CUBE

Autonomous Car
Network Security Platform
based on Blockchain

Executive Summary

CUBE is a platform for securely protecting network security of existing automobiles and autonomous vehicles with blockchain technology. Nowadays, automobiles are evolving rapidly as connected vehicles rather than traditional mechanical parts. As navigation routing, traffic information, and other high-tech elements are becoming basic features of vehicles, connected units inside vehicles such as the Engine Control Unit (ECU), Brake Control Unit (BCU) and Wheel Control Unit (WCU), as well as many others, are also becoming vulnerable to malicious attack.

More than 30% of the functions of autonomous vehicles depend on communication. The traffic control centres monitor whether the wheel and brake control units are operating without failure. The navigation required for vehicle operation also depends on communication.

With the above in mind, one of the most important concerns related to autonomous vehicles is securing them against malicious network attacks. To date, no fundamental defense mechanism has been developed against malicious attacks on networks. This risk is the biggest problem for autonomous vehicles.

CUBE solves the security problems of autonomous vehicles using blockchain technology. The key to blockchain is that the technology ensures trust. CUBE uses blockchain technology to ensure the security of autonomous mobile networks.

Autonomous cars are revealed to the potential malicious intended attackers in various channels. There are two kinds of weak channels that can be attacked, the inter-communication channel and intra-communication channel. The inter-communication channel includes the communication between outside information delivery sites and autonomous car gateway. It includes traffic information, navigation routing information, and remote firmware upgrade by automakers. Another channel is the intra-communication channel. An autonomous car has the intra-network, which includes ECU, BCU, WCU, and so on.

If an infected file arrives, the CUBE blockchain can verify that it is different from the hash of the infected file and the hash in the car firmware. If we can confirm on the blockchain that the new hash of the incoming information is trustworthy, we can easily check if it is a malicious attack.

CUBE also uses AI and machine learning to create a defense against possible malicious attacks in the future. In the end, malicious attacks are typically a combination of attacks that have already been introduced, so CUBE provides its own defense against malicious attack algorithms by using tens of millions of combinations of possible attack scenarios, which deep learning generate.

Finally, CUBE uses quantum hashing cryptography technology to improve security. Currently, blockchain technology uses hash as the core of its security; however, if a computer’s processing speed increases dramatically, there is no guarantee of security within an hour. CUBE's quantum hashing cryptography is based on the properties of quantum and technical elements that have already been established. This approach will serve as an upgrade to the security of the entire blockchain.

I. Introduction

Connected and autonomous cars are not only controlled by the camera recognition program Ladar - it is also controlled by a network. An autonomous car should always be connected to a network for receiving accurate location data, vehicle to vehicle data (V2V), traffic data, IoT assist data, and so on. If an autonomous car is connected to a local area network (LAN), it could be much simpler to detect hacking danger. However, the incredible expected number of network connections with wireless networks dramatically increases the danger of hacking. This high degree of connectivity makes it particularly challenging to secure smart vehicles. Malicious attack can intrude a vehicle, which endangers not only the security of the vehicle but also the life of passengers and the surrounding community.

CUBE is the security platform to prevent the hacking danger on the basis of the blockchain. For example, WannaCry ransomware attack struck organizations around the world in May 2017. The attack spread at a rate of almost 3,600 computers per hour or about one per second. The ransomware infected more than 300,000 devices. Although the infected servers and PCs suffered a lot of pain, malware against an autonomous car could obviously be much more dangerous. A hacked autonomous car could even threaten human life. CUBE platform decentralises the IoT control server and filters the hacked network data by blockchain private key identification.

Potential Dangers

Autonomous cars are revealed to potential malicious attackers throughout various channels. There are two kinds of weak channels that could be attacked, inter-communication channels and intra-communication channels. Inter-communication channels include the communication between outside information delivery sites and autonomous car gateway. It includes traffic information, navigation routing information, and remote firmware upgrades by automakers. Another channel is the intra-communication channel. An autonomous car has the intra-network, which includes the Electric Central Unit (ECU), Break Central Unit (BCU), Wheel Control Unit (WCU), and so on.

The Intra-Communication Channel needs high safety and security. Ironically, to secure the safety of this Intra-Communication Unit, this network should always be connected with the automaker control centre to check the status of the autonomous car, which then increases the possibility of a cyber-attack by malicious attackers.

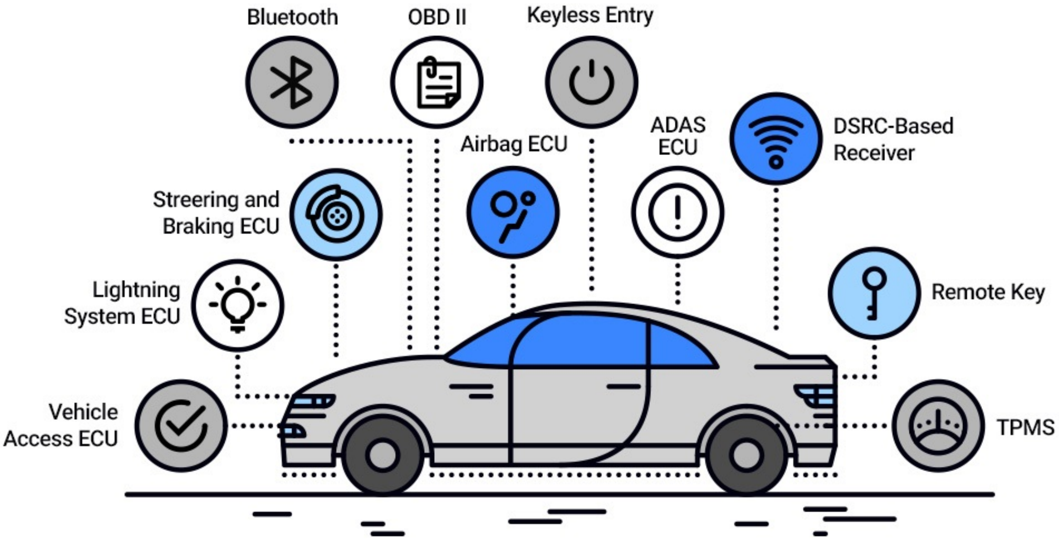


Fig.1. Most hackable points of autonomous car.

Inter-Communication Network Security

An autonomous vehicle must acquire as much information as possible about its surroundings to operate the vehicle alone. Such information may be path information for navigation, traffic information, or data for updating an old firmware of an autonomous vehicle. Receiving such a variety of data can be very helpful in operating autonomous vehicles, but at the same time increases the risk of malicious intrusions.

V2V, which means Vehicle to Vehicle communication, is an important function to make an autonomous car safer. In a connected car, the vehicle receives various vehicle data points from other nearby vehicles.
V2V helps to operate autonomous vehicles in various aspects. There are two types of V2V information, short range and long range. Representative information of the short range can be the distance between the vehicles and the behavior data of the driver. Long range information includes road conditions, accident information on the road, and traffic information.

IoT Security

Many IoT devices are used to operate autonomous vehicles. The most representative is the "Guide Assist IoT," which will be applied to smart roads. This IoT informs the autonomous car of its current position, receives speed and driving information from the autonomous vehicle, and sends this information to the clients who need it.
While a variety of technologies are available to ensure safety when an autonomous vehicle is operated, the technology within the vehicle alone is not enough. The most obvious method is to install the IoT on the road where the autonomous vehicle is running.
The autonomous vehicle is constantly in communication with the IoT on the smart road. In this case, it is necessary to certify that the IoT of the smart road is the authorized IoT.

The biggest problem here is the speed of authentication. An IoT should be manufactured at low cost because it must be distributed in large quantities. Therefore, we cannot expect a high level of processing power. In particular, it is impossible for a car running in the public chain of this type to operate IoT.

Therefore, a method of authenticating a chain closer to real-time than real-time authentication is needed. CUBE sees this IoT's real-time authentication method as one of the important future development factors.

Intra-Communication Network Security

Automakers need to communicate with autonomous cars continually. Most important is navigation routing information, which includes traffic information. For completely autonomous self-driving cars, the car should receive the routing information from the automaker's traffic management centre. Even though the car has the navigation map data, it should receive the best route information, which comes with live traffic information. The potential danger is a malicious attacker with fake traffic information, such as fake traffic or a fake road block.

An autonomous car has a much more complicated Electronic Control Unit, which includes Break Control Unit (BCU), Transmission Control Unit (TCU), Wheel Control Unit (WCU), and many other units to control self-driving functions. An ECU being penetrated by a malicious attacker could be seriously dangerous. A great problem arises in terms of security because of the network between automakers and the gateway of autonomous cars. An automotive company should check each autonomous car's IoT devices to make sure that every autonomous car's ECU works without problem. At the same time, an automotive company should upgrade their automotive car's firmware remotely through the network. These checks and upgrades must be done regularly as all of these network connections will make the automotive cars vulnerable to malicious attacks.

II. CUBE Security Platform

CUBE consists of three layers. The first is the BC Layer, the second is the AI Layer, and the third is the Quantum Layer. The first layer, the Blockchain Layer, is a layer using the technique of blockchain, while the AI Layer is a layer using artificial intelligence. The third quantum layer is a layer using Quantum Cryptography. The blockchain layer will be commercialised in 2018, the AI Deep Learning Layer will be commercialised in 2020, and the Quantum Hash Cryptography will be commercialised in 2022.

1. Blockchain Layer

The key to blockchain is that the technology ensures trust. CUBE uses blockchain technology to ensure the security of autonomous mobile networks. But there are various difficulties in applying traditional blockchain to autonomous vehicle safety. The problem of blockchain is the slow speed and the low scalability.

At the heart of blockchain is securing trust with technology. So far, no technology has been able to prevent hacking 100% in the network. But the blockchain has shown a remarkable ability to prevent hacking completely without any failure in the past decade.

By solving the slow speed problem and the scalability issues that the blockchain has, we will be able to provide the highest level of autonomous car security.

1) The problem of Conventional Security and Need for Blockchain

There are three major problems in traditional automotive technology.

The amount of data that the car must process is tens of times larger than the data amount of other virtual currencies.

Centralisation issue
The amount of data received from the outside while driving is estimated to be more than 4Terabite per day. Such a large amount of data causes a serious problem. Centralisation reduces the operation speed of the CPU and eventually stops the system if the number of cars increases.

Privacy issue
The centralised approach eventually threatens the privacy of the driver. If someone can access the central server, you can access the personal identification of all drivers as well as the driving record.

Safety issue
A malicious attack on a car's network cannot be blocked 100% by current security methods. Alternatives must be created in order to reach maximum security.

Considering the weakness of conventional security methods, CUBE adopted blockchain as a key security platform for autonomous car. Blockchain is a distributed database that maintains a growing list of blocks that are chained to each other. Blockchain is managed by a distributed peer to peer network.

There are various difficulties in applying traditional blockchain to autonomous vehicle safety. Blockchain instantiations suffers from high overhead and low scalability. All transactions and blocks are broadcast to the entire network which results in extremely large packets.[1]

[1] Ali Dorri et al., 'BlockChain: A Distributed Solution to Automotive Security and Privacy', IEEE Communications Magazine, 2017, pp2-3

2) CUBE as a Hybrid Blockchain

CUBE's autonomous vehicle security is based on decentralised blockchain technology. Each entity is a node, making it basically the same as the security systems running on Ethereum. However, in the case of an autonomous car, there is a limit to the use of existing blockchain methods. Due to the blockchain’s slow speed and scalability problems, the blockchain technique cannot be used “as-is.” For this reason, CUBE has been preparing a hybrid chain.

CUBE is composed of hybrid blockchains that use public and private blockchains together. When datafying a vehicle’s drive, tons of data is generated, though the data varies depending on how the data was accumulated. Even when counting only the driving information and the peripherally recognised information used in datafication, enormous amounts of data (up to 4TB) are generated every day. This takes a lot of time to process or share. By contrast, vehicles require fast data processing, transmission, and receipt to prevent accidents.

The security of current autonomous vehicles is inefficient, in terms of velocity and volume, when it comes to handling by the public blockchain. To date, we have seen Hyperledger, the Linux Foundation’s Umbrella, and R3, in addition to more than 75 banking consortiums around the world, as examples of private blockchains. CUBE constitutes the private blockchain of autonomous cars, operating as a private blockchain to solve the problems of velocity related to data processing and volume. This, however, requires a very high level of trust in critically important elements, such as firmware upgrades by automakers. Those elements that require such a high level of trust will rely on public blockchains, such as Ethereum.

In summary, CUBE uses its own private blockchain, and also uses a public blockchain for critically important elements; thus, CUBE is a hybrid blockchain that can be used for all aspects of autonomous cars.

3) CUBE’Automotive Blockchain Mainnet

CUBE's ultimate goal is to build an automotive blockchain mainnet, which will require two steps. The first step is Over-the-Air (OTA). OTA is a technology that remotely updates a car's firmware. OTA can easily and remotely update many bugs in the car. These updates do not require high chain speeds since as they only take about an hour; fast blockchain hashes are not seen. Therefore, blockchain speed is not a major issue. CUBE will complete these technologies in 2018.

The second step is the autonomous car's security platform. The security of an autonomous car requires high-speed confirmation of the incoming information. It does not have to be too quick to receive simple navigation path information; however, obstacle information and road information in front of the car require very fast validation. Therefore, CUBE plans to apply one method of deep learning for this rapid validation.

The application of the stochastic gradient descent (SGD) method, which is quicker than gradient descent in deep running, is applied. SGD is a bit slower than slow perfection and faster processing. Facebook's Mark Zuckerberg says, "Done is better than perfect".

Gradient descent uses the full-batch method to check all the cases and to make decisions; however, it takes too much time. SGD uses the mini-batch method for trial and error, but at a much faster rate.

Deep learning can provide a variety of applicable technologies for making automotive blockchain. Momentum can be applied for faster blockchain speed processing. The incoming information is considered validated once it is the same. Nesterov's accelerated gradient (NAG) first predicts the incoming information, and then calculates and checks the incoming information. AdaGrad can be applied when you have not heard anything. AdaGrad is a way to search more closely because it has not visited, yet. In this case, you can apply AdaDelta to prevent it from stopping because it will slow down if you validate it too precisely. Considering all these factors, Adam can be applied to a blockchain.

4) CUBE Governance Issue

CUBE's governance will come from the participating automakers and owners of autonomous vehicles. Each participant becomes a node and has suffrage in the main decision-making process. The cost of this transaction will be paid to the carmakers as Proof of Share (POS). Automakers will have exclusive rights to data upgrades that require high reliability, such as super nodes firmware for each autonomous vehicle.

5) DAAP Based on CUBE Platform

CUBE is a hybrid blockchain platform that allows vehicles to easily share reliable data peer to peer (p2p). On this platform, a variety of future Internet of Things (IoTs) (e.g., guidance assist IoT, traffic information assist IoT, collision avoidance IoT, etc.) can be easily shared with trust.

6) CUBE's Blockchain Security Operation

CUBE solves these limitations of traditional BC technology with two concepts of segmentation and permission. In the operation of autonomous vehicles, many IoTs provide information to autonomous vehicles. This information may be transmitted directly between the IoT and the vehicle or may be transmitted through a center that controls the IoT.

The invader may try to interfere between the traffic centre or IoT and autonomous vehicle by taking access to the main network. Eventually, the invader can take control of the software binary with an intention of introducing malware into a huge number of vehicles.

If an attacker enters a new information hash value is not associated with a chain of existing blocks, it is considered a malicious attack. In case of important update information, the CUBE platform and the automaker require multiple signatures and only perform remote update if the two private keys match.

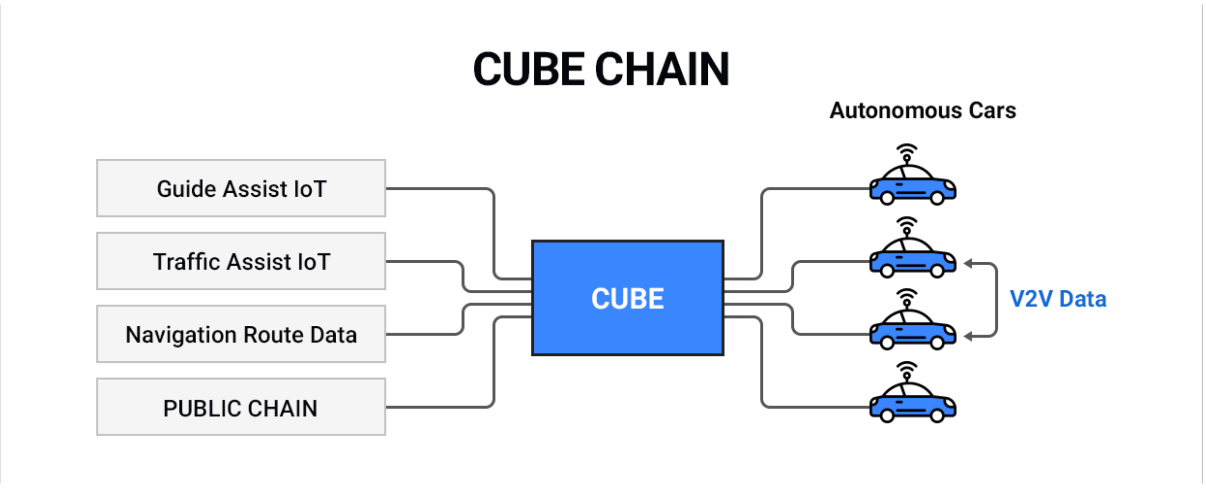


Figure 2

The data sent from the IoT to the car includes information such as location information and road conditions. Conversely, the information sent from the car to the IoT includes speed information and vehicle status information.

For the safety of autonomous vehicles, CUBE uses blockchain to handle communication between these vehicles and the IoT. Each of the IoTs becomes a node and the autonomous vehicle becomes a node, as well. The data transfer between these cars and the IoT is considered a transaction.

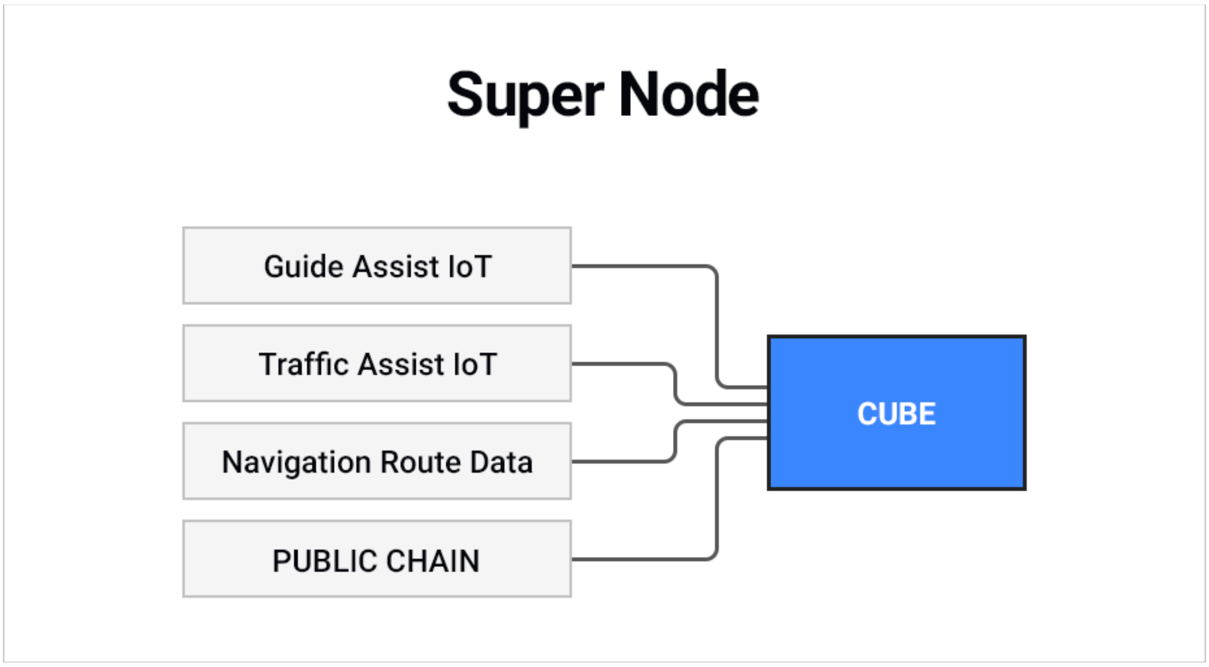


Figure 3

The essential information used in another autonomous vehicle is self-driving data provided by the automaker, the traffic management center, and so on. The automaker must remotely monitor the status of the vehicle from autonomous vehicles and remotely upgrade the firmware.
The autonomous car should receive only the authenticated data from the authenticated centre.
The authenticated centre should always be connected with the blockchain and should be updated continuously. Most malicious entities will disguise themselves using these centres, therefore this node is very important and needs to be trusted.

Blockchain was originally characterised as permission-free, but since communication with autonomous vehicles requires the highest security, only autonomous vehicles should be allowed to communicate with permission. Therefore, unlike the case with normal blockchain, the data should be processed based on permission.
To allow only authorised entities to access a node, CUBE uses the concept of a super node. A super node plays an important role, such as providing information to an autonomous vehicle and upgrading it, unlike a general autonomous vehicle. These super nodes can be specified by the automaker or the government.

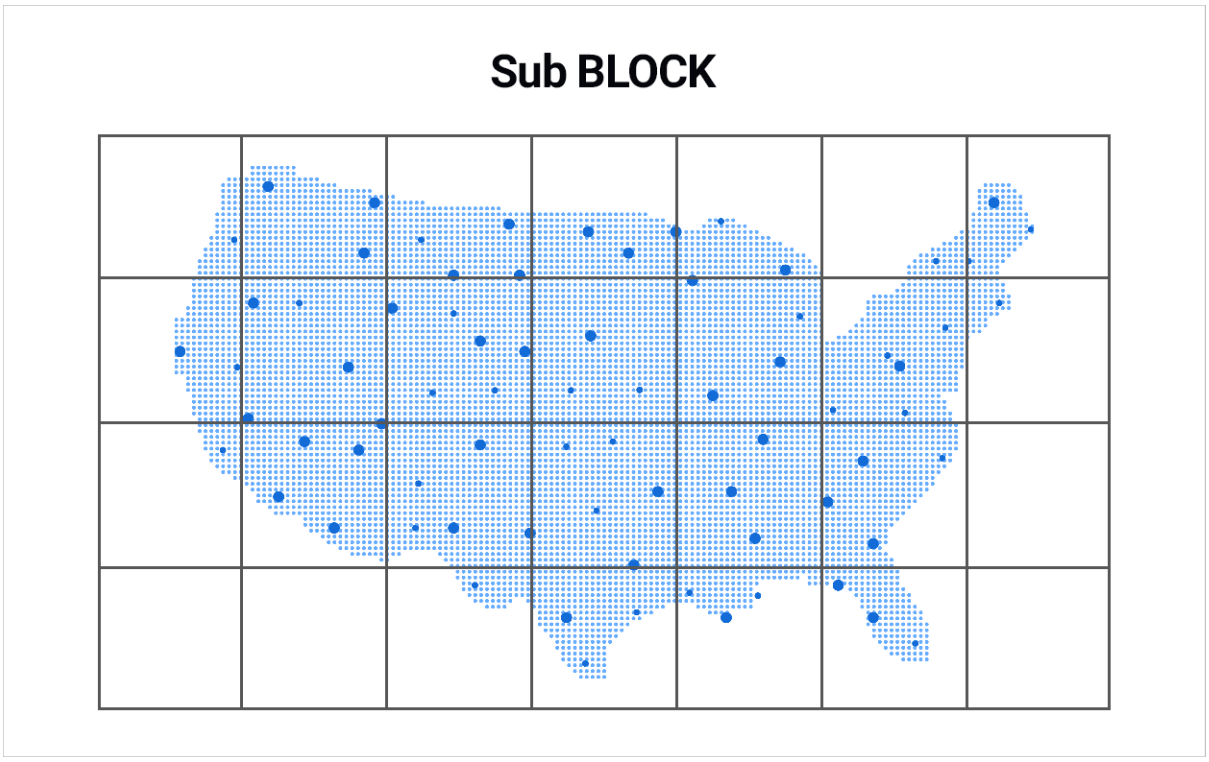


Figure 4

As seen in Figure 4, each sub-block works just like the current blockchain. It updates every nodes' transaction, such as traffic information, automakers' hardware upgrade and navigation route information. The size of the sub-block is relatively small, making the time to add a new block much faster than the current method.

7) Hand Shaking

If the autonomous vehicle's driving information needs to be handed over from one base station to another, the data may be interrupted in the meantime. In this case, the two base stations should negotiate so that the data can be transmitted well so that the data is not disconnected. These two protocols are called hand shaking.
The handshaking process generally occurs to set up guidelines for communication when a system tries to communicate with another device.
When a computer communicates with another device like a modem, printer, or network server, it needs to handshake with it to establish a connection.

Handshaking can adjust factors that are suitable for systems and equipment at all ends including coding alphabet, information transfer rate, interrupt procedure, parity and some other hardware features.
Handshaking is a technique of communication between two entities. However, within TCP/IP RFCs, the term "handshake" is most commonly used to reference the TCP three-way handshake.
A common handshaking protocol may include the receiver delivering the message meaning –“I got your previous message and you can send me the next one”
" A more complex handshaking protocol might allow the sender to ask the receiver if it is ready to receive or for the receiver to reply with a negative acknowledgment meaning “I did not receive your previous message properly, kindly send it again”

8) Single-Signature and Multi-Signature

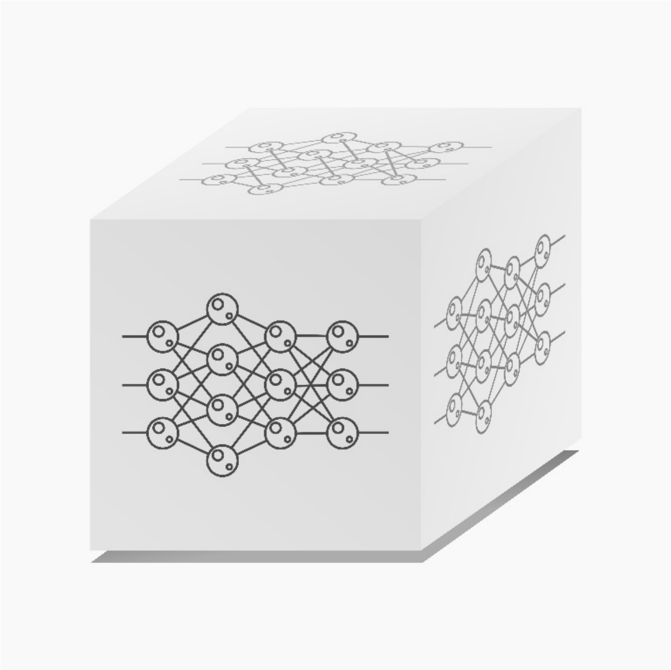
The way in which information comes into your car depends on how important the information is. If the information is related to entertainment, it can be accepted without any confirmation. However, the same level of traffic information is secured with a single signature. If it is important information, such

as upgrading the car's firmware, a single signature is not enough. In this case, the automotive manufacturer and the security platform of the CUBE must be approved at the same time; a multi-signature method is necessary for security approval.
Ali Dorri et al has made the desirable validity checking method as follows:

“All transactions are broadcast to all OBMs. An OBM checks the validity of the received transaction by verifying the affixed signature(s). If the transaction is valid, then it is stored in a pool of valid transactions which will be collated to form a block with a pre-defined block size, i.e., the total number of transactions stored in the block.”[2] “A multisig transaction that arrives at the OBM may yet need to be signed by the recipient, particularly when the recipient belongs to the cluster of that OBM. Each OBM retains a catalog of PK pairs that produce nodes which are permitted to communicate with each other.
The cluster members (i.e., overlay nodes) upload key pairs to the key list of their OBM to allow other overlay nodes to access them
In case the OBM discovers a PK pair in its catalog that goes with the PKs in the operation then it processes the transaction to the matching node which has uploaded the main pair. Or else, the operation is transmitted to further OBMs.

[2] Ali Dorri et al., ‘BlockChain: A Distributed Solution to Automotive Security and Privacy’, IEEE Communications Magazine, 2017, p.3

2. Artificial Intelligence (AI) Deep Learning Layer



To enhance the security level, artificial intelligence (AI) is applied at this stage. Recently, attacks on hackers' networks with malicious intent have rapidly been evolving. Until now, however, cybersecurity technology has been a passive method of collecting vaccines to defend against the attacks that have already been perpetrated. Cube has developed deep learning network security where a method is chosen based on predictions of malicious attacks that will occur, rather than a passive approach that uses defensive (instead of active) methods. CUBE will continue to learn how malicious attackers have attacked the network to prevent future attacks.

CUBE's Self-taught Learning

An invasion detection system thinks of a common kind of attach situation, where affected data packets are inserted into the in-vehicle Controller Area Network (CAN) vehicle.

Artificial neural networks have not worked well in the past to protect against these attacks, which is why new methods are needed. Three catalysts cause and maintain the explosions of malicious data—new mathematical computations are the spark, big data represent the fuel, and massive computation can be viewed as the horsepower. Cube uses previous cases of malicious attacks to recognise them. Cube allows the AI to train the Cube platform on cases of previous malicious attacks and predict hundreds of millions of new possible malicious attacks through this reinforcement learning. It then creates a defense system for each case.

Cube employs TensorFlow, an open-source library built by Google. There are many other ways of implementing deep running, but at present, TensorFlow has the best position in the market. In addition, there are a lot of data going on while watching the source code, which makes TensorFlow the most advantageous library. TensorFlow is an open-source software library for numerical computation using dataflow graphs; one reason for its popularity is that it can be developed with Python.

A graph is a connection between one node and another, while a dataflow graph is an operation. This edge is data to be easily said; this is called a data array. TensorFlow enables calculations through this process, and the TensorFlow runtime is a cross-platform library. Google designed TensorFlow for large-scale distributed training and inference, but it is also flexible enough to support experimentation with new machine learning models and system-level optimisation.

Cube builds the first graph in TensorFlow. First, it can create a “placeholder” node, and each node becomes a placeholder. When a placeholder is created, it passes the value to the “feed data” as the graph runs through the session. This graph is then executed and updated as needed, or it returns an output indicating whether a malicious attack has occurred. A large quantity of data must be input regarding previous malicious attacks in order to make the output more accurate. CUBE’s neural network is initially trained by being fed large amounts of data. Training consists of providing input and asking the network what the output should be. For example, to build a network for identifying malicious attacks, the initial training may include a series of past malicious attacks. Each input is accompanied by the matching identification. Providing the answers allows the model to adjust its internal weightings to learn how to do its job better. For example, if nodes A1, B1, and C1 tell node D1 that the current input data represent a malicious attack, while node E1 says they are normal data, and the training program confirms a malicious attack, CUBE will decrease the weight it assigns to E1's input and increase the weight given to A1, B1, and C1.

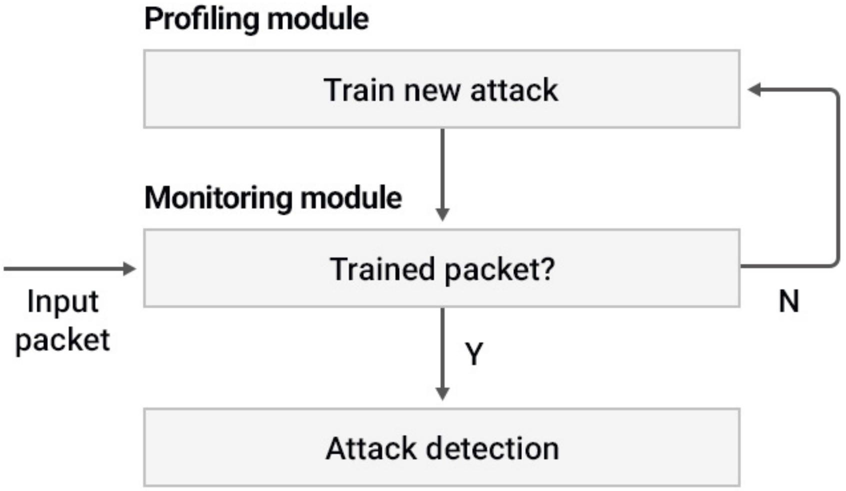


Figure 5: Architecture of the deep learning flow.

Deep Learning for Classification

Cube uses a neural network to determine the malicious attacks expected in the future. In fact, neural networks do not always provide good results. There are three problems with such networks, namely underfitting, low speed, and overfitting. *Underfitting* refers to a problem whereby the learning is insufficient. *Low speed* is an issue where it takes too long to learn. Finally, *overfitting* means that the network is inflexible, even when it has learned. These three problems make a neural network’s results unreliable.

Underfitting

The first problem, underfitting, means that learning is not effective enough. A neural network learns via backpropagation. It updates itself by repeating the processes of differentiation, multiplication, and adding, and all in vice versa. The problem, however, is that a sigmoid function is used for activation.

We have found a repeated issue with the vanishing gradient phenomenon: As the layer becomes deeper, the updates disappear. Therefore, underfitting occurs, which results in poor fitting.

Instead of a vanishing sigmoid, Cube uses an activation function that does not disappear. Specifically, rectified linear units (ReLUs) are used as the activation function. This solves the problems related to the vanishing gradient.

Low Speed

The second problem to be solved for neural networks is the low speed problem. Existing neural networks have used gradient descent (GD) to optimise the weighting parameters. The gradient is obtained from the current weight of the loss (or cost) function, and it is updated to reduce the loss. To put it briefly, this is wrong (Slide 35). There are hundreds of millions of training data on hacking, and if we consider those hundreds of millions of hits each time we hit a mark, the network will slow down significantly. This raises the following question: Could there not be a faster optimiser than GD? Here, we find the stochastic gradient descent (SGD) method. The concept of SGD is that it is a method that can be completed quickly, even if the results are not perfectly accurate. As Mark Zuckerberg has said, “Done is better than perfect.” Gradient descent is a method that takes one step after a full batch; in contrast, SGD uses mini-batches and moves forward step by step.

Cube employs Adam as an improved version of SGD. Combining the advantages of RMSProp + Momentum, this solution is suitable in terms of both the step size and direction. In the future, we can consider attaching NAG to Adam instead of Momentum.

Overfitting

The final problem with neural networks is their inflexibility. To solve this problem, we can deliberately omit information or turn off the intermediate nodes when training a neural network. Dropout lets us learn what the important factors are without obsessing over specific parts. Thus, the problem of overfitting relates to obtaining flexibility without dropout.

Cube solves the three problems related to neural networks, namely underfitting, low speed, and overfitting. The problem that Cube is trying to solve is not snapshot data like images, but sequential data that discriminate whether the signals are malicious attacks. Hence, Cube uses a recent neural network (RNN) or long short-term memory (LSTM).

How the CUBE token works?

CUBE's token has two areas of production and consumption. The production of tokens is provided to information producers who provide operating information to the CUBE platform. Information providers who install CUBE slots at the terminal of obd2 provide various operating information such as route, driving habit, speed, and location. In exchange for providing this information, the driver receives the CUBE token.

Users of CUBE tokens can use tokens when receiving automotive related services. Token owner can also use it when they gas, buy a car, or even as a highway pass. Our token buyers are primarily those who provide automotive-related services and those who receive automotive-related services. For automobile service companies, driving information is an important asset as big data. Therefore, the CUBE token becomes the production side of production information related to the production side, and the consuming side becomes the automobile related companies and consumers who need the car big data.

Transparency Policy

CUBE considers transparency to be of the utmost importance.
CUBE has established policy for transparent operations and will execute the following:

1) CUBE is to receive a fair audit from a well-known and reputable accounting firm. We are to be audited by voting 5 accounting firms that are globally recognised and credible.

2) CUBE shall publish monthly operational reports and financial reports to contributors to share the operational status of the company.

3) When hiring new staff members, such as new developers, CUBE shall build up a validation process as well as thoroughly examining portfolios from past and set the reward policies in accordance with their abilities.

4) The company's budget shall be tightly managed so that it would always be possible to operate and manage the company without additional funding for more than three years.

Contributors Communication

1) CUBE shall send a monthly report every month to share important company’s update.

2) In case of an important occasion, CUBE must share the important matters by email immediately.

3) Follow CUBE’s social media accounts for live company updates and to communicate directly with the team.

Token Valuation Operation Policy

To protect contributors and provide with better profits, CUBE will be operated as follows:

1. The executive managers of CUBE are under the effect of Lock-Up System, which means they are not entitled to token sale for one year. The Lock-Up policy is intended to make sure the executive managers to benefit suitable reward after the company grows enough.

2. CUBE shall strictly control the use of the budget to stably increase the value of CUBE Token. At least 2/3 of the beginning budget must remain after one year of funding. In case of any event which requires using more than 1/3 of the beginning budget, the approval of the board and the contributors participating in the ballot must be at least one-half.

Contribution Detail

The Contribution Period will begin November 27th, 2017.
Participants willing to contribute to and support the development of CUBE can do so by sending ether to the designated address. By doing so, contributors create CUBE at the rate of 1,000 CUBE per ETH.

The Contribution Period will run until March 15th, 2018, or at the moment of reaching the ceiling.
CUBE received by Contributors will be transferrable 7 days after the end of the Contribution Period.

Reference

1. G.V.Assche, ‘Quantum Cryptography and Secret-Key Distillation’, Cambridge University Press, 2006

2. C.Huang, Y.Shi, ‘Quantum hashing is maximally secure against classical leakage’, University of Michigan, 2017

3. Ali Dorri et al., ‘BlockChain: A Distributed Solution to Automotive Security and Privacy’, IEEE Communications Magazine, 2017, p.3

4. Mark V. Slusar, ‘Insurance system related to a vehicle-to-vehicle communication system’, US 9390451 B1, Jul 12, 2016