Plataforma de *Crowdsourcing Internet of Things* (Crowd-IoT) para detecção de emergências urbanas

Gabriel S. Barreto[1], Thiago C. Jesus[2], Gustavo A. A. Coelho[1], Gustavo F. Silva[1] e Daniel G. Costa[3]

[1]PGCC-UEFS, Universidade Estadual de Feira de Santana, Brasil

[2]DTEC-UEFS, Universidade Estadual de Feira de Santana, Brasil

[3]INEGI, Faculdade de Engenharia, Universidade do Porto, Portugal

gabrielalves@ecomp.uefs.br, tcjesus@uefs.br, coelho1914@gmail.com, gustavo.falcao@ifba.edu.br, danielgcosta@fe.up.pt

Abstract. *This paper proposes a platform that integrates data from IoT sensors and user contributions through crowdsourcing to achieve rapid and efficient detection of urban emergencies. The platform will provide reliable and relevant information, guiding and alerting stakeholders. The collaborative model will employe edge computing, artificial intelligence and gamification strategies to motivate contributors. Data security and privacy are prioritized. Evaluation will be based on real-world scenarios, exploring metrics such as detection time and user satisfaction, aiming to contribute to the advancement in urban emergency detection.*

Resumo. *Este artigo propõe uma plataforma que integra dados de sensores IoT e contribuições dos usuários por meio de crowdsourcing para realizar detecção rápida e eficiente de emergências urbanas. A plataforma fornecerá informações confiáveis e relevantes, orientando e alertando os envolvidos. O modelo colaborativo utilizará técnicas de computação de borda, inteligência artificial e estratégias de gamificação para motivar colaboradores. A segurança e privacidade dos dados são priorizadas. A avaliação será baseada em cenários reais, explorando métricas como tempo de detecção e satisfação do usuário, visando contribuir para o avanço na detecção de emergências urbanas.*

1. Introdução

Emergências urbanas, como acidentes de trânsito, incêndios, inundações, são eventos que podem afetar catastroficamente a qualidade de vida das pessoas nas cidades. A detecção rápida e precisa dessas emergências é essencial para acionar os serviços de socorro e mitigar os impactos negativos. No entanto, a detecção de emergências urbanas é um desafio complexo, que envolve a coleta, o processamento e a análise de grandes volumes de dados heterogêneos, provenientes de diferentes fontes [Fedele and Merenda 2020]. Assim, a *Internet of Things* (IoT) e o *crowdsourcing* surgem como paradigmas promissores para a detecção dessas emergências. A IoT permite a conexão de dispositivos e sensores

Este trabalho foi apoiado pelo Programa Interno de Auxílio Financeiro aos Programas de Pós-Graduação Stricto Sensu (AUXPPG) da UEFS e pelo Programa de Apoio à Pós-Graduação (PROAP) da CAPES.

inteligentes que podem captar e transmitir dados sobre o ambiente, como temperatura, umidade, localização, etc. O *crowdsourcing* permite a participação de pessoas equipadas com dispositivos geolocalizados, como *smartphones*, que podem fornecer informações complementares ou alternativas aos dados da IoT, como relatos, fotos, vídeos, etc. A integração da IoT e do *crowdsourcing* gera um sistema de *crowdsourcing Internet of Things* (Crowd-IoT), que combina as vantagens de ambos os paradigmas para a detecção de emergências urbanas [Ang et al. 2022, Shahrour and Xie 2021].

No entanto, uma plataforma de Crowd-IoT também apresenta desafios, como a heterogeneidade, a segurança e a privacidade dos dados, a escalabilidade, a latência e a confiabilidade do sistema, a motivação e a recompensa dos participantes, entre outros [S et al. 2023]. Assim, neste artigo propomos uma plataforma de Crowd-IoT para a detecção de emergências urbanas, integrando uma abordagem baseada em unidades multi-sensores IoT com uma abordagem colaborativa de *crowdsourcing*, visando aumentar a eficiência e a precisão das aplicações que lidam com tais emergências. A plataforma proposta utiliza técnicas de computação de borda e de névoa para distribuir o processamento e a análise dos dados entre os dispositivos IoT, os nós de borda e a nuvem, reduzindo a sobrecarga computacional e a latência do sistema. A plataforma também utiliza técnicas de inteligência artificial para extrair informações dos dados IoT e do *crowdsourcing*, e para classificar e priorizar as emergências detectadas. Técnicas de gamificação e incentivo serão implementadas para motivar e recompensar os participantes do *crowdsourcing*, e para garantir a qualidade e a confiabilidade das informações fornecidas.

O objetivo deste artigo é descrever a arquitetura e as funcionalidades de uma plataforma de Crowd-IoT para a detecção de emergências urbanas, bem como apresentar os resultados esperados de uma avaliação experimental. O artigo está organizado como segue. Na seção 2, revisamos a literatura relacionada à IoT, ao *crowdsourcing* e à detecção de emergências urbanas. Na seção 3, apresentamos a nossa proposta de plataforma de Crowd-IoT para a detecção de emergências urbanas. Na seção 4, descrevemos os resultados a serem alcançados em uma avaliação experimental. Finalmente, na seção 5, concluímos o artigo e apontamos as direções para trabalhos futuros.

2. Revisão de Literatura

A detecção de emergências urbanas é um desafio que requer soluções rápidas e precisas para minimizar danos e salvar vidas. É natural que, durante uma emergência, as agências e autoridades urbanas responsáveis para lidar com tais situações tentem coletar o máximo de informações possível para se preparar para o socorro. Porém esse processo pode ser muito moroso, de modo que pode prejudicar e atrasar bastante a detecção [Han et al. 2019]. Como solução, pode-se potencializar a conectividade ubíqua entre dispositivos diversos (dispositivos de IoT) agregando uma fonte secundária de informação (*crowdsourcing*), que gera dados mais detalhados e compreensivos que podem ser exploradas com precisão e oportunidade para melhorar a eficiência da assistência a emergências [Rauniyar et al. 2016].

No entanto, o uso do *crowdsourcing* e da IoT para a detecção de emergências urbanas também apresenta alguns desafios e limitações. Em arquiteturas centralizadas, para um grande número de usuários conectados e múltiplas interações, o grande volume de dados de sensoriamento cria sobrecargas computacionais significativas para as

técnicas de *crowdsourcing* convencional [S et al. 2023]. Eventualmente essas técnicas podem não atender aos requisitos de tarefas sensíveis ao tempo da IoT, devido a atrasos imprevistos e variações no tempo de resposta. Para isso, pode-se utilizar a abordagem de computação de borda e de névoa, que tenta usar as infraestruturas, componentes ou dispositivos atuais e circundantes para o processamento de informações e devolvê-las à nuvem [Aboualola et al. 2023, Kong et al. 2019], atendendo aos requisitos de computação, armazenamento e acesso distribuído da aplicação. Apesar dos benefícios, é crucial ponderar sobre o potencial uso mal-intencionado dos dados coletados ou detectados [Deshpande et al. 2019].

A implementação em larga escala do *crowdsourcing* suscita preocupações consideráveis em relação à privacidade. Uma razão para isso é a confiança depositada pelos usuários no servidor de *crowdsourcing*. No contexto dos participantes, as tarefas e os dados de sensoriamento podem conter informações sensíveis, como a sua localização [Shahrour and Xie 2021]. Reciprocamente, os solicitantes das tarefas podem inadvertidamente expor informações privadas, tornando essencial a manutenção da transparência das tarefas de sensoriamento perante o servidor [Nieto et al. 2019, Hamrouni et al. 2021].

Além das preocupações com a privacidade, a confiança assume um papel crítico na construção da integridade entre as entidades envolvidas. As abordagens existentes de *crowdsourcing* que abordam questões de privacidade e confiança, muitas vezes, não direcionam essas garantias de maneira suficiente durante as trocas de dados na IoT ou no *crowdsourcing* [Nieto et al. 2019, Hamrouni et al. 2021]. Além disso, a privacidade está interligada à segurança dos dados e à infraestrutura subjacente. As ameaças à segurança, predominantemente oriundas de ataques externos, podem envolver a interceptação de canais de comunicação para obter acesso aos dados de sensoriamento criptografados. Tais ataques, muitas vezes disfarçados como participantes legítimos, têm o potencial de enviar dados falsos aos nós na arquitetura de IoT [Ang et al. 2022]. Assim, o panorama de privacidade no *crowdsourcing* IoT demanda uma atenção criteriosa à confiança e à segurança, dadas as implicações significativas envolvidas [Ang et al. 2022].

Diante do exposto, fica evidente a necessidade de desenvolver uma plataforma de detecção de emergências urbanas [Coelho et al. 2023, Da Silva et al. 2023] que combine a agilidade e estabilidade de uma rede de dispositivos IoT, com a flexibilidade, dinamismo e compreensividade do alto volume de dados gerados por uma abordagem colaborativa de *crowdsourcing*. Tal plataforma potencialmente aumentará a eficiência e a precisão das aplicações que lidam com emergências urbanas.

3. Solução Proposta

Neste trabalho, propomos um modelo de detecção de emergências que visa possibilitar uma detecção rápida e precisa por meio de funcionalidades flexíveis e configuráveis. Isso facilitaria ações de mitigação e alertas imediatos à população ou às autoridades, minimizando os danos potenciais à região e aos seus habitantes. O modelo oferece uma detecção hierárquica em diferentes níveis da rede, pois cada unidade de detecção tem autonomia para inferir emergências. Ao mesmo tempo, incorpora uma detecção colaborativa, na qual dados são coletados por várias unidades de detecção e por um mecanismo de *crowdsourcing* para obter uma detecção de emergência mais precisa.

Para realizar a aquisição e a análise de sinais para detectar emergências dentro

de uma zona de interesse, utilizamos redes de sensores sem fio. Os sensores devem se comunicar para possibilitar a colaboração, pois um sensor pode precisar de dados de outro para determinar a ocorrência de uma emergência. A rede é composta por várias unidades de detecção de emergências com capacidades variadas, cada uma equipada com um conjunto específico de sensores ativos baseados no tipo de emergências que detecta.

Para garantir a segurança e a confiabilidade durante os processos de operação dessas unidades, é necessário modelar adequadamente uma infraestrutura de comunicação e definir componentes capazes de suportar dinamicamente as solicitações para a operação flexível das unidades de detecção. A plataforma proposta implementará políticas de segurança para assegurar a integridade, a autenticidade e a confidencialidade. Para isso, a abordagem será centrada em diferentes princípios orientadores, que são:

- Autenticidade e não repúdio para garantir a segurança e a confiabilidade durante os processos de operação dessas unidades de detecção de emergências;
- Infraestrutura adequada para armazenar, organizar e entregar atualizações de software para os dispositivos IoT;
- Protocolos de comunicação para possibilitar transmissões sem fio seguras. Embora não definamos um protocolo de referência, pretendemos avaliar nossa abordagem por meio do MQTT sobre o padrão WiFi;
- Segmentação e gerenciamento de dispositivos IoT para garantir que as mensagens sejam adaptadas às características específicas de cada grupo, evitando sobrecarga da rede e minimizando os riscos associados à comunicação mal sucedida;

Como a aplicação é focada em cidades inteligentes, será explorado o rápido desenvolvimento de *smartphones* e das tecnologias móveis e seus vastos recursos computacionais para explorar estratégias de *crowdsourcing*. Isso leva a um novo paradigma chamado *crowdsourcing* móvel [Abbasi et al. 2022]. O *crowdsourcing* móvel fornece um paradigma de sensoriamento e coleta de dados utilizando dispositivos inteligentes para adquirir dados de sensoriamento. Assim os usuários podem usar tanto a vantagem de sensoriamento quanto a de computação dos dispositivos inteligentes. Além disso, o *crowdsourcing* móvel permite a coleta de dados de outras fontes, como redes sociais e aplicações específicas. Esses dados podem incluir texto, imagem e vídeo postados pelos usuários sobre a situação de emergência, bem como dados deliberadamente informados pelos usuários, como alertas, *feedback*, sugestões, etc.

Esses dados serão analisados juntamente com os dados da rede IoT, com a finalidade de aumentar a acurácia da detecção de emergência. Para isso, serão utilizadas abordagens de *big data* e inteligência artificial, como mineração de dados, aprendizado de máquina, visão computacional, processamento de linguagem natural, etc. Os resultados da análise serão usados para gerar informações úteis e confiáveis sobre a emergência, como tipo, local, gravidade, impacto, etc. Essas informações serão usadas para alertar e orientar a população sobre detalhes da emergência em questão e como lidar com ela.

4. Resultados

Espera-se que a plataforma proposta seja capaz de:

- Detectar emergências urbanas de forma rápida, precisa e confiável, utilizando dados de diferentes fontes, como sensores IoT, dispositivos móveis, redes sociais e aplicações específicas, integrando dados de sensoriamento e *crowdsourcing*.

- Utilizar abordagens de *big data* e inteligência artificial, para classificar e priorizar as emergências urbanas detectadas
- Alertar e orientar os usuários, os socorristas e as autoridades sobre a ocorrência evolução das emergências urbanas, bem como formas de lidar com elas, como sugestões de rotas de evacuação.
- Motivar e recompensar os participantes do *crowdsourcing*, garantindo a qualidade e a confiabilidade das informações fornecidas, e utilizando técnicas de gamificação e de incentivo.
- Ser segura e privada, implementando políticas de segurança para assegurar a integridade, a autenticidade e a confidencialidade dos dados, e respeitando os direitos e as preferências dos usuários.

Para avaliar os resultados esperados da plataforma proposta, será seguida a seguinte metodologia de avaliação:

- Definir cenários de emergências urbanas, baseados em casos reais ou simulados, que envolvam diferentes tipos, locais, gravidades e impactos de emergências.
- Implementar um protótipo da plataforma, utilizando dispositivos IoT e *smartphones*, e uma infraestrutura de comunicação, processamento e armazenamento baseada na nuvem.
- Recrutar participantes voluntários para o *crowdsourcing*, que estejam dispostos a fornecer informações sobre as emergências urbanas, como relatos, fotos, vídeos, avaliações, etc.
- Medir o desempenho da plataforma, utilizando métricas quantitativas e qualitativas, como:
  - Tempo de detecção: o intervalo de tempo entre a ocorrência da emergência e a sua detecção pela plataforma.
  - Confiabilidade/Precisão de detecção: a proporção de emergências detectadas corretamente, em relação ao total de emergências ocorridas.
  - Satisfação do usuário: o grau de satisfação dos usuários, dos socorristas e das autoridades com a plataforma, em termos de utilidade, facilidade de uso, confiança, etc.
  - Motivação do participante: o grau de motivação dos participantes do *crowdsourcing* para fornecer informações sobre as emergências, em termos de interesse, engajamento, recompensa, etc.
- Comparar os resultados obtidos com os resultados de outras plataformas similares.

5. Conclusão

Neste artigo é idealizada uma plataforma de *crowdsourcing Internet of Things* para a detecção de emergências urbanas, que combina dados de sensores e de usuários, para melhorar a eficiência e a precisão da detecção de emergências, fornecer informações relevantes e confiáveis sobre elas, orientar e alertar os envolvidos, motivar e recompensar os colaboradores, e proteger a segurança e a privacidade dos dados. A plataforma será avaliada com base em cenários de emergências urbanas, usando um protótipo com dispositivos IoT e *smartphones*, e uma infraestrutura de nuvem, explorando métricas quantitativas e qualitativas, como tempo de detecção, confiabilidade/precisão de detecção, satisfação do usuário. Acredita-se essa plataforma possa contribuir para o avanço da área de detecção de emergências urbanas, e que possa ser aplicada em diferentes contextos e situações, beneficiando as pessoas, as cidades e o meio ambiente.

Referências

Abbasi, S., Vahdat-Nejad, H., and Hajiabadi, H. (2022). Trustable mobile crowd sourcing for acquiring information from a flooded smart area. In *2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*, pages 1–3.

Aboualola, M., Abualsaud, K., Khattab, T., Zorba, N., and Hassanein, H. S. (2023). Edge technologies for disaster management: A survey of social media and artificial intelligence integration. *IEEE Access*, 11:73782–73802.

Ang, K. L. M., Seng, J. K. P., and Ngharamike, E. (2022). Towards crowdsourcing internet of things (crowd-iot): Architectures, security and applications. *Future Internet*, 14(2).

Coelho, G. A. A., Jesus, T. C., and Costa, D. G. (2023). Urban emergency detection system using hierarchical, collaborative and configurable wireless sensor networks. In *XIII Brazilian Symposium on Computing Systems Engineering (SBESC)*, pages 1–6.

Da Silva, G. F. P., Costa, D. G., and De Jesus, T. C. (2023). A secure ota approach for flexible operation of emergency detection units in smart cities. In *IEEE International Smart Cities Conference (ISC2)*, pages 01–07.

Deshpande, V., Das, T., Badis, H., and George, L. (2019). Sebs: A secure element and blockchain stratagem for securing iot. In *2019 Global Information Infrastructure and Networking Symposium (GIIS)*, pages 1–7.

Fedele, R. and Merenda, M. (2020). An iot system for social distancing and emergency management in smart cities using multi-sensor data. *Algorithms*, 13(10).

Hamrouni, A., Alelyani, T., Ghazzai, H., and Massoud, Y. (2021). Toward collaborative mobile crowdsourcing. *IEEE Internet of Things Magazine*, 4(2):88–94.

Han, S., Huang, H., Luo, Z., and Foropon, C. (2019). Harnessing the power of crowdsourcing and internet of things in disaster response. *Annals of Operations Research*, 283(1):1175–1190.

Kong, X., Liu, X., Jedari, B., Li, M., Wan, L., and Xia, F. (2019). Mobile crowdsourcing in smart cities: Technologies, applications, and future challenges. *IEEE Internet of Things Journal*, 6(5):8095–8113.

Nieto, A., Acien, A., and Fernandez, G. (2019). Crowdsourcing analysis in 5g iot: Cybersecurity threats and mitigation. *Mobile Networks and Applications*, 24(3):881–889.

Rauniyar, A., Engelstad, P., Feng, B., and Thanh, D. V. (2016). Crowdsourcing-based disaster management using fog computing in internet of things paradigm. In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, pages 490–494.

S, A., A, S., and Pankaj, D. S. (2023). Crowdsourcing of internet of things: Applications, trends in technology and the future. In *2023 International Conference on Power, Instrumentation, Control and Computing (PICC)*, pages 1–6.

Shahrour, I. and Xie, X. (2021). Role of internet of things (iot) and crowdsourcing in smart city projects. *Smart Cities*, 4(4):1276–1292.