Topics for Research Project[Tentative]
COMP90043

Some suggestions for the topics are given below:

1. Security in Steganography and Watermarking

2. Security in Block Chain Technologies.

3. Electronic Voting Protocols

4. Attacks on SSL

   Dan Boneh, Twenty Years of Attacks on the RSA Cryptosystem, NOTICES OF THE AMS, pp 203-213, 1999.

5. Security for IoT.

6. Side channel resistant Cryptography.

7. Any Cryptographic implementation project from

   http://hms.isi.jhu.edu/acsc/

8. Cryptography for Privacy Preserving data aggregation
   Claude Castelluccia, Aldar C.-F. Chan, Einar Mykletun, Gene Tsudik: Efficient and provably secure aggregation of encrypted data in wireless sensor networks. TOSN 5(3) (2009)
9. Network Security, Man-in-the-Middle Attack Demonstration.
   An implementation project. You need to implement a client, a MITM server that sits between the client and a server.