

Proposição de um Sistema de Autenticação Simplificado e Interativo com Dispositivo IoT

**Fabio Lopes Brezolin¹, Erciles Andrei Bellei¹, Jucélia Giacomelli Beux¹,
Marco A. Sandini Trentin¹, Angelo Elias Dalzotto², Joao Mário L. Brezolin³**

¹ Programa de Pós-Graduação em Computação Aplicada (PPGCA)
Universidade de Passo Fundo – Caixa Postal 611 – 99.001-970 – Passo Fundo – RS

² Curso de Engenharia de Computação – Universidade de Passo Fundo

³ Instituto Federal Sul-rio-grandense – Passo Fundo – RS

{71856, 168729, 68428, trentin, 150633}@upf.br,
joao.brezolin@passofundo.ifrsul.edu.br

Abstract. *IoT devices become popular and the use of their resources extends into the possibility of creating interactive environments. However, this technology still seems to be restricted to people who have technical mastery of equipment and systems capable of supporting these environments. This study presents the development of an interactive authentication system with an IoT device, which allows people unfamiliar with technologies to understand the access control context while interacting with their resources in the access system made available on a web platform for visualization of data generated by the IoT device.*

Resumo. *Dispositivos IoT se popularizam e a utilização de seus recursos se estende na possibilidade de criar ambientes interativos. Entretanto, essas tecnologias ainda aparentam ser restritas a pessoas com domínio técnico de equipamentos e sistemas que dão suporte a esses ambientes. Neste estudo, é apresentado o desenvolvimento de um sistema de autenticação interativo com um dispositivo IoT que possibilita que pessoas não familiarizadas com tais tecnologias compreendam o contexto de controle de acesso e interajam com seus recursos, por meio um sistema de acesso disponibilizado em uma plataforma web para visualização dos dados oriundos do dispositivo IoT.*

1. Introdução

A convergência de diversas tecnologias surgidas nas últimas décadas permitiu a criação de ambientes interativos repletos de recursos e possibilidades. A Internet das Coisas (IoT) representa um novo paradigma que permite que as pessoas interajam com um ambiente por meio de dispositivos eletrônicos, sem ter de conhecer aspectos técnicos dos sistemas [Weiser 1991]. Nesses ambientes inteligentes, apresentam-se novos recursos de baixo custo e com ênfase na mobilidade. O desafio, nesse contexto, é desenvolver plataformas ou sistemas seguros e, ao mesmo tempo, acessíveis para o usuário comum.

Entretanto, a complexidade de aliar recursos computacionais heterogêneos nem sempre é traduzida em sistemas fáceis de serem utilizados pelo usuário comum. Para estabelecer uma experiência agradável e intuitiva, é preciso desenvolver soluções que abstraiam características técnicas de funcionamento e disponibilizem serviços de forma prática. Nessa perspectiva, a IoT pode permitir que as pessoas que até então não tinham

contato com dispositivos eletrônicos em rede passem a se familiarizar com essa tecnologia.

Um dos desafios associados a essa tecnologia é controlar a forma que seus serviços serão acessados por pessoas que possuem autorização. Sistemas habituais de autenticação valem-se de usuários identificados com credenciais, como *login* e senha, e um administrador de segurança e permissões que precisa do acesso a um computador. Entretanto, dispositivos de IoT podem ter a mobilidade como característica central, fazendo com que a brevidade de liberação de um administrador de segurança tenha papel central na Experiência do Usuário – UX, de *User Experience*.

A UX orienta-se com questões de contexto, como por exemplo o *design* estético, que garante que um botão tenha aparência agradável, enquanto o *design* funcional garante que o botão ative a função desejada corretamente. O *design* de experiência de usuário garante que o estético e o funcional operem com o contexto do resto do produto, garantindo que atenda às necessidades que se espera atingir com ele [Garrett 2011]. Ao projetar sistemas colocando o usuário como o centro do processo de desenvolvimento, consegue-se manter o foco das necessidades do usuário final e pode-se salvar tempo de desenvolvimento, evitando possíveis erros de escopo e aceitação [Lowdermilk 2013].

Para planejar um produto conectado no conceito de IoT, é necessária uma abordagem detalhada de experiência de usuário. Afinal, envolve muitas camadas e nem todas estão visíveis, porém há uma necessidade de colaboração entre diversas áreas. As novas tecnologias, incluindo a IoT, viabilizaram muitas possibilidades, sistemas e soluções acessíveis aos consumidores antes jamais imaginados. O estudo de Shi *et al.* (2017) apresenta um modelo de autenticação para dispositivos IoT utilizando o sinal de Wi-Fi para perceber a movimentação e gestos do usuário e disponibilizar serviços de dispositivos. Seu trabalho apresentou uma evolução na segurança dos sistemas de acesso ao possibilitar uma personalização da segurança dos dispositivos.

Considera-se a hipótese de que um sistema móvel de autenticação, no qual o administrador de segurança, de posse de um smartphone identificado, pode decidir se autoriza ou não o acesso a um dispositivo. A proposta deste estudo é a apresentação de uma abordagem para sua utilização em controle de acesso em casos simples, que mais tarde será testada com usuários para validação de aceitação. Essa proposta é demonstrada com um sistema web integrado a um dispositivo IoT que obtém dados de variáveis ambientais sobre a qualidade do ar e apresenta essas informações em uma página web. A interface da página web permite ao usuário se identificar de forma acessível e intuitiva, onde o administrador de segurança pode, por meio de um *smartphone*, liberar o acesso ao sistema, independentemente de sua localização. Da mesma forma, a abordagem proposta visa abreviar o controle de acesso para torná-lo simplificado e alinhado a casos simples, proporcionando ao usuário uma experiência agradável de interação.

No capítulo 2, apresenta-se o Dispositivo Brezobomba, detalhando o projeto de hardware do dispositivo IoT envolvido no estudo. Nesse capítulo também é apresentado o modelo de autenticação do dispositivo. Por fim, em Considerações Finais estão algumas observações sobre os objetivos alcançados e os próximos passos deste projeto.

2. O Dispositivo Brezobomba

Tecnologias IoT vêm sendo utilizadas para criar ambientes interativos, porém poucos estudos abordam a usabilidade dos sistemas de acesso desses dispositivos. Para criar um cenário de testes que possibilite avaliar a interação entre as pessoas e um dispositivo IoT,

foi desenvolvido o dispositivo Brezobomba. O diferencial desse dispositivo é sua simplicidade de utilização, em uma forma de introduzir pessoas que estão familiarizadas com o uso de computadores e smartphones, porém sem conhecimento avançado de como se relacionar com aparelhos que permitam interação.

O objetivo da Brezobomba é capturar dados do ambiente através de sensores, disponibilizar localmente essa informação e também transmiti-la para um servidor web, onde os dados podem ser repassados para visualização de usuários. O dispositivo possui uma estrutura em ferro de um extintor de incêndio, como reaproveitamento de materiais, que permite sua aplicação em ambientes externos, preservando a integridade dos elementos eletrônicos em seu interior. O projeto da Brezobomba, visto na Figura 1, busca traduzir a urgência da preocupação com a qualidade do ar com o desenho de uma bomba.



Figura 1. O Dispositivo Brezobomba

Os elementos de hardware que compõem a Brezobomba estão esquematizados na ilustração da Figura 2 e explicados no texto subsequente.

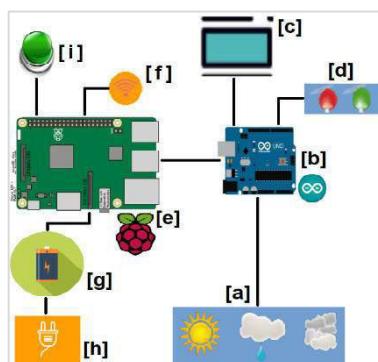


Figura 2. Arquitetura de hardware da Brezobomba

O dispositivo possui sensores [a] que aferem no ambiente os dados de umidade, temperatura e índice de CO₂ e transmitem os mesmos para um Arduino Uno [b]. Esse tem a função de exibir os dados em um monitor de LCD local [c] e controlar um sistema de aviso com luzes LED [d], no qual a concentração de CO₂ é representada com a luz verde, para casos de concentração até 420 ppm, ou vermelha, para valores acima de 420 ppm. O Arduino Uno [b] também transmite os dados para publicação através de um Raspberry Pi [e], que é responsável por receber esses dados e transmiti-los através de uma conexão Wi-Fi [f] para um servidor web. O Raspberry Pi fornece energia a todo o dispositivo, suportado por uma bateria [g], que é carregada através de uma tomada externa [h]. Essa estrutura permite que a Brezobomba tenha sua aplicação por determinado tempo em locais diversos, independentemente da existência de uma fonte de energia próxima, desde que conte com a presença de sinal Wi-Fi. Por fim, é disponibilizado o botão de

interação [i] que, quando executado, informa em tempo real os dados coletados assim como o aviso de alerta de concentração de CO₂ em níveis críticos.

Ao inicializar a Brezobomba, o sistema operacional Raspbian do Raspberry Pi é inicializado. Com ele, é carregado um software, desenvolvido em linguagem Python, que trabalha na aquisição de dados. As informações de umidade e temperatura chegam ao Raspberry por meio de um protocolo serial com um sensor DHT22. O Arduino Uno captura leituras analógicas de um sensor MQ-135, que é um sensor eletroquímico que identifica a concentração de CO₂. A comunicação entre o Arduino e o Raspberry acontece por meio do barramento I2C. O Arduino executa um firmware simples I2C-slave no qual realiza leituras da porta analógica escolhida.

2.1. Arquitetura do Sistema

Uma plataforma, após receber os dados capturados pela Brezobomba, tem a atribuição de armazenar os dados aferidos em um banco de dados relacional e publicá-los em tempo real, para visualização em uma interface gráfica em uma página web. O ciclo dos dados e organização dos componentes da plataforma é ilustrado na Figura 3.

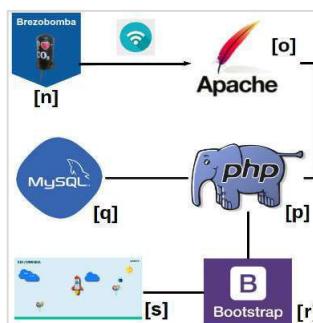


Figura 3. Arquitetura da plataforma

A transmissão dos dados aferidos pela Brezobomba [n] para o restante da plataforma ocorre a cada 60 segundos, independentemente da existência de requisições de usuários. Para recepção dos dados, a plataforma conta um servidor web Apache [o]. Os dados recebidos são armazenados em um banco de dados relacional MySQL [q], que é acessado e gerenciado com webservices criados em linguagem PHP [p]. Além disso, acontece a comunicação entre os webservices e a interface gráfica, criada com o framework Bootstrap [r], para exibição [s] dos dados aos usuários.

A interface, que é exibida após o controle de acesso concedido ao usuário, tem o objetivo de tornar a informação comprehensível também de maneira lúdica. A Figura 4 exemplifica como são apresentados na interface os dados capturados pela Brezobomba em um determinado ambiente.



Figura 4. Interface gráfica da página web para visualização dos dados

Os dados de umidade e temperatura são representados pelas nuvens [j] e pelo sol [k], que no caso da Figura 4 estão, respectivamente, com 44.3 % e 18 °C. No conjunto de balões [l], é apresentada a concentração de CO₂, em 320,4 ppm no caso ilustrado. O sistema verifica se a concentração de CO₂ está acima de 420 ppm e, se sim, apresenta uma tela de aviso de perigo para aquele ambiente. A interface gráfica permite ao usuário, por meio do ícone da Brezobomba [m], utilizar o botão de interação do dispositivo para simular o aviso de perigo de níveis críticos de CO₂.

2.2. O Controle de Acesso e Abordagem de Ensino

Roman *et al.* (2011) explicam que os sistemas IoT para se tornarem totalmente incorporados à realidade de utilização, devem ser testados quanto sua segurança. Apontam, ainda, que as tradicionais técnicas de segurança não são suficientes para garantir todas as necessidades desses novos ambientes, cabendo aos pesquisadores descobrir a real extensão de tais obstáculos. Vermesan e Friess (2013) esclarecem que a segurança de dispositivos IoT requer uma variedade de controles de acesso associados a papéis de usuários e esquemas de utilização. A heterogeneidade e diversidade dos dispositivos requerem o desenvolvimento de um controle de acesso leve e adaptado ao contexto de aplicação.

Na Figura 5 é ilustrado o modelo de funcionamento do controle de acesso do sistema da Brezobomba, envolvendo usuários, administradores e a manipulação da interface web.

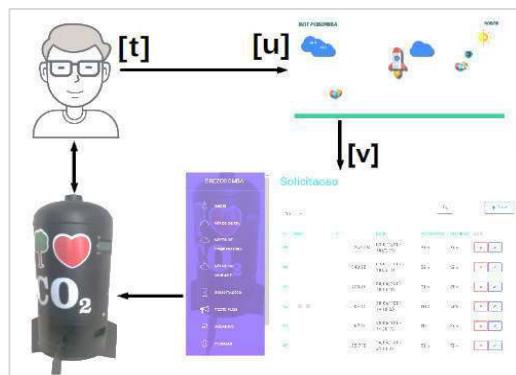


Figura 5. Esquema de autenticação de acesso

O usuário [t] faz uma requisição de acesso clicando no ícone da Brezobomba na interface gráfica da web [u], e se identifica informando seu nome ou vinculando sua rede social. A plataforma envia a solicitação ao painel de controle de acesso [v], que notifica com uma mensagem *push* o smartphone de um administrador responsável pela decisão de autorizar a requisição. Se autenticado pela rede social e autorizado, o usuário passa a ter direito de solicitar o botão de interação do dispositivo a qualquer momento. Por outro lado, se autenticado pelo nome, toda interação é intermediada pela autorização prévia de um administrador. O modelo de acesso ao sistema Brezobomba é gerenciado em uma interface web acessível de fácil compreensão. A interface web do administrador, apresentada na Figura 6, foi estruturada de maneira responsiva como forma para que possa ser utilizada em vários dispositivos e por pessoas leigas em tecnologia. Para ter acesso é necessário autenticar-se com nome ou a rede social.

O sistema é um modelo que tem uma abordagem educacional relevante, envolvendo e desafiando pessoas, independentemente da faixa etária ou grande conhecimento prévio, a conhecer e entender conceitos tecnológicos. A Brezobomba pode

envolver diversas áreas, sendo possível realizar trabalhos interdisciplinares em espaços públicos ou educacionais em escolas. Como é recorrente a necessidade de soluções de aprendizagem móveis sustentáveis sem incorrer em enormes custos em termos de infraestrutura [Yadav 2017], a Brezobomba se torna uma ferramenta em potencial.



Figura 6. Interface web de administrador

3. Considerações Finais

Este trabalho buscou apresentar um sistema de autenticação interativo com dispositivo IoT e demonstrar que é possível utilizar as tecnologias disponíveis, gratuitas e de baixo custo, para implementação de aparelhos IoT. Buscou-se estabelecer um acesso seguro a partir de uma política efetiva de controle de acesso simplificado. Como trabalhos futuros, pretende-se a execução de testes com usuários, vislumbrando a compreensão do contexto de utilização, para validar o objetivo da abordagem proposta, verificar sua aceitação, usabilidade e aspectos de interação do sistema, com grupos específicos em espaços públicos. Aspectos de experiência de usuário são fundamentais na construção de sistemas, inclusive no controle de acesso e sua integração com dispositivos IoT.

Referências

- Garrett, J. J. (2011). *The elements of user experience : user-centered design for the Web and beyond*. Thousand Oaks: New Riders.
- Lowdermilk, T. (2013). *User-centered design*. New York: O'Reilly Media.
- Roman, R., Najera, P. and Lopez, J. (sep 2011). Securing the Internet of Things. *Computer*, v. 44, n. 9, p. 51–58.
- Shi, C., Liu, J., Liu, H. and Chen, Y. (2017). Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT. In *18th International Symposium on Mobile Ad Hoc Networking and Computing*. ACM Press.
- Vermesan, O. and Friess, P. (2013). *Internet of things : converging technologies for smart environments and integrated ecosystems*. Aalborg: River Publishers.
- Weiser, M. (1991). The computer for the 21st century. *Scientific American*, v. 265, n. 3, p. 94–104.
- Yadav, D. (2017). Low-Cost Mobile Learning Solutions for Community Health Workers. *26th International Conference on World Wide Web Companion*, p. 729–734.