Chapter 5
Side Channel Attacks in Cloud Computing

Ramanujam Elangovan
Thiagarajar College of Engineering, India

Prianga M.
Thiagarajar College of Engineering, India

ABSTRACT

Cloud computing is used for storing and managing information using the remote servers, which is hosted on the internet instead of storing it in a normal server or personal computer. The main purpose of why most of the companies use the cloud for storing and managing data is to not have to pay money for storing data. The main aim is to allow users to benefit from all technologies. Virtualization is considered to be the main technology of cloud computing. Several privacy concerns are caused by the cloud because the service provider can access the data at any time. Cloud providers can also share the information for the purpose of law and order. The information gathered from the physical implementation is called a side channel attack. Some technical knowledge is required for side channel attacks and these attacks are based on statistical methods. It works by monitoring the security critical operations. The side channel attack is based on the information which is leaking and the information which is kept secret.

INTRODUCTION

Cloud computing is an open, widespread version, that's net-centric and gives various offerings both software or hardware. It offers new cost powerful offerings on-demand together with Software program as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). A massive interest in each enterprise and academia has been generated to discover and beautify cloud computing. It has 5 critical traits: on-call for self-provisioning, measured provider, speedy elasticity, extensive community get entry to and useful resource pooling. It's far aiming at giving abilities to apply effective computing structures to reduce value, boom efficiency and performance (Manikandakumar, 2018). It consolidates the monetary application version with the evolutionary enhancement of many utilized computing methods and technology, which consist of computing infrastructure along with networks of

DOI: 10.4018/978-1-5225-7522-1.ch005

computing and storage assets, applications and distributed services. Furthermore, there is an ongoing debate in Information Technology (IT) groups approximately that how cloud computing paradigm differs from existing models and how these variations have an effect on its adoption. One view remembers it as a current or a fashionable way to supply services over the net, even as others see it as a novel technical revolution (Younis, 2015).

However, with all of these promising centers and blessings, there are still some of technical barriers which could prevent cloud computing from becoming a genuinely ubiquitous provider (Haldorai, 2018). Mainly a consumer has strict and complex requirements over the safety of an infrastructure. Security is the primary inhibitor to cloud adaptation. Cloud computing may additionally inherit some security risks and vulnerabilities from the internet, such as malicious code like Viruses, Trojan Horses. Further, cloud computing suffers from facts privateness problems and conventional disbursed structures attacks, i.e. Disbursed Denial of provider attacks (DDoS), which can have a massive effect in its offerings. Moreover, cloud computing has added new issues together with shifting resources and storing information inside the cloud with a probability to be living in a foreign country with unique policies. Computing sources can be inaccessible because of many motives which includes natural disaster or denial of carrier.

Cloud computing is a shared surroundings in which stocks massive-scale of computing sources among big purchasers (organizations and organizations) comprising a huge quantity of users. Therefore, cloud computing tenants will equally share the physical sources and are in all likelihood to face co-residence vulnerabilities. Virtual Machine (VM) physical co-residency enables attackers to intrude with other digital machines going for walks at the equal physical machine by using hardware aspect-channels. In the worst state of affairs, attackers can exfiltrate victims' sensitive and personal data. There are numerous styles of aspect-channels attacks, which might be labeled consistent with a hardware medium they target and take advantage of, for example, cache side-channel assaults. Cache side-channel assaults are forms of Micro Architectural attacks (MA), which is a huge group of cryptanalysis techniques within the aspect-channel evaluation attacks.

This chapter have a look at side-channel attacks and also have a look at how the effect on the multitenancy and virtualization in cloud computing. It defines aspect-channel attacks offerings, The organization of this paper is structured as follows. Session 2 illustrates side-channel attacks and its effect on virtualization. Phase three describes extraordinary sorts of cache side-channel attacks and the way they can extract records from CPU caches. Indicates gaps within the current researches and some of proposed countermeasures to cache aspect- channel attacks in cloud computing.

In computing, the multi-tendency has the biggest advantage because the physical resource is shared among multiple client with the aid of the hypervisor, virtualization assists multitendency. Using the hypervisor, cloud provider utilizes the resource like CPU, network interfaces, memory and hard disk. Virtual machines are running on the same core machine which leads to the malicious or abnormal attacks like side channel attacks. The various types of side channel attacks are: Fault attacks, Power Analysis attacks, electromagnetic (EM) attacks, cache-based attacks. But in cloud, the cache-based side channel attacks are creating the major issues. The different VMs on the same core use the cache resources.

The cache is the similar to the CPU cache memory which contain various level of cache. In processor, there are various levels of cache are presented. The user request the date to cache and if the data are not in the cache memory, cache misses will occur due to the cause of main memory reference. Whenever main memory reference occurs, it takes more time to identify the content. In that situation, the attacker performs the cache based attack during that time to read the content in the memory. CPU cache is one of the major threat in the cloud computing (Anandakumar & Umamaheswari, 2018).