APRIMORANDO O *SMARTPARKING* ATRAVÉS DO USO DE CRIPTOGRAFIA COMPLETAMENTE HOMOMÓRFICA

Palavras-Chave: criptografia completamente homomórfica, machine-learning, privacidade de dados

Autores:

Pedro da Rosa Pinheiro, IC – UNICAMP

Prof. Dr. Hilder Vitor Lima Pereira, IC - UNICAMP

INTRODUÇÃO:

O projeto *SmartCampus*[1], desenvolvido e implementado na Universidade Estadual de Campinas (Unicamp), objetiva integrar técnicas e tecnologias de IoT (do inglês, *Internet of Things*) no espaço universitário, de modo a automatizar tarefas e facilitar o cotidiano daqueles que frequentam o campus. O projeto iniciado em 2016 é composto por diversos programas que envolvem múltiplos setores do ambiente universitário.

O *SmartParking* (Baggio et al., 2020), como parte do *SmartCampus*, tem como objetivo específico monitorar e verificar a ocupação de estacionamentos através de dispositivos IoT, com intuito de auxiliar usuários a acharem vagas livres dentro do campus. O sistema utiliza câmeras para obter imagens em tempo real dos estacionamentos e, com dispositivos locais como minicomputadores de placa única do tipo *Raspberry Pi*, aplica um algoritmo de *Deep Learning* para classificação de objetos e reconhecimento de vagas ocupadas.

Todavia, tal solução apresenta dificuldades na etapa de processamento, visto que os algoritmos de aprendizado de máquina utilizados são computacionalmente custosos. Com o poder computacional menor de um *Raspberry*, a precisão da classificação e da predição também é afetada negativamente. Em vista disso, uma alternativa envolve terceirizar tal etapa através de serviços de computação em nuvem, que, com poder computacional maior, garantem um melhor desempenho no reconhecimento de vagas livres. Contudo, essa alternativa requer necessariamente o compartilhamento das imagens feitas pelas câmeras com empresas privadas, estratégia essa que quebraria legislações, como a Lei Geral de Proteção de Dados (Lei 13.709/2018), vide o fato de as imagens conterem modelos de carros e suas placas associadas, rostos e identidades de indivíduos em ambiente público, entre outros fatores.

Para resolver tais problemas relacionados à privacidade, esquemas criptográficos são utilizados há décadas. Porém, cifras tradicionais não suportam processamento privativo de informações.

[1] https://smartcampus.prefeitura.unicamp.br

Diferentemente, a criptografia completamente homomórfica (CCH) não só garante a confidencialidade cifrando os dados em criptogramas, como também permite o processamento desses criptogramas, i.e., permite que terceiros possam computar qualquer função sobre dados cifrados, sem que sejam descriptografados. Consequentemente, a confidencialidade das informações é mantida ao longo de todas as etapas de uma análise realizada, por exemplo, em plataformas privadas de computação em nuvem.

Isto posto, esse projeto de pesquisa buscou avaliar as melhores formas de aplicar criptografia completamente homomórfica ao projeto *SmartParking*. Analisando diferentes redes neurais subjacentes e algoritmos e estratégias nas etapas cifradas, estuda-se os vários *tradeoffs* entre precisão e eficiência associados à adaptação à CCH. Além disso, as soluções propostas foram implementadas em *C*++, utilizando a principal biblioteca *open-source* moderna de CCH, OpenFHE[2].

METODOLOGIA:

A problemática do projeto *SmartParking,* bem como proposto, envolve a dificuldade de conciliar eficiência e privacidade na análise das fotografias dos estacionamentos. A solução proposta nesse projeto baseada em CCH pode ser dividida em duas partes, isto é, a do cliente e a do servidor.

A primeira refere-se às câmeras que coletam as fotos, aos minicomputadores que as processam e aos aplicativos que recebem e exibem a quantidade de vagas livres. Sendo assim, o lado do cliente foi incrementado com a implementação de funções de geração de chaves, cifração e decifração. Juntamente, é nessa etapa que o pré-processamento das imagens é realizado. Através de *scripts* desenvolvidos em *Python*, as fotografias do estacionamento são redimensionadas, recortadas e separadas para ficarem de acordo com as dimensões de entrada da rede neural construída.

Já a etapa do servidor é a responsável pela predição cifrada em si. Dentre uma gama de esquemas criptográficos possíveis, o escolhido foi o CKKS (Cheon et al., 2017), devido ao fato dele trabalhar nativamente com um tipo de dado que imita o ponto flutuante, sendo, portanto, compatível com aplicações e funções que processam valores reais ou aproximados, como é o caso de redes neurais.

O problema, no projeto *SmartParking*, era abordado com um algoritmo de reconhecimento de objetos que tentava separar os carros do demais itens no estacionamento e, a partir disso, contabilizar o número de vagas disponíveis. No entanto, visando reduzir a complexidade tanto das ferramentas e algoritmos quanto do problema em si, propõe-se nesse projeto, também, uma nova abordagem ao problema, abordagem essa que analisa cada vaga individualmente pela presença de um carro ocupando-a.

Assim, com tal estratégia e esquema criptográfico escolhidos, foram testados diversos modelos, com e sem filtros convolucionais, testes esses que resultaram na escolha de um modelo com apenas uma camada escondida densa, de 3 neurônios, que utilizam a função x^2 como função de ativação.

[2] https://www.openfhe.org/

Assim, ambos segmentos da solução proposta podem ser visualizados de forma integral na Figura 1 abaixo.

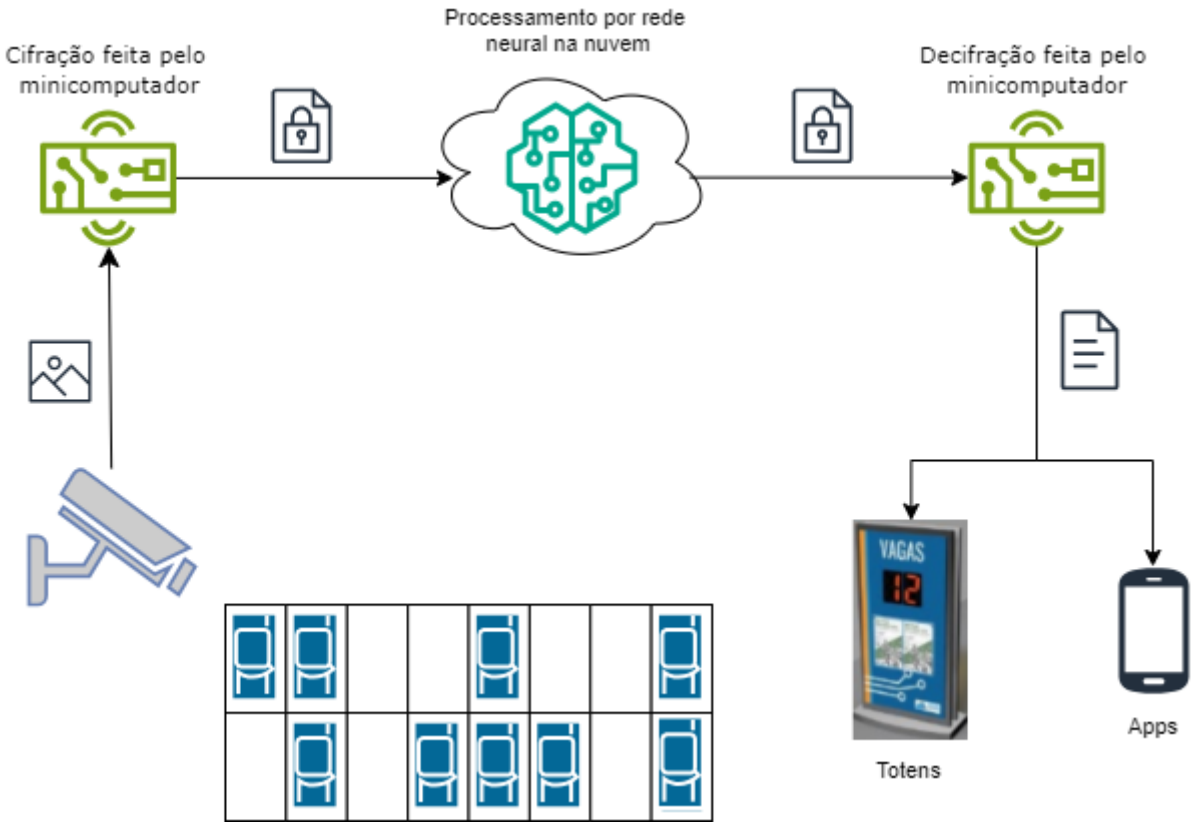

Figura 1: Arquitetura do sistema SmartParking implementado com criptografia completamente homomórfica.

Primeiramente, as imagens dos estacionamentos capturadas em tempo real pelas câmeras serão enviadas para os minicomputadores, onde seriam cifradas com CCH, e em seguida enviadas à uma plataforma de computação em nuvem. Nela, os criptogramas seriam processados em uma rede neural homomórfica, de modo a gerar a quantidade de vagas disponíveis. Válido notar que esse resultado também estaria cifrado. Assim, o criptograma resultante seria enviado novamente para o *Raspberry Pi*, onde a função de decifração seria executada, obtendo, por fim, o número, em claro, de vagas livres, que poderia ser então enviado aos aplicativos do lado do cliente, como no celular e totens presenciais.

RESULTADOS E DISCUSSÃO:

Embora simples quando comparada a arquiteturas comumente utilizadas em redes convolucionais, como a YOLO (Redmon et al., 2016) ou a ResNet (He et al., 2015), a rede final selecionada apresentou resultados relevantes para o problema em discussão. Construída e treinada sob as imagens em claro utilizando *frameworks* de aprendizado de máquina como *TensorFlow*[3], obteve 98.59% de acurácia no conjunto de treinamento e 98.37% no conjunto de validação, levando menos de 1 segundo para a inferência. Objetivando verificar a possibilidade de *overfitting* do modelo, realizamos

[3] https://www.tensorflow.org/?hl=pt-br

inferências sobre o conjunto de dados de teste, até então não utilizados, cujos resultados podem ser observados na Figura 2 abaixo.

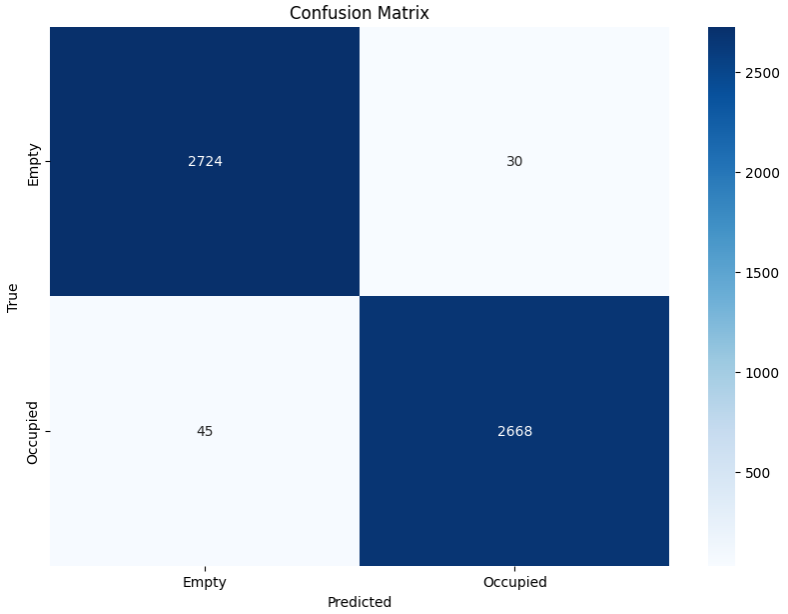

Figura 2: Matriz de confusão do modelo final construído

Importante ressaltar que a arquitetura final escolhida foi resultado de um processo de construção de diversos modelos com diferentes arquiteturas. Assim, uma estrutura era treinada, testada e, com base nos resultados, se julgado válido, construía-se uma versão mais simples, objetivando minimizar o tamanho através de baixas profundidades e larguras e, simultaneamente, manter uma alta acurácia.

Já no que se refere à eficiência computacional do modelo cifrado, foram realizados testes em um computador equipado com um Intel Core i5-1235U de 10 núcleos e 16GB de memória RAM DDR4. Assim, com a arquitetura de rede descrita, mantendo o grau de acurácia acima de 98%, é possível avaliar todo o processo do projeto localmente, isto é, desde cifração da imagem relativa a cada vaga até o valor decifrado da inferência, sem o uso de um servidor na nuvem, em, aproximadamente, 16.7 segundos.

CONCLUSÕES:

Conclui-se, portanto, que a aplicação de criptografia completamente homomórfica para o projeto *SmartParking* envolve um grande processo de adaptação, não somente técnica, mas do problema base em si. O que se tratava, originalmente, de um problema de reconhecer e contabilizar o número de carros dentre todos os objetos de uma imagem, foi reduzido para, dada a imagem de uma vaga, descobrir se a mesma está ocupada.

No entanto, tal adaptação facilitar com que o projeto respeite as limitações éticas no que se refere às informações sigilosas contidas em cada imagem do estacionamento do campus universitário. Embora venha à um custo de, atualmente, aumento do tempo de inferência em mais de 1500% em relação ao valor com a rede em claro, foi possível manter o relevante grau de acurácia enquanto, simultaneamente, fornecendo privacidade.

O projeto ainda está em constante desenvolvimento e será alvo de constantes atualizações e incrementações. O próximo objetivo a ser alcançado é interligar os minicomputadores *Raspberry Pi* com servidores na nuvem, possibilitando uma integração maior e permitindo a análise de viabilidade e de eficiência que uma arquitetura cliente-servidor garante ao projeto.

BIBLIOGRAFIA

BAGGIO**,** João V.; GONZALEZ, Luis F.; BORIN, Juliana F.; **SmartParking: A smart solution using Deep Learning. 2020.** Disponível em:. Acesso em: 30/07/2025.

CHEON, Jung H.; KIM, Andrey; KIM, Miran; SONG, Yongsoo; **Homomorphic encryption for arithmetic of approximate numbers.** Em Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 409-437, Cham, 2017. Springer International Publishing.

REDMON, Joseph; DIVVALA, Santosh; GIRSHICK, Ross; FARHADI, Ali; **You only look once: Unified, real-time object detection. 2016.** Disponível em: https://arxiv.org/pdf/1506.02640. Acesso em: 04/08/2025.

HE, Kaiming; ZHANG, Xiangyu; REN, Shaoqing; SUN, Jian. **Deep residual learning for image recognition. 2015.** Disponível em: https://arxiv.org/pdf/1512.03385. Acesso em: 04/08/2025.