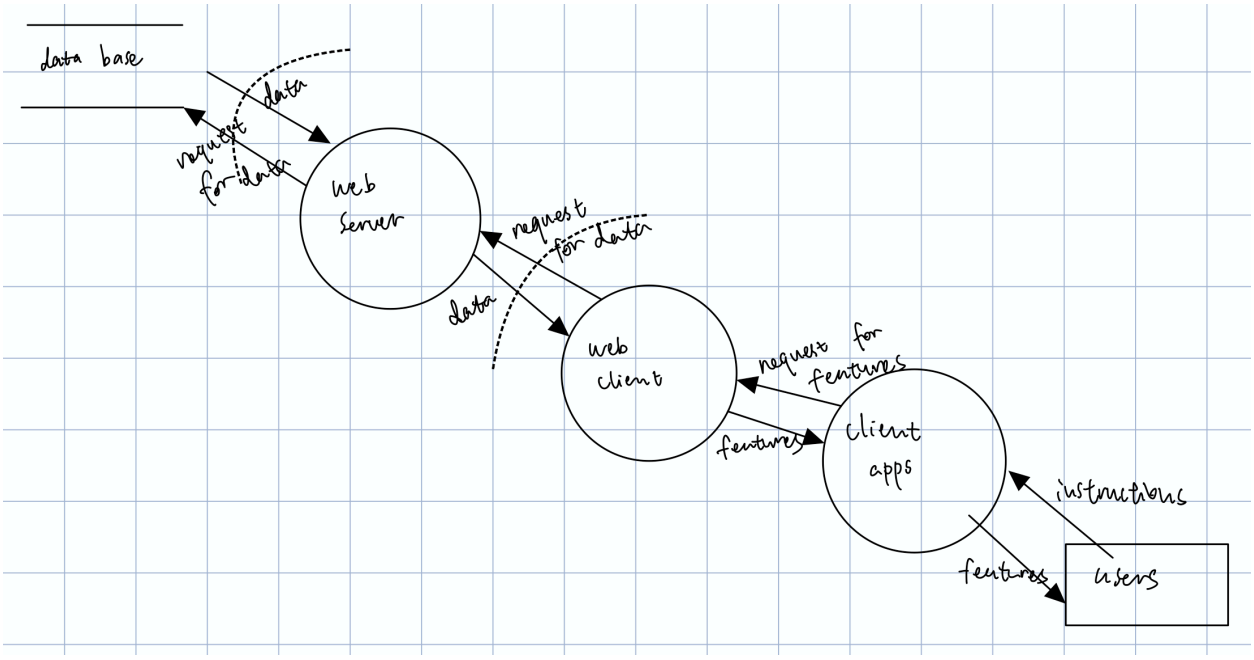

1.Spoofing: a man-in-the-middle might intercept request to web server or database and reply the false information. It can be mitigated with HMAC to make sure the data comes from authenticated source.
2. Tampering: database being intruded and modified maliciously. A solution can be using reliable firewalls to control incoming access and outgoing flow.
3. Repudiation: User action can be modified maliciously by changing the username associated with an action. It can be mitigated with digital signature so the user involved cannot deny it.
4. Information disclosure: An attacker might sniff off the data transmitted between the database and the web server. It can be mitigated with secrue protocols such as TLS.
5. Denial of service: a web server might be attacked and made unavailable to users. It can be mitigated by always keeping security software updated, so that attackers will find it harder to find a loophole.
6. Elevation of privilege: An attacker might utilize HTTP responses to fool the system into granting them higher power. It can be mitigated by encrypting the data sent to the server so it cannot directly read it and cannot be fooled.