CERTIFICATE NO : NCRASETHM /2024/C0124125

MITIGATING THE THREAT OF ZOMBIE ATTACKS IN CLOUD COMPUTING

S M FIRDAUS ZAKI RIZVI

Research Scholar, Ph. D. in Computer Science, Dept. of. Mathematics and Computer Science
Magadh University, Bodh Gaya - Bihar, India.

ABSTRACT

The proliferation of cloud computing has revolutionized IT infrastructure by providing scalable and flexible resources. However, this shift has also introduced new security vulnerabilities, notably the Zombie Attack, a sophisticated form of distributed denial-of-service (DDoS) attack. Zombie Attacks involve the hijacking of virtual machines (VMs) in the cloud, which are then used to disrupt services, steal data, and cause significant financial and reputational damage. This study delves into the architecture of cloud computing to understand the vulnerabilities that facilitate such attacks. We analyse the lifecycle of a Zombie Attack, from initial compromise to execution, and assess the effectiveness of current defensive measures. Our research proposes a novel mitigation approach that combines predictive analytics, adaptive firewalls, and decentralized monitoring to detect and prevent these attacks. We validate our approach through a series of controlled experiments, demonstrating a significant reduction in attack success rates and improved resilience of cloud services. Our findings provide actionable insights for cloud service providers and security professionals aiming to safeguard their infrastructures against emerging threats.