A Threat Based Approach to Computational Offloading for Collaborative Cruise Control

Al Tariq Sheik
Cyber Security Center, WMG
University of Warwick
CV4 7AL
Coventry,U.K
T.sheik@warwick.ac.uk

Carsten Maple
Cyber Security Center, WMG
University of Warwick
CV4 7AL
Coventry,U.K
CM@warwick.ac.uk

Tim Watson
Cyber Security Center, WMG
University of Warwick
CV4 7AL
Coventry,U.K
TW@warwick.ac.uk

Hussam Alhagagi
Cyber Security Center, WMG
University of Warwick
CV4 7AL
Coventry,U.K
H.Alhagagi.1@warwick.ac.uk

Nader Sohrabi Safa
Cyber Security Center, WMG
University of Warwick
CV4 7AL
Coventry,U.K
N.sohrabi-safa@warwick.ac.uk

Sang-Woo Lee
Information Security Research Division
ETRI
34129
Daejeon,
South Korea
ttomlee@etri.re.kr

ABSTRACT

The interaction between discrete components of Internet of Things (IoT) and Intelligent Transportation Systems (ITS) is vital for a collaborative system. The secure and reliable use of Cruise Control (CC) with Cloud and Edge Cloud to achieve complete autonomy for a vehicle is a key component and a major challenge for ITS. This research unravels the complications that arise when Adaptive Cruise Control (ACC) is incorporated into a collaborative environment. It mainly answers the question of where to securely compute Collaborative Cruise Control's (CCC) data in a connected environment. To address this, the paper initially reviews previous research in the domain of Vehicular Cloud, ITS architecture, related threat modelling approaches, and secure implementations of ACC. An overview application model for CCC is developed for performing a threat analysis with the purpose of investigating the reasons why a vehicle suffers collision. Through the use of interviews, the research analyses and suggests the location of computational data by creating a taxonomy between the Edge Cloud, Cloud and the On-board Unit (OBU) while validating the model.

Keywords: Collaborative Cruise Control; Connected Autonomous Vehicles; Secure Intelligent Transportation System; Threat Modelling; Vehicular Cloud Computing;

1. INTRODUCTION

IoT is a technological revolution, albeit one at its beginning stages which involves collaboration between sensors collecting data to predict and suggest a timely action for achieving a task, especially in an autonomous vehicle. It utilises the internet extensively, supported by Cloud and Edge-Cloud (i.e. fog computing) technology. There has been an estimation of 100 billion devices that would be connected to the internet by 2025 [1]. The internet would be a medium, responsible for a large amount of data which requires secure and reliable transmission, storage, processing and reception of data. Although there are various advantages with IoT, it further adds severity to the infrastructure if appropriate risk and threat analysis procedures are not performed respectively for each application.

ITS utilises the concepts that are involved in the IoT when major decisions are to be handled in the Cloud. In the past, transportation was the vital connecting power that helped in the advancement of technologies. Similarly, the advent of communication technologies was another major influential force that helped humanity boost its efficiency and capabilities. This interdependency between these two fields contributed to the development of autonomous technologies for the automotive industry. The amalgamation of these two fields of technology has given birth to numerous forms of Connected Vehicles (CV) programmes across Europe and the US which would mainly rely on the significant use of Cloud technologies in the near future and opening many gateways and opportunities in the domain of IoT [2].

CCC is a vital technology for autonomous driving and ITS and it is important to identify the different types of data for CCC that can be classified either as in cloud or on-board for computation while considering the communication latency, security, accuracy and reliability of the data for different vehicular applications. To be more specific, this study answers the question: *Where should we securely compute Collaborative Cruise Control data in a Cloud Based Connected Vehicular System?*

In order to understand which part of the computation an application can be offloaded onto the cloud, the application's data should be analysed in an overall manner, their criticality understood, a threat analysis modelled, their risks examined, their respective mitigations considered and their latency requirements be correlated. This paper lays emphasis on CCC because it encompasses various applications such as longitudinal and lateral speed control and lane changing using available communication mediums such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and direct communication to the Cloud using technologies such as IEEE

ICC '17, March 22 2017, Cambridge, United Kingdom
© 2017 ACM. ISBN 978-1-4503-4774-7/17/03...$15.00
DOI: http://dx.doi.org/10.1145/3018896.3056792

802.11x, WiMAX, 3G, 4G/ LTE and potentially 5G. Moreover, this paper will further set foundations for future work on establishing a taxonomy of data by raising questions for CCC and other vehicular applications.

In order to achieve this goal, the following four objectives have been formulated: Firstly, a review will be conducted on the existing research in the domain of vehicular cloud ITS and implementations of ACC, Cooperative ACC (CACC) and CCC, and the different threat analysis procedures. Secondly, a threat analysis is performed after building a conceptual overall data flow and on-board model for CCC. Thirdly, the critical data is analysed based on the latency, computation, location, accuracy and security, and we classify where the data could be processed (cloud/on-board) based on the feedbacks received from the academics and engineers with automotive and cyber security backgrounds. Finally, the accuracy of the developed model is verified and the outcomes discussed based on the analysis of the critical data.

The remainder of this paper is organised as follows. Section 2 carries out the literature review mentioned in first objective. Section 3 illustrates a proposed model in detail. Section 4 highlights the validation process of the model. Finally, Section 5 concludes the study and describes its findings while raising further questions concerning the data computation by providing a basis for future work.

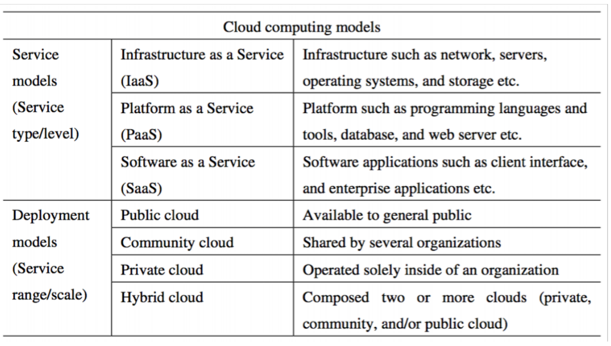
2. BACKGROUND AND RELATED WORK

2.1 Vehicular Cloud

Vehicles consist of numerous embedded systems such as Electronic Control Units (ECUs) which are responsible for coordination among many functions in a vehicle such as its acceleration, brakes, airbags etc. [3]. These functions do not require high computational power compared to data intensive applications such as traffic light detection, image recognition, and facial and voice recognition, none of which it is efficient to implement on the vehicle's OBU due to the limitations present in the computational power on-board [4]. Moreover, there is an increase in demand for computationally driven applications [5]. This raises a concern about software updates corresponding to the hardware components on-board as vehicles have higher longevity. These issues can be addressed by offloading the vehicles computation to the cloud. Therefore, the cloud facilitates the idea of offloading, but it brings along various consequences.

There are two main types of Cloud for vehicles: conventional cloud and edge cloud (fog computing). Yan and Xu [6] connected the use of cloud computing and IoT in order to provide a secure economic platform with two cloud services. Using this, a three-layered architecture is developed providing an application for intelligent parking cloud service and mining vehicular maintenance data. The conventional cloud can be classified into three broad categories based on the different services they offer: Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) [4], [6], [7]. In addition to this, authors in [8] have also proposed deployment models which provide public, community, private and hybrid cloud services. These can be inferred from Figure 1.

According to [6] and [9], edge cloud is an emerging technology that is designed to hold dynamic information which exchanges data with the conventional clouds based on the requirements of the applications such as services in infotainment, geo-distribution, location awareness and low latency applications. However, this is not the case with conventional clouds as interoperability, batch processing, real-time sensing and proximity to the vehicle are the limitations that would render it unable to cater to the needs of vehicles with latency-sensitivity applications.



Cloud computing models		
Service models (Service type/level)	Infrastructure as a Service (IaaS)	Infrastructure such as network, servers, operating systems, and storage etc.
	Platform as a Service (PaaS)	Platform such as programming languages and tools, database, and web server etc.
	Software as a Service (SaaS)	Software applications such as client interface, and enterprise applications etc.
Deployment models (Service range/scale)	Public cloud	Available to general public
	Community cloud	Shared by several organizations
	Private cloud	Operated solely inside of an organization
	Hybrid cloud	Composed two or more clouds (private, community, and/or public cloud)

Figure 1: Different Types of Cloud models [8]**.**

Similarly, the ITS cloud architecture (Figure 2) consists of three abstract layers: cloud layer, communication layer and end-user layer showing the use of the conventional clouds and edge cloud as previously mentioned [10]. The architecture is proposed for use with correspondence applications such as emails, web service applications, cloud backup, business applications, research applications and load balancing capability but has not addressed the use of computationally intensive and safety critical applications.

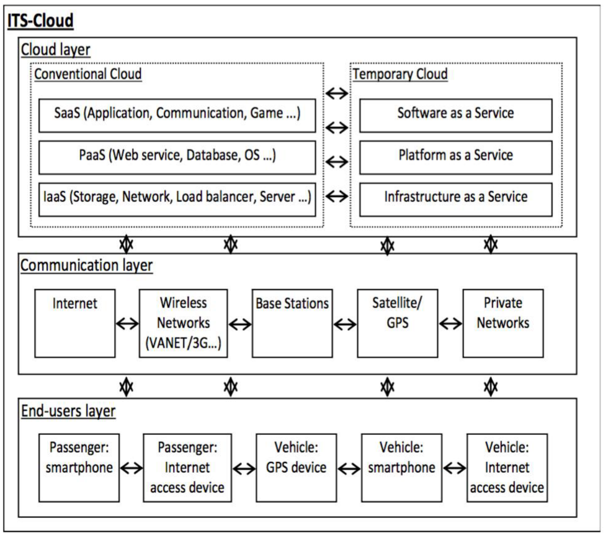

ITS-Cloud
Cloud layer
Conventional Cloud
SaaS (Application, Communication, Game ...)
PaaS (Web service, Database, OS ...)
IaaS (Storage, Network, Load balancer, Server ...)
Temporary Cloud
Software as a Service
Platform as a Service
Infrastructure as a Service
Communication layer
Internet
Wireless Networks (VANET/3G...)
Base Stations
Satellite/ GPS
Private Networks
End-users layer
Passenger: smartphone
Passenger: Internet access device
Vehicle: GPS device
Vehicle: smartphone
Vehicle: Internet access device

Figure 2: ITS Cloud [10]**.**

The implementation of these applications through the use of different types of vehicular clouds was explained by [6], [8], [10]. However, secure implementation ensuring *Confidentiality Integrity and Availability (CIA)* model was not addressed from a security point of view. Moreover, a secure data taxonomy for computational offloading related to the above mentioned applications was not acknowledged either in the ITS cloud architecture or others. On the other hand, the authors did not consider authorisation and authentication nor did they consider security as a parameter in the theoretical frameworks. In addition, trust relationships between the clouds were discussed briefly, concluding that there is a vital necessity for a balanced security.

Nevertheless, the lack of security measures mentioned above are discussed by the authors in [4] and they envisioned the use of three different vehicular cloud scenarios. These cloud scenarios include Mobile Vehicular Cloud, Mobile Personal Cloud, and Mission Oriented Mobile Cloud. Considering these cloud environments, the author has raised concerns for privacy and security protection, sensing, filtering aggregation of data, and secure management of contents based on trust management. Moreover, the author has also discussed about the use of vehicles sensors for environmental sensing, urban surveillance, route management for vehicular traffic management. These proposals have raised questions concerning how the data can be transferred to the cloud which leads us to the Section 2.2.

2.2 Offloading Vehicular Services and Data to the Cloud

Offloading provides a means of migrating the execution of computationally and data intensive tasks from OBU to the cloud. The authors in [5] have proposed the framework, as shown in Figure 3, for the use of cloud computing in vehicles. This enables the functions (modules) to decide what kind of tasks can be offloaded to the Cloud. This requires consideration of different parameters (input and output data size) of the application and cost incurred such as latency, network downlink, uplink speeds and execution time. Furthermore, they proposed a decision making process with the help of model execution time ratio (E) which considers offloading of applications only if E<1. The proposed framework was validated with road experiments by using an Android based Mobile device (Nexus 5) and Carnegie Melon University's (CMU) private cloud server to verify two applications: on-board hand gesture recognition and traffic lights and road sign recognition. Their experiment, with the use of cloud computing, showed a threefold increase in average response time compared to the on-board local computation irrespective of the vehicle's speed.

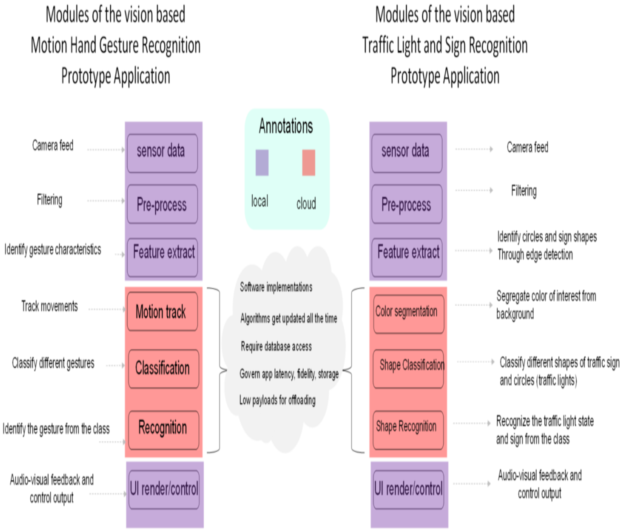

Modules of the vision based
Motion Hand Gesture Recognition
Prototype Application
Modules of the vision based
Traffic Light and Sign Recognition
Prototype Application
Annotations
local
cloud
Camera feed
sensor data
Filtering
Pre-process
Identify gesture characteristics
Feature extract
Track movements
Motion track
Classify different gestures
Classification
Identify the gesture from the class
Recognition
Audio-visual feedback and control output
UI render/control
Software implementations
Algorithms get updated all the time
Require database access
Govern app latency, fidelity, storage
Low payloads for offloading
sensor data
Camera feed
Pre-process
Filtering
Feature extract
Identify circles and sign shapes Through edge detection
Color segmentation
Segregate color of interest from background
Shape Classification
Classify different shapes of traffic sign and circles (traffic lights)
Shape Recognition
Recognize the traffic light state and sign from the class
UI render/control
Audio-visual feedback and control output

Figure 3: Distribution of Application Modules between Cloud and OBU [5].

Offloading with clouds often has trade-offs in terms of communication costs and latencies which could get counterbalanced by the efficiency of the computation. The author's work [5] is complemented by work [11] where the author proposes an execution prediction mechanism by comparing the benefits and efficiency of three different application's computational offloading processes in different environments. These applications include face detection, voice recognition and DroidFish (an Android alternative of a chess engine). However, the authors in [11] designed and illustrated the use of IC-Cloud system architecture as shown in Figure 4, which introduces the connectivity predictor, a parameter that predicts the future connectivity with the help of signal strength and historical signal information.

Another significant parameter, the offload controller, relies on an execution predictor and a connectivity predictor to decide if the task should be offloaded. As a result, the authors proposed three ways to reduce uncertainties: lightweight connectivity prediction, execution prediction and application trackers. These predictions are used in a risk controlled way to offload tasks.

The authors in [5] and [11] have both demonstrated experimental validations and showed that computational offloading and decision making process is possible with the use of the mentioned frameworks. The authors in [11] have proposed an IC-Cloud architecture. This concept plays an important role in influencing the decision making process for vehicles. However, both the studies did not consider security as a parameter to ensure Confidentiality, Integrity and Availability (CIA) during the offloading process which could further add latency due to the extended computation associated with encryption or other alternatives. Despite the drawback, the demonstrations and experiments play a vital role because further research on this concept would provide vehicular applications with the ability to offload data to a cloud environment in a secure manner.

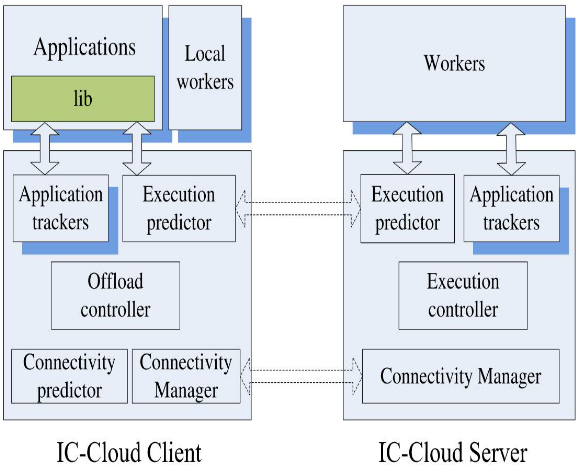


Figure 4: Overview model of IC-Cloud Architecture [11]**.**

2.3 ITS Architecture

The ITS architecture shown in Figure 5 consists of six major layers of which each layer has its own significance [2], [12]. The architecture consists of the application layer, facilities layer, networking and transport layer, access layer, management layer and security layer. Each layer has its own significance, however, the working of each layer is beyond the scope of this paper.

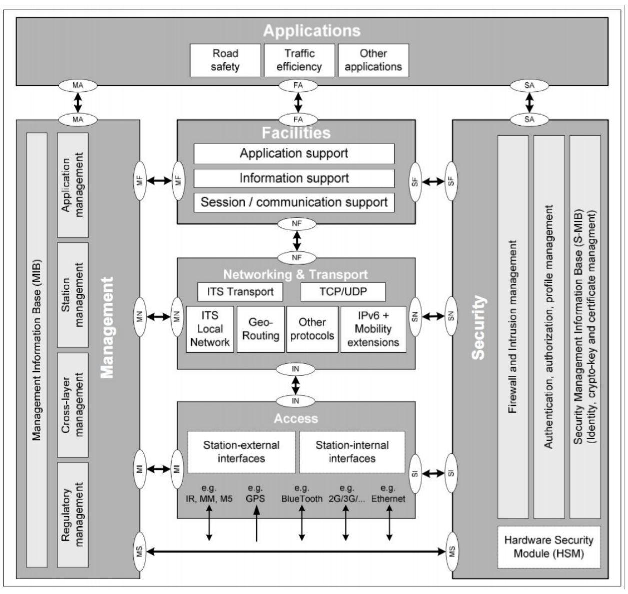


Figure 5: ITS architecture [2], [12]**.**

2.4 Threat Modelling Approaches

A threat model helps us to understand and identify different ways and parameters in which a software application or a system architecture can be attacked. It helps a threat analyst discover an anomaly with a system or an application in a structured manner and then provide questions to address the motivations of idealized attackers [13]. It will be useful for issues in a systematic manner while understanding the security requirements to model better system architectures and models for CCC by addressing the issues that other techniques would not address. Threat modelling is vital for CCC as it is one of the main functions in ITS. It is time and data critical to set the vehicle in motion in a synchronous fashion while being aware of the environment to ensure safety for the drivers, pedestrians and the surrounding vehicles. Streamlining the characters of threats to CCC, the system-centric approach is the appropriate threat model to use. This is because vehicles coordinate and interact as a group of embedded systems which are vulnerable and requires a systematic mitigation. The system-centric/asset-centric approaches can be explained with the help of the following four approaches: Microsoft's threat modelling (STRIDE/DREAD) [13], TRIKE [14], OCTAVE [15] and Composite Threat Modelling [16].

The use of STRIDE/DREAD is mainly oriented to software and business. However, the applicability of this model is wide and flexible enough that it can be used for vehicular systems. Alternatively, the author in [14] points out that although the benefits are in terms of accountability and integration the major drawback of the approach is its lack of the theoretical underpinning which thereby makes it unable to support academic work. Since the research is a qualitative study on CCC systems and its academic nature mainly relies on past theoretical works, this makes the methodology difficult to use for threat modelling.

TRIKE's in-depth methodology that involves the use of the different models (requirements, implementation, threat, risk) is tedious and difficult to alter to the needs of CCC. In addition, the tool restricts the use of the methodology as it is not as flexible as STRIDE, which any user can understand the methodology. Furthermore, TRIKE has a different approach where the models, distinct in nature when compared to STRIDE, involves a collective approach. Moreover, TRIKE's goals are mainly aligned to meet the needs of a stakeholder which is of stark contrast to the objectives of the research. Considering these requirement, the study has overlooked TRIKE as well and has decided to adopt an alternative approach.

Although OCTAVE is one of the approaches suggested by the Society of Automotive Engineers in 2016 (SAE), for its stable and robust threat analysis on vehicles, this study has not adopted the model. This is because the OCTAVE approach is mainly applicable for industries and organisations reliant on manufacturing vehicles. The approach undergoes an exhaustive testing of the developed model during the longitudinal phase of testing. Considering this cross-sectional study, it is much more inclined towards the use of a composite threat modelling approach, due to its simplicity.

Composite threat modelling, from an automotive point of view, is built according to the needs of a modern automotive vehicle and is an amalgamation of STRIDE/DREAD, TRIKE threat modelling and Application Security Framework (ASF) [17]. In the Composite model process, as shown in Figure 6, it can be observed that each step aligns with the objectives stated in the research for classifying the CCC's data by analysing its criticality. In addition, Phase 1 helps in identifying priority applications for analysis, which requires a working knowledge of a specific component/system and how it relates to other components/systems. This is achieved by analysing the interconnection diagrams through considering all the data paths and potential attacks. By contrast, Phase 2 involves two main processes: Threat Identification and Threat analysis. The former is a continuous process in which the threats are identified from multiple sources such as vulnerability database, information sharing from industries etc. The latter involves the study of entry points and access methods with the help the of use case elements such as STRIDE to create a Vehicle Threat Matrix.

3. PROPOSED APPLICATION MODELS

This section provides details of the changes to the proposed models discussed in Section 2.1, 2.2 and 2.3 while applying the same to the composite threat modelling approach mentioned in Section 2.4 due its ease and convenience, and its characteristics for vehicles. In addition, it would adapt to identify the reasons behind the collision for a vehicle while developing the use case. This section is organised based on Figure 6, considering Phase 1 and Phase 2 respectively. Section 3.1, 3.2 and 3.3 correlates Phase 1 with CCC by applying the modified ITS architecture in Figure 7. Phase 2 is discussed in Section 3.4, which highlights the threat identification and analysis.

3.1 Modified ITS Architecture

As Figure 7 illustrates, the ITS architecture is incorporated within four key modules to the facilities layer. Based on the work of the authors of [5], [11], the proposed ITS architecture model uses the concepts *connectivity predictor, execution predictor, offload controller and online placement framework module.*

As previously mentioned in Section 2.3, the ITS architecture consists of six major layers. The layers that require the modification are the application and facilities layer. The application layer is catered to by the rest of the five layers. It is in this layer that the CCC/ CACC module is incorporated as a traffic safety application in the modified ITS architecture.

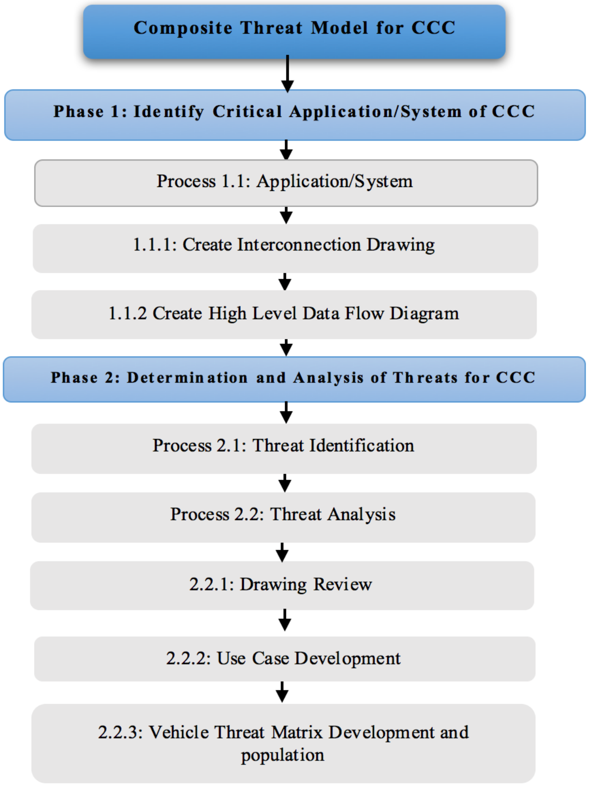

Composite Threat Model for CCC
Phase 1: Identify Critical Application/System of CCC
Process 1.1: Application/System
1.1.1: Create Interconnection Drawing
1.1.2 Create High Level Data Flow Diagram
Phase 2: Determination and Analysis of Threats for CCC
Process 2.1: Threat Identification
Process 2.2: Threat Analysis
2.2.1: Drawing Review
2.2.2: Use Case Development
2.2.3: Vehicle Threat Matrix Development and population

Figure 6: Composite threat modelling approach for CCC.

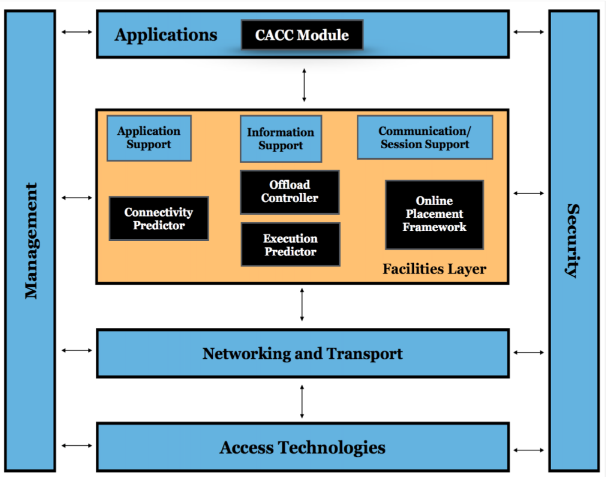


Figure 7: Modified ITS Architecture.

The facilities layer is mainly responsible for the transmission and reception of data and messages. This layer is modified with an *offloading controller* which uses data and information from a *connectivity predictor* and an *execution predictor* as proposed by the authors of [5], [11].

The offloading controller is responsible for periodically profiling the data associated with a module within an application that is considered to be safe to be offloaded. For offloading to be considered, the data size, network latency and execution time are the significant parameters [5]. Since the strength of the signal depends on the traffic density and interference, the offloading process is dynamic in nature. Moreover, the offloading controller is further informed by the connectivity predictor and execution predictor. The connectivity predictor keeps track of the strength of the signal in the form of network states and historic connections. The execution predictor accumulates the information from the CACC application and then calculates the execution time for each of the modules.

Once the offloading controller is informed by the connectivity predictor and execution predictor, the online placement framework makes dynamic run-time decisions concerning which task or module should be offloaded based on the Execution Time Ratio, as proposed by authors in [5].

3.2 Modified CVRIA Overall Flow Architecture.

The Modified ITS Architecture is associated with an OBU of a vehicle in Figure 8 and is applied for CCC. The modified Connected Vehicle Reference Implementation Architecture (CVRIA) gives an overall flow diagram and considers two key components: *the data centre's cloud* and its *edge cloud.* This proposed advancement functions to distribute the computational data for CCC.

The modified CVRIA architecture incorporates the use of cloud technology into the data centre and the edge cloud with the vehicle. For proper functioning of the CCC there are many entities that interact with each other. These entities involved are as follows:

3.1.1 Operations Personnel

These are the people who are stationed at the Traffic Management Centre (TMC) who are responsible for control of traffic control systems, surveillance systems, incident management systems, work zone management systems and travel demand management systems. Moreover, they are responsible for governing and controlling the Traffic Operator inputs to the TMC. These inputs would vary depending on the deployment and positon of the job (CVRIA, 2016) [17].

3.1.2 Traffic Management Centre (TMC)

The TMC is in charge of controlling and monitoring road traffic, road construction and unexpected changes. It is a main centre that supervises highway, rural and suburban roads, along with managing and informing the traffic in different areas by regularly communicating and updating its system using Roadside Equipment (RSE) and ITS Roadway equipment.

The TMC receives traffic flow information and environment sensed data from the ITS Roadside Equipment while it transmits processed traffic sensor and environmental sensor control data back to the same source. In addition, the TMC sends processed automated lane control data to the RSE after receiving the sensed lane status. The RSE also sends the relevant traffic situation data along with environmental sensed data.

In Figure 8, the TMC is further modified to provide Cloud services classified as a Platform as a Service (PAAS) (Section 2.1) such that it offers a variety of cooperative services and is not restricted to only providing traffic information but also hazardous location, lane change warning and parking warning to the vehicles directly. This is made possible by collecting information from both the RSE ITS Roadway Equipment and vehicles for further processing and continuous transmission of updates to the respective entities.

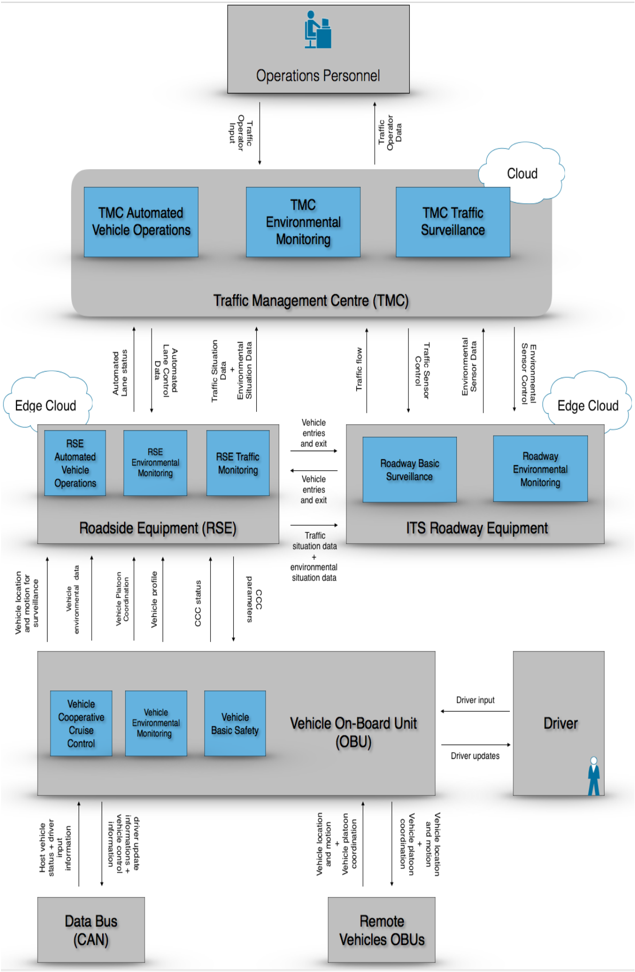

Operations Personnel
Traffic Operator Input
Traffic Operator Data
Cloud
TMC Automated Vehicle Operations
TMC Environmental Monitoring
TMC Traffic Surveillance
Traffic Management Centre (TMC)
Automated Lane status
Automated Lane Control Data
Traffic Situation Data + Environmental Situation Data
Traffic flow
Traffic Sensor Control
Environmental Sensor Data
Environmental Sensor Control
Edge Cloud
Edge Cloud
RSE Automated Vehicle Operations
RSE Environmental Monitoring
RSE Traffic Monitoring
Roadside Equipment (RSE)
Vehicle entries and exit
Vehicle entries and exit
Traffic situation data + environmental situation data
Roadway Basic Surveillance
Roadway Environmental Monitoring
ITS Roadway Equipment
Vehicle location and motion for surveillance
Vehicle environmental data
Vehicle Platoon Coordination
Vehicle profile
CCC status
CCC parameters
Vehicle Cooperative Cruise Control
Vehicle Environmental Monitoring
Vehicle Basic Safety
Vehicle On-Board Unit (OBU)
Driver input
Driver updates
Driver
Host vehicle status + driver input information
driver update informations + vehicle control information
Vehicle location and motion + Vehicle platoon coordination
Vehicle location and motion + Vehicle platoon coordination
Data Bus (CAN)
Remote Vehicles OBUs

Figure 8: Overall Data Flow Diagram of CCC.

3.1.3 ITS Roadway Equipment

The ITS Roadway Equipment is present all over the roads and functions to sense, monitor, manage and controls the traffic along the road. This entity regularly updates the roadside equipment and the TMC. It includes many physical devices such as [17]:

- Traffic detectors
- Sensors that monitor the surroundings such as the weather, road condition and the environment.
- CCTV cameras
- Traffic signals
- Video and image processing systems
- Dynamic message signs
- Lane automation system
- Barrier systems that regulates traffic to different roads such as tunnels and bridges
- Work zone systems such as detour ahead signs with zone surveillance for traffic monitoring and driver warning

3.1.4 Roadside Equipment (RSE)

The RSE is in-charge of sending CCC control parameters and receiving messages from vehicles such as the vehicle's environmental data, location and motion data, platoon and coordination data and CCC status. The transmission and reception of messages between vehicles is achieved through Dedicated Short Range Communication (DSRC) such as IEEE 802.11p.

The RSE not only supports the functioning of applications for vehicles but also communicates with other RSEs along with ITS Roadway equipment. It also updates the ITS Roadway equipment with entry and exist messages for the relevant vehicles, along with traffic situations, which are sent parallel to the TMC [18].

3.1.5 Vehicle OBU

The vehicle's OBUs are where all the safety critical functions take place after sensing the environment and processing it. This is where the ITS architecture is proposed to be instated from Section 2.2. The proposed ITS architecture when placed on vehicles with its offloading and online placement framework, would help transfer computational intensive tasks to the distributed components in the environment. These could be from neighbouring vehicles, RSEs, or from direct interactions with the cloud. The vehicle's OBU's provides the vehicle with computation, storage, and processing capabilities. The vehicle consists of communication technologies for V2V and V2I functionalities.

3.1.6 Remote Vehicle's OBU

This is the neighbouring vehicle that the host vehicle communicates with in order exchange each other's location and motion data along with platoon information. This information includes speed, acceleration, position, yaw rate, brakes and time. The remote vehicle can be a car, truck, motorbike or even a speciality vehicle [18].

3.1.7 Data Bus

The vehicle's data bus such as CAN, LIN, Ethernet/IP, FelxRay and MOST are the communication channels present on-board, comprising the ITS architecture, to help transmit data to and from the ECU governing the physical assets of a vehicle. This can be observed further in Figure 9.

3.3 Overall On-board Data Flow Diagram for CCC

The overall on-board data flow diagram of CCC has been illustrated in Figure 9. This illustration is important in order to perform a threat analysis upon CCC application.

The main components of the CCC are the Radar and Sensor systems. These are comprised of Radar based systems (long range radar and short/mid-range radar), Ultrasound sensors, Camera systems, Lidar systems and GPS systems. The workings of these sensors are beyond the scope of this study. However, the sensed data from these sensors are pre-processed and fused to form a multi-object detection from different sensors. Fusion of data is mandatory for overcoming the errors from different sensors [18]. These sensors also include the wheel sensors, yaw rate sensors and other motion sensors that are vital for a vehicle's movement [19].

Furthermore, other modules such as the brake control module, which depends on the brake actuator and speed sensors for it's source of information, cruise switches, and accelerometer are the main inputs to the system which would influence the operation of CCC. In addition to this the model has been designed to adapt to the collaborative nature of the ITS infrastructures by incorporating the modified ITS architecture and its external network. The external network, as seen in

Figure 9, comprises of V2V and V2I communication. The vehicle also communicates with the data centre which provides cloud services. Moreover, the vehicle is in contact with the edge cloud, which keeps its source of immediate information available. With the help of Figure 9 a threat model can be constructed and visualised.

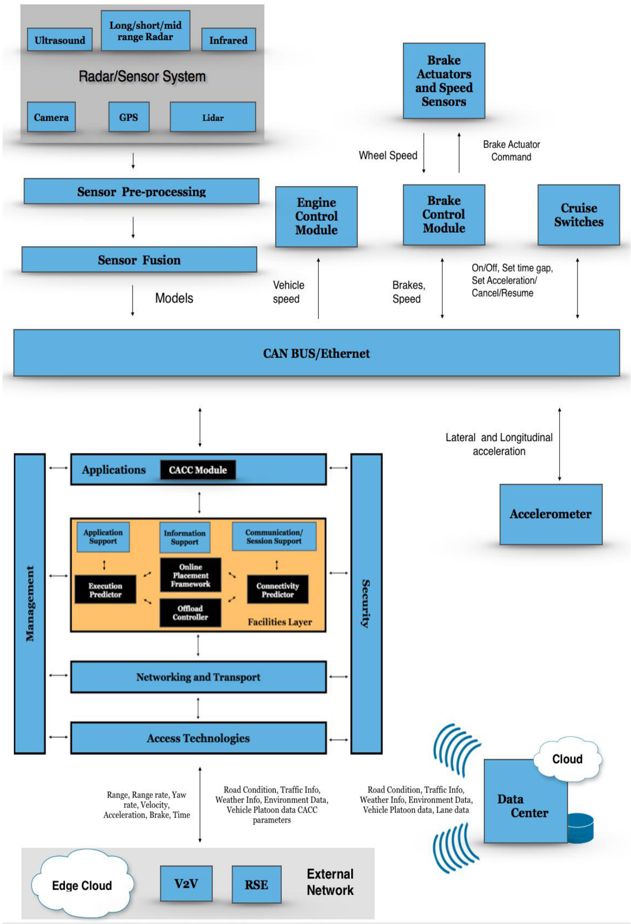


Figure 9: Overall on-board data flow diagram for CCC

3.4 Threat Modelling of CCC

Based on Phase 2 from Figure 6, a threat analysis shown in Figure 10 and 11 is performed considering the assets belonging to CCC as shown in Figure 9. A description of the assets is beyond the scope of this paper. The threat analysis considers the asset's respective inputs, processes and outputs [20]. Using this, the threats are modelled to prevent a collision.

One of the ways to achieve this is by maliciously gaining access to the Electronic Control Unit (ECU) of a vehicle which can enable an adversary to eventually gain complete control of a vehicle [3]. Through external communication and in-direct access, a vehicle is vulnerable to numerous attacks, as illustrated in Figure 11. This could harm the critical operations such as acceleration and is therefore riskier to be offloaded. Most of the vulnerabilities are present at the software level, as stated by the authors in [21]. The critical data for the vehicle include it's velocity, acceleration, GPS coordinates, and the vehicle's sensor data, along with Personally Identifiable Information (PII), Vehicle ID, Engine performance and diagnostic information.

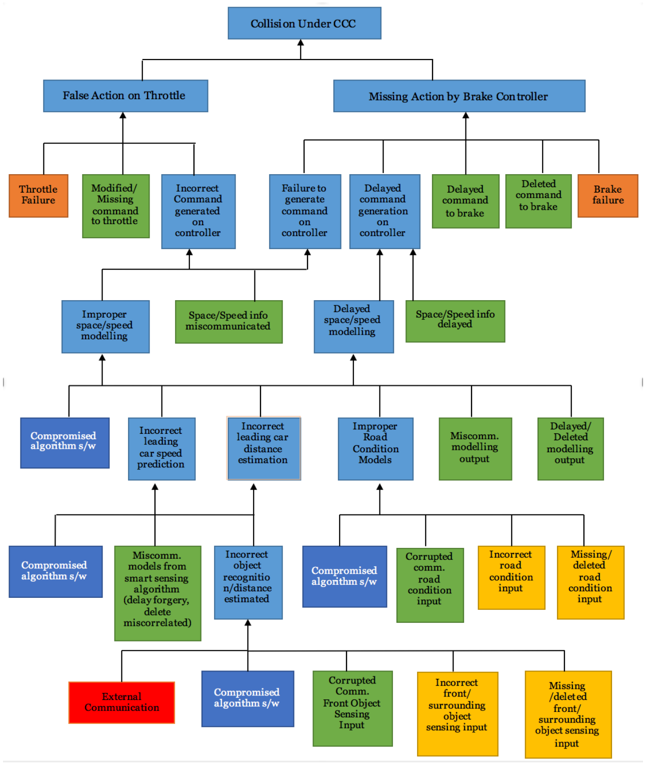

Collision Under CCC
False Action on Throttle
Missing Action by Brake Controller
Throttle Failure
Modified/ Missing command to throttle
Incorrect Command generated on controller
Failure to generate command on controller
Delayed command generation on controller
Delayed command to brake
Deleted command to brake
Brake failure
Improper space/speed modelling
Space/Speed info miscommunicated
Delayed space/speed modelling
Space/Speed info delayed
Compromised algorithm s/w
Incorrect leading car speed prediction
Incorrect leading car distance estimation
Improper Road Condition Models
Miscomm. modelling output
Delayed/ Deleted modelling output
Compromised algorithm s/w
Miscomm. models from smart sensing algorithm (delay forgery, delete miscorrelated)
Incorrect object recognitio n/distance estimated
Compromised algorithm s/w
Corrupted comm. road condition input
Incorrect road condition input
Missing/ deleted road condition input
External Communication
Compromised algorithm s/w
Corrupted Comm. Front Object Sensing Input
Incorrect front/ surrounding object sensing input
Missing /deleted front/ surrounding object sensing input

Figure 10: On-board Threat analysis of CCC

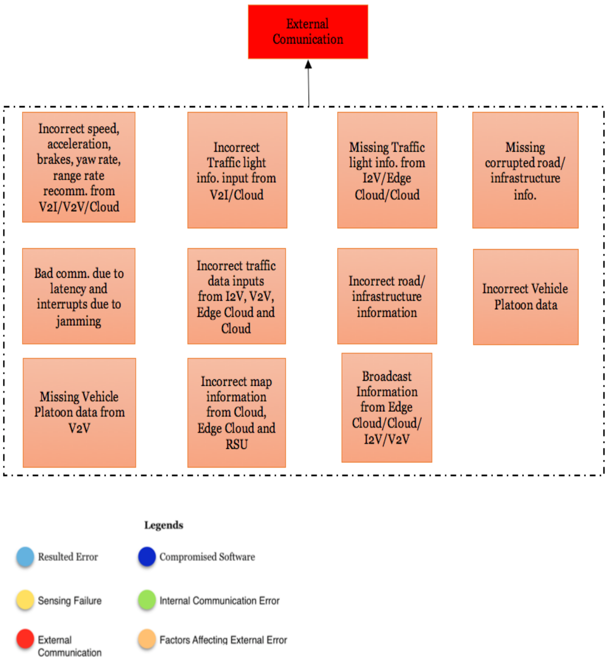

External Comunication
Incorrect speed, acceleration, brakes, yaw rate, range rate recomm. from V2I/V2V/Cloud
Incorrect Traffic light info. input from V2I/Cloud
Missing Traffic light info. from I2V/Edge Cloud/Cloud
Missing corrupted road/ infrastructure info.
Bad comm. due to latency and interrupts due to jamming
Incorrect traffic data inputs from I2V, V2V, Edge Cloud and Cloud
Incorrect road/ infrastructure information
Incorrect Vehicle Platoon data
Missing Vehicle Platoon data from V2V
Incorrect map information from Cloud, Edge Cloud and RSU
Broadcast Information from Edge Cloud/Cloud/ I2V/V2V
Legends
Resulted Error
Compromised Software
Sensing Failure
Internal Communication Error
External Communication
Factors Affecting External Error

Figure 11: Threat analysis of CCC based on external communication.

4. MODEL VALIDATION

This study has adopted the use of the semi-structured interview as a research instrument for obtaining feedback from automotive academics and engineers. It helps gain an understanding of the application model from an interviewees' perspective on the data taxonomy of CCC which, when compared to the research interpretation, will validate the proposed models and interpretations. Moreover, the validity of the proposed model is derived from the inclusion of comparative analysis and the Delphi method. In addition, the quality of the model was improved by feedback from experts in this domain in two separate rounds.

Table 1. Information of participants

Partici-pant No.	Role	Experience (yrs)	Interview Mode
P1	Lead Engineer in Automotive systems	4	In-person
P2	PhD Researcher in Human Machine Interface for Autonomous Vehicles	1	In-person
P3	PhD Researcher in Automotive Intrusion Detection System	1-2	In-person
P4	Associate Professor in Autonomous Vehicles	5	In-person
P5	Engineering Doctorate in ITS	1	In-person
P6	Principle Fellow (Cyber security in Vehicles and IoT)	20	In-person
P7	PhD researcher in Autonomous Vehicles	5	In-person
P8	Post-Doctoral Research Associate: Vehicular Cloud	10	Skype
P9	Reverse Engineer for Vehicles, CEO, Network security Engineer	5-6	Skype
P10	Assistant Professor: Experimental automotive Engineering	5	In-person

The participants were chosen based on their experience and reputation in the fields of automotive and cyber security. Ten participants were chosen for the interviews from the UK and other international countries based on their automotive experience. In order to maintain anonymity, the participants are referred to as P1, P2, P3, P4, P5, P6, P7, P8, P9 and P10.

Form Figure 12, it can be seen that the analysis was divided into 6 steps. Step 1 demonstrates that the interview was recorded. Step 2 involves the transcription process where the interview was summarized in the form of tabulation. The literature reviews in Section 2 are correlated with the summaries formed in Step 3. Next, Step 4 combines the summaries with the formulated themes.

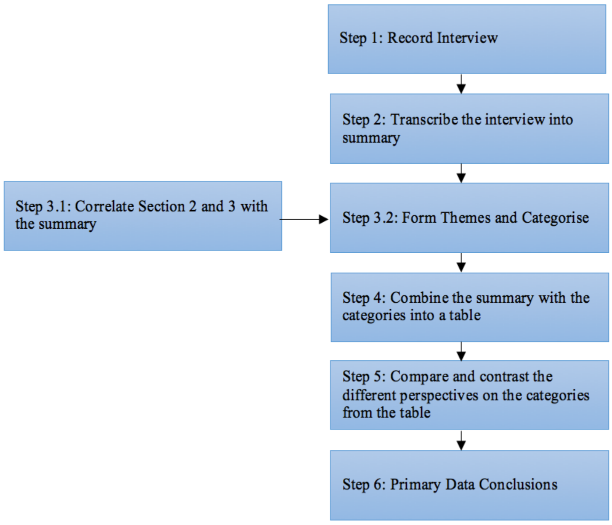

Step 1: Record Interview
Step 2: Transcribe the interview into summary
Step 3.1: Correlate Section 2 and 3 with the summary
Step 3.2: Form Themes and Categorise
Step 4: Combine the summary with the categories into a table
Step 5: Compare and contrast the different perspectives on the categories from the table
Step 6: Primary Data Conclusions

Figure 12: Flow Chart for Interview Analysis.

Step 5, as mentioned in Figure 12, is involved in the process of comparing and contrasting the different perspectives based on themes which help us form conclusions concerning the primary data collected for the purpose of validation from the participants. Figure 13 illustrates the themes that are formed for addressing the research gaps and locating the data storage and computation for CCC. The themes are framed in a broader perspective from Step 1, in order to understand the opinions of Collaborative Vehicles, ITS and Vehicular Cloud, and narrows down to Step 10 for data taxonomy. Finally, Step 11 validates the model and addresses the issues.

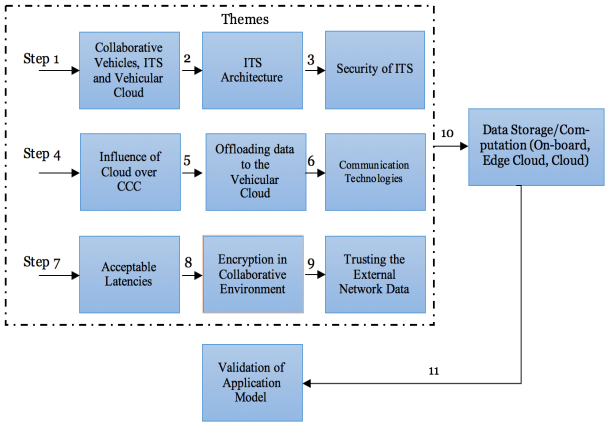

Themes
Step 1
Collaborative Vehicles, ITS and Vehicular Cloud
2
ITS Architecture
3
Security of ITS
Step 4
Influence of Cloud over CCC
5
Offloading data to the Vehicular Cloud
6
Communication Technologies
Step 7
Acceptable Latencies
8
Encryption in Collaborative Environment
9
Trusting the External Network Data
10
Data Storage/Com-putation (On-board, Edge Cloud, Cloud)
11
Validation of Application Model

Figure 13: Classification of themes for validation of Application Model.

5. CONCLUSION AND FUTURE WORK

Different Vehicular Cloud and Edge Cloud implementations are identified for the collaborative framework of ITS. Thus the ITS architecture is identified but does not consider a secure data taxonomy. Next, a critical analysis of threat modelling approaches is conducted for vehicles to identify the impact caused by harmful data. Overall dataflow of CCC and an overall OBU diagram for CCC are created and a threat analysis is performed. Based on the results, a discussion is formulated for the purpose of creating a data taxonomy for CCC.

According to the research gaps, interviews are conducted to gain feedbacks from the experts. With the help of the primary data collected, a preliminary analysis is performed to identify the critical operations and data for CCC while correlating CCC's overall models. This helped form primary data conclusions. Later, an analysis was performed on the literature in order to gain an insight into creating a data taxonomy. This brought to attention the critical question of who would be responsible for the data being computed, if offloaded. However, considering the safety-criticality of the function, the objective has successfully classified critical data and operations such as image and sensor recognition to be computed on-board, fundamental value added services such as location oriented events to the edge cloud and strategic decisions such as map data to the vehicular cloud.

To achieve this taxonomy, an analysis of the overview models was performed and validated with interviews, resulting in the proposal of the refined models (Section 3). Therefore, the four research objectives are answered by reviewing and gaining support from the past literature for creating a model to perform a threat analysis and to obtain feedback for the qualitative research on the models, thus creating the data taxonomy while developing coherent CCC models. Furthermore, this research has contributed significantly to CCC in the field of ITS and has raised a major concern for the standardisation of ITS architecture for a further reliable development in the domain, in order to integrate automotive manufacturers and governments in the development of ITS.

However, trust being a major factor for vehicles to make decisions, further research is required to determine the level of trust needed for data being transmitted between different collaborative entities. This is because an adversary can alter any critical data and encrypt it in an authentic manner, before transmitting it to the neighbouring vehicles. This has brought innovative answers from the participants, some of which contribute towards the development of a concept of web-of-trust among vehicles, or of maintaining trust if the vehicles happen to travel in the same road segment and communicate with the RSU regularly. In addition, different levels of automation require different levels of data administration. However, autonomous vehicles require stable communication and robust security to monitor and maintain the vehicle as it is exposed to numerous acts of human interference. Due to these issues, further research is necessary to determine the level of security corresponding to different levels of automation.

Finally, ITS is exposed to different types of vehicles, each-with different communication capabilities. Because of these issues, extensive research is needed in order to determine which standards are required to support secure interoperability between the ITS technologies among the heterogeneous vehicles. Looking at collaborative vehicles from a broader perspective, this research has determined the computation of CCC's data. However, further study of how this data can be used for different applications and who will hold responsibility for the data also needs to be addressed.

6. ACKNOWLEDGEMENT

This work is partially conducted under international technology R&D collaboration program which is supported by the Ministry of Trade, Industry & Energy (MOTIE) and Korea Institute for Advancement of Technology (KIAT) (N0001710).

7. REFERENCES

[1] V. A. F. Almeida, D. Doneda, and M. Monteiro, 'Governance Challenges for the Internet of Things', *IEEE Internet Comput.*, vol. 19, no. 4, pp. 56–59, 2015.

[2] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, 'Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation', *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 84–95, 2009.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, 'Experimental security analysis of a modern automobile', *Proc. - IEEE Symp. Secur. Priv.*, pp. 447–462, 2010.

[4] M. Gerla, 'Vehicular cloud computing', *Ad Hoc Netw. Work. 2012 11th Annu. Mediterr. Ad Hoc Netw. Work.*, pp. 152–155, 2012.

[5] A. Ashok, P. Steenkiste, and F. Bai, 'Enabling Vehicular Applications using Cloud Services through Adaptive Computation Offloading', *Proc. 6th Int. Work. Mob. Cloud Comput. Serv. ACM*, pp. 1–7, 2015.

[6] W. He, G. Yan, and L. Da Xu, 'Developing vehicular data cloud services in the IoT environment', *IEEE Trans. Ind. Informatics*, vol. 10, no. 2, pp. 1587–1595, 2014.

[7] H. Abid, L. T. T. Phuong, J. Wang, S. Lee, and S. Qaisar, 'V-Cloud: vehicular cyber-physical systems and cloud computing', *Proc. 4th Int. Symp. Appl. Sci. Biomed. Commun. Technol.*, p. 165, 2011.

[8] E. Qin, Y. Long, C. Zhang, and L. Huang, 'Cloud computing and the internet of things: Technology innovation in automobile service', *Int. Conf. Hum. Interface Manag. Inf.*, vol. 8017 LNCS, no. PART 2, pp. 173–180, 2013.

[9] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, 'Fog Computing and Its Role in the Internet of Things', *Proc. first Ed. MCC Work. Mob. cloud Comput.*, pp. 13–16, 2012.

[10] S. Bitam and A. Mellouk, 'ITS-Cloud: Cloud Computing for Intelligent Transportation System', *Int. J. Soft Comput. Eng.*, vol. 2, no. 3, pp. 568–572, 2012.

[11] C. Shi, P. Pandurangan, K. Ni, J. Yang, M. Ammar, M. Naik, and E. Zegura, 'IC-Cloud: Computation Offloading to an Intermittently-Connected Cloud Cong', 2013.

[12] R. Bossom, R. Bringolo, T. Ernst, K. Evensen, A. Frotcher, E. Hofs, J. Jaaskelainen, Z. Jeftic, P. Kompfner, T. Kosch, I. Kulp, A. Kung, A.-K. Mokaddem, A. Schalk, E. Uhlemann, and C. Wewetzer, 'D31 European ITS Communication Architecture: Overall Framework Proof of Concept Implementation', Information Society Technologies, 2009.

[13] A. Shostack, *Threat Modelling: Designing for security*. 2014.

[14] P. Saitta, B. Larcom, and M. Eddington, 'Trike v. 1 Methodology Document', 2005.

[15] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, *Introduction to the OCTAVE Approach*, no. August. Pittsburgh, 2003.

[16] C. McCarthy, K. Harnett, and A. Carter, 'Characterization of Potential Security Threats in Modern Automobiles A Composite Modeling Approach', Washington DC, 2014.

[17] CVRIA, 'Connected Vehicle', Aug-2016. [Online]. Available: http://www.iteris.com/cvria/html/about/connectedvehicle.html. [Accessed: 02-Aug-2016].

[18] Texas Instruments Inc., 'Paving the way to self-driving cars with advanced driver assistance systems', 2015.

[19] C. Nowakowski, S. E. Shladover, and D. Cody, 'Cooperative Adaptive Cruise Control : Testing Drivers ' Choices of Following Distances', California PATH, 2011.

[20] M. Zhao, *Advanced Driver Assistant System: Threats, Requirements, Security Solutions (White Paper)*. Intel Labs, 2015.

[21] S. Checkoway, D. Mccoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces', *USENIX Secur. Symp.*, 2011.