Sol 2. Firewalls are used in operating systems to prevent uninvited network traffic.

In protecting private information, a firewall is considered a first first line of defence. firewalls are generally designed to protect network traffic and connections and therefore do not attempt to authenticate individual users when determining who can access a particular computer or network.

we can implement a firewall in either hardware or software form, or a combination of both. All messages entering or leaving the intranet (a local network to which you are connected) must pass ~~the~~ through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Sol 1. XSS attack is used to infuse malicious code in a website's comment section or feedback section of any webpage.

XSS stands for Cross Site Scripting.

XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-~~sid~~ site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting carried out on websites accounted for roughly 84% of all security vulnerabilities documented by Symantec up until 2007. XSS effects vary in range from petty nuisance to significant security risk, depending on the sensitivity of the data and the nature of any security mitigation implemented by the site's owner network.

Sol 3. Man-in-the-middle attack (MITM) uses the description given in question. it is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.
A MITM attack can succeed only when the attacker impersonates each endpoint sufficiently well to satisfy their expectations.
most cryptographic protocols include some form of endpoint authentication specially to prevent MITM attacks.

Sol 4. Name of the Portal → SACHET (An SLCC initiative)
official link → sachet.rbi.org.in

Sol 5. Patching prevent ransomware and malware attacks completely. Every time, you update your software, will include the latest security patches and maximise ransomware prevention.
The particular piece of malware focused on a vulnerability found in the server Message Block (SMB) protocol used in almost every windows system. Those lacking a system for windows patch management faced data loss due to permanently encrypted files.