**Introduction:**

Secure communication over the internet is made possible by the widely used cryptographic technologies Transport Layer Security (TLS) and Secure Sockets Layer (SSL), which TLS replaced. They are made to make sure that information transferred between two parties is private and cannot be intercepted, altered, or read by unauthorized people. TLS/SSL has advantages for internet security, however, they are not impervious to attacks and flaws. Attackers have taken use of TLS/SSL flaws in some high-profile instances in recent years to steal sensitive data or launch cyberattacks. Man-in-the-middle (MitM) attacks are among the most frequent TLS/SSL attack types. An attacker can eavesdrop on a conversation between two people, manipulate the data being shared, or insert harmful content into a transmission by intercepting it. Another attack is SSL stripping when the communication is downgraded from HTTPS to HTTP so that it is simpler to intercept and manipulate. This kind of attack is particularly harmful because it can go unnoticed by the user because the URL bar's padlock icon still makes the website appear secure. The POODLE attack, which uses a flaw in the SSLv3 protocol to decrypt sensitive information, and Heartbleed, which enables an attacker to extract sensitive information from the server's memory, are other sorts of attacks and vulnerabilities in existing libraries that can harm TLS/SSL. The goal of this paper is to give a general overview of some of the most prevalent TLS/SSL attack methods and vulnerabilities. We'll look at the technical specifics of these assaults and consider how they might affect the safety of web services and apps. We will also go through some preventative actions that may be done, such as using the most recent TLS/SSL versions and routinely updating software and security patches, to lessen the impact of these vulnerabilities. Ultimately, this paper will emphasize how crucial it is to comprehend the dangers posed by TLS/SSL and the precautions that may be done to maintain the security of sensitive data sent over the internet.