ABSTRACT

Cloud computing is becoming a key driver in supporting all on-demand needs of corporate IT today. With its ubiquitous influence, it delivers the next-generation computing paradigm showcasing the possibilities of apt resource sharing, true elasticity, and maximum resource utilization as compared to any of its early competitors. In addition, corporates are also fascinated with its attractive tag of ‘pay-as-you-use’ business model. Despite its benefits, many organizations ranging from medium to large enterprises fear migrating to this computing paradigm because of the security issues associated with it. The reason being, today’s business computing world breathes solely on customers and their data, which require sophisticated mechanisms to protect it against theft and misuse. Subsequently, due to the public and multi-tenancy nature of cloud, the security threats and the velocity of consequences are higher in cloud, than in in-premises computing.

This research investigation introduces an innovative security solution named “eCloudIDS – A security enhancement framework for cloud computing environment”, which is built based on hybrid two-tier expert engines, namely uX-Engine (tier-1) and sX-Engine (tier-2). eCloudIDS is a prototype hybrid security system that will monitor user behavior and sound alerts on intrusions from both inside and outside sources based on artificial intelligence machine learning mechanisms (both supervised and unsupervised). eCloudIDS can ease the contemporary urgent security threats present in today’s cloud computing environment; specifically the top three state-of-the-art cloud computing security taxonomies, such as logical storage segregation & multi-tenancy security issues, identity management issues, and insider attacks.