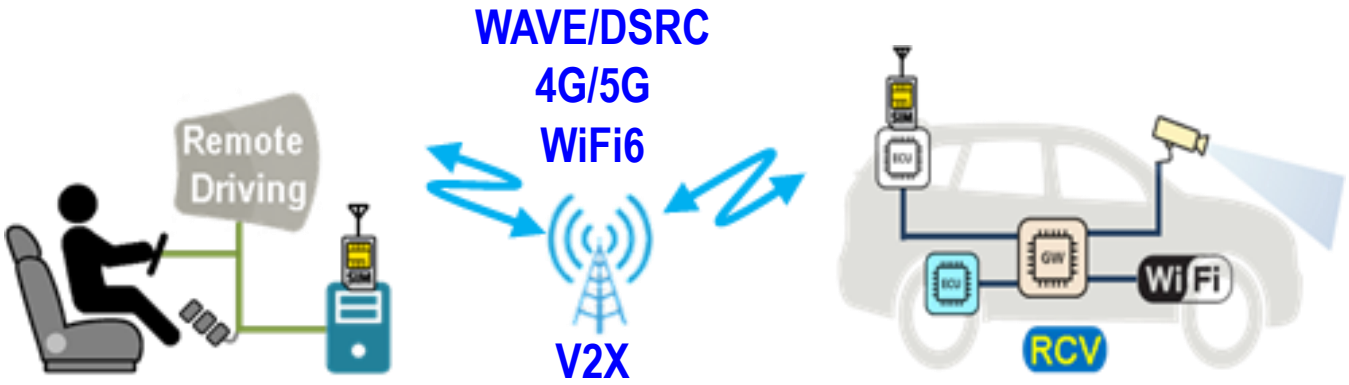
Cybersecurity for Remote Control Vehicle – KR Partners

You-Jun CHOI (KATECH) and TaeSang CHOI(ETRI)

2nd CARAMEL OEM Workshop

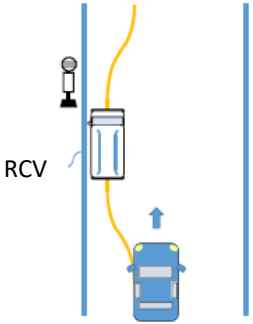
15th November 2021

Remote Control Vehicle



Possible Use Cases for RCV (1/2)

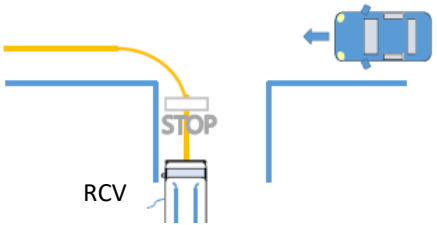
Source : ISO/TC204 WG14 N1674



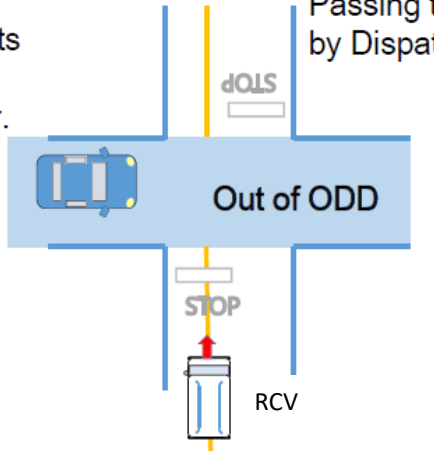
Re-starting after stopping on the shoulder at a station.
The remote driver checks that there are no vehicles around, especially from behind, and operates the "start" operation

Remote support when out of ODD due to rain, fog or other environmental conditions

Joining the priority road from a side road, no traffic lights
The vehicle automatically stops at the stop line,
the remote driver checks the safety and "starts" the car.



Passing through a region outside the ODD by Dispatcher Input (ISO 22737)

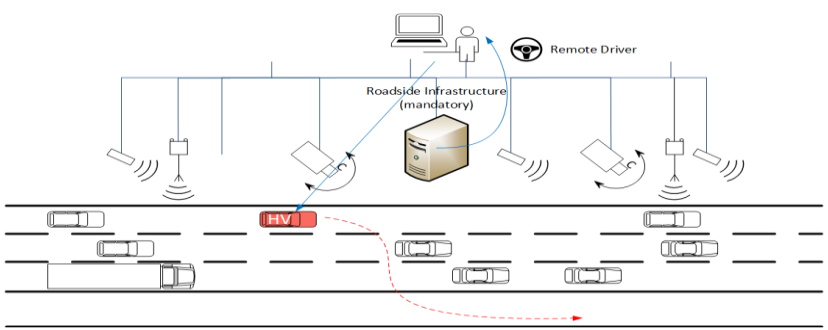


ISO 22737 : Intelligent transport systems — Low-speed automated driving (LSAD) systems for predefined routes — Performance requirements, system requirements and performance test procedures

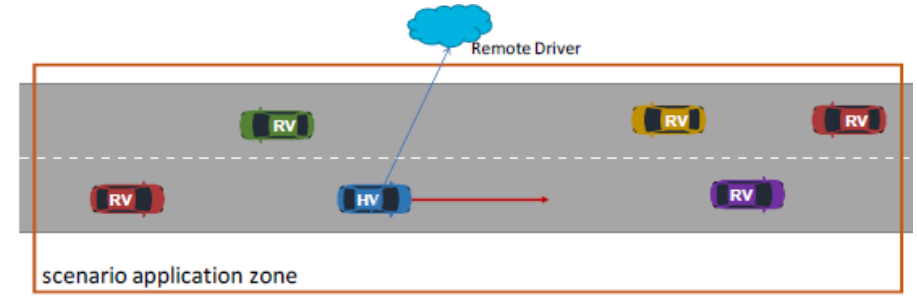
Possible Use Cases for RCV (2/2)

CARAMEL

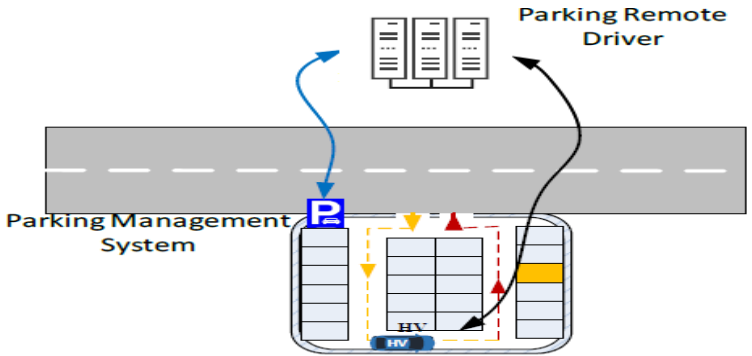
Infrastructure-Based Tele-Operated Driving



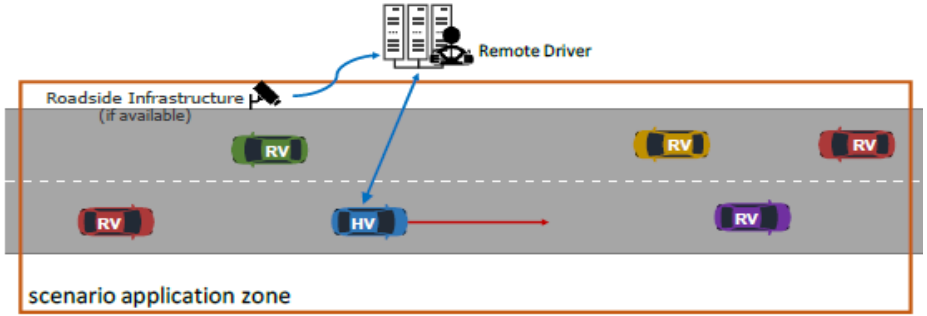
Tele-Operated Driving (TOD)



Tele-Operated Driving for Automated Parking



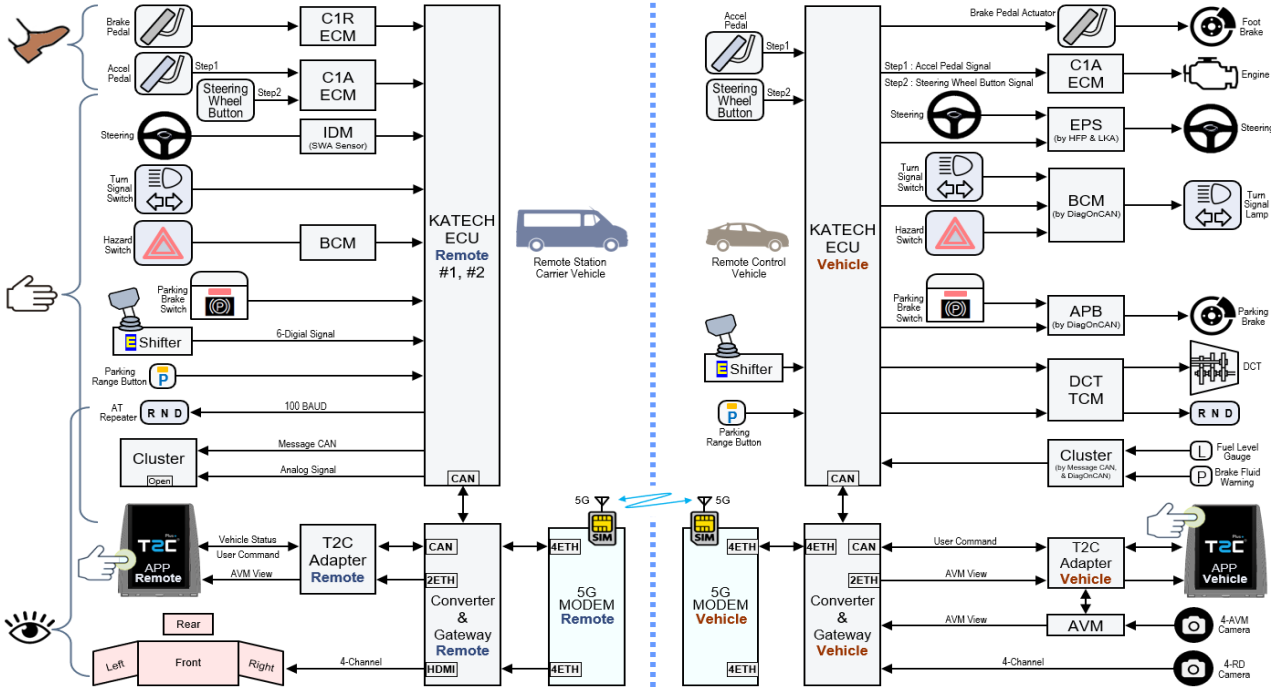
Tele-Operated Driving Support



Source : 5GAA C-V2X use Cases and Service Level Requirements Volume II

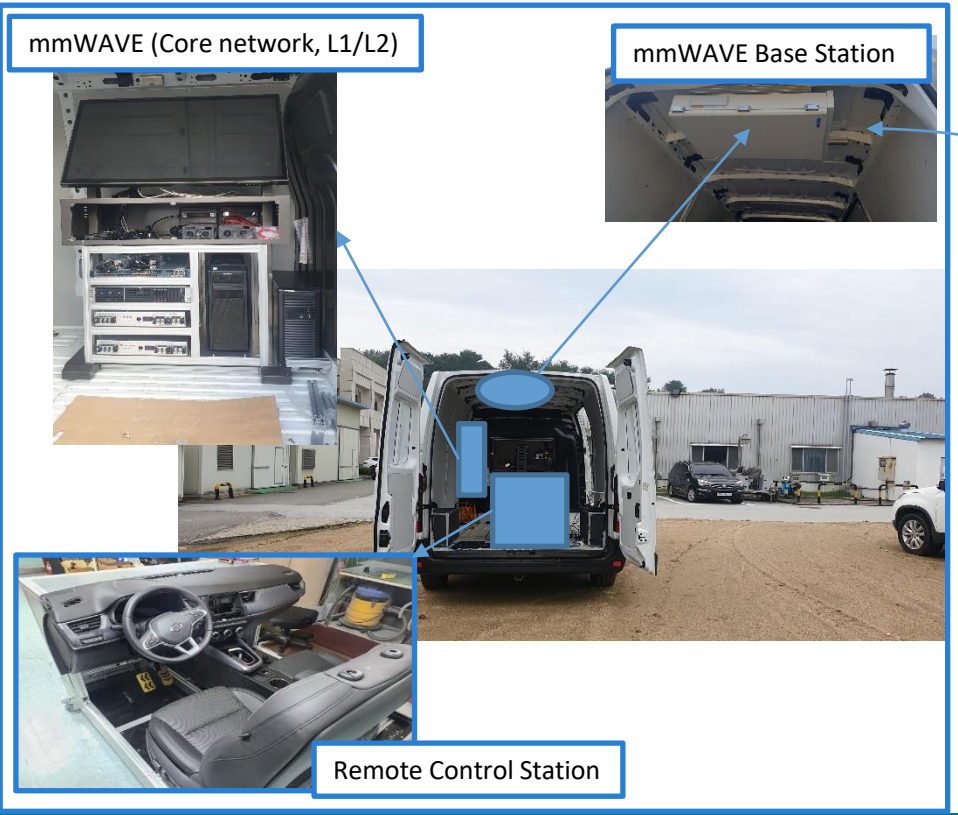
Remote Control Vehicle

- System design of remote control station using automotive parts i.e. ECM, BCM, IDM
  - Control Input (to RCV) : Steering Wheel, Linker, Accel. Brake, P-Brake, E-Shifter
  - Status Monitoring (from RCV) : Speed, RPM, Fuel level, Steering wheel angle, Accel, Brake, E-Shifter position, Linker, and etc.

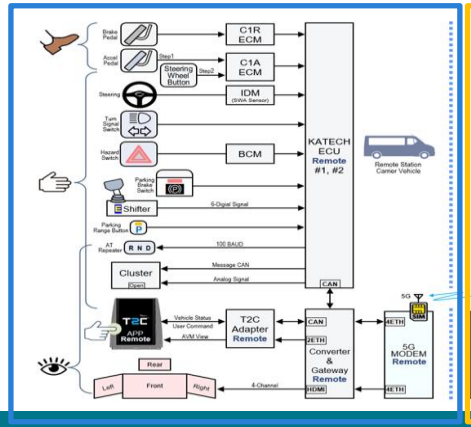


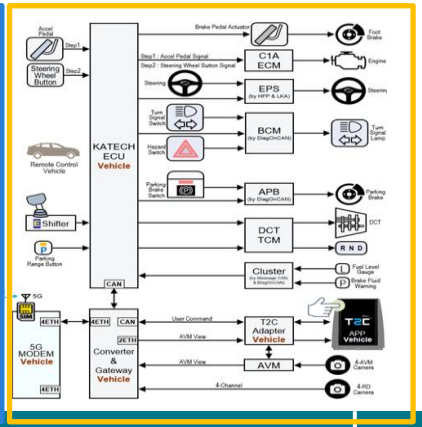
Remote Control Vehicle

- Implementation of the remote control station based on mmWAVE communication



mmWAVE
(23GHz)





ETRI and MOBIGEN (WP4)

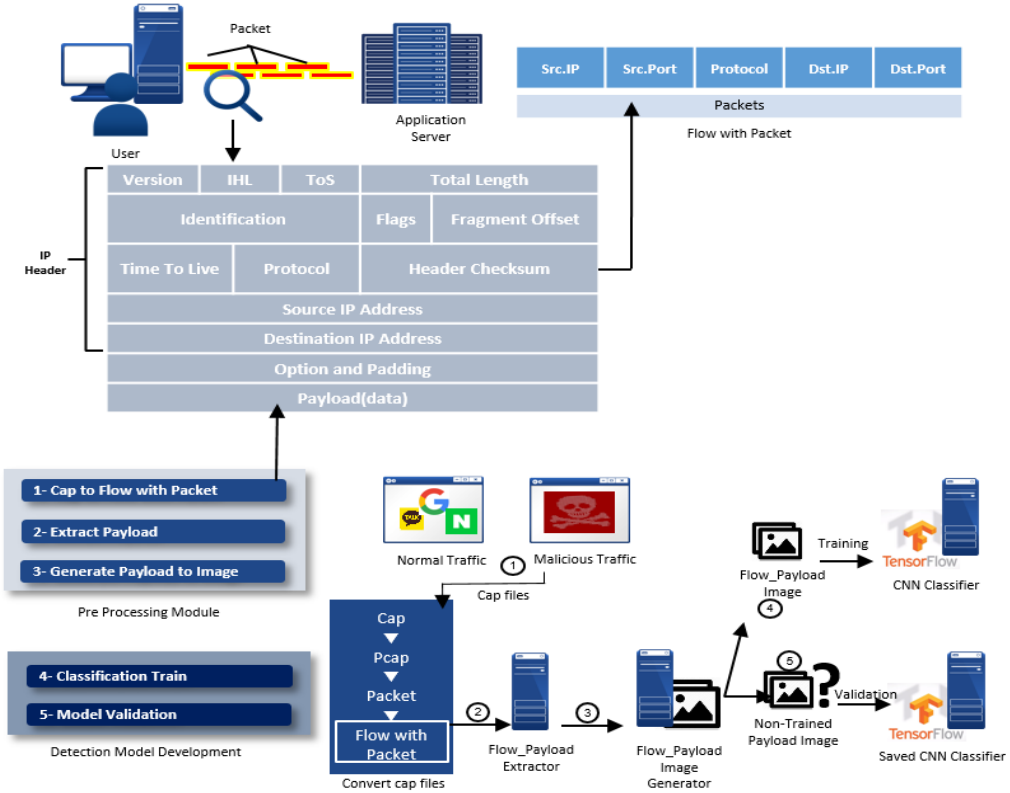
Scenario Name	Attack on RCV Control & Status Message Transmission
Related Pillar	Connected Mobility
Scenario Descriptions	There are two scenarios: a) Control message from a control center to a RCV is attacked, b) Status message from a RCV to a control center is attacked.
Challenges	▪ Deploy a PKI system to register RCVs, distribute security credentials, authorize vehicles to transmit signed messages, revoke certificates and distribute lists of revoked certificates. ▪ Ability to detect fake messages: not signed, signed with a non-valid certificate, signed with revoked certificates, replayed and non-authorized.
Assumptions & Preconditions	▪ The scenario is provided with a communications infrastructure: namely OBUs, RSUs, Small Cells and RCV control (currently proprietary) communications protocol suite. ▪ RCVs are equipped with an HSM to store cryptographic material and a location system.
Goal(Successful End Conditions)	▪ RCVs drop fake messages and prevent safety applications from being misinformed. ▪ Control center identify fake status messages and prevent from RCVs being misinformed
Involved Actors	▪ Malicious attacker ▪ Fixed infrastructure ▪ Outside infrastructure
Scenario Initiation	▪ The cyber attacker transmits different types of fake control messages to RCV ▪ The cyber attacker transmits different types of fake status messages to Control center
Main Flow	Case a) Fake messages: 1a. Normal RCVs register to the PKI system and transmit and receive messages. 2a. The attacker sends fake messages. 3a. Normal RCVs check the signature of these messages, detect which messages are not compliant and drop them.
Novelty	This scenario will implement a complete security infrastructure for a RCV communications system: PKI servers with capacity to distribute ATs and revoked certificate lists, message signature ability in the OBUs and a machine learning based algorithm to choose when a vehicle has to change the AT to avoid being tracked.
Evaluation Criteria	Case (a) fake messages: Normal RCVs detect all non-compliant messages.

ETRI and MOBIGEN (WP4)

Scenario Name	Attack on RCV Status Image Transmission
Related Pillar	Connected Mobility
Scenario Descriptions	Status images from a RCV to a control center is attacked.
Challenges	▪ Deploy a PKI system to register RCVs, distribute security credentials, authorize vehicles to transmit signed messages, revoke certificates and distribute lists of revoked certificates. ▪ Ability to detect fake status images: not signed, signed with a non-valid certificate, signed with revoked certificates, replayed and non-authorized.
Assumptions & Preconditions	▪ The scenario is provided with a communications infrastructure: namely OBUs, RSUs, Small Cells and RCV control (currently proprietary) communications protocol suite. ▪ RCVs are equipped with an HSM to store cryptographic material and a location system.
Goal(Successful End Conditions)	▪ RCVs drop fake status images and prevent safety applications from being misinformed.
Involved Actors	▪ Malicious attacker ▪ Fixed infrastructure ▪ Outside infrastructure
Scenario Initiation	▪ The cyber attacker transmits different types of fake status images to Control center
Main Flow	Case a) Fake status images: 1a. Normal RCVs register to the PKI system and transmit and receive messages. 2a. The attacker sends fake messages. 3a. Normal RCVs check the signature of these messages, detect which messages are not compliant and drop them.
Novelty	This scenario will implement a complete security infrastructure for a RCV communications system: PKI servers with capacity to distribute ATs and revoked certificate lists, message signature ability in the OBUs and a machine learning based algorithm to choose when a vehicle has to change the AT to avoid being tracked.
Evaluation Criteria	Case (a) fake status images: Normal RCVs detect all non-compliant status images.

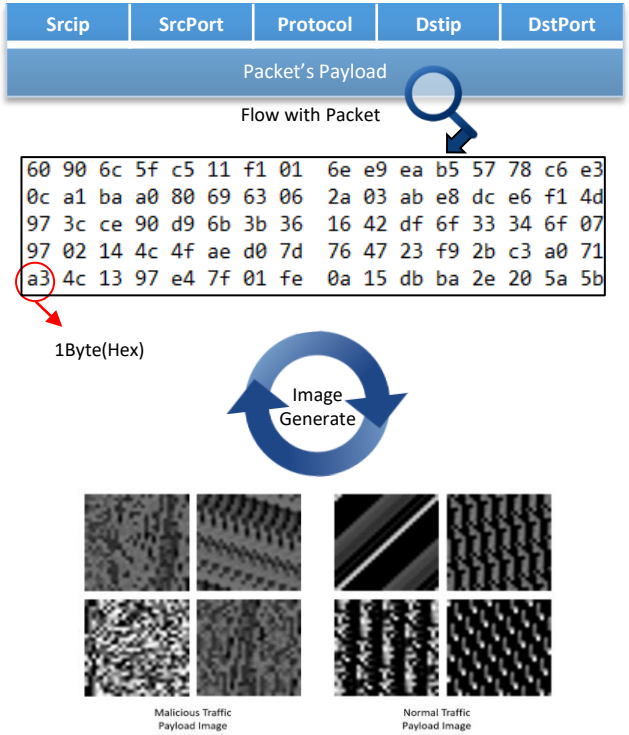
Malicious Traffic Detection Based on CNN

- System Architecture



Malicious Traffic Detection Based on CNN

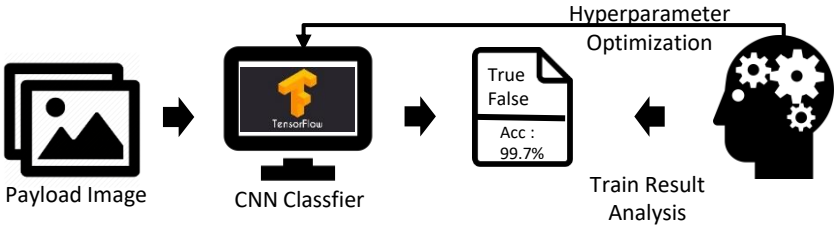
- Extract Flow Payload & Image Generation
  - Extract up to 784(28 x 28) payload values of Flow with Packet
  - Extracting the payload values up to 784 is to match the size of the Mnist image
  - Each 1 byte payload values are shaded between 0 and 255 to the image



28 x 28 payload image

Malicious Traffic Detection Based on CNN

- Model Training



- Model Validation

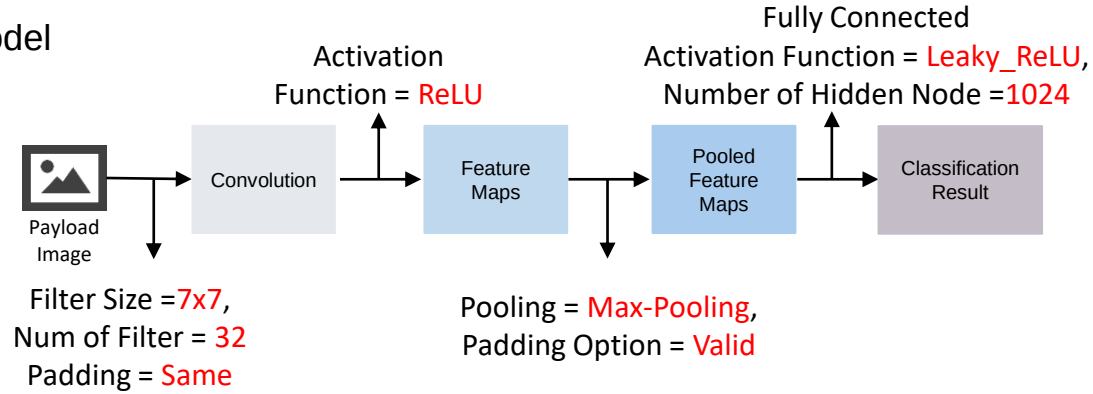
Malicious Traffic Detection Based on CNN

- Hyperpameter Set
  - Out of 1440 Hyperparameter combination, Optimization Set selection

Convolution Acticvation Function	Convolution Filter Size	Pooling & Padding	FullyConnected Activation Function	Number of Hidden Node
Sigmoid	3x3	Conv Same MaxPool Same	Sigmoid	10
Tanh	5x5	Conv valid MaxPool Same	Tanh	20
ReLU	7x7	Conv Same MaxPool Valid	ReLU	30
Leaky_ReLU		Conv Valid MaxPool Valid	Leaky_ReLU	
		Conv Same AvgPool Same	Softmax	1024
		Conv Valid AvgPool Same		
Optimization Set		Conv Same AvgPool valid		
		Conv Valid AvgPool Valid		

Malicious Traffic Detection Based on CNN

- Final CNN Model

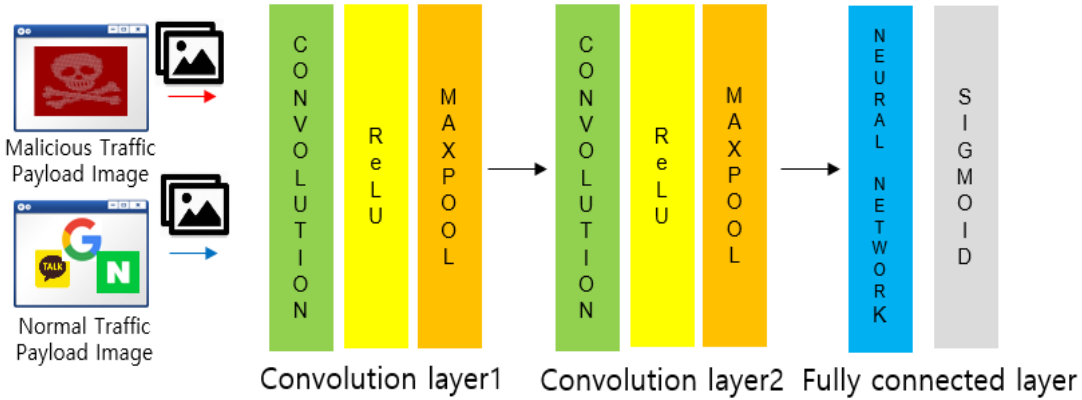


- Optimization Set

Convolution Acticvation Function	Convolution Filter Size	Pooling & Padding	FullyConnected Activation Function	Number of Hidden Node
ReLU	7x7	Conv Same MaxPool Valid	Leaky_ReLU	1024

Malicious Traffic Detection Based on CNN

- CNN Model Architecture based on Mnist Model



- Convolution : Extract feature map from training data
- Relu : Activation Function applied to feature maps
- Max pool : Extract the largest value from feature map
- Softmax : Functions for multiple identification

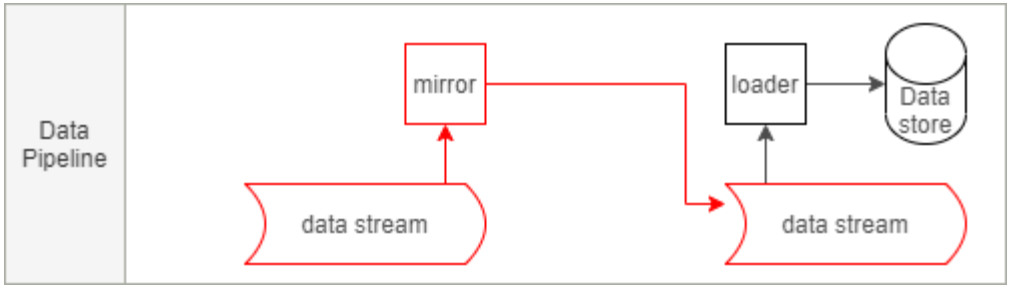
Experiment Result & Conclusion

- Result

Traffic	Number of Data	Train Step	Accuracy	Precision	Recall
Maliciious Traffic	1000	1000	97.3%	97.6%	97.0%
Normal Traffic				97.0%	97.7%

Data Pipeline Performance Test (1)

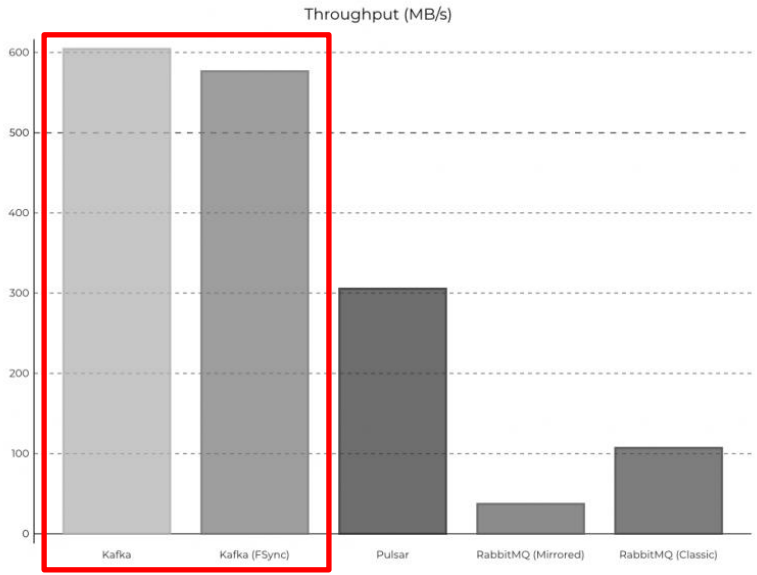
- In our platform, Kafka was chosen for data stream processing
- A preliminary test was performed to ensure that the target data transfer rate was satisfied



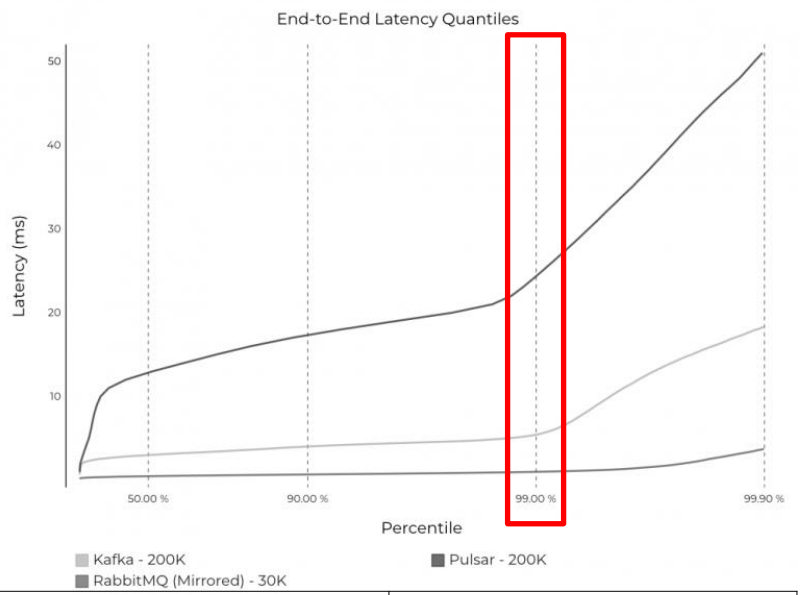
- In addition to kafka, we have selected several additional solutions (Which Supports real-time message delivery)
  - Kafka (selected)
  - Pulsar
  - RabbitMQ

Data Pipeline Performance Test (2)

- Throughput



- Latency



	kafka	Pulsar	RabbitMQ
Throughput	605 MB/s	305 MB/s	38MB/s
99p Latency	5 ms	25 ms	1ms (low)

Thank you for your attention