**Conclusion:**

Secure online communication is now more important than ever in the current digital era. It is crucial to make sure that data carried over the internet is secure to prevent snoopers from accessing it because of the rise in e-commerce, internet banking, and other confidential online transactions. SSL/TLS offers safe internet connection by shielding data from interception, modification, and eavesdropping. However, SSL/TLS has encountered numerous attacks and flaws over the years, despite its usefulness. These flaws have brought to light the significance of secure implementation and frequent updates. For this project, we reviewed a few of the noteworthy vulnerabilities because of which attackers were able to obtain confidential data, reduce encryption levels, and sometimes even decipher SSL/TLS connections. In order to make sure that security flaws are fixed and that powerful cryptographic techniques and protocols are employed, SSL/TLS installations must be periodically updated.

SSL/TLS technology is constantly being innovated upon and looks to have a bright future ahead. These days, more secure encryption protocols and algorithms like ChaCha20 and TLS 1.3 are being developed. These new innovations provide enhanced security, quicker performance, and better defense against new threats. Moreover, SSL/TLS implementations are updated more regularly to fix known flaws and stop the emergence of brand-new ones. Despite these developments, SSL/TLS technology still has room for improvement. The usage of insecure encryption techniques and protocols, which attackers can take advantage of, is one of the key causes for concern. Also, website owners and developers need to be better informed on the value of SSL/TLS security as well as how to apply it correctly. These problems can be solved, ensuring that SSL/TLS is a dependable as well as reliable technology for many years to come.

In summary, SSL/TLS technology has had a number of weaknesses over the years, with ongoing attempts to bolster and increase its security, the technology's future appears bright. We can make sure that SSL/TLS is a dependable and trustworthy system for the future by resolving its flaws and putting best practices into practice.