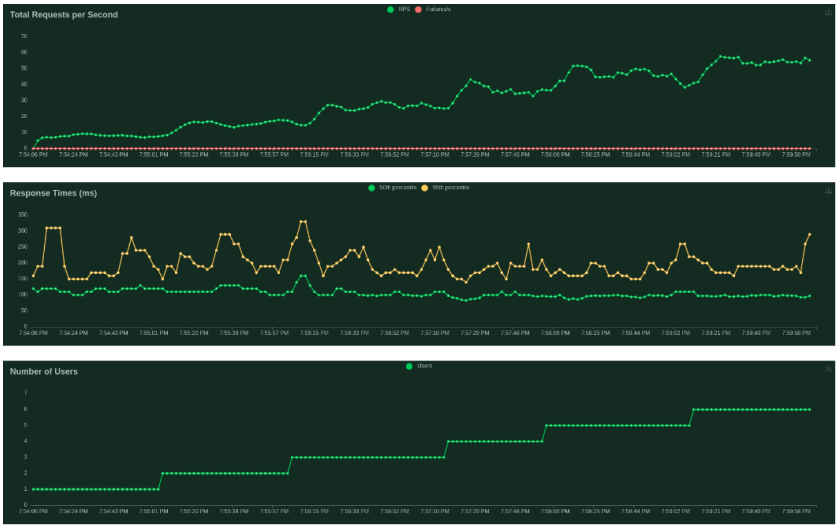

Figura 6 – Resultado do primeiro teste de requisições. O primeiro gráfico se refere ao Total de Requisições por Segundo. O segundo gráfico se refere ao Tempo de Resposta em ms. O terceiro grafo se refere a Quantidade de Usuários.

A partir dos resultados dos testes, pode-se observar que o tempo de resposta da API não sofreu alterações significativas à medida que o número de usuários aumentou, também não sendo detectadas falhas durante o período de teste.

O segundo teste foi realizado simulando o envio de solicitações de socorro por um grupo de usuários, além de outro grupo iniciando a sessão no aplicativo móvel.

O segundo teste teve uma duração de aproximadamente 9 minutos e teve como objetivo aumentar progressivamente o número de usuários enviando solicitações simultaneamente para as rotas de SOS e Sessões. O número total de solicitações enviadas durante o experimento foi de 18.089. O teste iniciou com um único usuário e finalizou com dez usuários. Os resultados obtidos nos testes podem ser observados na Figura 7, enquanto a Figura 8 ilustra os gráficos para “Total de Solicitações por Segundo”, “Tempo de Resposta (ms)” e “Número de Usuários”, respectivamente.

Método	Nome	# Requisições	# Falhas	Média (ms)	Min (ms)	Max (ms)	Tamanho médio (bytes)	RPS	Falhas/s
POST	/sessions	8993	0	166	73	1129	409	16.0	0.0
POST	/sos	9096	0	196	62	1779	89	16.1	0.0
	Agregado	**18089**	**0**	**181**	**62**	**1779**	**248**	**32.1**	**0.0**

Figura 7 – Resultado do segundo teste de requisições

Figura 8 – Resultado do segundo teste de requisições. O primeiro gráfico se refere ao Total de Requisições por Segundo. O segundo gráfico se refere ao Tempo de Resposta em ms. O terceiro grafo se refere a Quantidade de Usuários.

Mais uma vez, os testes mostram que mesmo com um alto número de solicitações por segundo, não há indicação de falha ou instabilidade na API localizada na Nuvem IoT.

Os testes realizados demonstram a robustez e confiabilidade da arquitetura proposta. Mesmo sob cargas elevadas de requisições, tanto para solicitações de SOS quanto para inicializações de Sessões, a API na Nuvem de IoT se mostrou confiável, sem apresentar sinais de falha ou instabilidade. Isso reforça a capacidade do sistema em lidar eficientemente com emergências, garantindo uma resposta rápida e precisa. A integração bem-sucedida entre o aplicativo móvel, botão de pânico e a infraestrutura de segurança da universidade destaca a eficácia do projeto AMORIS em assegurar a segurança e proteção dos membros da comunidade acadêmica da Universidade de Brasília.

4.1. Aplicativo Móvel

O aplicativo móvel por sua vez necessita de uma rápida comunicação com a API para, em caso de emergência, o sinal de SOS ser emitido o mais rápido possível. Para garantir essa entrega rápida, foram realizados testes de tempo de resposta no dispositivo móvel, avaliando todo o processo desde o clique da confirmação da solicitação até o recebimento da resposta, o que garante a entrega do pedido de socorro à aplicação como um todo, logo, à equipe de segurança.

Neste teste, foi utilizado um dispositivo móvel da fabricante Samsung, modelo SM-M625F/DS, sendo realizadas 20 solicitações manualmente. Os tempos obtidos são exibidos na Figura 9. Nota-se um tempo crescente nas 7 primeiras solicitações, uma oscilação entre a 8ª e a 12ª solicitação e por fim uma normalização dos tempos, um possível fator para tal distúrbio é a utilização da rede móvel do celular, assim como possíveis variações no tempo para obter a localização pelo GPS.

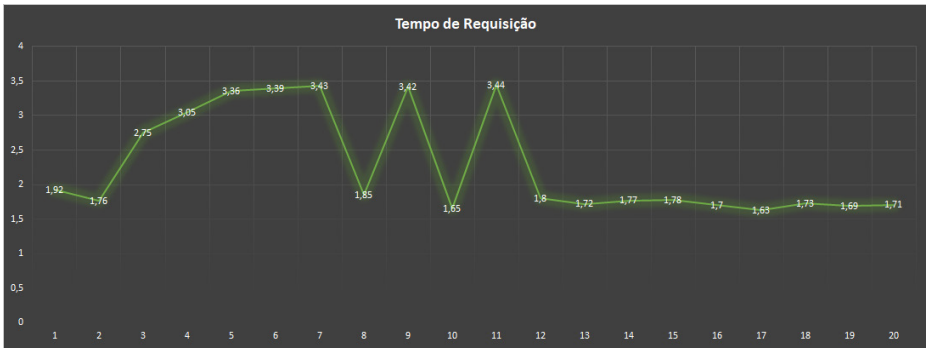

Figura 9 – Tempo de resposta de cada solicitação do teste da aplicação.

Os testes mostraram um tempo médio de resposta de 2,28 segundos, com tempo máximo de 3,44 segundos e o mínimo 1,63. O que mostra possíveis melhorias a serem implementadas no software mas garante o envio da solicitação em tempo hábil. Já considerando apenas as solicitações após a normalização da rede móvel, obteve-se uma média de 1,73 segundos entre a décima segunda e a vigésima solicitação, com máxima de 1,8 segundos e mínima de 1,63 segundos.

5. Conclusão

Os testes realizados demonstram a robustez e confiabilidade da arquitetura proposta. Mesmo sob cargas elevadas de requisições, tanto para solicitações de SOS quanto para inicializações de Sessões, a API na Nuvem de IoT se mostrou confiável, sem apresentar sinais de falha ou instabilidade. Isso reforça a capacidade do sistema em lidar eficientemente com emergências, garantindo uma resposta rápida e precisa.

Foram feitas integrações bem-sucedida entre o aplicativo móvel, botão de pânico e a infraestrutura de segurança da universidade destaca, onde em apenas poucos segundos é possível realizar um pedido de socorro e ter seu pedido visualizado e atendido pela equipe de segurança. Essa integração foi realizada com segurança na comunicação, onde é necessária uma autenticação através de um token JWT para realizar requisições para Nuvem IoT.

É possível então, concluir que, em conjunto, todos esses elementos demonstram o sucesso do projeto AMORIS em criar uma solução abrangente e confiável para garantir a segurança e proteção da comunidade acadêmica da Universidade de Brasília, além de possibilitar o desenvolvimento de soluções agregadas a este trabalho, como por exemplo, a construção de camadas de inteligência dentro na Nuvem IoT, que teriam como funcionalidade a priorização de pedidos de socorro, bem como a atribuição da prestação de socorro à equipe de segurança mais próxima do local do pedido de socorro.

Como trabalhos futuros, têm-se a potencialização da Nuvem IoT e dos botões de pânico, através de uma abordagem para a implementação da funcionalidade de envio e compartilhamento da localização em tempo real, visando aprimorar a precisão na identificação da localização das vítimas. Nesse sentido, é necessário aprimorar a eficiência do botão de pânico para otimizar o consumo de energia, garantindo uma operação contínua e eficaz.

Quanto ao aplicativo móvel, têm-se como objetivo a implementação de uma opção de envio de localização em tempo real, de modo que a equipe de segurança possa atender e acompanhar com mais precisão a todos os tipos de pedidos de socorro. Já visando a segurança e comodidade dos usuários, estuda-se a possibilidade de integração de login diretamente pela conta institucional da universidade ou até mesmo pelo Login Único do governo brasileiro (GOV BR).

Outro caminho promissor é a exploração de técnicas avançadas de inteligência artificial na Nuvem IoT, com o objetivo de priorizar pedidos de socorro de maneira mais inteligente. Sistemas de aprendizado de máquina podem ser empregados para analisar padrões e contextos, proporcionando respostas rápidas e adaptadas a situações específicas, ampliando a eficácia do sistema em situações críticas.

Também pode-se considerar a adaptação do sistema AMORIS para ambientes além do acadêmico. Esta perspectiva amplia o alcance do projeto, possibilitando a sua aplicação em diferentes contextos, como ambientes urbanos, industriais ou de saúde.

Ao direcionar esforços para essas áreas, o projeto pode não apenas consolidar seu papel como solução de segurança eficiente, mas também posicionar-se como uma iniciativa inovadora, adaptável e de impacto em diversos cenários e contextos.

Agradecimentos

Os autores agradecem o apoio técnico e computacional do Laboratório LATITUDE, da Universidade de Brasília, ao TED 01/2019 da Advocacia Geral da União (Outorga AGU 697.935/2019), ao TED 01/2021 da Secretaria Nacional de Assistência Social – SNAS/DGSUAS/CGRS ao Decanato de Pesquisa e Inovação - DPI (Outorga 7129 FUB/EMENDA/DPI/COPEI/AMORIS) ao Projeto SISTER City –Sistemas Inteligentes Seguros e em Tempo Efetivo Real para Cidades Inteligentes (Outorga 625/2022), a FAP/DF e ao INDT Instituto de Desenvolvimento Tecnológico

Referências

Agência Brasil. (2023, março). No Brasil, uma mulher é vítima de violência a cada quatro horas. Agência Brasil. https://agenciabrasil.ebc.com.br/geral/noticia/2023-03/no-brasil-uma-mulher-e-vitima-de-violencia-cada-quatro-horas

Apple Support. (2023, April). Set up emergency information on my iPhone. https://support.apple.com/en-us/HT208076

Awodeyi, A. I., Moses, O., Opeyemi, M., & Abraham, B.-O. (2018). Design and construction of a panic button alarm system for security emergencies. International Journal of Engineering and Techniques, 4(3), 649–652.

Azman, F., Suraya, Q., Rahim, F. A., Mohd, M. S., & Mohd Ariffin, N. A. (2018). My Guardian: A personal safety mobile application. In 2018 IEEE Conference on Open Systems (ICOS) (pp. 37–41). https://doi.org/10.1109/ICOS.2018.8632808

Biradar, P., Kolsure, P., Khodaskar, S., & Bhangale, K. B. (2020). IoT based smart bracelet for women security. International Journal of Research in Applied Science & Engineering Technology (IJRASET), 8(11), 688–691.

Damayanti, S. D., Suryanegara, M., Enriko, I. K. A., & Nashiruddin, M. I. (2019). Designing a LoRa-based panic button for Bali Smart Island project. In 2019 7th International Conference on Smart Computing & Communications (ICSCC) (pp. 1–5). https://doi.org/10.1109/ICSCC.2019.8843614

K. Srinivas, S. Gothane, C. S. Krithika, A. Anshika, & T. Susmitha. (2021). Android app for women safety. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 7(3), 378-386. https://doi.org/10.32628/CSEIT1217368

Malekzadeh, M., Clegg, R. G., Cavallaro, A., & Haddadi, H. (2018). Protecting sensory data against sensitive inferences. In Proceedings of the 1st Workshop on Privacy by Design in Distributed Systems (W-P2DS'18) (pp. 2:1–2:6). ACM. https://doi.org/10.1145/3195258.3195260

Motorola Mobility. (n.d.). Set up emergency information on my Motorola phone. https://en-in.support.motorola.com/app/answers/detail/a_id/133870/~/emergency-information

Nasir, N.H., Lestari, F. and Kadir, A. (2022), "Android-based Mobile Panic Button UI application design development in responding to emergency situations in Universitas Indonesia (UI)", International Journal of Emergency Services, Vol. 11 No. 3, pp. 445-470. https://doi.org/10.1108/IJES-07-2020-0041

Prayogo, S. S., Al Rafi, F., & Mukhlis, Y. (2019). Design and built IoT home panic button for smart city. Journal of Physics: Conference Series, 1175, 012097. https://doi.org/10.1088/1742-6596/1175/1/012097

Rave Mobile Safety. (2021, June). Rave panic button. Retrieved April 15, 2024, from https://www.ravemobilesafety.com/products/rave-panic-button

React Native. (n.d.). React Native. https://reactnative.dev/

Samsung NZ. (2022, May). Samsung SOS smart phone emergency message guide. https://www.samsung.com/nz/support/mobile-devices/samsung-sos-smart-phone-emergency-message-guide/

Sumra, M., Asghar, S., Khan, K. S., Fernández-Luna, J. M., Huete, J. F., & Bueno-Cavanillas, A. (2023). Smartphone apps for domestic violence prevention: A systematic review. International Journal of Environmental Research and Public Health, 20, 5246. https://doi.org/10.3390/ijerph20075246

Sunehra, D., Sreshta, V. S., Shashank, V., & Kumar Goud, B. U. (2020). Raspberry Pi based smart wearable device for women safety using GPS and GSM technology. In 2020 IEEE International Conference for Innovation in Technology (INOCON) (pp. 1–5). https://doi.org/10.1109/INOCON50539.2020.9298449

Swathi, S., Nidhishree, V., RamyaC, V. M., Ashwini, A., & others. (2022). Women safety device using panic button. Journal of Algebraic Statistics, 13(3), 5337–5342.

Thamaraiselvi, K., Rinesh, S., Ramaparvathy, L., & Karthick, V. (2019). Internet of Things (IoT) based smart band to ensure the security for women. In 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1093–1096). https://doi.org/10.1109/ICSSIT46314.2019.8987928

U. C. S. Ltd. (n.d.). Red Panic Button app – Safety app for emergency – SOS call app for iOS and Android. https://www.redpanicbutton.com

Yaswanth, B. S., Darshan, R. S., Pavan, H., Srinivasa, D. B., & Murthy, B. T. V. (2020). Smart safety and security solution for women using kNN algorithm and IoT. In *2020 Third International Conference on Multimedia Processing, Communication & Information Technology (MPCIT)* (pp. 87–92). https://doi.org/10.1109/MPCIT51588.2020.9350431

Yoon, H., Shiftehfar, R., Cho, S., Spencer, B. F. Jr., Nelson, M. E., & Agha, G. (2016). Victim localization and assessment system for emergency responders. Journal of Computing in Civil Engineering, 30(2), 04015011. https://doi.org/10.1061/(ASCE)CP.1943-5487.0000483