Thank you, Edison.

After talking about these challenges, let’s focus on some solutions for them. In order to avoid the data leakage issues, we can apply AES algorithm to encrypt the data. The AES algorithm has 256-bit keys with fast operation speed, which could provide high confidentiality. In addition, the Key distribution should be used to verify the identity of the cloud provider since KDC could ensure only users in the system could use the services. Lastly,

TLS provides the secure environment for data exchange and prevents eavesdropping and tampering. So it effectively avoids the information integrity problem with low overhead.

However, these solutions may have limitations. First, the self-drive car requires sufficient cloud providers to support various services. And for key distribution and TLS, the system may encounter man-in-the-middle attack, which leads to the exposure, decryption and tampering of the communication. The key distribution system also has to face to the replay attack.

Our presentation demonstrated the development, challenges and solutions of IoT and the self-driving car. Actually, the self-driving car technique is still not mature. It has to face various security challenges, such as confidentiality, authentication, privacy and access control. Hence, to solve these problems, we used the cryptographic algorithm and related techniques. AES has the fast encryption and decryption speed with high performance in maintaining data security. However, key distribution system and TLS may encounter some attacks. The disadvantages of them should be considered to figure out in the future.

Here is the reference list.

This is the end of our presentation. Thank you!