



**National Conference on Advanced Research in Science,
Engineering and Technology (NCARSET – 2020)**

27TH December 2020

CERTIFICATE NO : NCARSET /2020/ C1220973

**A STUDY OF SECURITY AND PRIVACY OF CLOUD
APPLICATIONS IN CLOUD SOFTWARE SYSTEM**

HIRA LAL

**Research Scholar, Ph.D. in Computer Science,
Dr. A.P.J. Abdul Kalam University, Indore, M.P.**

ABSTRACT

As a result of cloud computing, the user location is out of the company's hands data they save. As a consequence, the cloud's data is more susceptible to being compromised by a bug or incursion. In terms of data security, the three most common issues are: the legitimacy of the data, its accessibility, and its controllability. Cloud applications have their own set of security difficulties, including those relating to data privacy and authenticity, application integrity, and virtualization. Network security is the most common problem with cloud computing. The internet or intranet must be tunneled to avoid data breaches and theft, and good network or hardware precautions must be in place. For packets to be tracked and validated, scanner updates are required. Even though cloud computing provides organisations with a fast and low-cost option; we ensure that cloud security and privacy are not compromised. The secrecy of a business application must be maintained at a high level in order to protect data from unauthorised access. There are likely exceptions to the rule of obeying justified laws in order to fulfill strict security needs in the banking and government sectors. Institutions that enable cloud applications to jeopardise security have been criticized by regular and compliance authorities.