

Uma Revisão Sistemática sobre Privacidade do Usuário em Aplicações MCS

Guibson Souza¹, Ingrid Santos¹, Karla Pereira¹, Eduardo Feitosa¹

¹Instituto de Computação – Universidade Federal do Amazonas (UFAM)
CEP 69.077-000 – Manaus – AM – Brazil

{nedel,efeitosa}@icomp.ufam.edu.br

Abstract. *Mobile Crowd Sensing (MCS) applications allow mobile users to collect, share and comment on information provided by third parties or himself through different sensors (GPS, accelerometer, camera, microphone, etc.). As the handling of this information is carried out directly by end users, privacy has become a critical and important issue that should be evaluated. This paper presents a Systematic Literature Review on user privacy in MCS context. The goal is to help the end users understand their privacy and how to secure it in MCS applications.*

Resumo. *Aplicações de Mobile Crowd Sensing (MCS) permitem que usuários de dispositivos móveis colem, compartilhem e comentem informações fornecidas por terceiros ou ele mesmo, através de diferentes sensores (GPS, acelerômetro, câmera, microfone, entre outros). Como a manipulação dessas informações são realizadas diretamente por usuários finais, sua privacidade tornou-se uma questão crítica e importante que deve ser avaliada. Neste trabalho é apresentada uma Revisão Sistemática da Literatura sobre privacidade do usuário no contexto de MCS. O objetivo é contribuir para que o usuário entenda o que é a sua privacidade e como garanti-la em aplicações MCS.*

1. Introdução e Conceituação

Mobile Crowd Sensing, ou simplesmente MCS, é um paradigma de sensoriamento que tira proveito do número de dispositivos que um usuário possui e de sua mobilidade para adquirir conhecimento local (informações ambientais, de infraestrutura e social) e compartilhar esse conhecimento dentro de uma esfera social. A ideia é que os dados coletados por um usuário comum, através dos diferentes sensores (GPS, acelerômetro, câmera, sensor de temperatura) do dispositivo móvel, podem contribuir de alguma forma para melhorar e/ou auxiliar a vida das outras pessoas.

Para Ganti et al. [Ganti et al. 2011], os pesquisadores responsáveis por cunharem o termo, *Mobile Crowd Sensing se refere a uma variada e ampla gama de modelos de sensoriamento no qual indivíduos com dispositivos computacionais e sensores são capazes de coletar e contribuir com dados valiosos para diferentes aplicações.* A principal diferença entre MCS em relação a outras plataformas de sensoriamento participativo reside no fato de que toda ação de registro (coleta de dados, informações e comentários sobre os dados) é feita a partir do dispositivo móvel do participante, podendo estar conectado a qualquer rede de acesso à Internet. Um grande benefício deste paradigma é o baixo

custo de implantação, pois não é preciso ter uma estrutura de hardware específica para ser participante ou usuário deste tipo de aplicação.

Contudo, devido a suas características únicas, a privacidade em MCS traz preocupações com a divulgação direta da identidade dos participantes bem como com a divulgação de atributos sensíveis, incluindo locais (por exemplo, endereço residencial ou do trabalho) e outras informações privadas como atividades pessoais ou condições (por exemplo, estilo de vida ou doença) que permitam inferir a identidade dos participantes [Pournajaf et al. 2014].

Neste contexto, este artigo visa investigar se a privacidade do usuários é considerada em aplicações MCS, através de uma Revisão Sistemática da Literatura (RSL).

2. Revisão Sistemática da Literatura

O objetivo desta Revisão Sistemática da Literatura (RSL), delineada a partir do paradigma GQM [Basili and Rombach 1988], é **Analisar** publicações científicas relacionadas à privacidade em MCS; com o **Propósito** de identificar conceitos, características, fatores e ferramentas; no que diz **Respeito** ao usuário; no **Contexto** de aplicações Móveis.

Com base neste objetivo, três (3) questões de pesquisas foram criadas: **Q1** - Existe preocupação com a privacidade do usuário em MCS? **Q2** - O que usuário percebe ou entende sobre privacidade em MCS? **Q3** - Quais técnicas são utilizadas na privacidade do usuário em aplicações MCS?

2.1. Execução e Resultados

A revisão sistemática da literatura foi realizada entre Março e Junho de 2016, utilizando a máquina de busca Scopus (<https://www.scopus.com>), resultando no retorno de 193 artigos. Inicialmente, como primeiro filtro, foram analisados e considerados apenas o título do artigo, o *abstract* e as palavras-chave. Ao final desta etapa, foram selecionados 71 artigos. No segundo filtro foi considerada e analisada a leitura completa dos artigos selecionados. Nesta fase foram selecionados 16 artigos. Também foram realizadas pesquisas manuais que retornaram 6 artigos, resultando em duas inclusões. Ao final do processo, 18 artigos foram selecionados por estarem relacionados a esse domínio.

Vale ressaltar que alguns dos trabalhos encontrados relacionam características empregadas em paradigmas fora ou além de *Mobile Crowd Sensing*, como Sensoriamento Participativo e *Mobile CrowdSourcing*.

3. Análise

Esta seção discute as questões de pesquisa com base nos trabalhos encontrados na RSL sobre Privacidade de Usuário em MCS.

3.1. Existe preocupação com a privacidade do usuário em MCS?

Sim. Existem alguns estudos [Pournajaf et al. 2014, Christin 2010, Brush et al. 2010] que correlacionam a preocupação com a privacidade com as diferentes modalidades de sensoriamento usadas, bem como a forma como os usuários entendem, selecionam e se comportam em relação a privacidade. Contudo, todos são unânimes em afirmar que os usuários não são considerados no processo de avaliação da usabilidade e utilidade das soluções de privacidade, mesmo sabendo que tais aplicações gerenciam grandes volumes de informações que tipicamente são e podem ser tornadas públicas.

3.2. O que usuário percebe ou entende sobre privacidade em MCS?

De forma geral, os dados obtidos e coletados pelos e dos usuários são controlados pela infraestrutura da aplicação e o usuário não tem conhecimento algum do que acontece com seus dados. Entretanto, alguns aspectos de segurança dependem unicamente do usuário, ou melhor, das suas preferências (intervenções realizadas para ajustar parâmetros de acordo com suas preferências).

Christin et al. [Christin 2010] afirmam que a privacidade no sensoriamento participativo está centrada em dois componentes estritos: pessoa e dados. Assim, o usuário deve entender, escolher e controlar os dados coletados que serão compartilhados, bem como filtrar quem receberá esses dados e a duração da disponibilidade destes. O objetivo é aumentar a consciência dos usuários acerca das questões de privacidade.

Gustarini et al. [Gustarini et al. 2016] definiram uma métrica (intimidade) para investigar a percepção do anonimato do usuário em MCS, os fatores que o influenciam a aceitar ser anônimo ou não, e o contexto em que tomam a decisão de compartilhar os dados. A intimidade concentra o contexto do usuário em três elementos principais: localização semântica dos usuários, o número e o tipo de pessoas que estão ao seu redor. Ao aplicarem um questionário sobre intimidade - escala de valores entre 1 (completamente) e 6 (não estou íntimo) - com usuários de MCS no contexto de onde se encontrava naquele momento (local), quantas pessoas estavam ao seu redor e se eles se sentiam a vontade de compartilhar o conteúdo da pesquisa anonimamente ou não, os autores perceberam que a maioria dos usuários tem dificuldades para inferir sobre os dados que estão sendo coletados, para qual finalidade e como são coletados.

3.3. Quais técnicas são utilizadas na privacidade do usuário em aplicações MCS?

De acordo com [Laurido and Feitosa 2015], as principais técnicas para garantir a privacidade do usuário em aplicações MCS são: (i) permitir que os usuários expressem suas preferências de privacidade; (ii) a distribuição de tarefas de sensoriamento anonimamente, para assegurar o anonimato e a privacidade de localização; e (iii) o uso de anonimato, para remover qualquer informação que possa identificar o usuário durante a distribuição e realização de tarefas.

Dentre essas, a mais relevante e com maior grau de interdisciplinaridade é permitir que o usuário tenha a capacidade de expressar suas preferências sobre privacidade em uma determinada aplicação. Das et al. [Das et al. 2010] propuseram um esquema binário, com acesso completo ou nenhum acesso aos dados do usuário. A ideia é que os usuários possam decidir ativar seletivamente as medições do sensor, dependendo de uma variedade de fatores como a presença em locais sensíveis (casa ou escritório) e de pessoas de seu convívio social (presença de amigos ou familiares). Por exemplo, amostras podem ser recolhidas a cada hora ao invés de a cada 15 segundos ou informações de localização podem ou não ser capturadas dependendo da localização.

Christin et al. [Christin et al. 2014] argumentam que existe a viabilidade de dar controle aos usuários sobre a proteção de sua privacidade, permitindo que personalizem suas preferências. Para tanto, elaboram um projeto para conscientizar os usuários sobre ameaças de privacidade em aplicações de sensoriamento móveis, a fim de motivar a necessidade de configurar uma aplicação para preservação da privacidade. Selecionaram um aplicativo que monitora ruídos no ambiente através de smartphones e realizaram um

experimento em dois (2) passos. O primeiro foi projetar interfaces explicando a funcionalidade da privacidade no aplicativo e como o usuário pode fazer sua proteção escolhendo as configurações de acordo com as suas preferências. O segundo foi realizar um estudo com 20 participantes, testando e avaliando diferentes interfaces de privacidade, completando tarefas guiadas e tarefas livres de acordo com as definições dadas e personalizando suas próprias configurações. O resultado do estudo mostrou que os participantes gostaram deste controle adicional oferecido, mas alguns se complicaram devido à complexidade do problema. O experimento foi realizado no sistema iOS e as interfaces projetadas foram integradas ao aplicativo "NoiseCapture".

4. Conclusões

Neste trabalho foi apresentada uma Revisão Sistemática da Literatura sobre privacidade do usuário em aplicações MCS. Dos 193 artigos encontrados na pesquisa, 18 artigos foram selecionados e estudados. A partir dos estudos pode-se observar que existem poucos trabalhos visando melhorar a privacidade do usuário nos diversos ambientes de sensoriamento usando dispositivos móveis. Além disso, constatou-se que nem mesmo os maiores interessados, os usuários dessas aplicações, sabem o significado de privacidade e como é feito esse processo para garantir a integridade dos seus dados.

References

- Basili, V. R. and Rombach, H. D. (1988). The tame project: Towards improvement-oriented software environments. *IEEE Trans. on software engineering*, 14(6):758–773.
- Brush, A. B., Krumm, J., and Scott, J. (2010). Exploring end user preferences for location obfuscation, location-based services, and the value of location. In *Proceedings of the 12th ACM UbiComp*, pages 95–104. ACM.
- Christin, D. (2010). Impenetrable obscurity vs. informed decisions: privacy solutions for participatory sensing. In *2010 8th IEEE PERCOM*, pages 847–848.
- Christin, D., Engelmann, F., and Hollick, M. (2014). Usable privacy for mobile sensing applications. In *IFIP International Workshop on Information Security Theory and Practice*, pages 92–107. Springer.
- Das, T., Mohan, P., Padmanabhan, V. N., Ramjee, R., and Sharma, A. (2010). Prism: platform for remote sensing using smartphones. In *Proceedings of the 8th MobiSys*, pages 63–76. ACM.
- Ganti, R., Ye, F., and Lei, H. (2011). Mobile crowdsensing: current state and future challenges. *Communications Magazine, IEEE*, 49(11):32–39.
- Gustarini, M., Wac, K., and Dey, A. K. (2016). Anonymous smartphone data collection: factors influencing the users' acceptance in mobile crowd sensing. *Personal and Ubiquitous Computing*, 20(1):65–82.
- Laurido, J. and Feitosa, E. (2015). Segurança em Mobile Crowd Sensing. In *Livro de Minicursos do SBSeg2015*, chapter 2, pages 49–98. SBC.
- Pournajaf, L., Xiong, L., Garcia-Ulloa, D. A., and Sunderam, V. (2014). A survey on privacy in mobile crowd sensing task management. Technical report, Emory University.