UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

VINICIUS HENRIQUE SOARES

DESENVOLVIMENTO DE APLICAÇÕES COM INTEL SGX PARA COMPUTAÇÃO CONFIDENCIAL: UMA ANÁLISE QUANTITATIVA E QUALITATIVA

CAMPO MOURÃO

2023

VINICIUS HENRIQUE SOARES

DESENVOLVIMENTO DE APLICAÇÕES COM INTEL SGX PARA COMPUTAÇÃO CONFIDENCIAL: UMA ANÁLISE QUANTITATIVA E QUALITATIVA

Developing Applications with Intel SGX for Confidential Computing: A Quantitative and Qualitative Analysis

Trabalho de conclusão de curso de graduação apresentado como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação, Universidade Tecnológica Federal do Paraná (UTFPR).
Orientador: Rodrigo Campiolo.

CAMPO MOURÃO

2023

VINICIUS HENRIQUE SOARES

DESENVOLVIMENTO DE APLICAÇÕES COM INTEL SGX PARA COMPUTAÇÃO CONFIDENCIAL: UMA ANÁLISE QUANTITATIVA E QUALITATIVA

Trabalho de conclusão de curso de graduação apresentado como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação, Universidade Tecnológica Federal do Paraná (UTFPR).

Data de aprovação: 16/junho/2023

Rodrigo Campiolo
Doutorado
http://lattes.cnpq.br/2822469089227391
Universidade Tecnológica Federal do Paraná

Luiz Arthur Feitosa Dos Santos
Doutorado
http://lattes.cnpq.br/3725232561617394
Universidade Tecnológica Federal do Paraná

Rogério Aparecido Gonçalves
Doutorado
http://lattes.cnpq.br/1677599200632096
Universidade Tecnológica Federal do Paraná

CAMPO MOURÃO

2023

RESUMO

SOARES, Vinicius Henrique. **Desenvolvimento de aplicações com Intel SGX para computação confidencial: Uma análise quantitativa e qualitativa**. 2023. Trabalho de conclusão de curso (Bacharelado em Ciência da Computação) – Universidade Tecnológica Federal do Paraná, Campo Mourão, 2023.

A computação em nuvem apresenta problemas de segurança durante o processamento de dados, visto que não há medidas de proteção eficientes implementadas na execução de programas ou até mesmo no hardware em que será executado. Uma solução para esse problema é a aplicação de computação confidencial, que utiliza métodos para tornar o processamento de dados mais seguro. No entanto, por ser recente, as técnicas podem apresentar perda de desempenho. Este trabalho tenta avaliar o impacto causado no desenvolvimento e no desempenho pela tecnologia de computação confidencial Intel SGX. Para tal, foram criadas duas aplicações, em duas versões cada, uma versão base para controle e uma versão utilizando o Intel SGX. A primeira aplicação realiza operações matemáticas, que deverão ser tratadas e criptografadas pelo SGX em diferentes momentos. Já a segunda aplicação consiste na execução de um algoritmo de ordenação processado totalmente pelo SGX, para assim avaliar o processamento de um grande volume de dados. Foram realizadas medições para avaliar o desempenho obtido em cada um dos cenários. Considerando os resultados da primeira aplicação, a aplicação base obteve melhor desempenho, já na segunda, a aplicação com Intel SGX obteve melhor desempenho. A execução dos experimentos revelou diversas dificuldades para adaptar um programa para suportar a tecnologia, mostrando que a opção de uso em aplicações consolidadas deve ser extensivamente avaliada. Entretanto, a sua utilização pode ser considerada para aplicações novas.

Palavras-chave: cibersegurança; desempenho; computação em nuvem; enclave; hardware confiável.

Autorizo a disponibilização do seguinte correio eletrônico para contato:
viniciussoares@alunos.utfpr.edu.br

ABSTRACT

SOARES, Vinicius Henrique. **Developing Applications with Intel SGX for Confidential Computing: A Quantitative and Qualitative Analysis**. 2023. Trabalho de conclusão de curso (Bacharelado em Ciência da Computação) – Universidade Tecnológica Federal do Paraná, Campo Mourão, 2023. Desenvolvimento de aplicações com Intel SGX para computação confidencial: Uma análise quantitativa e qualitativa.

Cloud computing presents security problems during data processing, since there are no efficient protection measures implemented in the execution of programs or even in the hardware in which it will be executed. One solution to this problem is the application of confidential computing, which uses methods to make data processing more secure. However, as it is recent, the techniques may present loss of performance. This paper attempts to assess the impact on development and performance of Intel SGX confidential computing technology. For this, two applications were created, in two versions each, a base version for control and a version using Intel SGX. The first application performs mathematical operations, receiving values outside the enclave and processing them inside. The second application consists of running a sorting algorithm within the enclave, in order to evaluate the processing of a large volume of data in the enclave. Measurements were carried out to evaluate the performance obtained in each of the scenarios. In the results of the first application, the base application had better performance, in the second, the application with Intel SGX had better performance. The execution of the experiments revealed several difficulties to adapt a program to support the technology, showing that the option of using it in consolidated applications must be extensively evaluated. However, its use can be considered for new applications.

Keywords: cybersecurity; performance; Cloud computing; enclave; trusted hardware.