**Literature Review: Surveying existing libraries that implement SSL/TLS protocol (e.g., in browsers, in IoT devices, etc.) and reviewing past vulnerabilities in these libraries (both protocol-based, and software based)**

**Abstract**

In this we reviewed different papers related SSL/TLS protocols. We also investigated the existing libraries that implement these protocols in IoT devices as well as in the browsers and the past vulnerabilities in these libraries both the protocol based as well as software based.

Keywords: SSL/TLS protocols, vulnerabilities, IoT, attacks, software based, Internet

Today, the internet has grown significantly in significance for the economy, education, business, and nearly all other facets of society. It has become an indispensable tool for work and for obtaining the information needed for tasks. Most businesses conduct all their daily operations online, including distribution, purchase, selling, marketing, and product servicing. Environments like e-banking, e-commerce, e-business, and others provide their customers with several advantages. Online transactions are the simplest method to conduct financial transactions. The use of cloud environments is growing in popularity, and the options it gives its users—access to data from any location, using any device, at any time—are very beneficial. The use of the Internet is growing in prominence but comes with some risks.

1. **Background**

A cryptographic protocol called SSL (Secure Sockets Layer), later renamed TLS (Transport Layer Security), is intended to guarantee the security of data transmitted over the Internet. This protocol was created by the Netscape business in 1994, and the most recent iteration, SSL3.0, was released by the company in 1996. The IETF organisation took over the protocol's further development and release, but the protocol was subsequently renamed TLS. Data on the transit layer is protected by the protocol. It offers security services for any application-based protocols, including HTTP, FTP, LDAP, POP3, and others. It is situated between the transport and application layers in the ISO/OSI reference architecture. It is used in a client/server environment and offers the following benefits to communication participants:

* Integrity
* confidentiality
* authentication

**Methodology**

To achieve the said objectives, the researchers adopted a simple yet effective methodology to develop and present a systematic review paper.

**Literature search**

As primary steps, this study searches the related literature using keywords from the database. The selected databases are Scopus and google scholar, as these two databases are well known for their availability of a wide range of scientific articles, search are "SSL/TLS Protocols " and "vulnerabilities."

We carefully screen the title and abstract of articles to narrow down the quantity.

**Literature analysis**

After the screening stage, eight articles are carefully reviewed and analyzed to state the current state of the art in the literature on the Attacking SSL/TLS implementations.

**Defining themes, approaches, and gaps**

This study evaluates comparatively different researchers' different aims and objectives and unique research approaches. Therefore, this study reviews the selected papers about the shortlisted protocols and their vulnerabilities and aggregates the factors objectively.

**Outline the structure**

The results are then summarised and discussed within the group in order to show them in a more organised manner as a reviewed paper for our term project for the course INSE 6120.

The following paper is structured with eight sections, including an introduction where we introduce the SSL/TLS protocols and their background. Next, we describe all the attacks and vulnerabilities related to these attacks in a defined way. In the last section, we summarized our findings and concluded the topic.