IFS4205 Group 2 Security Claims

S/N	Claim	Description
1	An adversary will not be able to escalate the privileges of a user without signing into that specific role.	If the user is both a public user and an admin user, he can only perform one role at one time.
2	An adversary will not be able to access pages that require login without logging in.	Login_required from flask-login is implemented.
3	An adversary will not be able to successfully compromise the integrity of the dongle data transferred.	The implementation of HMAC SHA256 ensures that messages which have been tampered with would be dropped.
4	An adversary will not be able to compromise the authenticity of the data during transmission.	
5	An adversary will not be able to interact with the dongle to get the dongle data, without a legitimate scanner.	This is achieved through: 1) a customised protocol between the legitimate scanner and dongle. 2) checksum challenge (specific to each dongle) that the dongle requires from the connecting device after initiating a connection.
6	An adversary will not be able to compromise the confidentiality of the data in the dongle.	Secret key is not transmitted and a new DH public, private and secret key will be generated for every new connection.
7	An adversary will not be able to read the traffic between the web and database server in plaintext.	The implementation of SSH tunnel between the client's web browser to the database server prevents data from being seen as plaintext through the transmission.
8	An adversary will not be able to identify the user from the information provided to the researchers.	Data has been anonymised using generalisation and suppression techniques from k-anonymity.
9	An adversary will not be able to elevate the access of users outside of their determined functions.	Access control has been done on the database server. There are mainly five roles in the database, namely, admin, public, staff, contact tracer and researcher. These different roles have been granted

		permissions to tables that they respectively need.
10	An adversary cannot get pass the authentication without the facial recognition check	The adversary will require to show his face or an image of the user before he is able to login.
11	An adversary will not be able to successfully sniff the original message sent from the client on the following connections: • Web server to outward facing clients • Dongle scanners to inbound dongle server	The implementation of TLS prevents data from being seen as plaintext through the transmission.