ABSTRACT

Cloud computing is an emerging technology that allows multiple users to access the computational resources and data over the internet. It supports multi-tenancy to satisfy the users' demands for accessing resources and simultaneously it increases revenue for cloud providers. Cloud providers adopt multi-tenancy by virtualizing the resources like CPU (Central Processing Unit), network interfaces, peripherals, hard drives and memory using a hypervisor to fulfill the demand. In a virtualized environment, many virtual machines (VMs) instances are created and managed on the same core with the help of the hypervisor by sharing the resources. The virtual machines (VMs) running on the same core are the target for the malicious or abnormal attacks. These attacks may include data leakage, privacy breach and unauthorized access to cloud resources. These attacks may be due to inside attackers or outside attackers in a cloud environment. The outsider attacks may be, server spoofing attack, stolen verifier attack, password guessing attack, impersonation attack and replay attack which occur at the network layer of the cloud. Similarly, the insider attacks may be side channel attacks to gain access to shared resources. Since the technology is based on the sharing of resources, lack of security is a major issue. To secure the cloud environment from inside and outside attacks, this research proposes a new system with an intention to provide secured access to computational resources through virtual machines. The proposed system works in three different phases to secure the virtual machines in cloud architecture.

In the first phase of security, registration and mutual multilevel authentication are performed by proposing a novel protocol called as Adaptive Mutual Multilevel Authentication Protocol (AMAP) to handle outside attackers. This protocol is proposed in two phases: Registration and Authentication. The Authentication Center (AC) authenticates the user and the server using four different messages. The cloud user is verified using hashing function and ECC (Elliptic Curve Cryptography). The verification follows a six-level of the authentication process to allocate the virtual machines to access the computational resources in the cloud. The proposed protocol provides security, considering multiple parameters like OTP (One Time Password), session password, and so on. This protocol will
provide resistance against server spoofing attack, stolen verifier attack, password guessing attack, impersonation attack and replay attack. Thus, the protocol will allow the cloud user to gain secure access to the virtual machine by offering robustness with the utilization of Elliptic Curve Cryptography (ECC) and a hashing function.

In the second phase, the detection of insider attack is proposed. Here the insider attack is the cache side-channel attack on virtual machines. Virtual machines (VMs) running on the same core are the target for the malicious or abnormal attacks like side-channel attacks like fault analysis, acoustics attacks, electro-magnet attacks, cache-based side channel attacks. Among these various side-channel attacks in cloud computing, cache-based side channel attack is one that leaks private information of the users based on the shared resources. A process running inside the VM can utilize the cache of another VM creating cache contention in the system. Cache sharing provides a way for the attackers to gain considerable information so that the key used for encryption can be inferred. Discovering this side channel attack is a challenging task. This requires identification of a feature that influences the attack. Even though there are various techniques available in the literature to mitigate such attacks, a practical solution to reduce and mitigate the cache-based side channel attack is still an issue. Therefore, the proposed work integrates a novel fuzzy rule-based mechanism to detect and mitigate the cache side-channel attacks by monitoring the cache data access. The primary factor that determines the attack is CDA (Cache Data Access) in a log file created by the methodology during the authorization of virtual machines.

The final phase of proposed work presents a novel cache contention-aware Adaptive Artificial Bee Colony (AABC) algorithm in the cloud computing platform to mitigate cache attack. The cache-based attack on Physical Machine (PM) creates the cache contention. There are two solutions available to reduce the cache contention, Flush the cache or Relocate the attacker virtual machine to another physical machine. Flushing of the cache is not cost effective as other VMs are also running on the same PM. Therefore, the proposed work has chosen the second solution, i.e., shifting the attacker VM to new PM. The proposed AABC algorithm is the improvement to existing ABC (Artificial Bee Colony) algorithm, such that
its parameters are made self-adaptive. The AABC algorithm aims to identify the optimal PM within range of various PM for the VM migration. After identifying the optimal PM through the optimization procedure, the attacker VM, which has caused the cache contention, is migrated to the optimal PM. Relocation of the VM to the optimal PM makes the VM free from cache contention and it also mitigates the cache side-channel attack in the cloud environment.