

**CHENNAI – PONDICHERRY**

**Architectural Protection of Application Privacy Against Software and Physical Attacks in Untrusted Cloud Environment**

**Abstract:**

In cloud computing, it is often assumed that cloud vendors are trusted; the guest Operating System (OS) and the Virtual Machine Monitor (VMM, also called Hypervisor) are secure. However, these assumptions are not always true in practice and existing approaches cannot protect the data privacy of applications when none of these parties are trusted. We investigate how to cope with a strong threat model which is that the cloud vendors, the guest OS, or the VMM, or both of them are malicious or untrusted, and can launch attacks against privacy of trusted user applications. This model is relevant because applications may be small enough to be formally verified, while the guest OS and VMM are too complex to be formally verified. Specifically, we present the design and analysis of an architectural solution which integrates a set of components on-chip to protect the memory of trusted applications from potential software and hardware based attacks from untrusted cloud providers, compromised guest OS, or malicious VMM. Full-system performance evaluation results show that the design only incurs 9% overhead on average, which is a small performance price that is paid for the substantial security gain.

**Existing System:**

In particular, cloud users are confronted with a more complex software stack, which includes the Virtual Machine Monitor (VMM) or hypervisor, and the guest Operating System (OS). The importance of secure cloud computing has been well recognized and there have been studies on various aspects of cloud security. However, it is often assumed that the cloud vendor is trusted; the guest OS and VMM are secure. These assumptions are questionable given the discovery of vulnerabilities in the commodity VMM and the fact that OS vulnerabilities often facilitate cyber attacks.

**Proposed System:**

The processor deployed in the cloud computing infrastructure is fully trusted. They can store secret values safely and it is very hard for an attacker to tamper the computation process;

VMM and guest OS are not trusted. Due to potential vulnerabilities, an attacker may access the application’s data without permission;

The cloud vendor is not trusted. The cloud computing vendor may also take advantage of high privilege to snoop the application’s data even if both the VMM and guest OS are in normal running statuses;

The application running on top of guest OS is also fully trusted. The application is free from backdoors/ trojans and it is hard for an attacker to break into the application and cause information leakage.