20º WRNP Workshop RNP | 6 E 7 DE MAIO GRAMADO | RS

SAMD4IoT - Serviço de autenticação multicamada para dispositivos de Internet das Coisas

EQUIPE

Coordenador :
Kleber Vieira Cardoso (UFG)

Equipe executiva:
Marcos Felipe Barboza de Abreu (UFG)
Pabllo Felipe Sousa Alves (UFG)

PARCEIROS
Microsoft
UFG

SITE
samd4iot.labora.inf.ufg.br

CONTATO
kleber@inf.ufg.br

DESCRIÇÃO

A Internet das Coisas trouxe novos desafios em segurança e autenticação. O rápido aumento do número de coisas conectadas impôs uma carga adicional aos administradores de rede para gerenciar as redes, sobretudo, em termos de segurança. Essa é a razão pela qual o gerenciamento de identidades deve ser considerado um desafio-chave na Internet das Coisas.

Um ataque bastante conhecido em redes de computadores, que se repete em *IoT*, é o roubo de identidade. A diferenciação de dispositivos sem fio, por padrão, é baseada em identificadores únicos, como o endereço MAC (*Media Access Control*) no Bluetooth e no Wi-Fi. Entretanto, esses identificadores podem ser forjados por alguém mal intencionado para se passar pelo dispositivo, abrindo assim portas para execução de outros ataques. Outro problema, envolvendo segurança em *IoT*, é a autenticação de aplicações, onde um dispositivo pode ser comprometido e passar a transmitir dados falsos.

Dados esses desafios de segurança em *IoT*, propomos uma solução que fornece um serviço de autenticação externo aos dispositivos *IoT*, baseado no padrão de transmissão do sinal de radiofrequência do dispositivo e de padrões de transmissão das suas aplicações, fornecendo um serviço de autenticação de camada física e de aplicação (ou serviço).

Solução proposta

A primeira forma de autenticação é baseada na camada física. Dispositivos sem fio podem ser diferenciados com base em sua assinatura eletromagnética, coletada na camada física. A diferenciação de placas é possível devido a imperfeições, não propositais, criadas nos chips no processo de fabricação dos módulos geradores de sinais. Com base nisso é possível analisar o sinal transmitido por um dispositivo e criar uma assinatura para o mesmo.

Recentemente, a equipe desse projeto implementou uma prova de conceito analisando o sinal eletromagnético de placas nrf24L01. Os resultados mostram que podemos atingir uma alta acurácia na diferenciação das placas utilizando técnicas simples de aprendizado de máquina. A solução pode ser estendida para os diversos padrões de rede sem fio. Em outro trabalho, ainda em processo de revisão para a publicação em uma revista, analisamos a acurácia da classificação perante cenários onde há ruídos e interferências.

A segunda forma de autenticação (de aplicações) é baseada nos dados coletados na camada de rede, tornando possível criar uma identidade baseada nos padrões das aplicações (ou serviços) que o dispositivo utiliza ou fornece. Além de roubo de identidade, essa técnica pode ser usada para detectar dispositivos comprometidos na rede, visto que o dispositivo passa a se comunicar de forma diferente, i.e., apresentando outro padrão.

Metodologia do desenvolvimento da solução

O primeiro passo na metodologia é a coleta e a preparação dos dados. Nesta fase faremos vários experimentos, com o objetivo de decidir quais os melhores algoritmos de classificação e quais as melhores características para o modelo. Os algoritmos de Aprendizado de Máquina na fase de treinamento requerem máquinas potentes, com alto poder de processamento. A Microsoft, parceira do projeto, disponibilizará recursos na plataforma Azure para os testes da solução. A plataforma oferece um serviço, denominado *Azure Machine Learning Service* , que permite criar soluções completas de Aprendizado de Máquina e facilmente colocá-las em produção.

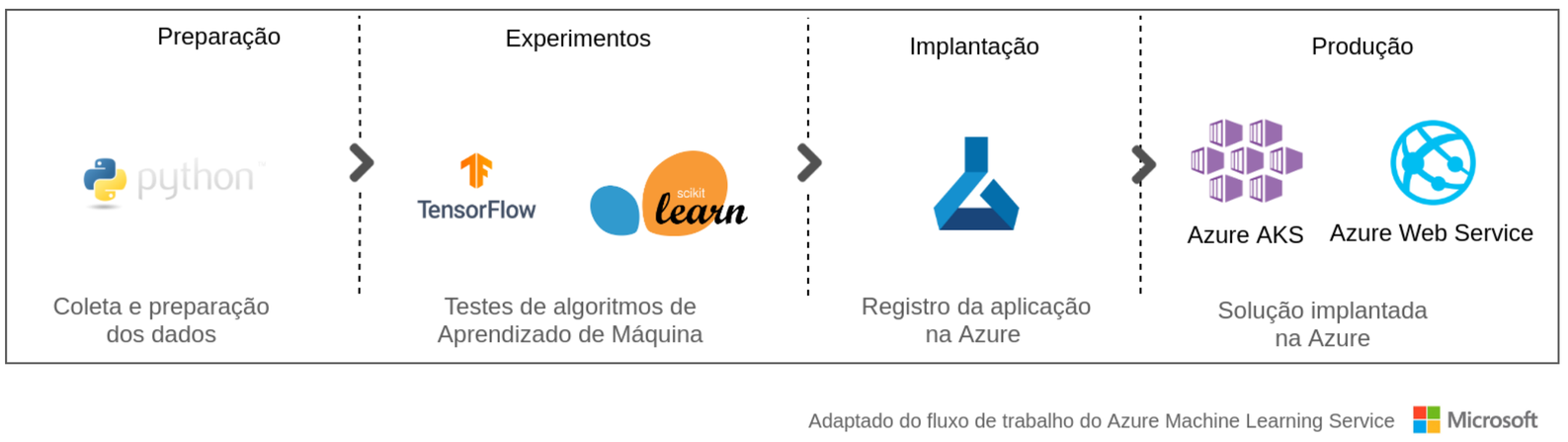

Fig. 1: Metodologia a ser aplicada no desenvolvimento da solução.

Após a fase experimental, quando se tem o modelo já testado e finalizado, pode-se implantá-lo facilmente na nuvem, em contêineres *Docker* que são gerenciados pela Azure através do *Kubernetes*, provendo escalabilidade para o serviço de acordo com a utilização do mesmo. A Figura 1 ilustra esse processo.

Arquitetura

A Arquitetura do serviço é composta por dois módulos, local e na Nuvem. A aplicação do cliente, que deseja verificar a autenticidade de um dispositivo, interage com o módulo local do SAMD4IoT enviando os dados recebidos para a análise. O módulo local (SDK) poderá receber como entrada as informações de duas formas:

- **Dados da camada física**: Obtidos através de um rádio definido por software (SDR), que irá receber os dados dos sinais eletromagnéticos transmitidos pelo dispositivo e extrair as características necessárias.
- **Dados da camada de rede**: Obtidos dos dispositivos através de uma interface de rede.

A partir desses dados são extraídas as características necessárias para a geração da assinatura. O SDK interage com o módulo na nuvem através de uma API, enviando o padrão extraído e requisitando a autenticação.
O módulo que opera na nuvem é responsável pela classificação e tomada de decisão. O custo da classificação pode se tornar alto conforme novos dispositivos vão sendo inseridos na rede e a nuvem possibilita o redimensionamento de recursos, possibilitando a escalabilidade do serviço conforme o crescimento do número de dispositivos. Esse módulo atuará como um serviço na plataforma da Azure, podendo atender diversos clientes.

Após a análise dos dados, o serviço informará se o dispositivo que está transmitindo a informação é válido ou não. Caso o classificador identifique um comportamento anômalo o cliente será alertado, cabendo a ele tomar a decisão do que fazer.

Interação do usuário com o serviço

A interação do usuário com o SAMD4IoT acontecerá através de um painel de controle. Nele será possível ver os dispositivos cadastrados, monitorar o serviço de autenticação através de gráficos, ver estatísticas de alertas, gerenciar módulos ativos, dentre outras funções.
A Figura 3 apresenta o protótipo do painel de controle.

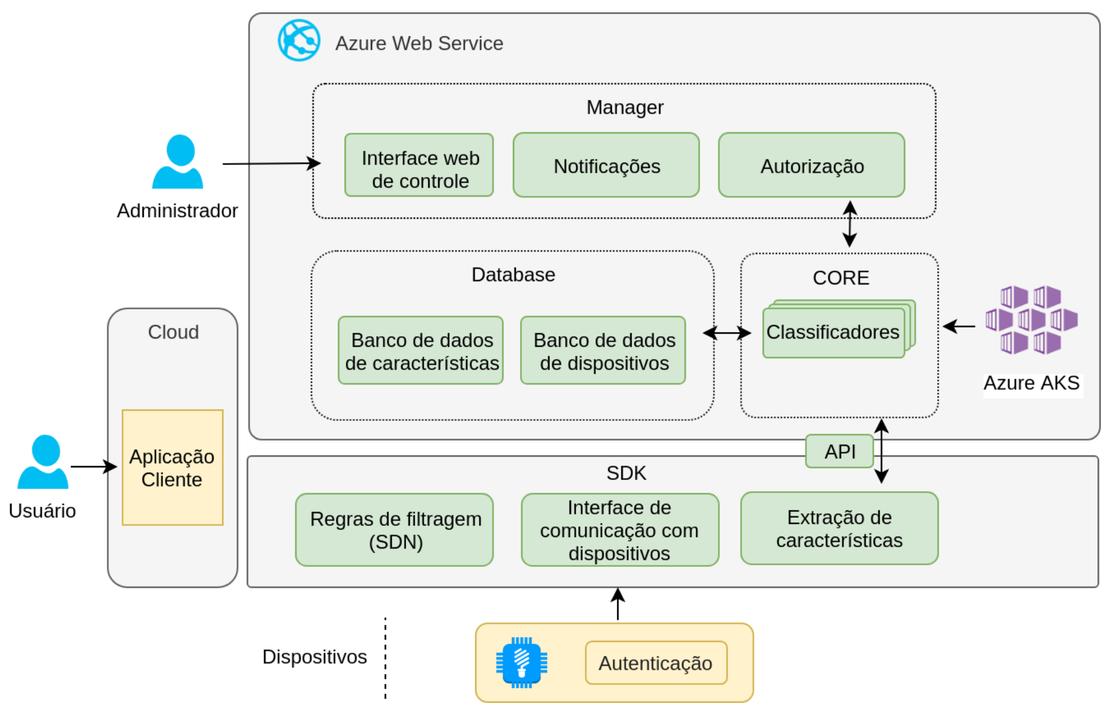

Fig. 2: Arquitetura da solução

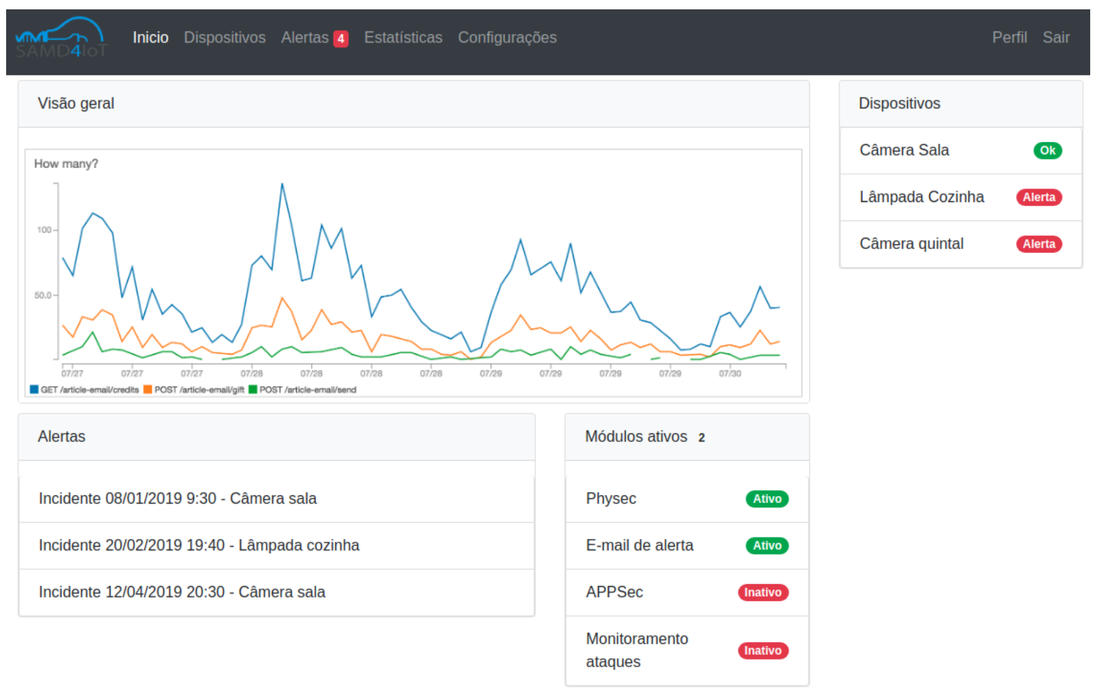

Fig. 3: Painel de Controle, em que o usuário pode gerenciar o serviço