

**CHENNAI – PONDICHERRY**

**SECURE: Self-Protection Approach in Cloud Resource Management**

**Abstract:**

In the current scenario of cloud computing, heterogeneous resources are located in various geographical locations requiring security-aware resource management to handle security threats. However, existing techniques are unable to protect systems from security attacks. To provide a secure cloud service, a security-based resource management technique is required that manages cloud resources automatically and delivers secure cloud services. In this paper, we propose a self-protection approach in cloud resource management called SECURE, which offers self-protection against security attacks and ensures continued availability of services to authorized users. The performance of SECURE has been evaluated using SNORT. The experimental results demonstrate that SECURE performs effectively in terms of both the intrusion detection rate and false positive rate. Further, the impact of security on quality of service (QoS) has been analyzed.

**Existing System:**

Researchers focused on identifying new techniques for detection and prevention of intrusions in computing systems and discovered that the Intrusion Detection System (IDS) is an effective way to protect network from attacks. IDS stops attacks, performs recovery after attacks, and investigate security loopholes to help avoid such problems in the future. IDS can be categorized into two types based on anomaly and signature. Signature-based IDS is used to detect the signatures of known attacks in the database, while anomaly-based IDS analyzes abnormal activities. SNORT13 is the most effective IDS that can be used for attack detection. Different machine learning techniques are used for anomaly-based IDS, but State Vector Machine (SVM) is the most commonly used anomaly-based detector.

**Proposed System:**

Proposes a Self-protEction approaCh in cloUd Resource managEment (SECURE) approach for dealing with security attacks. SECURE can create new signatures automatically and provide security against DDoS, Probing, U2R, R2L and DoS security attacks. Based on MAPEK loop, an algorithm for different phases has been developed to monitor, analyze, plan and execute. SECURE continuously monitors security attacks during the execution of workloads, performs analysis to understand alerts in the case of security attacks, makes a plan to perform required actions to manage threats, and executes the action. Security agents (sensors) are created on SVM as an anomaly detector. SECURE increases the security of cloud-based services and increases intrusion detection rate if the same threat arrives again.