V2C: A secure vehicle to cloud framework for virtualized and on-demand service provisioning

Article · August 2012

DOI: 10.1145/2345396.2345422

5 authors, including:

Anand Kannan

KTH Royal Institute of Technology

14 PUBLICATIONS **75** CITATIONS

SEE PROFILE

Ayush Sharma

Lasell College

7 PUBLICATIONS **74** CITATIONS

SEE PROFILE

V2C: A secure vehicle to cloud framework for virtualized and on-demand service provisioning

Sathyanarayanan Rangarajan
Fraunhofer AISEC
Parkring 4, 85748 Garching, Germany
sathya.rangarajan@aisec.fraunhofer.de

Monica Verma
Siemens CERT
Otto-Hahn-Ring 6, 81739 Munich, Germany
monica.verma@siemens.com

Anand Kannan
School of Information and Communication Technology
KTH, Royal Institute of Technology, Stockholm, Sweden
anandk@kth.se

Ayush Sharma
Fraunhofer AISEC
Parkring 4, 85748 Garching, Germany
ayush.sharma@aisec.fraunhofer.de

Ingmar Schön
Fraunhofer AISEC
Parkring 4, 85748 Garching, Germany
ingmar.schoen@aisec.fraunhofer.de

ABSTRACT

Cloud computing has revolutionized the IT industry by enabling a virtualized resource provisioning model for organizations. The Network-as-a-Service (NaaS) provisioning model enables new ways of providing virtually isolated and on-demand networking capabilities in existing cloud provisioning models, resulting in best-effort performance, scalable data throughput, reduced latency, and reduced configuration complexity. In this paper we propose V2C, an elastic Vehicle-to-Cloud infrastructure that integrates NaaS into the automotive ecosystem and enables provisioning of vehicle-based services for automobile users. However, V2C introduces various security challenges and the main objective of this paper is to propose a secure provisioning model to address them.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Network communications; C.2.4 [**Distributed Systems**]: Client/server; D.4.6 [**Security and Protection**]: Information flow controls; D.4.8 [**Performance**]: Measurements

General Terms

Design, Management, Performance, and Security

Keywords

Vehicular networks, Security architecture, Cloud networking, Next-Generation networks

ICACCI '12, Aug 3-5, 2012, Chennai, T.Nadu, India
Copyright 2012 ACM 978-1-4503-1196-0/12/0010 ...$10.00.

1. INTRODUCTION

Cloud computing is arguably one of the major game changers experienced by the IT industry during the past decade. Defined by the National Institute of Standards and Technology(NIST) in [1] and [2], cloud computing has gradually enabled a transition of the enterprise infrastructure into the cloud, the driving force for this transition being a reduced capital expenditure (CAPEX) coupled with a reduced operational expenditure (OPEX).

Cloud computing so far, has been targeted solely towards large and medium-scale enterprises. However, with the advent of widespread cloud service penetration into mobile phones and other devices, clouds have moved beyond simply infrastructure and into our daily lives. Apart from the amount of time spent at home and work, one spends a great deal of time commuting by cars. The performance and quality of current features offered in a car such as navigation services, infotainment services etc., rely heavily on the hardware and software available in the car. These features can be improved further by the integration of cloud services into automobiles. This not only offers bigger and better processing power and storage capabilities, but also facilitates in reducing the amount of existing in-car hardware and software, and paves way for a whole new range of services.

However, cloud computing, similar to other growing technologies, has its own set of problems. Qualitative provisioning of navigation and infotainment services for automobiles not only requires on-demand compute and storage resources, but also heavily depends on the available network bandwidth. The existing service provisioning models viz. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), exhibit unreliable performance, low dependability, and throughput due to the lack of concrete and mature network resources [3].

The European project SAIL [3] introduced Network-as-a-Service (NaaS), which tightly integrates the provisioning of virtualized network resources along with the existing service provisioning models, viz. SaaS, Paas, and IaaS. Further, SAIL introduces the CloNe architecture [4], which defines a generic Cloud Network (CloNe) architecture, and allows service users to request network parameters, along with their desired service constraints. Therefore, NaaS aims to negate the unreliability in existing cloud service provisioning models, and promote dependability and guaranteed QoS [3]. Thus, it is safe to state that the varied requirements of the cloud service provisioning model for cars will be satisfied by a service provisioning model similar to the one proposed by the CloNe architecture.

This paper further extends the existing CloNe architecture and CloNe security architecture, and modifies them for the automobile ecosystem. The main contribution of the paper is the definition of a cloud service provisioning model, namely V2C infrastructure, customized for the automobile ecosystem, and a security architecture which integrates with the V2C provisioning model and secures the complete provisioning infrastructure. Moreover, use cases and example scenarios are described for cloud service provisioning in automobiles.

The paper is organized as follows. Section 2 provides the related work with respect to cloud security architectures, cloud service provisioning in cars, and other related research areas. Section 3 describes the customized CloNe architecture, namely V2C infrastructure, to be used in the automobile ecosystem. Section 4 elaborates on the security architecture, which secures the service provisioning architecture described in Section 3. Section 5 explains sample use cases for the service provisioning model for cars namely *cloud-based navigation* and *cloud-based infotainment*. Section 6 summarizes the results of the paper, and compares it with the state of the art. Section 7 concludes the work and shows future working directions.

2. RELATED WORK

Vehicular communication has experienced a rapid momentum shift from a research-oriented topic to being integrated in production ready cars of leading industry manufacturers, namely Intel's WiMax-connected car [5] and Toyota's LTE-connected car [6]. Since the spectrum allocation for Inter-Vehicle Communications (IVC) by the Federal Communications Commission and the amendment of IEEE 802.11p standard for Wireless Access in Vehicular Environments (WAVE)[7], several research works have been carried out on vehicle-to-vehicle and vehicle-to-infrastructure communication[8, 9]. Daiheng Ni [10] proposed an architecture which allows vehicles to communicate with any available roadway infrastructure, in order to transmit the speed and location of the vehicle to a centrally located server. Jegor Mosyagin [6] proposed the usage of 4G technology for vehicular communication and the experiments covered in the paper exhibited maximum data transfer rates of 10 Mbps for a vehicle travelling at a maximum speed of 140 km/hr. However, newer technologies such as LTE and 4G introduce new security challenges.

Seddigh et al. [11] presents a study of security advances and challenges associated with emergent 4G wireless technologies. The paper describes potential areas for future vulnerabilities and evaluates areas in 4G security which warrant immediate attention. Moreover, the paper proposes potential future work to mitigate these challenges. Yu-Hunag Chu [12] proposed and implemented a new network architecture design suitable for cloud models. This model is experimentally proven to be cost effective from a networking perspective, especially for a scenario where the networking resources are provisioned on-demand. On-demand, secure provisioning of networking resources utilizing the newer networking technologies such as LTE is the basis for our study. This paper presents our vision on the evolution of smarter automobiles which are connected to the cloud using enhanced (network) technologies in a secure manner.

3. THE V2C MODEL

The original CloNe architecture [4] defines a virtualized network resource provisioning model, which allows a tight integration between the existing virtualized service provisioning models, viz. SaaS, Paas, and IaaS and the proposed NaaS provisioning model. Moreover, the provisioning model in CloNe has been defined over multiple service hierarchy levels, and transcends multiple administrative boundaries. The V2C model proposed in this paper shares the same basic properties as the CloNe ecosystem, namely multiple levels in the service hierarchy, multiple administrative boundaries, and on-demand network resource provisioning. This section describes how the CloNe architecture is used as a reference model and further customized according to the specifications of the automobile ecosystem. Sections **??** and 3.3 describe the automobile ecosystem and the V2C provisioning infrastructure in detail.

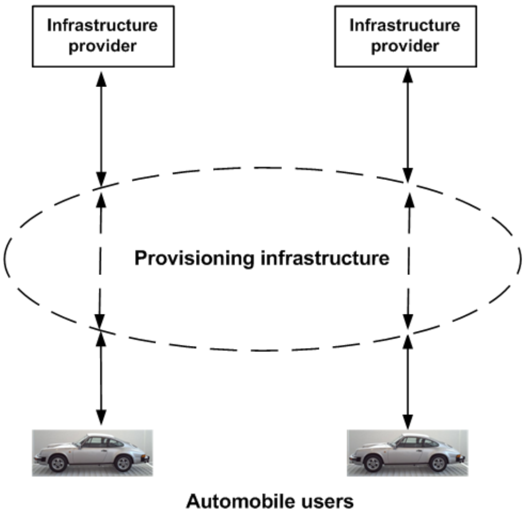

Figure 1: Abstract architecture of cloud service provisioning model

3.1 Abstract architecture

Figure 1 shows an abstract architecture of the proposed V2C model for automobiles. The two central roles in the abstract architecture are the *automobile user* and the *infrastructure provider*. The *automobile user* initiates a service request to the *infrastructure provider* by utilizing the provisioning infrastructure, which takes care of the propagation of the abstract service request to the *infrastructure provider*, and might translate the request further into more concrete expression(s). The request is received by the *infrastructure provider*, who is then responsible for the delegation of the service request within different (internal or external) administrative units, and manages the collaboration between those

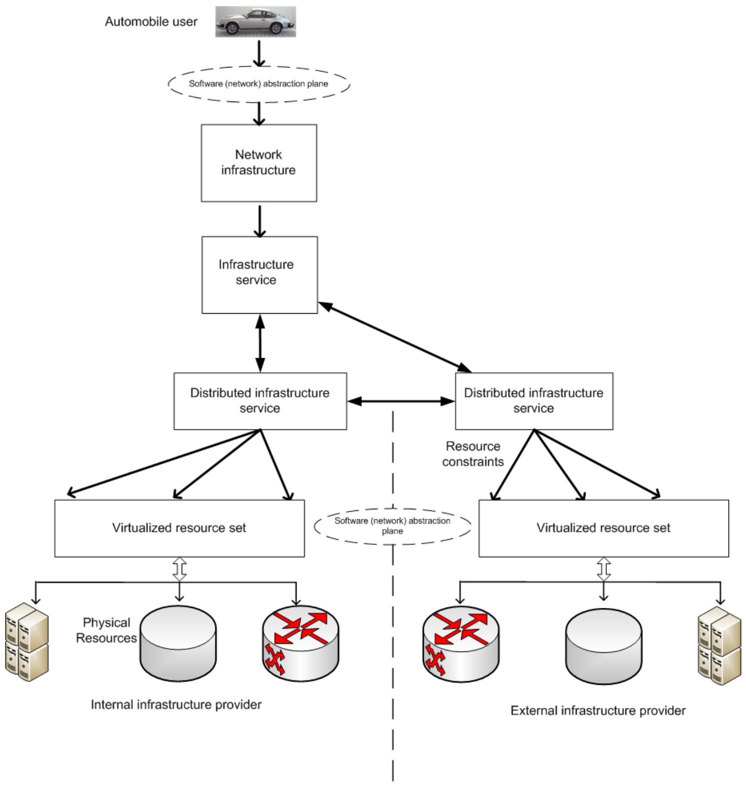
Automobile user
Software (network) abstraction plane
Network infrastructure
Infrastructure service
Distributed infrastructure service
Distributed infrastructure service
Resource constraints
Virtualized resource set
Software (network) abstraction plane
Virtualized resource set
Physical Resources
Internal infrastructure provider
External infrastructure provider

Figure 2: Distributed architecture of cloud service provisioning model

units through internal and external SLAs. The *infrastructure provider* is responsible to ensure that the overall QoS constraints of the *automobile user* are met. Therefore, it needs to have a tightly-knit control over the entire propagation path, including the provisioning infrastructure.

The provisioning infrastructure is only visible to the *automobile user* in the form of an interface (possibly integrated into the automobile's dashboard) and thus the entire backbone infrastructure will be opaque to the user. This is extremely important in order to ensure sufficient service penetration across a diverse end user base. The *automobile user* should be agnostic to the exact hardware and software details of the backbone infrastructure, and should be allowed to provide their desired service request using abstract terms and expressions. The *automobile user's* request will be encapsulated inside VXDL [13] packets, which is the same format as that used by CloNe.

3.2 Detailed architecture

Figure 2 describes a more detailed version of Figure 1 and includes the entire component-wise distribution of the V2C provisioning model. The original role *infrastructure provider* is divided into further sub-roles, namely, *internal infrastructure provider* and *external infrastructure provider*. Each *infrastructure provider* virtualizes and provisions its own set of resources to the end-user or tenant. An *internal infrastructure provider* is defined as the entity which manages the set of resources housed inside the administrative domain of the original *infrastructure provider*. The second sub-role is the *external infrastructure provider*, which controls its own set of resources and is housed outside the administrative boundaries of the *internal infrastructure provider*. The *external infrastructure provider* might collaborate with the *internal infrastructure provider* if the latter is unable to provision the requested resources on its own.

Each *infrastructure provider* provides a resource administration interface. The resource administration interface offers a set of APIs and management functions to the higher entity in the service level hierarchy. The set of management functions includes a goal translation function, a resource management function, and a fault management function deployed by the *infrastructure provider*. The goal translation function accepts abstract service requests from the *automobile user* and translates them to concrete resource specifications using a multi-level translation process. The concrete resource specifications are further provided to the resource management function. Before deploying the concrete specifications on the underlying physical resource set, the resource management function collaborates with the fault management function and generates fault reports. The generated fault reports contain information regarding resources which are partially or completely compromised, or are experiencing performance fluctuations. The information provided by fault reports help the resource management function in avoiding faulty resource allocation to fulfill the requests of the *automobile user*.

3.3 Service provisioning

The *automobile user* sends a service request to the *infrastructure service*, which is a role played by the automobile manufacturer, or any other service provider chosen by the *automobile user* to provision the requested service. The

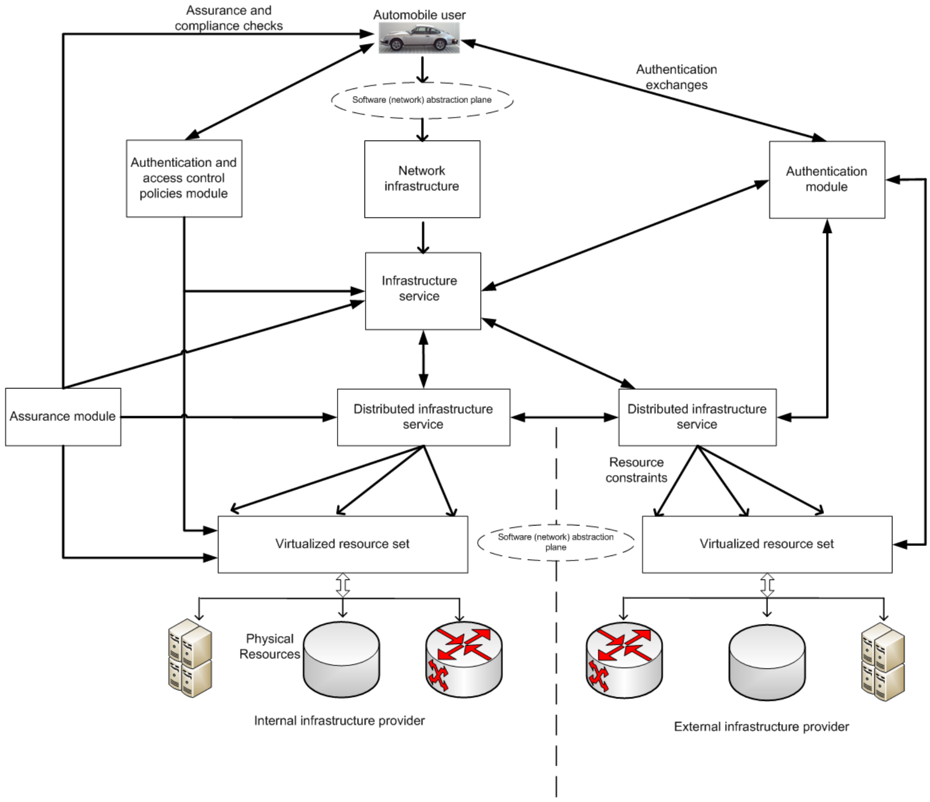
Assurance and compliance checks
Automobile user
Authentication exchanges
Software (network) abstraction plane
Authentication and access control policies module
Network infrastructure
Authentication module
Infrastructure service
Assurance module
Distributed infrastructure service
Distributed infrastructure service
Resource constraints
Virtualized resource set
Software (network) abstraction plane
Virtualized resource set
Physical Resources
Internal infrastructure provider
External infrastructure provider

Figure 3: Security architecture of cloud provisioning model for automobiles

infrastructure service employs a control unit at its center, which is responsible for carrying out the initial goal translation of the user request. The initial abstract request depicts the SLO and QoS constraints expected by the *automobile user*. The *infrastructure service* is also responsible for storing a registry of *distributed infrastructure service* components, which are defined as subsets of the *infrastructure service* component. Each administrative domain houses a *distributed infrastructure service* component that is responsible for accepting the service request from the *infrastructure service* component. The *distributed infrastructure service* further translates the request into concrete resource configurations and provides them to the *infrastructure provider* by utilizing the resource administration interface.

The *infrastructure service* component aims to provision the service request by utilizing only the resources present in its respective administrative domain. However, in some exceptional cases, either the resources in its domain are overbooked, are experiencing technical faults, are compromised, or the resources aren't acceptable by the user in the price point at which they are provisioned. In such a scenario, the *infrastructure service* provisions the available/acceptable resources from its respective administrative domain, and advertises the remaining resource requirements (including the security, non-functional, and economic requirements) among the different competing *distributed infrastructure service* components. The *distributed infrastructure service* components that can successfully provision the resources respond with their respective remote references. The *infrastructure service* component then selects the desired *distributed infrastructure service* component(s) that would provision the remaining resources. The *infrastructure service* component conveys the address information of the selected *distributed infrastructure service* components to the primary *distributed infrastructure service* component, and the latter carries out remote reference resolution to communicate and collaborate with each other to provision the service request.

Schoo et al. [14] describes multiple security challenges which plague the NaaS provisioning model. Some of the security challenges covered include information security issues, threats in virtualization environments, and communication security for cloud networks. Subsequently, Fusenig et al. [13] proposed an abstract security architecture to negate the security challenges covered in [14]. They defined a security goal translation function, which builds on the goal translation function proposed by Bjurling et al. [15] and enhances it by adding security-specific translation functionalities. The purpose of the security goal translation function is to accept security requirements from multiple entities, and produce pareto-optimal solutions to address them. This paper uses the security goal translation function suggested by Fusenig et al. [13], maps it to the V2C architecture described in Section 3, and extends it further by integrating three additional security modules. These modules include an authentication module, an authorization and access control policies modules, and an assurance module. The placements of these modules, and their interaction with the security architecture is depicted in Figure 3.

4. SECURITY ARCHITECTURE

The authentication module plays an important role in the security goal translation process, as the security goals provided by entities in the V2C infrastructure require accurate identification of the involved entities. Authentication is carried out not only on the entities, but on the physical/virtual resources as well. Vijaykumar et al. [16] proposed a lightweight and extensible key management algorithm, which can be customized for the V2C model. A second alternative is using an industry standard like OAuth 2.0 [17, 18] for implementing authentication.

The authorization and access control policies module sets access control policies for every *automobile user* and implements them during the resource allocation process. It is important to utilize access control policy models which can be reflected all the way down to the heterogeneous network resources, and thus models like OrBAC [19] are not a viable option. Suitable replacements for an access control model include an ACL model [20], or a MAC/MLS [21, 22, 23] model. Furthermore, cross-enterprise Security and Privacy Authorization (XSPA) profile of eXtensible Access Control Markup Language (XACML) [24] can be deployed in the V2C model. XACML ensures that different participating entities can exchange their privacy attributes and requirements consistently. This would prevent an occurrence whereby different entities are unable to interchange and understand privacy attributes due to the use of different languages to set and describe their privacy policies.

An often overlooked security module is the assurance module, which is responsible for ensuring that the different infrastructure entities in the V2C model are compliant with the overall legal requirements of the operational area(s), industry-specific requirements and service-specific requirements, and requirements provided by the different entities. The assurance module is deployed throughout the entire architecture, and correlates the management actions with the desired requirements.

5. USE CASES

Two use cases can be provisioned by the V2C model for the automobile ecosystem, namely *cloud-based navigation* and *infotainment*.

5.1 Cloud-based navigation

Cloud-based navigation allows navigation requests to be processed and transmitted to an *automobile user* from the *infrastructure provider*. The *automobile user* has access to an interface provided by the *infrastructure provider*, which can be used to input navigational requests with specific constraints. For example, a request to avoid routes with high traffic congestion. Each *infrastructure provider* (or a conglomerate of *infrastructure providers*) can manage large data centers to simultaneously compute multiple routes, each specifying a subset of the service request inputted by the user. The goal translation function discussed in Section 3.2 is employed to select the best possible route. This process requires simultaneous usage of multiple processing units. However, the overall provisioning cost for the *infrastructure provider* is vastly reduced due to economies of scale, and the service being subscribed by a large number of *automobile users*. Moreover, the *infrastructure provider* is able to reliably transmit high quality navigational data by utilizing the network resources provisioned to the *automobile user*. A prominent advantage of the enhanced networking capabilities is the ability to send high-definition “street views”, in addition to the basic navigational information available on state-of-the-art navigational devices fitted into automobiles. Google street view [25] offers similar street views through its Google maps [26], but the application has not experienced widespread market penetration into automobile-navigation devices. However, the reasons for its low penetration, range from low network bandwidth to operational and organizational factors.

With the V2C model proposed in this paper, a cloud-based navigation service can be easily deployed by the automobile manufacturer in collaboration with external service/resource providers. The resource providers will benefit from economies of scale [27] and have a low OPEX while provisioning the services. On the other hand, the automobile manufacturers can benefit by deploying the entire backbone resource provisioning infrastructure, and obtain two successive revenue channels, namely via the *automobile user* and the *external infrastructure provider*.

5.2 Cloud-based infotainment

Cloud-based infotainment allows the *automobile user* to request a multimedia streaming service through the interface provided by the *infrastructure provider*. The *infrastructure provider(s)* manage a backbone infrastructure and collaborate with the external content providers to seamlessly provision a multimedia streaming service. A range of multimedia services, their provisioning requirements, actors involved, and business analysis are discussed in [28]. Of these, two use cases important for the automobile ecosystem are video conferencing and elastic video distribution.

Video conferencing is extremely beneficial if the *automobile user* experiences network latency and QoE, with acceptable jitter [29]. Chen et al. [30] proposed the deployment of ad-hoc wireless relay networks over moving vehicles, but the model fails to provide reliable, secure, elastic, and on-demand network provisioning to handle traffic bursts and fluctuations. Our V2C model ensures better QoE to the *automobile user* as it integrates NaaS along with the existing service provisioning models. The key requirements for video distribution are covered in [31], and the model described in this paper also ensures security and reliable delivery for mobile units.

6. RESULTS AND COMPARISON

There are three major security architectures and toolkits which secure the backbone cloud service provisioning model(s), namely IBM cloud computing architecture [32], Google cloud computing architecture [33], and Eucalyptus cloud computing architecture [34]. Table 1 compares these different (security) architectures proposed for cloud computing with our V2C model. The parameters for the comparison are measured based on their relevance to the performance, dependability and security of our model. These include access control, packet and circuit switched network convergence, on-demand network provisioning, packet-based access policy, auditing and assurance function, stateful VM migration, software network abstraction plane, and multi-level security.

In terms of security parameters, our model fares reasonably well. All the four models have an access control module, and auditing and assurance mechanism in place. However, as our model is in the early stages, multi-level security has not been incorporated in the service provisioning architec-

Table 1: Comparison between different architectures

	V2C Model	Google	IBM	Eucalyptus
Access Control	Yes	Yes	Yes	Yes
Packet and circuit switched network convergence	Yes	-	-	-
On-demand network provisioning	Yes	-	-	-
Packet-based access policy	Yes	-	-	-
Auditing and assurance function	Yes	Yes	Yes	Yes
Stateful VM migration	Yes	-	-	-
Software network abstraction place	Yes	-	-	-
Multi-level security	-	Yes	Yes	Yes

ture. On the other hand, our model fares better in terms of its networking capabilities. It is the only model which supports on-demand network provisioning, which improves the network latency and throughput. Moreover, packet and circuit switched network convergence [31] integrates both circuit and packet switching and offers both stability and flexibility. Our model also includes a software network abstraction plane (depicted in Figure 2) and stateful VM migration which improves flexibility and prevents vendor lock-ins. Finally, our model supports packet-based access policy [4] which allows the *automobile user* to set different access control policies for different services.

7. CONCLUSION AND FUTURE WORK

In this paper a secure cloud service provisioning architecture customized for the automotive ecosystem, namely V2C has been proposed. The V2C model with its tightly integrated security architecture ensures that the requested resources can be provisioned in an elastic, on-demand, reliable, and secure manner. Furthermore, the paper describes example use case scenarios for cloud service provisioning in automobiles.

Future work includes introduction of a key management algorithm to support the authentication module and a (network and/or host-based) intrusion detection system to support the assurance module.

8. ACKNOWLEDGMENTS

We would like to thank Peter Schoo, Volker Fusenig, and Rajya Deep Dhungana from Fraunhofer AISEC, Munich, Germany for their valuable comments and suggestions regarding the core networking architecture and the automotive ecosystem.

9. REFERENCES

[1] Lee Badger, Robert Patt-corner, and Jeff Voas. DRAFT Cloud Computing Synopsis and Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, 117:84, 2011.

[2] Peter Mell and Timothy Grance. The NIST Definition of Cloud Computing (Draft) Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, 145(6):7, 2011.

[3] Thomas Edwall. Scalable & Adaptive Internet Solutions (SAIL). Technical report, European Commission's 7^{th} Framework Program, 2011.

[4] Paul Murray. D-5.2 (D-D.1) Cloud Network Architecture Description. Technical report, European Commission's 7^{th} Framework Program, 2011.

[5] K Kaplan. Intel's Smart WiMAX Car - Mobility "Innovision" for Centrino 2, July 2008.

[6] J. Mosyagin. Using 4G wireless technology in the car. In *Transparent Optical Networks (ICTON), 2010 12^{th} International Conference on*, pages 1–4, July 2010.

[7] Weidong Xiang, Yue Huang, and S Majhi. The Design of a Wireless Access for Vehicular Environment (WAVE) prototype for Intelligent Transportation System (ITS) and Vehicular Infrastructure Integration (VII). In *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, pages 1–2, Sept. 2008.

[8] J. Miller. Fastest path analysis in a Vehicle-to-Infrastructure intelligent transportation system architecture. In *Intelligent Vehicles Symposium, 2009 IEEE*, pages 1125 –1130, June 2009.

[9] M. Torrent-Moreno, J. Mittag, P. Santi, and H Hartenstein. Vehicle-to-Vehicle Communication: Fair Transmit Power Control for Safety-Critical Information. *Vehicular Technology, IEEE Transactions on*, 58(7):3684–3703, Sept. 2009.

[10] Daiheng Ni. Determining traffic-flow characteristics by definition for application in ITS. *Intelligent Transportation Systems, IEEE Transactions on*, 8(2):181–187, June 2007.

[11] N. Seddigh, B. Nandy, R. Makkar, and J.F. Beaumont. Security advances and challenges in 4G wireless networks. In *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, pages 62–71, Aug. 2010.

[12] Yu-Hunag Chu, Yao-Ting Chen, Yu-Chieh Chou, and Min-Chi Tseng. A simplified cloud computing network architecture using future internet technologies. In *Network Operations and Management Symposium (APNOMS), 2011 13^{th} Asia-Pacific*, pages 1–4, Sept. 2011.

[13] Volker Fusenig and Ayush Sharma. Security Architecture for Cloud Networking. In *International Conference on Computing, Networking and Communication (ICNC), Maui, Hawaii, USA*, 30^{th}Jan. - 2^{nd} Feb. 2012.

[14] Peter Schoo, Volker Fusenig, Victor Souza, Marcio Melo, Paul Murray, Herve Debar, Houssem Medhioub, and Djamal Zeghlache. Challenges for Cloud Networking Security. In *MONAMI*, pages 298–313, 2010.

[15] Björn Bjurling, Rebecca Steinert, and Daniel Gillblad. Translation of probabilistic QoS in hierarchical and decentralized settings. In *APNOMS*, pages 1–8, 2011.

[16] P. Vijayakumar, S. Bose, A. Kannan, and S Siva Subramanian. A Secure Key Distribution Protocol for Multicast Communication. In *Communications in Computer and Information Science*, volume 140, page 249Ŭ257. Springer, 2011.

[17] Yating Hsu and D. Lee. Authentication and authorization protocol security property analysis with trace inclusion transformation and online minimization. In *Network Protocols (ICNP), 2010 18th IEEE International Conference on*, pages 164 –173, oct. 2010.

[18] Wang Bin, Huang He Yuan, Liu Xiao Xi, and Xu Jing Min. Open Identity Management Framework for SaaS Ecosystem. In *e-Business Engineering, 2009. ICEBE '09. IEEE International Conference on*, pages 512–517, Oct. 2009.

[19] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, and G Trouessin. Organization Based Access Control. In *4^{th} IEEE International Workshop on Policies for Distributed Systems and Networks (Policy'03)*, June 2003.

[20] J Qian. ACLA: A framework for Access Control List (ACL) Analysis and Optimization. In *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security Issues of the New Century*, pages 4–, Deventer, The Netherlands, The Netherlands, 2001. Kluwer, B.V.

[21] D. Clark and D Wilson. A Comparison of Commercial and Military Computer Security Policies. In *IEEE symposium on security and privacy*, pages 184–194, 1987.

[22] Myong H. Kang, Judith N. Froscher, Brian J. Eppinger, and Ira S. Moskowitz. A Strategy for an MLS Workflow Management System. In *In Proceedings of the 18^{th} IFIP Working Conference on Database Security*, 1999.

[23] Konstantin Knorr. Multilevel Security and Information Flow in Petri Net Workflows. Technical report, In Proceedings of the 9^{th} International Conference on Telecommunication Systems - Modeling and Analysis, Special Session on Security Aspects of Telecommunication Systems, 2001.

[24] Bill Parducci, Hal Lockhart, and Erik Rissanen. XACML v3.0 Privacy Policy Profile Version 1.0. *Policy*, pages 1–11, August 2010.

[25] Amir Roshan Zamir and Mubarak Shah. Accurate Image Localization Based on Google Maps Street View], booktitle = Proceedings of the European Conference on Computer Vision (ECCV. 2010.

[26] Christopher C Miller. A Beast in the Field: The Google Maps Mashup as GIS/2. *Cartographica The International Journal for Geographic Information and Geovisualization*, 41(3):187–199, 2006.

[27] Joseph Berechman and Genevieve Giuliano. Economies of scale in bus transit: A review of concepts and evidence. *Transportation*, 12:313–332, 1985. 10.1007/BF00165470.

[28] T. Levä, J. Gonçalves, and R. J. Ferreira. Description of project wide scenarios and use cases. Technical Report FP7-ICT-2009-5-257448-SAIL/D2.1, European Commission's 7th Framework Program, http://www.sail-project.eu/wp-content/uploads/2011/09/SAIL_DA1_v1_2_final.pdf, 2009.

[29] IEEE Standard for Measurement of Video Jitter and Wander. *IEEE Std 1521-2003*, pages c1–14, 14 2009.

[30] Zong Da Chen, H.T. Kung, and Dario Vlah. Ad hoc relay wireless networks over moving vehicles on highways. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '01, pages 247–250, New York, NY, USA, 2001. ACM.

[31] Thomas Edwall. Description of project wide scenarios and use cases. Technical report, European Commission's 7^{th} Framework Program, 2011.

[32] B Schmidt-Wesche, Brian Snitzer, Gerd Breiter, Gerhard Widmayer, Jim Whitmore, Julissa Villareal, Michael Behrendt, R Caponigro, R Chang, S Pappe, and Et Al. IBM Cloud Computing & Common Cloud Management Platform Reference Architecture (CC & CCMP RA) 1.0, 2010.

[33] J I A Xiaojing. Google Cloud Computing Platform Technology Architecture and the Impact of Its Cost. *2010 Second World Congress on Software Engineering*, (70801067):17–20, 2010.

[34] Eucalyptus Systems. Eucalyptus Systems Eucalyptus Open-Source Cloud Computing Infrastructure - An Overview Eucalyptus Systems An Overview. *Technology*, 180:012051, August 2009.