A Reputation-Based Adaptive Trust Management System for Vehicular Clouds

Eun-Ju Lee and Ihn-Han Bae(✉)

School of IT Eng., Catholic University of Daegu, Gyeongsan, Korea
{eunjulee,ihbae}@cu.ac.kr

Abstract. Advances in vehicular networks, embedded devices and cloud computing will enable the formation of vehicular clouds of computing, communication, sensing, power and physical resources. Owing to the dynamic nature of the vehicular cloud, continuous monitoring on trust attributes in necessary to enforce service-level agreement, This paper proposes RA-VTrust, Reputation-based Adaptive Vehicular Trust model for efficiently evaluating the competence of a vehicular cloud service based on its multiple trust attributes. In RA-VTrust, an adaptive trust and a reputation managements based on variable precision rough sets are suggested to trust data mining and reputation knowledge discovery. The adaptive trust management provides cloud consumers with the most suitable trust for vehicular services because it is performed by considering vehicular service level agreement (VSLA) documents and reputation services. The performance of RA-VTrust is evaluated through a simulation.

Keywords: Cloud Computing · Reputation · Rough Sets · Service Level Agreement · Trust · Vehicular Cloud

1 Introduction

The vehicle of 2020 will be a core element of a Smarter Planet. The vehicle of the future will be a communications wonder and as yet another node on the Internet cloud, it will connect with other vehicles, the transportation infrastructure, homes, businesses and other sources. This connection will happen through a convergence of different electronic technologies and telematics that range from infotainment, speech recognition and linguistics, to thermal, power train and safety systems. Innovation will emerge mostly from software, electrical systems, sensors and driver-assistance services that will improve safety and the overall driving experience. At the same time, a new level of owner/vehicle personalization and customization will be delivered by leveraging a mobility framework over the cloud [1].

The trust mechanism provides a good way for improving the system security. It is a new and emerging security mode to provide security states, access control, reliability and polices for decision making by identifying and distributing the malicious entities based on converting and extracting the detected results from security mechanisms in different systems and collecting feedback assessments continually. Before interaction occurs between cloud providers and consumers, trust in the vehicular cloud relationship is very important to minimize the security risk and malicious attacks. Accordingly, we propose an RA-VTrust model for efficiently evaluating the competence of a vehicular cloud

V.C.M. Leung et al. (Eds.): TridentCom 2014, LNICST 137, pp. 77–86, 2014.
DOI: 10.1007/978-3-319-13326-3_8

service based on its multiple trust attributes. The RA-VTrust is designed on the VSLA model which supports the effective execution of automotive services in vehicular clouds, and evaluates the trustworthiness of the services of vehicular clouds through the collection of monitored evidence and the trust mining from the evidence using rough sets on the base of trust information system.

The rest of this paper is organized as follows. Section 2 surveys related work. Section 3 proposes VSLA model. Section 4 designs RA-VTrust system for vehicular clouds. Performance of RA-VTrust is described in Section 5. Section 6 concludes this paper.

2 Related Works

2.1 Vehicular Cloud

Cloud computing combines these two drivers: both usage and costs change based on user needs. Because of the flexible nature of cloud computing, it can meet user needs from an availability and performance perspective and still keep operating costs low because expenses are based on services that are actually used, as opposed to a capital investment that is based on projections of potential needs [1].

With the advent of smart phone in recent years, more and more intelligent vehicle services with cloud computing technique support can be easily implemented. This trend will become more obvious in the future as various types of sensors are embedded into the smart phone such as audio, video, accelerometer, GPS and biomedical sensors. Taking smart phone as an interface between human and internet as well as network, more and more customized services can be implemented in the future for vehicle users [2].

Advances in vehicular networks, embedded devices and cloud computing will enable the formation of vehicular clouds (VCs) of computing, communication, sensing, power and physical resources. There are two types of VCs. In the first type called Infrastructure-based VC, drivers will be able to access services by network communications involving the roadside infrastructure. In the second type called Autonomous VC (AVC), vehicles can be organized on-the-fly to form VC in support of emergences and other ad hoc events [3].

2.2 Cloud Service Level Agreement (CSLA)

As consumers move towards adopting such as a service-oriented architecture (SOA), the quality and reliability of the services become important aspects. However the demands of the service consumers vary significantly. It is not possible to fulfill all consumer expectations from the service provider perspective and hence a balance needs to be made via negotiation process. At the end of the negotiation process, provider and consumer commit to an agreement. In SOA terms, this agreement is referred to as a service level agreement (SLA). This SLA serves as the foundation for the expected level of service between the consumer and the provider. The QoS attributes that are generally part of SLA (such as response time and throughput) however change constantly and to enforce the agreement, these parameters need to be closely monitored [4].

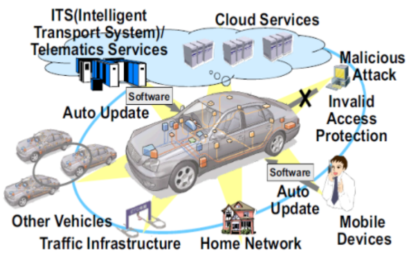

Fig. 1. Vehicular cloud services

Vehicular cloud services (VCSs) that are illustrated Fig. 1 include many IT infrastructures, mobile devices, cloud services, traffic infrastructure, home network, and vehicles [5]. They interact with one another in vehicle-centric manner everywhere at anytime. The key challenges of the VCSs are discussed.

- Guarantee of Real-time Performance
  The vehicular service needs to assure the strict time constrains. If the specified timing is not met, controllability may be diminished or the system failure to work in the worst case. Accordingly, the guarantee of real-time performance in VCSs becomes a challenge.
- Assurance of Safety, Reliability and Security
  The automotive software must be safety-critical. Therefore safety and reliability are the critical requirements in the development of the vehicular software systems. Even if the information devices outside of vehicle are failed, the automotive ECU needs some mechanism to tolerate the impact of the failure.

2.3 Trust Models

Trust models have been proven useful for decision making in numerous service environments. The concepts have also been adapted in grid computing, cloud computing environments, and web services. In recent years, many scholars have made a lot of research on trust model for cloud computing. Alhamad *et al.* [6] developed a model for each of the dimensions for IaaS using fuzzy-set theory. Li, X. and Du, J. [7] represented Cloud-Trust, an adaptive trust management model for efficiently evaluating the competence of a cloud service based on its multiple trust attributes. Noor *et al.* [8] proposed a framework to improve ways on trust management in cloud environments. This framework helps distinguish between credible trust feedbacks and malicious trust feedbacks through a credibility model.

Also, a lot of trust and reputation management approaches for VANETs have been presented. Abumansoor *et al.* [9] proposed a trust evaluation model based on location information and verification in a NLOS (None Line Of Sight) condition. The model provides a trust attribute for applications and services to evaluate their own trust levels. Ding *et al.* [10] proposed an event-based reputation model to filter bogus warning messages, where a dynamic role-dependent reputation evaluation mechanism is presented to determine whether an incoming traffic message is significant and trustworthy to the driver. Yang, N. [11] proposed a trust and reputation management framework for VANETs. In the framework, a similarity mining technique is used for identifying similar message and similar vehicles, and a reputation evaluation algorithm is proposed for evaluating a new vehicle's reputation based on the similarity theory.

3 Vehicular Service Level Agreement (VSLA) Model

We present our VSLA architecture in Fig. 2. The VSLA supports the effective execution of automotive services in vehicular clouds that is inherently dynamic and the resource usage changes dynamically.

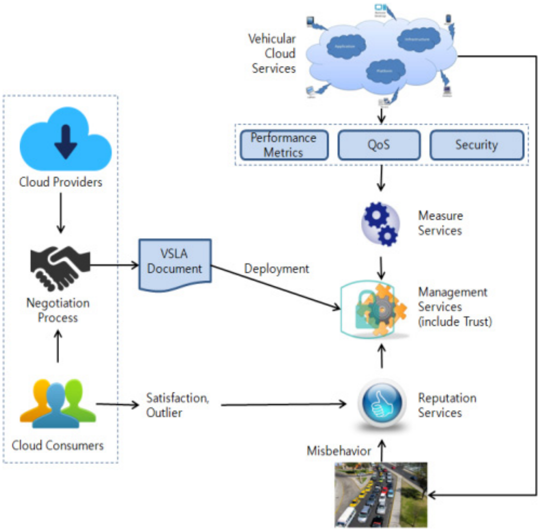

Fig. 2. VSLA architecture

In VSLA structure, we have assumed that the cloud provider and the cloud consumer already participated in the negotiation process and have an agreed set of service parameters. Once the VSLA document is established, it needs to be deployed. The term VSLA deployment is defined as the process of validating and distributing the VSLA, in part or full, to involved parties.

- Vehicular Cloud Services: While vehicular clouds have several services for vehicles and traffics, we consider only two types of vehicular services which are included in SaaS: driver assistance services and safety message dissemination services. Based on intelligent sensor technology, driver assistance services constantly monitor the vehicle surroundings as well as the driving behavior to detect potentially dangerous situations at an early stage. In critical driving situations, these systems warn and actively support the driver and, if necessary, intervene automatically in an effort to avoid a collision or to mitigate the consequences of the accident. Safety and comfort messages are the main types of messages transmitted in VANET. With the safety messages, the drivers can be made aware of the occurrence of accidents even in low visibility situations.
- Measurement Services: These services are responsible for measuring the runtime parameters of cloud provider resources. These services identify the following service parameters to enforce VSLA through vehicular cloud monitoring.
- Reputation Services: These services involve efficient storage of identities and past experiences concerning those identities. Positive or negative experiences may be

stored, based on satisfactory completion of transactions, fulfillment of expectations, or some other form of verifiable fiduciary action. In the reputation service of our model, satisfaction and outlier are provided for the reputation of vehicular cloud applications. Also, misbehavior is provided for the reputation of vehicles.

4 RA-VTrust System

A vehicular cloud with the function of trust management is implemented by three layers: trust management layer, VSLA management layer and resource management layer (Fig. 3). The trust management layer is used to evaluate the trustworthiness of service provider through the collection of monitored evidence and the trust mining from the evidence using rough sets on the base of trust information system. The VSLA management layer is used to negotiate an agreement between two parties, where one is the user and another is the service provider. The resource management layer is charged by the service provider, and it provides a set of virtual machines that are configured according to user request and user reputation.

Specifically, each layer consists of several modules and databases. Theses modules and databases are listed as follows:

- Adaptive trust mechanism: This mechanism is the core of trust evaluation. Based on the following information bases, each user maintains a ATM to guide itself in evaluating cloud services through its direct interactions with these services.
  - User reputation information system: This information contains the vehicle reputation that is constructed from valid actions of moving nodes in VANETs and the user reputation that is based on outlier in voting of the satisfaction for vehicular services.
  - Evidence base: The measured and assessed information through service monitoring module is stored in evidence base.
  - Trust information system: The trust information system contains data on the objects of interested characterized in terms of some trust attributes.
- Service monitoring mechanism: This mechanism is needed to continuously measure and assess infrastructure or application behavior in terms of performance, reliability, power usage, ability to meet VSLAs, security, etc [14].
- VSLA manager: The service provider registers its services on VSLA management system. The service user negotiates with service provider about the VSLA details; they finally make an VSLA contract.
- Log information: This mechanism is managed by the cloud manager. Cloud manager sort high-performance cloud services for providing highly trusted resources when there are user requests.

Trust decision task for vehicular services is a multi-attribute decision-making problems based on monitored evidences by the service monitoring agent. Monitored trust evidence acts as initial input data. Each input data is *m*-dimensional vector, and it consists of m input evidences. We construct the trust information system (Table 1) for a vehicular service use it to initiate trusted knowledge discovery. The trust information system contains data on the objects of interested characterized in terms of some trust attributes and trust value according to the attribute data.

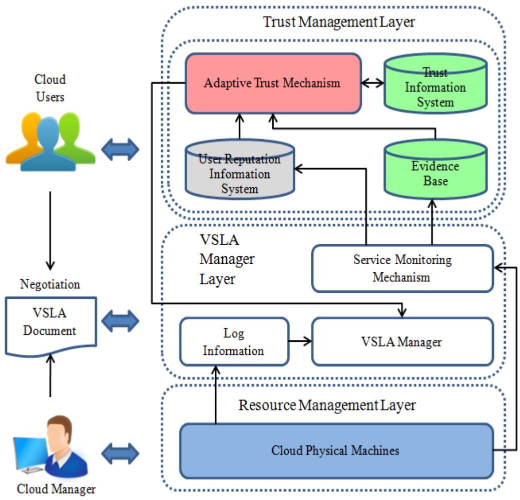

Fig. 3. RA-VTrust architecture

Table 1. The structure of trust information system

U	Th	Av	RT	Se	Sc	Trust
x_1	H	VH	VH	VH	H	VG
x_2	H	H	H	H	H	G
x_3	H	H	H	M	M	E
x_4	M	M	M	M	M	P
x_5	L	L	M	M	L	VP
x_6	M	H	H	H	M	E
x_7	H	H	VH	H	M	G
x_8	H	H	VH	VH	VH	VG
x_9	M	VH	H	VH	M	G
x_{10}	H	M	M	H	M	P
x_{11}	H	M	H	H	M	E
x_{12}	M	M	H	H	M	E

The trust information system consists of condition and decision attributes. The information system is denoted by S=(U, C, D), where U is a non-empty finite set of objects called universe of discourse, C and D represent conditional attributes and decision attributes of trust measurement, respectively. The information system uses five fuzzy sets for the input value of condition attributes and five fuzzy sets for the output value of decision attribute. In Table 1, C={Th, Av, RT, Se, Sc} denote the condition attribute, and D={Trust} denotes the decision attribute.

To enforce VSLA for a service, the RA-VTrust mechanism evaluates appropriate trusts in consideration of specified trust of VSLA, trust information system, the measured information of evidence base and user reputation. The relative classification error between the trust information system and the VSLA is computed by equation (1).

$$e(X,Y)=\sum_{i=1}^{n}\left[\left(\mu(x_i)-\mu(y_i)\right)\times w_i\right] \quad (1)$$

In equation (1), X and Y are the conditional attribute vectors of trust information system and VSLA, respectively. $\mu(x_i)$ and $\mu(y_i)$ represent the defuzzified values for the i-th elements of the conditional attributes of trust information system and VSLA, respectively. Also, n is the number of conditional attributes, and w_i is the relative weight of i-th conditional attribute. Therefore, the similarity between the trust information system and the VSLA is as follows:

$$s(X,Y)=1-e(X,Y) \tag{2}$$

We classify user reputation information into five fuzzy sets: VH, H, M, L, VL. Table 2 shows the allowable values of error, β, in the relative classification of user reputation information in case the trust degree of VSLA is E (excellent).

Table 2. Allowable classification error values for fuzzy reputation sets

Fuzzy reputation set	Allowable classification error value (β)
VH	[0.2, 0.3)
H	[0.1, 0.2)
M	[0.0. 0.1)
L	[-0.1, 0.0)
VL	Service suspension

Adaptive trust mechanism selects feasible trust objects from the trust information system through use of the specified trust of VSLA and the allowable classification error that depends on user reputation information. Then, it also selects the best trust that has the minimum classification error as the most suitable VSLA. The adaptive trust mechanism submits the best trust to VSLA manager. The VSLA manager submits the best trust to management services. The management services schedule and allocate the resources according to the best trust VSLA. The service monitoring mechanism is needed to continuously measure and assess infrastructure or application behavior regarding the execution of the service, and also forwards the values of trust attributes to evidence base. If these values of trust attributes of evidence base are different from the values of best trust attributes, the adaptive trust mechanism stores these values of trust attributes of evidence base in the trust information system.

To illustrate our idea, an example is used. Assume that the VSLA of the user who requests a vehicular service is (M, M, H, H, M, E), w_i=(0.15, 0.2, 0.25, 0.25, 0.15), $\mu(VH)$=1.0, $\mu(H)$=0.8, $\mu(M)$=0.6, $\mu(L)$=0.4 and $\mu(VL)$=0.2. Firstly, if the user reputation is H, the feasible trust objects are computed as follows:

$$e(x_2,VSLA)=0.2\times(0.15+0.2+0.15)=0.1,$$

$$e(x_7,VSLA)=0.2\times(0.15+0.2+0.25)=0.12,$$

$$e(x_9,VSLA)=0.2\times(0.4+0.25)=0.13.$$

Accordingly, x_2=(H, H, H, H, H, G) is selected as the best trust for the requested vehicular service.

Secondly, if the user reputation is L, the feasible trust objects are computed as follows:

$$e(x_4,VSLA)=0.2\times(-0.25-0.25)=-0.1.$$

Accordingly, x_4=(M, M, M, M, M, P) is selected as the best trust for the requested vehicular service. Therefore, the adaptive trust mechanism sends the best trust to VSLA manager and management services.

5 Performance Evaluation

The performance of proposed scheme is evaluated with the variation of reputation and trust values. The performance of RA-VTrust is compared with that of Alhamad [6]. Reputation and trust values are computed as follows:

- Reputation value variation

  The reputation value of each vehicle or its driver can be calculated by equation (3).

$$\text{Rep}_i^{(n)} = \begin{cases} \alpha \, \text{Rep}_i^{(n-1)} + (1-\alpha) r_i^{(n)}, & n > 1 \\ 0.5, & n = 1 \end{cases} \tag{3}$$

  Where $0 \le \alpha \le 1$ and $r_i^{(n)}$ is the reputation value for the user i after confirming the n-th event message.

$$r_i^{(n)} = \begin{cases} 0.9, & \textit{if the } n-th \textit{ event message is rational behavor} \\ 0.7, & \textit{if the } n-th \textit{ satisfaction message is normal} \\ 0.3, & \textit{if the } n-th \textit{ satisfaction message is outlier} \\ 0.1, & \textit{if the } n-th \textit{ event message is misbehavior} \end{cases}$$

- Trust value variation

  The trust value for each vehicular service can be calculated by equation (4).

$$Trust_{val} = \sum_{i=1}^{n} w_i \mu(x_i), \tag{4}$$

  where $0 \le w_i \le 1$ and the summation of w_i is 1. .

We evaluate the performance of RA-Trust in the MATLAB [12] by applying the parameters and values of Table 3.

Table 3. Simulation parameters

Parameter	Value
Number of service requests	50
Number of vehicles	10
Probability that abnormal event is occurred	0.1~0.7
μ(VH, H, M, L, VL)	1.0, 0.8, 0.6, 0.4, 0.2
w_i	(0.15, 0.2, 0.25, 0.25, 0.15)
Interval-valued for reputation fuzzy sets, {VH, H, M, L, VL}	{[1.0, 0.8], (0.8, 0.6], (0.6, 0.4], (0.4, 0.2], (0.2, 0.0]}
Interval-valued for trust fuzzy sets, {VG, G, E, P, VP}	{[1.0, 0.9], (0.9, 0.8], (0.8, 0.7], (0.7, 0.6], (0.6, 0.0]}
Initial value of reputation	0.5
Initial trust of VSLA	E

Fig. 4 and Fig. 5 show the evaluation results for reputation. Fig. 4 shows average reputation value according to the probability that abnormal event is occurred, where the larger abnormal probability, the smaller average reputation value. But, Alhamad model has a fixed reputation value even if abnormal events are occurred. Also, Fig. 5 shows the number of occurrences for reputation fuzzy sets according to the abnormal probability. The smaller abnormal probability has, the more high reputations (VH and H) are occurred, while the larger abnormal probability has, the more low reputations (L and VL) as compared with other abnormal probabilities are occurred. Additionally, we know that 8 service requests are suspended in case that abnormal probability is 0.7, but 2 service request is suspended in case that abnormal probability is 0.3 from Fig. 5.

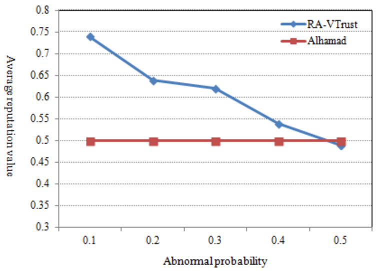

Fig. 4. Average reputation value with abnormal probability

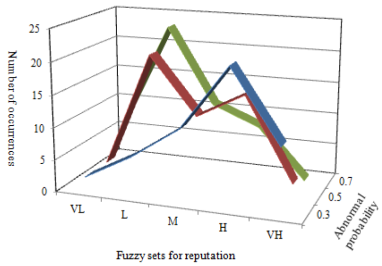

Fig. 5. The frequency of reputation fuzzy sets with abnormal probability

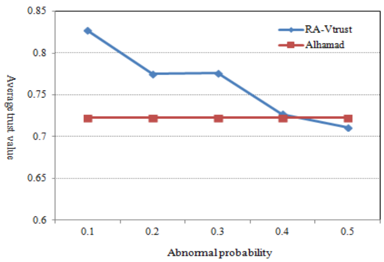

Fig. 6. Average trust value with abnormal probability

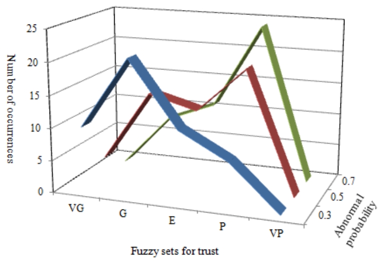

Fig. 7. The frequency of trust fuzzy sets with abnormal probability

Fig. 6 and Fig. 7 show the evaluation results for trust. Fig. 6 shows average trust value according to the probability that abnormal event is occurred. Similarly to reputation values, the larger abnormal probability, the smaller average trust value. But, Alhamad model has a fixed trust value even if abnormal events are occurred. Also, Fig. 7 shows the number of occurrences for trust fuzzy sets according to the abnormal probability. The smaller abnormal probability has, the more good trusts (VG and G) are occurred, while the larger abnormal probability has, the more poor trusts (P) are occurred. From the results of our simulation, we hereby confirm that our RA-VTrust is efficient adaptive trust management model for vehicular clouds regarding VSLA and reputation.

6 Conclusion

To development of efficient trust management model for the services of vehicular clouds, we propose firstly the VSLA which supports the effective execution of automotive services in vehicular clouds, and design next the RA-VTrust which evaluates the trustworthiness of service provider through the collection of monitored evidence and the trust mining from the evidence using trust information system. The performance of RA-VTrust is evaluated through a simulation. As a result, our RA-VTrust has proven to handle adaptively trust management for vehicular clouds regarding VSLA and reputation.

Our future work includes RA-VTrust extension which not only considers user and service reputations, but also has the service recommendation function that takes account of user service reputation.

References

1. Marco, J.D.: Cloud computing for automotive. IBM Global Business Services, IBM Cooperation, GIW03003USEN, 1–20 (2012)
2. Wang, T., Cho, J., Lee, S., Ma, T.: Real time services for future cloud computing enabled vehicle networks. In: International Conference on Wireless Communications and Signal Processing, pp. 1–5. IEEE Press, New York (2011)
3. Olariu, S., Eltoweissy, M., Younis, M.: Towards autonomous vehicular clouds. ICST Transactions on Mobile Communications and Applications. **11**, 7–9 (2011)
4. Keller, A., Ludwig, H.: The WSLA Framework: Specifying and Monitoring Service Level Agreements for Web Services. Journal of Network and Systems Management. **11**, 57–81 (2003)
5. Iwai, A., Aoyama, M.: Automotive Cloud Service Systems Based on Service-Oriented Architecture and Its Evaluation. In: Int. Conf. on Cloud Computing, pp. 638–645. IEEE Press, New York (2011)
6. Alhamad, M., Dillon, T., Cjanh, E.: A Trust-Evaluation Metric for Cloud applications. Int. Journal of Machine Learning and Computing. 1, 416–421(2011)
7. Li, X., Du, J.: Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing. IET Information Security **7**, 39–50 (2012)
8. Noor, Talal H., Sheng, Quan Z.: Credibility-Based Trust Management for Services in Cloud Environments. In: Kappel, Gerti, Maamar, Zakaria, Motahari-Nezhad, Hamid R. (eds.) Service Oriented Computing. LNCS, vol. 7084, pp. 328–343. Springer, Heidelberg (2011)
9. Abumansoor, O., Boukerche, A.: Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services. In: Global Telecommunications Conference, pp. 1–5. IEEE Press, New York (2011)
10. Ding, Q., Li, X., Zhou, X.: Reputation-based Trust Model in Vehicular Ad Hoc Networks. In: International Conference on Wireless Communications and Signal Processing, pp. 1–6. IEEE Press, New York (2010)
11. Yang, N.: A Similarity based Trust and Reputation Management Framework for VANETs. Int. Journal of Future Generation Communication and Networking. 6, 25–34(2013)
12. Kay M. G.: Basic Concepts in Matlab
`http://www.ise.ncsu.edu/kay/Basic_Concepts_in_Matlab.pdf`