Internet of Things: Security and Privacy Challenges - CLOUD

Carla Cruz, Diogo Sobral, and Pedro Freitas

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a80564,a82523,a80975}@alunos.uminho.pt

Abstract. A Cloud e a IoT têm crescido exponencialmente no dia a dia da sociedade e é necessário a procura de soluções para a proteção e segurança dos nossos dados e informações pessoais de forma a manter a nossa privacidade. A Cloud é um novo modelo de computação emergente que move todos os dados e as aplicações dos usuários para grandes centros de armazenamento. Apesar de ser um modelo assente em conceitos antigos, ainda existem diversos desafios a serem solucionados. Sendo que IoT tem a capacidade de coletar e transmitir dados também este tem vários desafios à espera de serem resolvidos.

1 Introdução

No último século, o mundo tem sido caraterizado por avanços e progressos nas mais diferentes áreas e a internet não ficou para trás. O termo "Internet of things" pode ser definido como a rede gigante que consegue conectar todos os dispositivos que a ela se conseguem ligar desde câmaras de vigilância a carros modernos [1]. Atualmente, segundo [2], existem cerca de 23 mil milhões de dispositivos ligados a esta rede, no entanto este número não fica por aqui. Prevê-se que, no ano 2025, este número já tenha ascendido aos 75 mil milhões o que levanta alguns problemas como a segurança e a privacidade de cada utilizador.

Vivemos numa era tecnológica em que quase tudo o que fazemos no nosso dia-a-dia passa pelo meio digital. Vivemos conectados que tal maneira que a distância deixou de ser o problema. Temos isto tudo e muito mais, mas a grande pergunta é: será que no meio de tanta tecnologia estamos seguros? será que toda a informação que partilhamos através dos nossos dispositivos continua a ser a nossa informação e não a informação de outra pessoa?

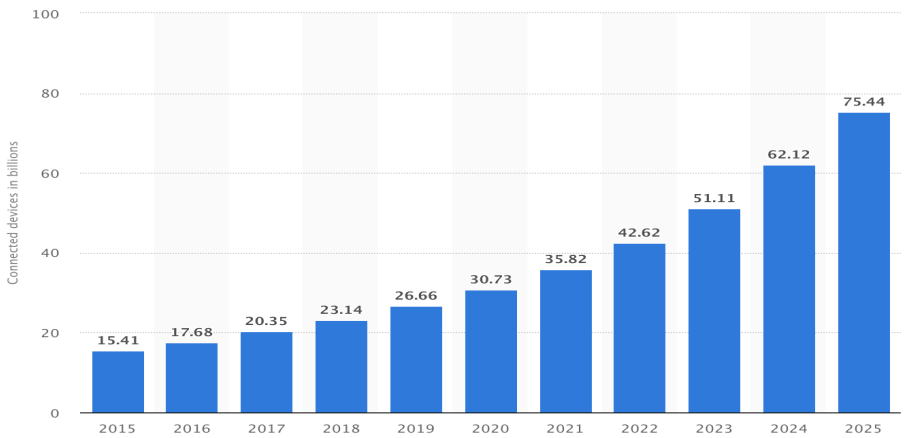

Fig. 1. Dispositivos ligados à Internet [2]

2 Internet of Things

A IoT cria um canal de partilha e troca de massivas quantidades de informação com o mínimo uso por parte de um utilizador [4]. Assumindo que o número de dipositivos cresça da maneira que está projetado e com pacotes de 100 bytes a uma frequência de chegada de 1 Hz, em 2020, a IoT vai precisar de conseguir 6 hexabytes de informação por segundo [5]. Esta informação pode ser de qualquer tipo desde uma foto pessoal até os valores de temperatura de uma região, o que aconteceria se caísse nas mãos para pessoa errada?

2.1 Segurança

Segundo [4], o facto de tudo estar ligado à internet, a existência da capacidade de comunicar entre si e da internet juntar a tradicional internet com as redes de comunicação e de sensores fazem com que a IoT constitua um alvo vulnerável a ataques. Os ataques são, na sua maioria, de DDOS (distributed denial of service), no entanto existem outros como Insertion Attack e Evasion Attack. Todos estes tipos tentam aproveitar falhas no sistema de modo a roubar informação ou a desativar os sistemas de seguranças existentes. Infelizmente, os protocolos standard só conseguem garantir a segurança por definição, estes não conseguem garantir a mesma quando são recebidas combinações de implementações especiais desses standards [5].

Se ter tudo ligado e ter que lidar com todo o tipo de dispositivos já era algo difícil, manter a segurança na IoT fica ainda mais complicada, visto que a maior parte dos fabricantes não têm a segurança como uma prioridade, mas sim como uma funcionalidade adicional o que complica tudo isto [4]. Para além do fabrico, muitos dos dispositivos ao fim de algum tempo deixam de poder receber atualizações devido a incompatibilidades de hardware fazendo-os assim vulneráveis a ataques [5].

2.2 Privacidade

Os dispositivos IoT estão presentes no nosso dia-a-dia e podem gerar uma quantidade absurda de informação valiosa que pode ser utilizada por fabricantes, vendedores e todo o tipo que sociedades que nela tenham interesses [1]. Toda esta informação contém dados sobre aquele que é o nosso dia-a-dia, informação sobre os nossos gostos, onde moramos, a nossa rotina, se toda esta informação deixar de ser privada, ficamos vulnerável e suscetíveis a ataques. Segundo [5], esta análise da nossa rotina pode beneficiar também as empresas de publicidade e os vendedores ao atraírem novos consumidores com os seus produtos e serviços. Exemplo disto é a LG que foi encontrada a recolher informação do áudio capturado pelas suas smart tv.

Dispositivos como sensores recolhem informação a toda a velocidade e mais tarde transferem a informação coletada para uma could ou outros lugares. Quando a informação é transferida, o seu dono perde o controlo total sobre a mesma [1]. A privacidade é fundamental e alguns modelos sugerem que para que esta permaneça seja necessário a existência das seguintes qualidades [5]:

1. Um utilizador deve poder usar um recurso sem desmascarar a sua identidade.
2. Um individuo deve usar várias vezes um recurso sem que as outras pessoas consigam estabelecer uma ligação entre as utilizações.
3. Um individuo deve poder usar um recurso sem que os outros possam ver que recursos estão a ser usados.

3 Cloud

3.1 O que é a Cloud?

O termo Cloud é um termo utilizado para descrever uma rede global de servidores, cada um deles com uma função única. A cloud não é uma entidade física, mas sim uma rede

vasta de servidores remotos em todo o mundo que estão interligados e que devem funcionar como um ecossistema único. Os dados não se encontram armazenados no computador, mas numa rede e, por isso, é possível guardar todo o trabalho que for feito e ter acesso a este em qualquer lugar.

Assim, este conceito, que tem revolucionado a tecnologia, refere-se à utilização da memória e à capacidade de armazenamento de computadores e servidores compartilhados e interligados por meio da internet. Tudo o que é armazenado na cloud pode ter acesso em qualquer parte do mundo, em qualquer computador, sem a necessidade de instalar softwares, sendo possível aceder-lhes através de um dispositivo com Internet [6].

3.2 Diferentes tipos de Cloud

A Cloud, pode ser categorizada em quatro tipos, dos quais, cloud privada, pública, comunitária e híbrida.

- **Cloud Privada** pode ser propriedade ou alugada por uma organização. Toda a cloud é utilizada como uso privado dessa mesma organização. Um exemplo, é uma cloud que é criada para satisfazer as aplicações essenciais de empresa relativamente aos seus negócios [3].
- **Cloud Pública** é executada por terceiros. Não tem grandes custos iniciais nem investimento de tempo na criação de uma infra-estrutura interna. Pode-se utilizar a infra-estrutura e as aplicações pagando uma assinatura mensal. A infra-estrutura de clouds é disponibilizada para o público em geral, sendo acedida por qualquer utilizador que conheça a localização do serviço. Neste modelo de implantação não podem ser aplicadas restrições de acesso quanto à gestão de redes nem aplicar técnicas de autenticação e autorização [3].
- **Cloud da Comunidade** é semelhante à cloud privada mas o recurso da cloud é partilhado por os membros pertencentes a esta comunidade fechada com interesses semelhantes. Um exemplo, de uma cloud da comunidade/partilhada é o Media Cloud, configurado pela Siemens IT Solutions and Services para o setor de media. Quando se trata de um cloud deste tipo, esta pode ser operada por terceiros, ou pode ser controlada e operada de forma coletiva [3].
- **Cloud Híbrida** é uma mistura da cloud privada com a cloud pública. Possibilita manter uns sistemas na cloud privada e outros na cloud pública, simultaneamente. Por exemplo, sistemas críticos ou que manipulam informações confidenciais podem ser utilizados numa rede privada enquanto outros sistemas, que não lidam com dados sigilosos, podem ser utilizados numa rede pública [3].

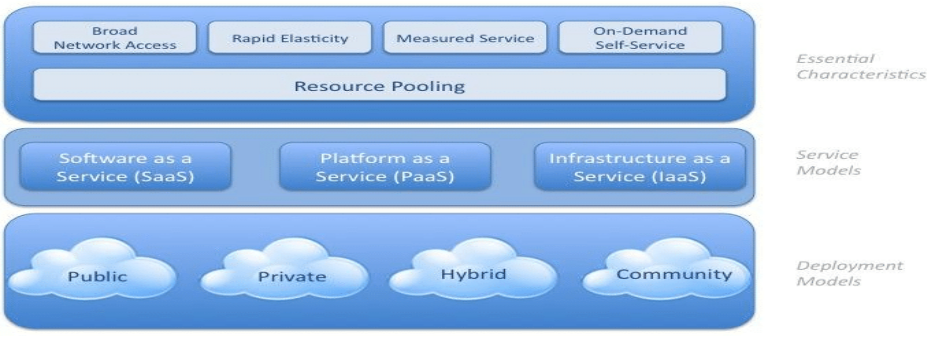

Fig. 2. Tipos de Cloud

3.3 Modelos de Serviços da Cloud

A Cloud pode ser dividida em quatro tipos de Modelos de Serviço. Estes Modelos diferenciam-se principalmente nos recursos disponíveis, a quem é direcionada e a forma como é implementada.

- **Software como Serviço (SaaS)** O modelo de Software como Serviço (SaaS) proporciona softwares com propósitos específicos que estão disponíveis para os utilizadores através da Internet, podendo ser assim acedidos a partir de um navegador Web. No SaaS, o usuário não administra ou controla a infraestrutura subjacente, incluindo rede, servidores, sistemas operacionais, armazenamento, ou mesmo as características individuais da aplicação, exceto configurações especificas. Isto leva ao desenvolvimento rápido de softwares. Como o software esta na Web, ele pode ser acedido pelos utilizadores de qualquer lugar e a qualquer momento, permitindo mais integracao entre unidades de uma mesma empresa. Assim, novos recursos podem ser incorporados automaticamente aos softwares sem que os usuários percebam. O SaaS reduz os custos, pois e dispensada a aquisição de licenças de softwares. Como exemplo de SaaS pode-se destacar o Google Docs.
- **Plataforma como Serviço (PaaS)** O modelo de Plataforma como Serviço (PaaS) oferece uma infraestrutura de alto nível de integração para implementar e testar aplicações na nuvem. O utilizador não administra a infraestrutura subjacente, incluindo rede, servidores, sistemas operacionais ou armazenamento, mas tem controle sobre as aplicações implantadas e sobre as configurações das aplicações. A PaaS fornece um sistema operacional, linguagens de programação e ambientes de desenvolvimento para as aplicações, auxiliando a implementação de softwares.
- **Infraestrutura como Serviço (IaaS)** Infraestrutura como Serviço (IaaS) é parte responsável por prover toda a infraestrutura necessária para a PaaS e o SaaS. O principal objetivo do IaaS e tornar mais fácil e acessível o fornecimento de recursos, tais como servidores, rede, etc. Em geral, o usuário não administra ou controla a infraestrutura da nuvem, mas tem controle sobre os sistemas operacionais, armazenamento e aplicações implantadas, e, eventualmente, seleciona componentes de rede, tais como firewalls. O termo IaaS refere-se a uma infraestrutura computacional baseada em técnicas de virtualização de recursos de computação. Esta infraestrutura pode escalar dinamicamente, aumentando ou diminuindo os recursos de acordo com as necessidades das aplicações.

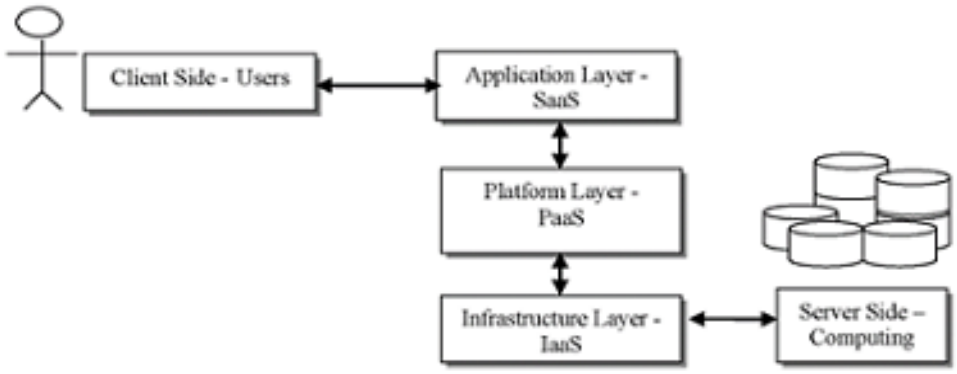

Fig. 3. Relação dos Modelos [9]

3.4 Segurança e Privacidade da Cloud

Os termos Cloud e Virtualização a que hoje em dia estamos sujeitos, são termos que nos levam a pensar nas variadas vantagens que nos podem trazer. Porém ainda são muito frágeis devido à dúvida acerca da total segurança e privacidade dos dados e informação que podemos guardar na própria Cloud.

Segundo um estudo da Gartner em 2012 os servidores virtualizados serão aproximadamente 60% menos seguros que os servidores físicos que eles substituem sendo que seria de esperar que em 2015 estes seriam "apenas" 30% menos seguros. [8]

A segurança de uma Virtual Machine (VM) depende do Sistema Operativo em uso, sendo que se deve seguir as práticas de segurança como se a VM fosse o host. Do ponto de vista da segurança o servidor físico e a VM não são diferentes, existindo duas formas principais de se aceder a uma Virtual Machine. Uma através do sistema que faz correr a própria VM e outra através das conexões da rede. Uma VM comprometida pode ser utilizada para afetar os host servers e outras VMs que estão ligadas à mesma rede física ou virtual. Assim podem ser lançados ataques contra estas Virtual Machines. Sistemas Operativos de Disco também podem ser atacados através de um ataque feito ao próprio host server. No caso de ambiente de Clouds o risco é ainda maior visto que não é necessário comprometer uma VM para se poder atacar outras na mesma rede. Basta pagar por uma cloud service, como se fosse um usuário normal, e começar a atacar evitando os dispositivos de segurança de rede tradicionais. Um ataque à superfície pode ser definido pela natureza e pela extensão dos recursos a que um sistema está exposto e, concretamente, atacável. Toda a virtualização do sistema aumenta a vulnerabilidade visto que além de todos os ataques que uma VM está sujeita, também acrescenta o ataque à Virtual Machine Manager (VMM). Em termos de cloud, tecnologias virtualizadas além de partilhar estes problemas de segurança também são aumentados outros devido à arquitetura de multiutilizador. Devido às Virtual Machines poderem comunicar através do sistema que faz correr as VMs em vez de ser através de rede física, o controlo da segurança das redes tradicionais torna-se inútil e expressa-se uma enorme necessidade destes controlos terem uma nova forma num ambiente também virtual. Outro ponto importante da segurança é a partilha de recursos entre utilizadores, VM's e owners. A não ser que seja desenvolvida uma nova arquitetura que não dependa de nenhuma rede para se proteger, o risco vai estar sempre presente.

A Cloud cai na confiança entre quem a implementou e quem a utiliza, para que os seus dados sejam protegidos e guardados. A confiança cai no pensamento que toda a gente vai agir de forma correta e dentro da lei e não tentará infiltrar/roubar/corromper todas as informações das mesmas.

4 Conclusão

Neste trabalho foi apresentada uma visão geral do que se trata a IoT e como a segurança e privacidade nesta é preservada. Foi também dado a conhecer a tecnologia Cloud. Pela informação recolhida para a realização deste projeto é possível observar que este tema está em constante progressão, sendo encontrados alguns problemas, sendo de imediato, a procura de uma solução para os mesmos. Apesar disto, a Cloud é um modelo recente e por consequência um modelo vulnerável que necessita de uma nova abordagem na resolução deste problema, pois é necessário uma maior segurança e proteção dos nossos dados e privacidade. Quanto a IoT, também é um sistema vulnerável, pois estamos constantemente sujeitos a ataques devido a falhas existentes no sistema. Procura-se assim, a inovação e esta está em unir todos os conceitos num sistema muito maior e mais complexo, sistema esse que ainda possui uma série de desafios, sendo a segurança, sem dúvida o maior deles. É necessário que sejam estudados novos mecanismos de proteção de dados para que a sensação de insegurança por parte dos utilizadores seja reduzida e este modelo tenha uma maior aceitação.

References

1. Zejun Ren, Xiangang Liu, Runguo Ye,Tao Zhang.: Security and Privacy on Internet of Things (2017)
2. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ .: Internet of Things (IoT) connected devices
3. Weiwei Kong, Yang Lei, Jing Ma.: Data Security and Privacy Information Challenges in Cloud Computing (2016)
4. Sophia Moganedi, Jabu Mtsweni.: Beyond the Convenience of the Internet of Things: Security and Privacy Concerns (2017)
5. Glenn A. Fink, Dimitri V. Zarzhitsky, Thomas E. Carrol and Ethan D. Farquhar .: Security and Privacy Grand Challenges for the Internet of Things (2015)
6. Descrição geral de Cloud.: https://azure.microsoft.com/pt-pt/overview/what-is-the-cloud/
7. Imagem Cloud.: https://www.researchgate.net/figure/NIST-Visual-Model-of-Cloud-Computing-a-Service-Models-Cloud-computing-can-be-classified$_{fig2_241195178}$
8. Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore .: Cloud Computing Security (2013)
9. Imagem da relação dos modelos da Cloud Sean Carlin (University of Ulster, UK) and Kevin Curran (University of Ulster, UK) Cloud Computing Security