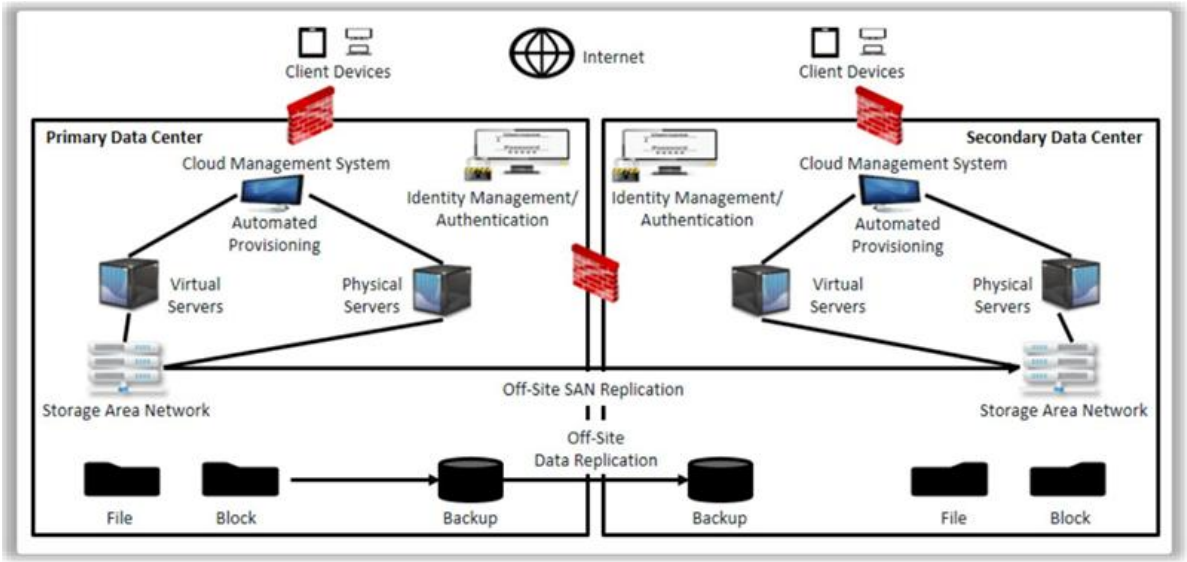
Day 9

“CLOUD SECURITY”

Authentication and Credentials:

1. **Importance of Strong Authentication in Cloud:**
    a. Cloud services are internet-accessible, making accounts vulnerable if credentials are stolen.
    b. Federation (e.g., Single Sign-On) increases risk due to reliance on a single credential.
2. **Multi-Factor Authentication (MFA):**
    a. Requires 2 or more factors to access a resource, reducing account takeover risk.
    b. Identity provider must relay MFA status to relying party in federated setups.
3. **Types of MFA:**
    a. **Hard Tokens:** Hardware-based, high security (e.g., RSA tokens).
    b. **Soft Tokens:** App-based OTPs, vulnerable if device is compromised.
    c. **Out-of-Band (OOB):** OTP via SMS/email—convenient, but interception-prone.
    d. **Biometrics:** Used locally on device; not shared with cloud providers.

Architecture of Cloud data centre:



--The End--