Security Implications of Parallelism in Cloud Computing: Addressing Race Conditions and Side-Channel Attacks

Abstract:

This study explores the critical security vulnerabilities introduced by parallel computing in cloud environments, specifically focusing on race conditions and side-channel attacks. In cloud systems, parallelism is essential for enhancing performance, scalability, and efficiency; however, it also creates new attack vectors that can undermine data integrity, confidentiality, and overall system security. Race conditions occur when multiple processes in a parallel system access shared resources without proper synchronization, potentially leading to data inconsistencies and security breaches. Side-channel attacks exploit physical characteristics like timing or cache usage in shared cloud resources to infer sensitive information. These vulnerabilities are particularly concerning in cloud environments, where multi-tenancy and dynamic resource allocation heighten the risk of exploitation. In this study, we will provide a detailed theoretical analysis of both race conditions and side-channel attacks within cloud computing, investigate how these threats manifest in practical cloud scenarios, and propose strategic mitigation techniques. Our findings aim to contribute to the field of secure parallel computing by offering theoretical solutions to these persistent security challenges.

Key Words: Parallel Computing, Cloud, Race Conditions, Side-Channel Attacks, Security.

Name: Mohith Ankem

SJSU ID: 017400825

E-Mail: Mohith.Ankem@sjsu.edu