Secure and Reliable Cloud Networks for Smart Transportation Services

Dhananjay Singh*, Madhusudan Singh**, Irish Singh***, Hoon-Jae Lee****
*Dept. of Electronics Engineering, Hankuk University of Foreign Studies, Yongin, South Korea
**Display Research Team, Samsung Display Co. Ltd. (SDC), Yongin, South Korea
***Dept. of Computer Science, Birla Institute of Technology (BIT), Mesra (Allahabad Campus), India
*** Div. of Information Network Engineering, Dongseo University, Busan, South Korea

dan.usn@ieee.org, sonu.dsu@gmail.com, singhirish15@gmail.com, hjlee@dongseo.ac.kr

Abstract— **This paper has discussed about smart transportation services in cloud (Cloud-STS) for safety and convenience. STS provide driver centric board services in the cloud networks. STS composed of Vehicle to WiFi networks (VtoWiFi), Vehicle to Cloud Network (VtoCN), Vehicle to Vehicle (VtoV), and Cloud Network to service provider (CNtoSP). The idea is to utilize the (WiFi enabled) Smart Highways and 3Dcamera enabled dash board navigation device to enhance accident prevention / monitoring and control. Hence, in the event of accident, the video recorded using the collectors and the information about the location, specified by the GPS module are transferred to reliable cloud so that the concerned authorities can have a look at the evidence stored at same time and provide additional services to capture and share real-time accident/traffic footages.**

***Keywords*—Cloud computing; Smart Transportation; Security; Vehicular Network.**

I. Introduction

We are fast transforming technologically, and already have achieved much technological advancements in the field of accident, management, data gathering and storage for any type of incident management [1]. According to National Institute of Standards and Technology (NIST), cloud computing provides a convenient on demand network access to a shared pool of configurable computing resources [2]. Cloud Computing is the internet based computing where the application software, infrastructure and platform are available in the cloud and the end users (businessman, developers) can access it through, as a client. Cloud Computing is rapidly growing area in the IT security space because Cloud architectures are popping up all over. The major dynamic thought Cloud providers present in the cutting-edge market segment are Amazon, Microsoft, Google, IBM, Oracle, Eucalyptus, VMware, Eucalyptus, Citrix, Salesforce and Rackspace as well as there are many different vendors offering different Cloud services [3].

In this paper we are considering cloud computing system for a smart transportation system (STS) which is the domain of futuristic transportation systems. This is an advanced technics of upcoming technologies such as more advanced wireless sensor networks, distributed system architectures, cloud computing, sensing and actuating, control and detection in multiple types of automobiles on roads to improve safety of the passengers, optimized service of the transportation system and real time traffic situation. STS is coming fast towards the integration of virtual technology in the transportation field. We are trying to explore new possibilities to enhance the framework of the STS to a valuable cloud computing system.

Cloud computing has very vast application field, which includes both machine side and client side. So, people from different walks of technologies can contribute to this ever developing field of research. However, the vision of application development on the platform of cloud is still in nascent stages. The proposed techniques consider an internet enabled STS system which can play a very crucial role through using Cloud computing to enhance accident prevention/monitoring and control.

A. Motivation

Today the economy of every country is increasing at a tremendous pace. People in every part of the world are having vehicles to travel. Some buy it for status symbol while others buy it for necessity.

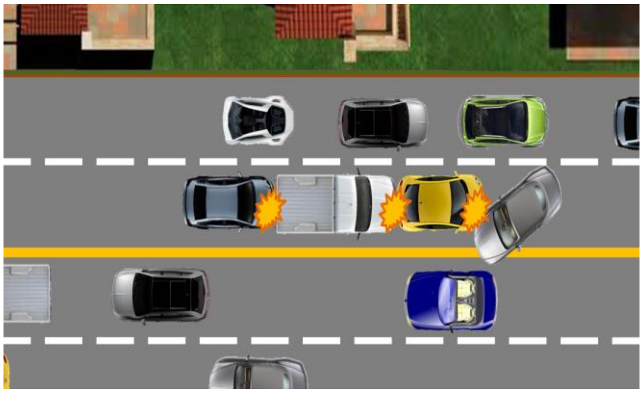
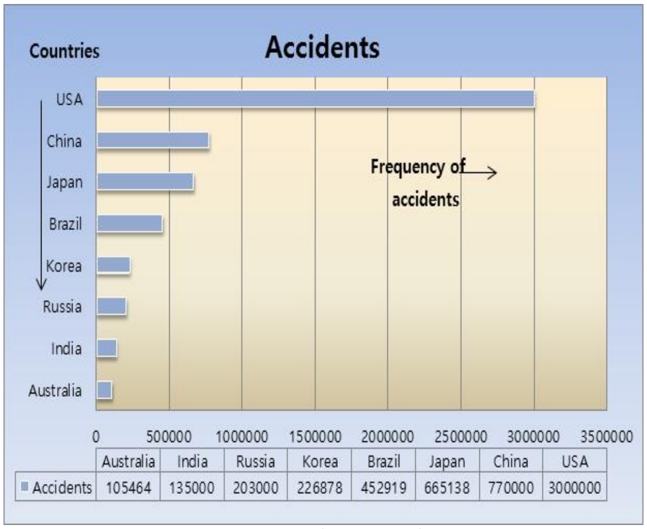


Fig.1. Present Transportation System.

We can often see the increasing overflow of vehicles in every street. On the other hand, there are an increasing number of disastrous vehicle accidents which have become a commonplace incident. Fig.1 shows a road-show of present transportation system. We have searched some economically stable countries and listed the numbers of accidents that have taken place according to the latest reports. Due to the ever increasing number of accidents, there have been cases of vehicle crash debates or road rage after the accidents have taken place. We have analyzed in this aspect also and have presented few statistics as given: vehicle crash debate or road rage is a common phenomenon after the accident has taken place which sometimes takes a bad shape and results in death of a person. In fig. 2 we present a few statistics about the vehicle accidents that take place in several countries [5].



	Australia	India	Russia	Korea	Brazil	Japan	China	USA
Accidents	105464	135000	203000	226878	452919	665138	770000	3000000

Fig. 2 Statistics of accidents frequency.

The remaining of the paper is organized as follows. Section 2 presents a brief discussion of cloud computing and its security issue as well as possible solutions. Section 3 presents novel secure cloud based STS model. Finally, we have concluded the paper in section 4.

II. Security Issue in Cloud Computing

Cloud Computing is being widely adopted across many industry sectors. With adoption comes, security concerns. Cloud Computing is experiencing significant growth, with rapid adoption among various regions around the world. The essential characteristics of cloud computing are broad network access, on demand self-service, rapid elasticity, resource pooling and measured service. Broad network access is the access of the various resources hosted in a cloud network from a wide range of locations which offers online access. On demand self-service is the availability of services and resources by the cloud vendors, when needed. Rapid elasticity is to provide scalable services by the vendors, when required. Resource pooling is serving maximum clients and customers with scalable and provisional services. Measured service is the monitoring of the services provided by the vendors to the client which includes billing and adequate use of resources.

The three building blocks or the well -known and commonly used service models in the Cloud Computing are Software as A Service (SAAS), Platform as A Service (PAAS), and Infrastructure as A Service (IAAS), where SAAS provides the software and applications on demand across the internet which reduces the cost of software, maintenance and operations. PAAS provides the platform on demand across the internet for developing software using tools or/and libraries from the provider. It also supports software deployment and configuration settings. IAAS provides the infrastructure on demand across the internet for the infrastructure of processing, storage and network resources [1].

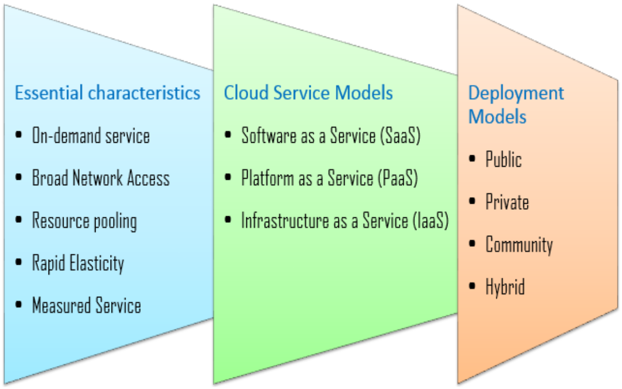


Fig. 3. Cloud Computing Building Block.

As cloud is gaining more popularity, more and more organizations want to move towards cloud but the key concern about moving towards cloud has been security. Today security is required in each of the deployment models. According to NIST [1], the cloud model is composed of major four deployment models such as Public, Private, Community and Hybrid cloud. The public cloud infrastructure is procured for open use by the general public. It may be held, managed, and operated by a business, academic, or government organization, or some combination of them. The private cloud infrastructure is procured for privileged use by a single organization comprising numerous consumers. The community cloud infrastructure is procured for privileged use by a specific community of consumers from organizations that have shared interest (e.g. mission, security requirements, policy, and compliance considerations) and hybrid cloud infrastructure is an amalgamation of two or more distinct cloud infrastructures (private, community, or public) that have unique existence, but are bound together by standardized or proprietary technology that facilitates data and application portability.

Hence, cloud service provider have less transparency then other information security policy. The reason for such difference is the policy. As a result it may create clash with the enterprise's information. The enterprise needs to have detailed understanding of the service level agreements that requires desired level of security, provided by the cloud service providers.

III. Security concerns in Cloud Computing

There are various security concerns which are data security, data confidentiality and compliance with government regulations, trust, identity management, architecture, software isolation and availability. Generally, the security is a joint responsibility of the cloud client and provider. However, the organization itself is accountable for its all resources over the cloud. Although the cloud computing offers many benefits, for instance, low cost, but the data security and privacy issues pose serious concerns. Therefore, most of the cloud users are unaware of the risk of storing and transmitting private information in a shared environment. Therefore, key technological constraints like transparency, multi-tenancy, velocity-of-attack, information assurance, data privacy and ownership, compliance, encryption, integrity should be addressed carefully.

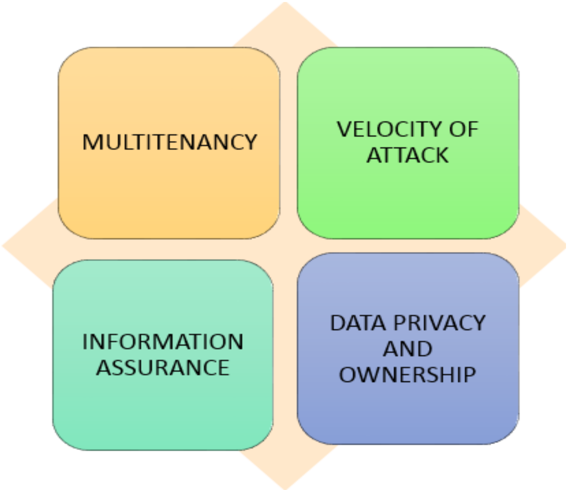


Fig.4. Security concerns in Cloud Computing

The transparency is the biggest challenge for the enterprises at present, and due to this, they are not willing to switch to cloud computing environment. Once the cloud becomes transparent, the cloud users can have easy access control and they can easily manage their data and thus social trust will be build up. Therefore the software isolation, data protection, trust, identity management, architecture, and availability are the primary security issues related to cloud computing. Multi-tenancy is an important security concern for cloud clients, colocation of multiple Virtual Machines in a single server and sharing the same resources that increases the attack surface. Velocity- of-attack threats amplify and spread quickly in a cloud infrastructure which is comparatively larger in platform/components that can also increases the speed of the attack. Information assurance concerns for cloud users, authenticity and authorized use which concerns data ownership for cloud clients for data belonging to a client who has access to the data, but is not the legitimate owner of it. This raises concern of potential unauthorized data access and misuse. Data should be protected using encryption and access control mechanism. Data privacy is a potential for unauthorized disclosure of private data of a cloud client. Private data may include individual identity of the client, details of the services requested by the client and proprietary data of the client. For the security of information both the cloud provider and the client are equitably responsible [4].

IV. Smart Transportation System (STS)

The advancement of STS technology now provide functions to prevent/monitor accidents for vehicles and pedestrians as well as quickly find destinations. Furthermore, it also transfer accident information to the concern people with the help of cloud networks. The major advantage of the proposed system is the conventional cloud that can support sustainable and permanent services like computing, amateur radio, aviation etc.

Algorithm: Vehicle Detour Routing Procedure in STS

```
Generate Test Message
  //Bootstrapping
  For All vehicle
          Set pheromone 0
  End For
   //One-hop broadcast of a test message in the air
  Advertise pheromone
  Update Neighbor Node list
//Routing decision process
Vehicle DetourRouting
  If queue>0 then
    If (Neighbor vehicle list for Destination) then
      ForwardingVehicle = Get Highest Pheromone (Neighbor Node list)
    Else
      ForwardingVehicle = Random(Neighbor Vehicle)
    End If
    Send a packet to ForwardingVehicle
    delta =1
  Else
    delta = 0
  Enf If
  // Pheromone update
 Result = Compute_pheromone(Vehicle)
 Set pheromone Result
```

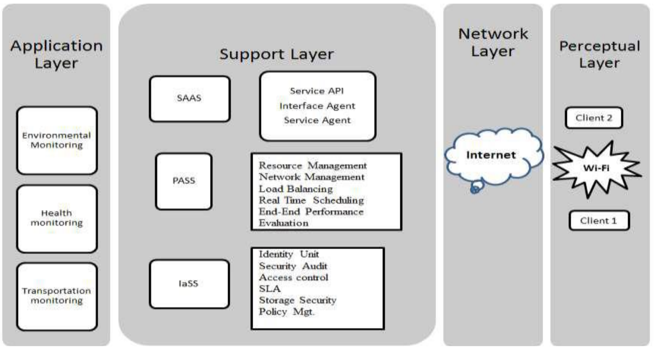


Fig. 5. Cloud computing architecture for STS system.

The proposed cloud computing architecture for STS is described in Fig. 5 where four layers is presented from cloud computing to end-user (Vehicle). The communication layer contains a transportation stratum for sharing of information between end-user via an ad hoc network or to a cloud server in the event of an accident. In the transportation stratum, if we have a Wi-Fi module and a Bluetooth module connected using their respective interfaces to the processor. Here, there are two processors for processing the data. First is the main processor and the second one is the subsidiary processor. The main processor will just share the data (video, audio, information about the location using GPS/WiFi etc.) to the clients in the range of ad hoc network or to a cloud-based server using Internet services. The last part is the conventional cloud which is responsible of data collector stratum. It consists of various modules for collecting and transferring data and information like camera modules for rear and front, LCD module, GPS Module, pressure sensor for accident detection, temperature sensor for protecting the data which could be destroyed from excessive temperature, proximity sensor for vehicular lane change detection, and speed sensor.

V. Reliable cloud networks

Any technology's strong point is measured by its degree of reliability and availability. The reliability denotes how regularly resources are available without trouble (loss of data, code reset during execution) and how commonly they fail. One of the important aspect that creates serious problems for the reliability of cloud computing is down time.

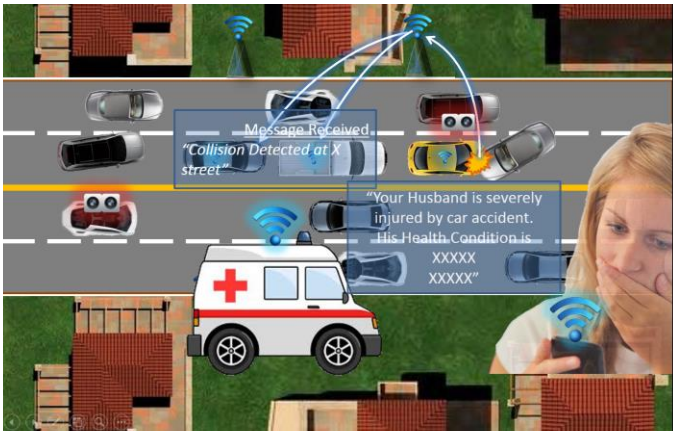
To understand routing performance in a cloud network, we assess three routing strategies: vehicle-touring, random-touring, and vehicle-detouring. By using only local information similarly to [9], for each strategy, we set the probability that node i chooses node j as a forwarding node among m neighbors as follows:

$$\text{Vehicle-touring:} \quad \prod_{i->j} = \frac{g_j^1}{\sum_m g_j^1}, \qquad (1)$$

$$\text{Rrandom-touring:} \quad \prod_{i->j} = \frac{g_j^0}{\sum_m g_j^0}, \qquad (2)$$

$$\text{Vehicle-detouring:} \quad \prod_{i->j} = \frac{g_j^{-1}}{\sum_m g_j^{-1}}, \qquad (3)$$

where g is the degree of node (number of one-hop neighbors).



Message Received

"Collision Detected at X street"

"Your Husband is severely injured by car accident. His Health Condition is XXXXX XXXXX"

Fig.6. Cloud based Smart Transportation System.

Fig.6 shows the overview of a Smart Transportation System (STS) based on cloud computing. Where we can see the information is collected using the collectors namely front and rear camera module for recording the pre and post-accident data. The information gathered is processed using a processor. The information is simultaneously sent to the end users who are nearby the ad-hoc network without any intervention from third party electronics device so that they can receive the news about the nearby vehicles and the drivers then decide for themselves whether to overtake the preceding cars or not. In the event of accident, the video recorded using the collectors and the information about the location specified by the GPS module are transferred to a Wi-Fi-based server so that the concerned authorities can have a look at the evidence stored. Therefore the reliability is redundant resource utilization and availability can be understood as the possibility of attaining the resources whenever they are needed with the consideration to the time it takes for these resources to be provisioned. Irrespective of employing architectures having attributes for high reliability and availability, the services in cloud computing can experience in Denial of service attacks, Performance slowdowns, Equipment outages and natural disasters. In order to remove FUDD (fear, uncertainty, doubt, and disinformation) probably the reliability, availability and security are important. The level of reliability and availability of cloud resources must be considered as a serious problem in the organization's planning to set up the cloud infrastructure in order to provide effective services to the consumers.

VI. Performance Analysis and Final Remark

We have analyzed the routing performance with respect to topology alternating cycle. As the alternating time is shorter and shorter, the performance gap becomes smaller and smaller. In a rapidly dynamic topology, vehicles frequently change and thus, the portion of vehicle roles diminishes. We interpret that mobility or unstable link quality, which contributes to changing an intrinsic network topology, minimizes dependencies of specific vehicle. Even though we examine this interpretation, we observe that vehicle-detouring maintains the best performance among the strategies. Conclusively, it is beneficial to accommodate a vehicle-detouring strategy to fully utilize available network resources and to minimize undesirable impact of a specific vehicle to an entire network. Along with load balancing capability of vehicle-detouring, we review previous works which deal with the vulnerability of vehicles and its impact to an entire network.

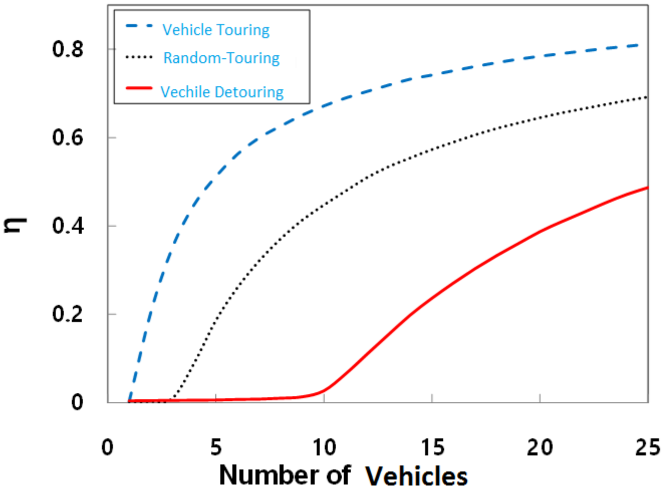


Fig. 7. Network traffic states for different topology alternating cycle.

In this paper, we have mainly focused STS based on reliable cloud networks especially in vehicular safety of drivers while driving on highways roads. This system is going to support various services such as economy, traffic congestion, pollution and comfortable driving. Further, it would be easier for the investigation end to collect the information statistics of the accident (if any) from the cloud server. This system will avoid the road rage as people would be priory aware about the traffic statistics. Thus this system would act as an alert eye for the travellers. Hence, cloud computing provides a highly scalable and on demand computing platform to End to End user with high elasticity and availability to the Smart Transportation Services.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology. (grant number: NRF-2011-0023076). And it also supported by the BB21 project of Busan Metropolitan City and Hankuk University of Foreign Studies research fund 2015.

REFERENCES

[1] Junping, Z., Fei-Yue, W., Kunfeng, W., Wei-Hua, L. Xin, X., Cheng, C., "Data-Driven Intelligent Transportation Systems: Survey", IEEE Transactions on Intelligent Transportation Systems, Vol. 12 (4) pp. 1624-1639, 2011.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory, (2009) NIST- www.csrc.nist.gov Accessed by March 2015.

[3] K. Julisch and M. Hall, "Security and Control in the Cloud", Information Security Journal: A Global Perspective, (9) pp. 2099-309, (2010).

[4] D. Singh, et.al., "SEE: A Smart-Eye for Intelligent Transportation System", The 2nd International Symposium on Advanced and Applied Convergence (ISAAC 2014), Jeju Island, Korea, Nov. 13-16, 2014

[5] D. Singh and A. Alberti,"Developing NovaGenesis Architecture for Internet of Things Services: Observation, Challenges and ITMS Application", International Conference on ICT Convergence 2014, Paradise Hotel in Busan, Korea, October 22-24, 2014.

[6] Kang, W.M.; Lee, J.D.; Jeong, Y.-S.; Park, J.H. VCC-SSF: Service-Oriented Security Framework for Vehicular Cloud Computing.*Sustainability* 2015, *7*, 2028-2044.

[7] M. Gunes, U. Sorges, and I. Bouazizi, "ARA - the ant-colony based routing algorithm for MANETs," in *Proc. of IWAHN*, 2002.

AUTHORS

Dhananjay Singh (SM 14) received his M Tech. in IT from IIIT, Allahabad, India in 2006 and PhD in IT from DSU, Korea in 2010. After that, he has worked at NIMS and ETRI, Korea 2010-2012. In Sept. 2012, he joined as an Asst. Prof. in the Dept. of Electronics Engineering at Hankuk University of Foreign Studies, Korea. He has published 75+ referred scientific papers, delivered 25+ invited talks, 10+ editorial board and 100+ TPC membership in International conferences. He is a senior member of IEEE. His field of Interest IoT, Cloud Computing, Future Internet, Wireless Sensor Networks and Signal System.

Madhusudan Singh (M 14) received his Ph.D. degree in the Dept. of Ubiquitous IT, from Dongseo University, South Korea in Feb. 2012. M. Tech. degree from IIIT-A, India in July 2008. He was a visiting research scholar at University of Pisa, Italy in 2010. His research interests focus on the design, analysis and implementation of algorithms and protocols to solve real-world problems in the emerging fields, cloud computing, IoT, WMN, and Mobile Display Technology.

Irish Singh is doing M. Tech in Computer Science and Engineering from Birla Institute of Technology, Ranchi (Allahabad campus). She did her B. Tech in Computer Science and Engineering from UP (State) Technical University, Lucknow, India. Her fields of research interests are Security issue in Big Data, Cloud computing, ICN and IoT.

Hoon-Jae Lee is a professor of the School of Computer and Information Engineering at Dongseo University, Busan, South Korea. Before joining DSU, he was a Research Associate at the Agency for Defense Development (ADD) in Korea. He received the BS, MS, and PhD degrees in Electronic Engineering from Kyungpook National University, Daegu, South Korea, in 1985, 1987, and 1998, respectively. He has published 300+ papers and 50+ patents. He has served as a reviewer for many conferences and journals.