ABSTRACT
Cloud computing is an emerging paradigm in ICT. The aforementioned future is incontestable due to its obvious advantages. It provides a gigantic storage with ubiquitous platform access and minimal hardware requirement at user end. The security issues in cloud computing become highly enunciated. The security challenges are viewed to be main obstructions that prevent potential users from drawing the obligating advantages of the cloud computing model. Authentication, Authorization and Access management (AAA) are the keys to security mechanism. Strong user authentication is a vital requirement for cloud computing that restrict the illegal access of cloud resources. In fact password based authentication is the most commonly used authentication methods which has been suffered many inherent drawback and day by day security attacks. Modern cryptographic techniques are easily computed with modern hardware and becoming vulnerable to upcoming attacks. Cloud computing and botnet building tools which are commonly available are highly demanding indispensible password policy requirements to ensure a secure cryptosystems. Kerberos is widely deployed authenticated protocol in client/server environment with its unique features of single sign on and mutual authentication using symmetric keys cryptography. On the other side Homomorphic encryption is emerging as panacea for dealing security issues in cloud computing. In proposed research work, enhancement of Kerberos protocol using homomorphic encryption algorithm, will improve a significant security level in cloud computing authentication. By keeping in mind the SSO and mutual authentication proposed model will cover the maximum limitation of standard Kerberos protocol and make it immune to many known attacks. As well as it provides user privacy and anonymous identity in generic cloud computing.

KEYWORD
Cloud Computing, Authentication, Kerberos, Homomorphic Encryption, SSO, Denial of Service