INTERNATIONAL CONFERENCE ON RECENT CHALLENGES IN ENGINEERING, SCIENCE AND INFORMATION TECHNOLOGY (ICRCESIT – 2020)
25TH OCTOBER, 2020

CERTIFICATE NO : ICRCESIT /2020/ C1020713

A STUDY OF NETWORK LEVEL SECURITY ATTACKS IN CLOUD COMPUTING

HIRA LAL

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

ABSTRACT

LAN, MAN, and WAN are all exposed to the same security concerns as cloud computing is. It is possible for a user to attack the cloud for any reason, or for an insider to be malicious and target a CSP and a user at the same time. To protect data integrity and confidentiality, we'll discuss network-level security breaches and viable responses The act of renaming a domain without the owner's or developer's permission is known as domain hijacking. It is possible for hackers to get access to private corporate information and carry out illegal acts such as phishing by replacing an existing website with one that looks just like the original. To prevent domain hijacking, ICANN has recommended that domain owners must wait 60 days before changing their registration details or moving to another service provider. Most likely, the domain's original owner will be alerted to any changes during this time. Several domain registrars use the Extensible Provisioning Protocol (EPP) as an alternative. To prevent unauthorised name changes, EPP uses an authorization number that can only be obtained by the domain registrant. When an attacker pretends to be a legitimate system in order to gain access to a computer, this is known as IP spoofing. IP spoofing may be used to carry out DDoS and Man in the Middle attacks.