Internet of Things (or Smart Cities): Security and Privacy Challenges

Fábio Silva, Mário Real, and Rita Gomes

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a82331,a72620,a87960}@alunos.uminho.pt

Resumo A transição e evolução das nossas sociedades para cidades inteligentes em constante evolução só será possível se os desafios de segurança e privacidade forem salvaguardados de uma forma confiável e activa. Neste ensaio temos como objectivo apresentar abordagens explicativas sobre as tecnologias às quais chamamos actualmente de internet das coisas (IoT), como a partir delas deu-se a origem a uma existência progressiva de cidades inteligentes, e da qual a sua existência só será possível com a presença de fortes alicerces de segurança e privacidade aliada à construção da sua infraestrutura, para que possa tornar a vida dos seus habitantes mais fácil e ágil, sem trazer medos e problemas que se sobreponham às suas benesses. Ao longo deste estudo será explorado o impacto destas cidades tecnológicas nas nossas vidas e quais os seus desafios de segurança e privacidade, onde iremos analisar métodos e soluções em temas como: a importância das ameaças de privacidade no compartilhamento de dados, e que tecnologias podemos usar para as proteger; de que forma é possível proteger os nossos dados em nuvem na nossa sociedade, e qual a importância da existência de leis e políticas para que estes sejam salvaguardados da forma mais correcta; e, por último, de que forma os avanços e inovações na eficiência energética, proporcionados pelo nascimento das cidades inteligentes, podem se traduzir em melhores condições de segurança na vida dos seus residentes. É assim desejável, que os desafios de segurança numa cidade inteligente, interligada, e com mudanças ao segundo, consiga garantir um sistema de defesa unificado e abrangente a todos os seus elementos e diferentes áreas, para poder proporcionar a desejada qualidade de vida aos seus habitantes.

1 Introdução

A Internet das Coisas (IoT) é um paradigma de comunicação revolucionário que visa trazer uma estrutura invisível e inovadora para conectar uma infinidade de dispositivos digitais à Internet.[1] Permite que dispositivos eletrónicos no nosso ambiente circundante sejam participantes ativos, compartilhando informações com outros membros da rede, tornando possível reconhecer eventos e mudanças ao nosso redor e agir e reagir de forma autónoma, sem qualquer interação humana. Desta forma, com o tremendo crescimento do paradigma em questão, seria de esperar que diversos fatores do dia-a-dia fossem incorporados no mesmo, daí o aparecimento de *Smart Cities*. Sendo assim, uma cidade inteligente integra tecnologia inteligente de uma maneira que serve para aumentar a eficiência, segurança e conveniência.[2] No entanto, a existência de uma rede tão grande de entidades conectadas certamente representará novas ameaças de segurança, privacidade e confiança que colocam todos esses dispositivos em alto risco, prejudicando os usuários afiliados.

O sucesso de uma cidade inteligente irá depender da capacidade de saber lidar com possíveis preocupações com a privacidade e segurança antes que a infraestrutura esteja pronta. As atuais deliberações e tentativas de resolver os desafios de segurança e privacidade irão abrir caminho para a compreensão de como as cidades inteligentes podem ser construídas com segurança.[2] Neste documento, segurança e privacidade de dados referem-se à proteção de quaisquer dados coletados ou armazenados em qualquer sistema IoT. Isso significa que a qualquer momento o sistema IoT precisa fornecer confidencialidade, integridade e

disponibilidade de dados e isso pode ser obtido utilizando autenticação, controle de acesso, criptografia de dados e redundância de dados por meio de backups.

Ao longo deste trabalho iremos focar-nos nas técnicas existentes de preservação da privacidade que são aplicáveis no desenvolvimento de cidades inteligentes e identificar lacunas de pesquisa em torno das mesmas.

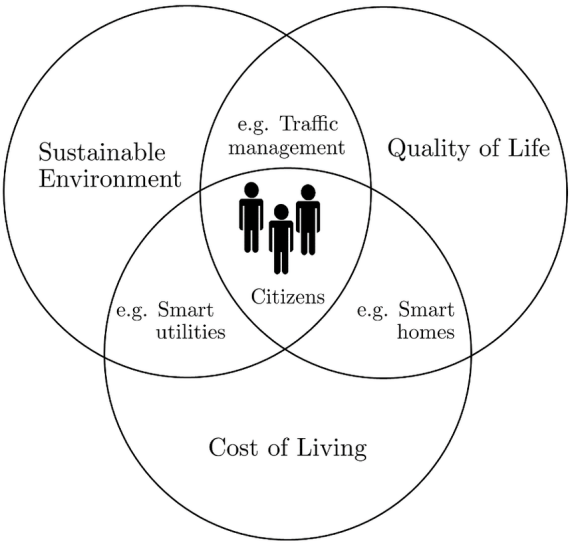

Figura 1. Objetivos fundamentais das *smart cities*.[3]

2 Segurança e privacidade

A segurança desempenha um papel importante na proteção dos dispositivos, dados e redes contra invasores, projetando as políticas e tecnologias para manter a integridade dos dados e também monitorizar o acesso não autorizado às informações. Como as cidades inteligentes fornecem conexão à Internet para uma ampla variedade de dispositivos, a segurança torna-se um desafio muito crítico.[1]

A restrição ou falta de compreensão dos desafios e requisitos de segurança da cidade inteligente pode levar à implementação e execução inadequadas e inseguras da cidade inteligente. De seguida, discutiremos os requisitos indispensáveis para uma cidade inteligente segura, que devem ser levados em consideração na fase de implementação de uma *smart city*. Sendo assim, a fim de projetar uma *smart city* de sucesso , as seguintes questões devem ser abordadas:

- **(2.1)** Garantir a qualidade e integridade dos dados
- **(2.2)** Segurança na nuvem
- **(2.3)** Efeciência Energética

2.1 Ameaças de privacidade no compartilhamento de dados

Como podemos garantir a privacidade pessoal numa cidade inteligente que depende do compartilhamento rápido de dados com várias partes interessadas?

Pela natureza da cidade inteligente, os dados serão transferidos e utilizados em todos os processos da cidade inteligente, com várias partes comunicando entre si e obtendo acesso às informações. Cada organização que contribui para a cidade inteligente usará e tratará os

dados de maneira exclusiva, o que pode colocar em risco a privacidade pessoal. Além disso, uma vez que cada parte interessada da cidade inteligente terá prioridades diferentes, haverá lacunas entre os padrões de privacidade das diferentes partes interessadas.[2] Por exemplo, nas redes inteligentes de energia elétrica, *smart grids*, grande volume de dados está a ser coletado de diferentes clientes. Esses dados contêm informações úteis, como padrões de uso e indicações de falha. Esses dados são usados pelos operadores da rede elétrica para otimizar seu desempenho, consertar rapidamente qualquer falha de energia e diminuir o consumo geral de energia da cidade. No entanto, se a qualidade e integridade dos dados não forem garantidas, os dados coletados podem estar comprometidos e os operadores da rede podem tomar decisões erradas.

Além disso, podemos tomar como exemplo as empresas que fazem avaliações de risco / lucro ao decidir sobre o quanto de proteção de privacidade é suficiente. O objetivo das empresas é lucrar com a oferta de produtos ou serviços, de forma que as empresas ofereçam proteção de privacidade suficiente para garantir que a marca não seja manchada e que os clientes continuem a comprar os produtos. O setor público provavelmente terá uma intenção mais ambiciosa no que diz respeito à privacidade, mas o seu financiamento e sustento não estarão diretamente vinculados ao seu sucesso em alcançar a proteção da privacidade, ao contrário do setor privado. Por exemplo, os cuidados de saúde em uma cidade inteligente podem contar com parcerias contínuas entre os setores público e privado. Nesse cenário, as informações confidenciais sobre a condição do paciente precisarão ser transferidas e analisadas pelas partes relevantes.

Esse processo de transmissão de dados entre várias organizações para um propósito comum geralmente resulta em técnicas chamadas mashup de dados e integração de dados. Em um ambiente de cidade inteligente, mashups de dados de alta dimensão com preservação de privacidade permitirão que várias partes compartilhem e acessem dados pertinentes sem comprometer a privacidade individual. No entanto, as práticas atuais de mashup de dados têm seus próprios desafios. Por exemplo, ao combinar vários conjuntos de dados privados, o conjunto de dados resultante revelaria informações mais confidenciais para os outros provedores de dados. Deste modo, as cidades inteligentes não podem contar com métodos tradicionais de preservação de privacidade ao participar do mashing de dados. [2]

2.1.1 Tecnologias que aumentam a privacidade :

Assim, ao considerar métodos para preservar a privacidade individual em conjuntos de dados de cidades inteligentes, o conceito de privacidade diferencial deve ser considerado. A privacidade diferencial possibilita que as empresas de tecnologia coletem e compartilhem informações agregadas sobre os hábitos do usuário, mantendo a privacidade de usuários individuais. O modelo de privacidade diferencial garante que, mesmo que alguém tenha informações completas sobre 99 pessoas de um conjunto de dados 100 pessoas, elas ainda não poderão deduzir as informações sobre a pessoa final. O principal mecanismo para conseguir isso é adicionar ruído aleatório aos dados agregados.[4]

2.2 Segurança na nuvem

O que acontece com os dados coletados em uma cidade inteligente? Como é que uma cidade inteligente é protegida contra ataques cibernéticos? Quem é o responsável pelas violações de dados?

As cidades inteligentes apresentarão inúmeros dispositivos inteligentes, cada um dos quais se comunica com a rede inteligente enviando, copiando e processando dados. Este processo irá gerar uma imensa quantidade de dados, alguns dos quais serão confidenciais e deverão ser protegidos. Para armazenar grandes quantidades de dados, é provável que as cidades inteligentes utilizem serviços em nuvem. Esses serviços em nuvem, junto com o armazenamento de dados em nuvem, ajudarão as cidades inteligentes a evitar as limitações impostas pela capacidade de computação e memória física, mas também apresentarão alguns desafios. A distribuição de serviços de dados gera pontos de violação adicionais, com os provedores de serviços em nuvem complicando, ao adicionar padrões e práticas adicionais para privacidade e segurança.[2] Quando lidamos com enormes quantidades de informação confidencial, a responsabilidade e o consentimento numa cidade inteligente torna-se uma questão importante. O desafio aqui é a eficiência e confiabilidade, uma vez que o compartilhamento e o armazenamento de dados são cruciais para o bom funcionamento de uma cidade inteligente. Uma questão também relevante é, se, perante a impossibilidade de impedir todos os ataques cibernéticos, então, quando um ocorrer, qual será a responsabilidade por parte das empresas fornecedoras de serviços de *Cloud*? Se as empresas não conseguem garantir a total segurança e integridade dos seus dados, isto gera um alto grau de risco, o qual, combinado com uma possível punição forte, compromete a viabilidade financeira destas empresas. Uma forma de eufemizar esta questão seria a partilha desta responsabilidade entre as empresas e o governo, incentivando à maior segurança possível na *Cloud*. O gerenciamento de dados vai além dos serviços de nuvem ou organizações governamentais; na verdade, cada dispositivo que contribui para a rede inteligente armazenará e manipulará dados. Se objetos inteligentes, como smartphones, sensores ou scanners, mantiverem réplicas locais de dados confidenciais, eles podem ser violados, especialmente se forem fisicamente acessíveis. Isso pode ser problemático para os defensores da privacidade se as réplicas de dados forem feitas sem transparência ou consentimento do usuário. Pode parecer improvável, mas se a privacidade de um habitante for violada, a segurança da cidade inteligente diminuirá.

Dependendo dos aplicativos numa cidade inteligente, as agências que gerenciam as tecnologias devem optar, em relação ao processamento de dados, se estes vão ser tratados em nuvem ou localmente.[3] Dependendo, por exemplo, da natureza do aplicativo ou de restrições temporais, estas agências decidirão qual a melhor abordagem para cada aplicativo.

2.2.1 Gerenciamento de dados e conformidade com políticas :

Para que exista uma correta produção, transmissão e exploração dos dados que levam à existência das *smart cities*, precisamos de uma organizada e eficiente gestão da informação que torne possível satisfazer todas as necessidades associadas aos seus habitantes e entidades.

Se analisarmos a possibilidade de vivermos com os nossos principais serviços e infraestruturas conectados digitalmente, dos quais toda a nossa sociedade depende diariamente, a importância na segurança dessa gestão de dados torna-se exponencialmente mais importante com todos os perigos inerentes.

Para que essa segurança seja assegurada é necessário a existência de incentivos, criação de leis e de um aparelho regulador direcionado às empresas para que se identifique de forma ágil todas as possíveis irregularidades na preservação dos nossos dados e que possa haver confiança por parte da população e dos clientes alvo. Simultaneamente, deve ser atingido um equilíbrio ponderado entre as responsabilidades de segurança exigidas, com a limitação da quantidade de risco financeiro que uma empresa corre em guardar os nossos dados sem

falhas de segurança. Assim conseguiremos ter empresas ativamente empenhadas na manutenção da nossa segurança e privacidade, sem estas temerem radicalmente repercussões ao prestar esses mesmos serviços.[2]

Um dos emergentes modelos e conceitos utilizados nas políticas de segurança de dados são os "Law-as-a-Service" (LaaS), criados para diferentes áreas da rede, entre as quais os fornecedores de serviços em *cloud*, para que os seus serviços prestados estejam em conformidade com as políticas legais na transferência e manipulação dos dados dos seus utilizadores.[5]

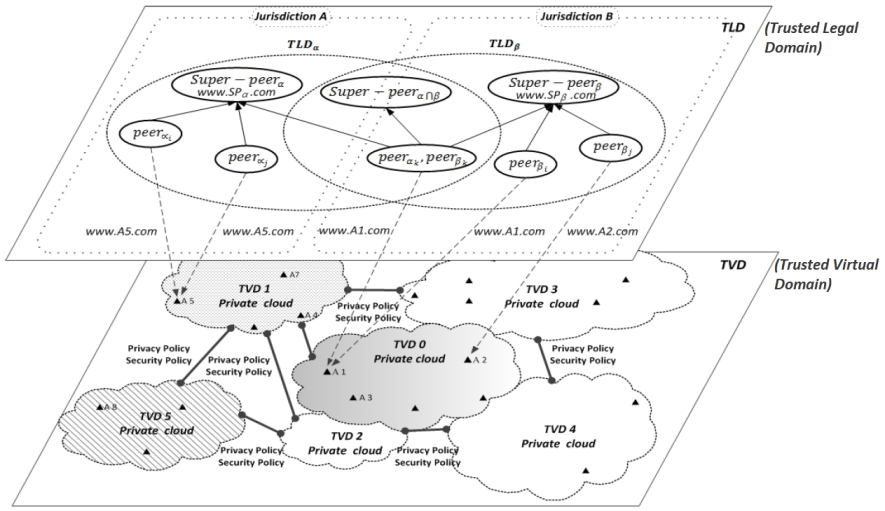

Figura 2. "A conceptual layout of the law-aware semantic policy infrastructure in the cloud".[6]

2.3 Eficiência Energética

Como um dos objetivos da cidade inteligente é desenvolver-se economicamente ao mesmo tempo que aumentam a qualidade de vida dos habitantes, as ferramentas de aquisição de dados e respetivas técnicas precisam de ser reformulados à luz do consumo de energia. Ferramentas de aquisição de dados precisam de reduzir a sua pegada de carbono. Isso pode ser realizado tornando essas ferramentas mais eficientes em termos de energia, ou pela incorporação de fontes renováveis de energia, onde a energia armazenada pode ser usada posteriormente. Um exemplo dos benefícios que a eficiência energética proporciona é o resultado da cidade de Buenos Aires, que alterou mais de 75% da sua iluminação pública para lâmpadas LED conectadas ao sistema de gerenciamento de iluminação pública *CityTouch*.[7] Com esta aplicação é possível que as luzes da via pública de uma cidade se liguem e desliguem de forma autónoma, de acordo com as necessidades de iluminação. [8]Como resultado dessas mudanças, Buenos Aires pôde melhorar a sua eficiência operacional e economizar mais de 50% em energia.[7] Um outro exemplo que oferece uma maior segurança aos utilizadores são as *smart homes* que, através da automação, permitem o controlo e interligação de vários sistemas como a iluminação, persianas ou fechaduras. A Internet das Coisas (IoT) possibilita que, através da voz ou do telemóvel, possamos gerir este tipo de aplicações em tempo real. Isto ajuda a diminuir o desperdício que irá resultar na melhoria da eficiência energética, visto que podemos, por exemplo, desligar luzes que possam ter ficado ligadas ao sair de casa.[9]

3 Conclusões

Como as *smart cities* ainda são um trabalho em desenvolvimento, há naturalmente uma infinidade de oportunidades para pesquisas futuras sobre seus desafios de segurança e privacidade.[2] A viabilidade das cidades inteligentes depende da sua capacidade de aumentar a qualidade de vida dos cidadãos de maneira segura, reduzir o custo de vida e alcançar um ambiente sustentável. Para isso, examinamos vários casos de uso e implantações de infraestrutura de cidade inteligente, aplicativos e serviços.

Apresentamos ainda vários desafios de segurança e privacidade tais como: Como podemos garantir a privacidade pessoal em uma cidade inteligente que depende de compartilhamento rápido de dados e técnicas com várias partes interessadas? O que acontece com os dados coletados em uma cidade inteligente? Para que os dados coletados podem ser usados? Como podemos melhorar a eficiência energética de uma *smart city* aumentando a qualidade de vida dos habitantes ? As soluções para esses vários desafios incluem o mapeamento do perfil de risco da cidade inteligente, conceito de privacidade diferencial, técnicas criptográficas, transparência de dados e planos de contingência. Em última análise, as soluções para os desafios da cidade inteligente serão mais eficazes quando utilizarem uma abordagem global à segurança e privacidade. A cidade inteligente é composta por uma infinidade de dispositivos interconectados, portanto, as soluções de segurança e privacidade precisam se concentrar em um único sistema de defesa em vez de uma soma de defesas individuais.[2]

Referências

1. Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., Guizani, S.: Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. IEEE Communications Magazine (2017)
2. Braun, T., Fung, B. C., Iqbal, F., Shah, B: Security and privacy challenges in smart cities. Sustainable cities and society (2018)
3. Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., Al-Fuqaha, A.: Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys & Tutorials (2017)
4. Zhu, T.: What is differential privacy and how can it protect your data?. TheConversation Press (2018)
5. Khokhar H. R., Benjamin C.M. Fung, Iqbal F., Alhadidi D., Bentahar J.: Privacy-preserving data mashup model for trading person-specific information. Electronic Commerce Research and Applications (2016)
6. Yuh-Jong Hu, Win-Nan Wu, Di-Rong Cheng.: Towards law-aware semantic cloud policies with exceptions for data integration and protection. Association for Computing Machinery (2012)
7. Eficiência energética é trunfo das cidades inteligentes. [Artigo de blogue] Consultado em www.planetsmartcity.com.br/eficiencia-energetica-e-trunfo-das-cidades-inteligentes/ (2018)
8. A Iluminação Conectada Terá Um Papel Fundamental na Construção das cidades Inteligentes. [Artigo de blogue] Consultado em construir.pt/2017/05/26/a-iluminacao-conectada-tera-um-papel-fundamental-na-construcao-das-cidades-inteligentes/ (2017)
9. Bacelar, R.: Vantagens de ter uma casa inteligente ou Smart Home. [Artigo de blogue] Consultado em 4gnews.pt/vantagens-casa-inteligente-smart-home/ (2020)