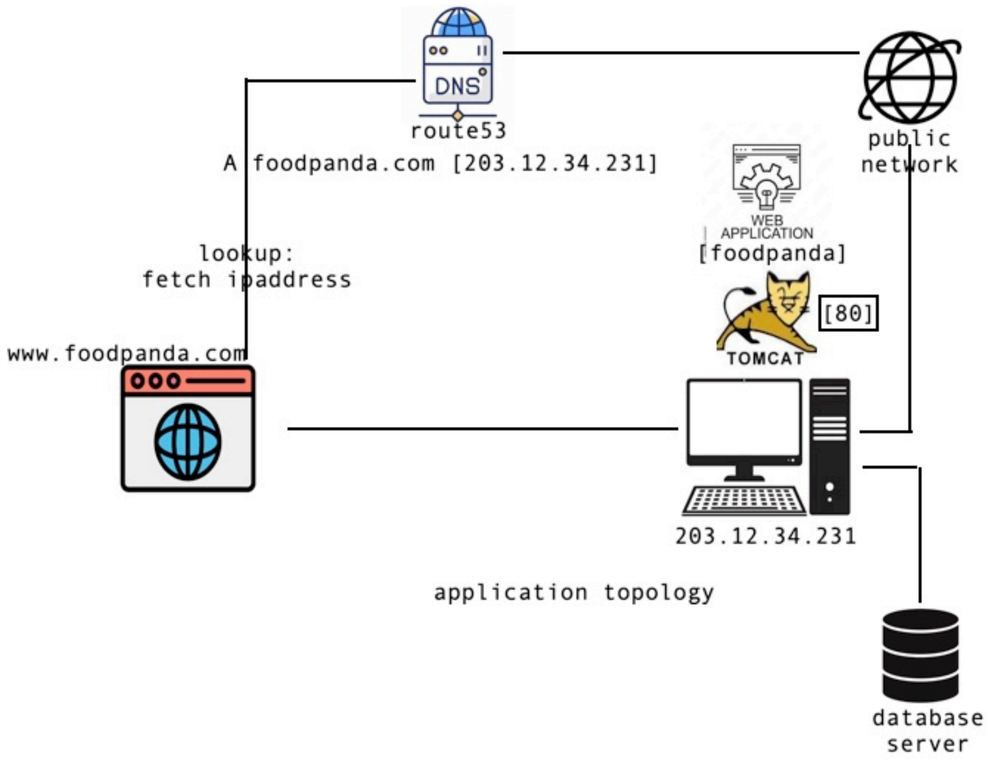


here all the data exchange that takes place between the client/server is in plain/text format which is not recommended. because an intruder can steal the data packets over the transmission that causes loss/damage to either the client/business.

To avoid this we need to enable SSL (TLS) (Trasport Layer security). TLS is an encryption at transport. all the data that is exchanged between the client/server would be encrypted/decrypted and transmited, so that no intruder can steal the datapackets that are exchanged over the network.

browser : browsers are the http client programs designed to build for TLS, which means browsers can participate in encrypt/decrypt of the data over the request/response

Backend Servers = backend application servers supports TLS.
[Tomcat|Netty|Jetty|IIS|Lamp|Flask]
If we enable TLS on these servers by configuring public/private certificates to them, they participate in
 1. establishing the session with client
 2. generates an session key (encryption key) that is shared/kept private between the client/server using which both the parties will communite
SSL = secure socket layer

These SSL keys are generated and provided CA authorities
CA = certificate authorities

Website = sealed with an SSL certificate
1. authenticity
2. secure communication