NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

School of Computer Science and Engineering
College of Engineering

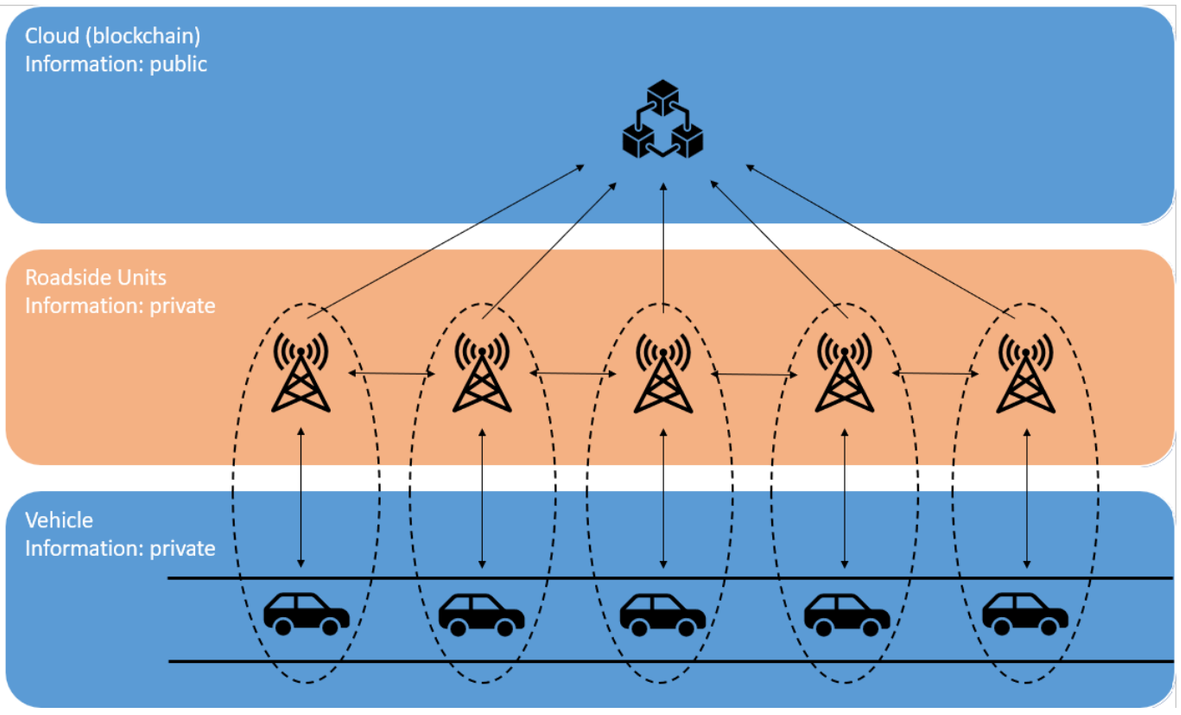
Privacy of Blockchain-enabled Internet of Vehicles

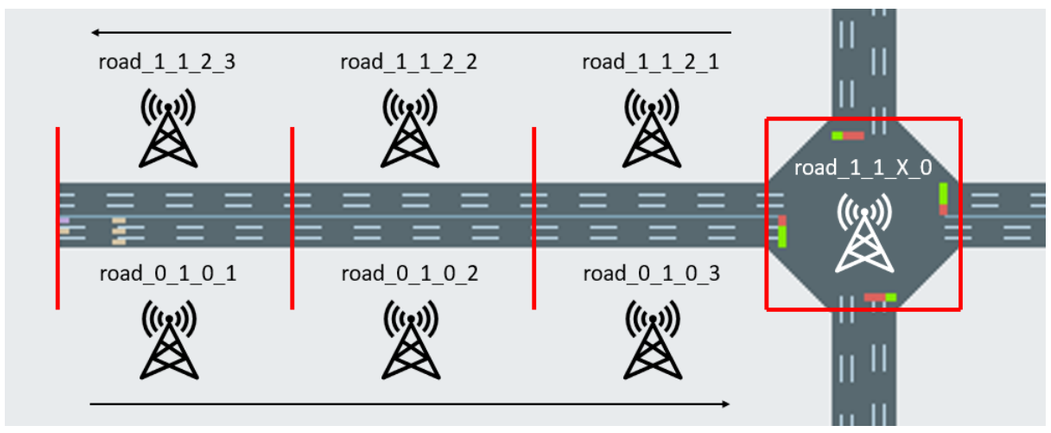
Student: Tan Ke Xiang

Supervisor: Dr Sourav Sen Gupta

Project Objectives:

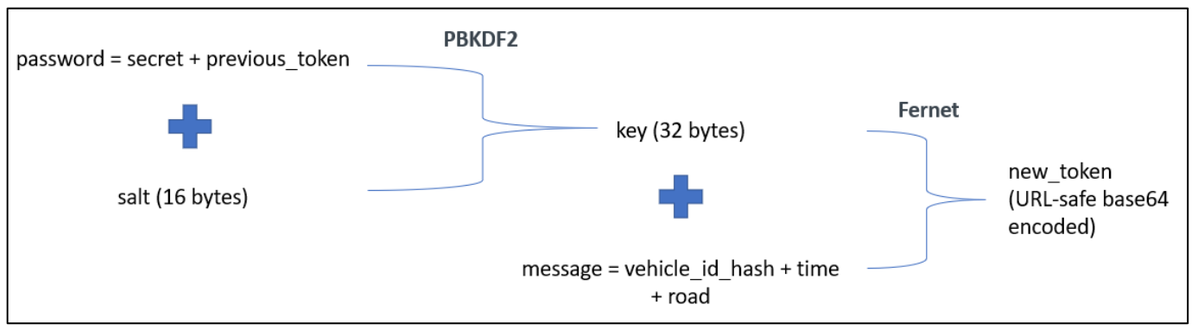
This project aims to address the privacy concerns in blockchain-based IoV by providing on-demand privacy guarantees. Privacy schemes were designed to allow vehicular information to be written to the blockchain without specifically identifying each user. Additional schemes were designed to provide mutual authentication and prevent malicious exploitation of the system. These safeguards were then simulated in the traffic control and management scenario.





Features:

- Tokenisation of vehicular details through the usage of cryptographic salts, the Password-Based Key Derivation Function 2 (PBKDF2) function and the Fernet symmetric encryption algorithm
- Digital certification of the vehicles and RSUs, allowing messages between these entities to be digitally signed and encrypted, providing data confidentiality, integrity and authenticity
- Token verification and mutual authentication between vehicles and RSUs using the vehicle's one-time-use tokens




```
Transaction sent: 0x7dad3dbc92785ef6b93c960df248789a19c476c80ff8786d61c06e60fcbb422f
  Gas price: 20.0 gwei   Gas limit: 813800   Nonce: 2
  Blockchain.setSectionCount confirmed   Block: 390   Gas used: 738363 (90.73%)

Transaction sent: 0x3577b6d43d18862e5c00fcd895972ad400a5eb1af97b3f3189e6ec635f3744ea
  Gas price: 20.0 gwei   Gas limit: 54044   Nonce: 163
  Blockchain.predictRoadCount confirmed   Block: 391   Gas used: 49131 (90.91%)
```