ISSN:0975-9646

Thwarting Perils through Cloud Provisioning using Security Issues in Vehicular Cloud

N. Nijanthan[1], B.Mohankumar[2], Dr. P. Marikkannu[3]

[1] *PG Scholar, Department of IT, Anna University, Regional Centre, Coimbatore, India*
[2] *PG Scholar, Department of IT, Anna University, Regional Centre, Coimbatore, India*
[3] *Head of the Department, Department of IT, Anna University, Regional Centre, Coimbatore, India*

***Abstract* - The Vehicular Cloud concept is a wideadoption and significant societal impact. Security & privacy issues are to be addressed. The most important contribution of this work is to recognize and analyze a number of security challenges and prospective privacy threats in VCs. Even though security issues are covered they receive to cloud computing & vehicular networks. Security challenges that are specific to Vehicular Clouds are identified. Example challenges of authentication of high-mobility vehicles, scalability, single interface, tangled identities, locations updates, and the complexity of establishing trust relationships among multiple players caused by intermittent short-range communications. The most problem is vehicle information about the tracking vehicle's place and time updates. To overcome the above existing problem, new parallel hybrid genetic algorithm. The excellent performance of the proposed approach indicates its potential to be applied in real world applications, running on cloud computing servers.**

Keywords: Vehicular Cloud, Certificate Authority and Virtual Machine

I. INTRODUCTION

In an effort to help their vehicles compete in the marketplace, car and truck manufacturers are offering increasingly more potent onboard devices, including powerful computers, a large array of sensors, radar devices, cameras, and wireless transceivers. These devices cater to a set of customers that expect their vehicles to provide seamless extension of their home environment populated by sophisticated entertainment centers, access to internet, and other similar wants and needs. Powerful onboard devices support new applications, including location-specific services, online gaming, and various forms of mobile infotainment.

In spite of the phenomenal growth of third-party applications catering to the driving public, it has been recently noticed that, most of the time, the huge array of onboard capabilities are chronically underutilized. In a series of recent papers, Olariu and his co-workers have put forth the vision of vehicular clouds (VCs), a nontrivial extension of conventional cloud computing, intended to harness the excess capabilities in our vehicles.

Vehicular Cloud Computing is a new technological shifting, which takes advantage of cloud computing to serve the drivers of VANETs with a pay as you go model. Thus, the objectives of VCC are to provide several computational services at low cost to the vehicle drivers; to minimize traffic congestion, accidents, travel time and environmental pollution; and to ensure uses of low energy and real time services of software, platforms, and infrastructure with QOS to 326 Md. Whaiduzzaman et al. / Journal of Network and Computer Applications 40 (2014) 325–344 drivers (Gerla, 2012). VCC can address the convergence of ITS and the tremendous computing and storage capabilities of MCC. Furthermore, VCC provides a technically feasible incorporation of the ubiquitous sensing of WSN, ITS and MCC for better road safety and secured intelligent urban traffic systems

Obviously, security and privacy issues need to be addressed if the VC concept is to be widely adopted. Conventional networks attempt to prevent attackers from entering a system. However, in VC, all the users, including the attackers, are equal. The attackers and their targets may be physically collocated on one machine. The attackers can utilize system loopholes to reach their goals, such as obtaining confidential information and tampering with the integrity of information and the availability of resources. Fig. 1 shows one possible example of tampering with the integrity of information in the case of a road accident. Imagine that an accident has occurred at an intersection, and the accident will be reported to the VC. The driver liable for the accident can invade the VC and modify the accident record. Later, when the law enforcement or the vehicle insurance company queries the accident, they cannot link the accident to the driver who caused it.

II. RELATED WORKS

Toward Cloud-based Vehicular Networks with Efficient Resource Management: Vehicular networks are in the progress of merging with the Internet to constitute a fundamental information platform which is an indispensable part of Intelligent Transport System (ITS). This will eventually evolve into all vehicles connected in the era of Internet of Things (IoT). By supporting traffic-related data gathering and processing, vehicular networks is able to notably improve transport safety, relieve traffic congestion, reduce air pollution, and enhance driving comfort ability. It has been reported that, in Western Europe, 25% of the deaths due to car accidents could be reduced by deploying safety warning systems at the highway intersections. Another example is that real-time traffic information could be collected and transmitted to data center for processing, and in return, information could be broadcasted to the drivers for route planning. City traffic congestion is alleviated and traveling time is reduced, leading to greener cities.

A variety of information technologies have been developed for intelligent vehicles, roads, and traffic infrastructures such that all vehicles are connected. Smart sensors and actuators are deployed in vehicles and roadside infrastructures for data acquisition and decision. Advanced communication technologies are used to interconnect vehicles and roadside infrastructures, and eventually access to Internet. For instance, Dedicated Short Range Communications (DSRC) is specifically designed for Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) communications.

The IEEE 802.11p, called Wireless Access in Vehicular Environments (WAVE), is currently a popular standard for DSRC. Besides, the Long-Term Evolution (LTE), LTE-Advanced and Cognitive Radio (CR) are all fairly competitive technologies for vehicular networking. Despite of the well-developed information technologies, there is a significant challenge that hinders the rapid development of vehicular networks. Vehicles are normally constrained by resources, including computation, storage, and radio spectrum bandwidth. Due to the requirements of small size and low-cost hardware systems, a single vehicle has limited computation and storage resources, which may result in low data processing capability. On the other hand, many emerging applications demands complex computation and large storage, including in-vehicle multimedia entertainment, vehicular social networking, and location-based services. It becomes increasingly difficult for an individual vehicle to efficiently support these applications. A very promising solution is to share the computation and storage resources among all vehicles or physically nearby vehicles. This motivates us to study the new paradigm of cloud-based vehicular networks. Recently, a few research works are reported to study the combination of cloud computing and vehicular networks. In the concept of Autonomous Vehicular Clouds (AVC) is proposed to exploit the under-utilized resources in vehicular ad hoc networks (VANETs).

A Cloud-Assisted Design for Autonomous Driving: Recently, much research has been focused on developing autonomous vehicles. Such systems aim to navigate along an efficient and safe path from a source to destination, in the presence of changes in the environment due to pedestrians and other obstructions. Further, these systems need to deal with unexpected events such as road-blocks, traffic and accidents. Thus, autonomous vehicles need detailed and real-time information about their surroundings.

Typically, they use on-board sensors such as laser range-finders to build a *3D point-cloud* representing the 3D (x, y, z)-coordinates of points on the surface of obstacles. However, such sensors cannot deliver vehicles information about hidden obstacles which are not directly in their line-of-sight, such as pedestrians hidden from view at an intersection. Further, these sensors are limited in range, and hence cannot report long-range data with sufficient accuracy; thereby limiting the vehicle's ability to plan ahead. For these reasons, the report from the DARPA Urban Challenge identifies the need for autonomous vehicles to have access to each other's information as a key lesson learned from the contest.

Toward Reliable Off Road Autonomous Vehicles Operating in Challenging Environments: The potential applications of robotic ground vehicles have long been recognized. Off road mobile robots must operate effectively under forest canopy which occludes positioning satellite signals while the trees themselves present natural mazes to challenge motion planning. They must function in alpine areas where terrain slopes require safe operation in constant proximity to tip over, while precipitous ledges persistently threaten to end the mission in an instant.
They must function in fields and forests where ground covering vegetation obscures both the shape of the ground and any occluded hazards. In short, off road autonomy is among the most ambitious of our aspirations for mobile robot technology. Much of the work to date has been motivated by military and space applications although agriculture mining and forestry have received more recent attention.

The system described in this paper has evolved from local and global planning systems that we developed for the Demo II program. Unlike most or perhaps all historical work on outdoor autonomous mobility, the PerceptOR program emphasizes independently administered evaluative testing as the primary mechanism to drive progress. The overall goal has been to Tests are conducted on an unrehearsed basis, meaning the development team has no detailed knowledge of specific terrain before the test. While the development team may see the test courses during the conduct of the tests, individuals who operate the system are prevented from seeing the test courses until all tests are complete. The overall intent is to simulate the conditions of actual deployment of UGVs. This paper outlines the final design of the system produced by the CMU PerceptOR team, results achieved, and some of the most immediate challenges that remain to be addressed simultaneously maximize autonomy, reliability, and speed.

An Overview of Emerging Results in Networked Multi-Vehicle Systems: There are many applications where "coordinated" control of multiple vehicles or systems is desirable, e.g. automotive vehicles in various stages of automation ranging from automated highway systems to coordinated adaptive cruise control systems , to "platooning" of passenger and military vehicles.

Also, there is a trend in the military towards autonomous air and underwater vehicles; these vehicles perform coordinated missions and require some communicated information among them. Some of these applications include coordinated ocean platform control for the Mobile Offshore Base (MOB), coordinated operation of several Autonomous Underwater Vehicles (AUVs), and/or of Unmanned Combat Air Vehicles (UCAVs). Currently, there exists no unified theory to aid in the design of networked multi-vehicle systems. Analytical techniques to deal with crucial issues such as coordination mechanisms, maneuver design, control strategies and performance, communication system, overall architecture design and implementation are not readily available to the control or

communication systems designer. It is currently not possible to specify performance and stability requirements for a closed loop system where some of the loops are closed by communicated variables [1]. The goal of this paper is to discuss some emerging results in the area of networked multi-vehicle systems. It is clear that the number of these types of systems will be increasing exponentially as the wireless revolution continues and new control and communications techniques are developed.

III. Proposed Work

AES DEAL ALGORITHM

Proposed new parallel hybrid genetic algorithm for update the vehicle place and time information's. Public Key Infrastructure (PKI) and digital signature-based methods have been well explored in VANETs. A certificate authority (CA) generates public and private keys for nodes. The purpose of digital signature is to validate and authenticate the sender. The purpose of encryption is to disclose the content of messages only to entitled users. PKI is a method that is well suited for security purposes, particularly for roadside infrastructure. The receiving vehicles must be physically present in a certain geographic region specified by the sender to be able to decrypt the message.

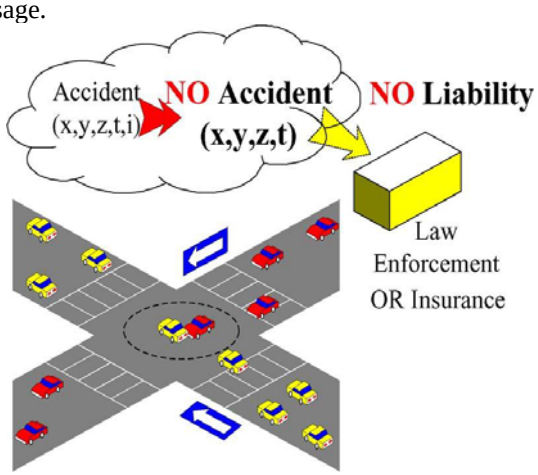

Figure 1 Issues in vehicular clouds

Vehicular networking has become a significant research area due to its specific features and applications such as standardization, efficient traffic management, road safety and infotainment. Vehicles are expected to carry relatively more communication systems, on board computing facilities, storage and increased sensing power. Hence, several technologies have been deployed to maintain and promote Intelligent Transportation Systems (ITS). Recently, a number of solutions were proposed to address the challenges and issues of vehicular networks. Vehicular Cloud Computing (VCC) is one of the solutions.

VCC is a new hybrid technology that has a remarkable impact on traffic management and road safety by instantly using vehicular resources, such as computing, storage and internet for decision making. This paper presents the state-of-the-art survey of vehicular cloud computing. Moreover, these schemas present a taxonomy for vehicular cloud in which special attention has been devoted to the extensive applications, cloud formations, key management, inter cloud communication systems, and broad aspects of privacy and security issues. Through an extensive review of the literature, we design architecture for VCC, itemize the properties required in vehicular cloud that support this model. We compare this mechanism with normal Cloud Computing (CC) and discuss open research issues and future directions. By reviewing and analyzing literature, we found that VCC is a technologically feasible and economically viable technological shifting paradigm for converging intelligent vehicular networks towards autonomous traffic, vehicle control and perception systems.

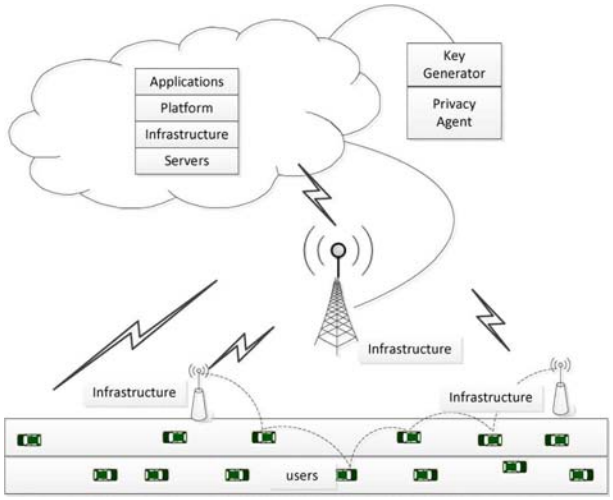

Figure 2 Privacy agent and key generator

Terminal -1

The terminal-1 is act as a server and performing the task of starting terminal point. It's also handling another process (i.e.) public key process. These public key was send to the agent. Public key must be need for agent monitoring. Agent could act individually. Server sent public key to the agent then after agent doing all the process.

Terminal-2

The terminal-2 process act as second reaching place of the vehicle cloud computing network system. Then terminal -1 point reach the terminal-2 then after some second waiting after data going to termina-3.

Terminal-3

The terminal-3 process of act as third reaching place of the vehicle cloud computing network system. Then terminal -1 point reaches the terminal-3.

Terminal-4

The terminal-4 process of act as end of place of the vehicle cloud computing network system. Then terminal -1 point reaches the terminal-4.

Agent monitoring:

The agent monitor control the all the process of client terminal. It provides the security process of the client authentication. It provides private key authentication for each and every client terminals. It provides the random key generation network. That key using only one time another process is not using.

IV. METHODOLOGY

Vehicular network design

To design vehicular network by using the cloud computing system with several terminal and Vehicular network agent system.

Initializing location

To initializing the location of transmitting vehicular information's from source terminal to destination terminal.

Vehicular network agent monitoring

Agents are use to monitoring the process of transmitting vehicular information's from source terminal to destination terminal.

Implementing security process

A certificate authority (CA) generates public and private keys for each terminal and digital signature is used to validate and authenticate the sender.

Location and time status updates

To update location and time information's about the transmitting vehicular information's.

Accident tracking system

To tracking accident information during the transmitting vehicular processes with time and place where it held.

V. EXPERIMENTATION & RESULTS

It is important to allow the VC to dynamically configure the security protocols and to independently replace security strategies. We will start with the configuration of security protocols and then describe an intelligent task management method.

More Vehicles Involved, More Secure Cloud Needed: The cloud will provide vehicles a single system image that is trans-parent of details of security scheme changes. As vehicles are dynamically moving in and out of a cell, the security protocols of a cell in its virtual machine need to be dynamically adjusted. We observe the fact that the more vehicles are involved, the more secure and the stricter a protocol should be. Similar facts can be found in daily life. Airports are often crowded, and security is often stricter than that in many other places. Events such as football games, auto races, and air shows often attract more people, as well as more policemen who patrol the area more often to ensure the security of attendees.

Therefore, it is important to know the expected volume of vehicles at any time to dynamically switch security protocols. We are interested in the following problem to evaluate the expected number of vehicles at any given time. Consider a cell with finite capacity N. At time $t= 0$, the cell contains $n_0 \geq 0$ cars. After that, cars arrive and depart at time-dependent rates, as described next. If the cell contains k, $(0 \leq k \leq N)$ cars at time t, then the car arrival rate $\alpha_k(t)$ is

$$\alpha_k(t) = {}^{N-k}\lambda(t)\, N$$

and the car departure rate $\beta_k(t)$ is

$$\beta_k(t) = k\mu(t)$$

where, for all $t \geq 0$, $\lambda(t)$ and $\mu(t)$ are *integrable* on $[0,\ t]$. It is worth noting that both $\alpha_k(t)$ and $\beta_k(t)$ are functions of both t and k. In particular, it may well be the case that, for $t_1=t_2$, $\alpha_k(t_1)= \alpha_k(t_2)$, and similarly for $\beta_k(t_1)$and $\beta_k(t_2)$, giving a mathematical expression to the fact that, at different times of the day, for example, the departure rate depends on not only the number of cars present in the cell but on the time-dependent factors as well.

Consider the counting process $\{X(t)|t \geq 0\}$ of continuous parameter t, where, for every positive integer k, $(1 \leq k \leq N)$, the event $\{X(t) =k\}$ occurs if the cell contains k, cars at time t. We let $P_k(t)$ denote the probability that the event $\{X(t) =k\}$ occurs. In other words

$P_k(t) = \Pr[\{X(t) = k\}]$.

To make the mathematical derivations more manageable, we set $P_k(t) = 0$ for $k < 0$ and $k > N$. Thus, $P_k(t)$ is well defined for all integers $k(-\infty,\infty)$ and for all $t \geq 0$. In particular, the assumption about the cell containing n_0 cars at $t= 0$ translates into $P_k(0) = 1$ if $k=n_0$ and 0 otherwise. Let t, $(t \geq 0)$, be arbitrary, and let h be sufficiently small such that, in the time interval $[t,\ t+h]$, the probability of two or more arrivals or departures, or of a simultaneous arrival and departure, is $o(h)$. With h chosen as stated, the probability $P_k(t + h)$that the cell contains $k,(0 \leq k \leq N)$cars at time $t + h$ has three components.

1) $P_k(t)[1- h(N - k/N)\lambda(t)- kh\mu(t) + o(h)]$.
2) $P_{k-1}(t)[h(N - k +1/N)\lambda(t) + o(h)]$.
3) $P_{k+1}(t)[(k +1)h\mu(t) + o(h)]$.

Enhancing Scalability of Security Schemes: When vehicle population increases in a certain area, not only the scalability of the VC but also the scalability of security schemes becomes a tough problem. In our cloud model, the scalability of the security scheme can be enhanced by a virtual machine division algorithm, a highly scalable algorithm. When the number of access of a virtual machine grows sufficiently large, compared to an empirical threshold, the virtual machines (as a super-VM) will divide itself into multiple sub virtual machines (as sub-VMs). Each virtual machine will obtain the same amount of resources as the original super VM. The middleware of the super VM can randomly forward request to sub virtual machines to load balance. The middleware of the super VM also caches the most recently accessed and frequent information. It caches and executes information such as frequently asked questions (FAQs) and answers. If access from a vehicle hits the FAQ, the middleware directly sends back the answer. If the access misses the FAQ, the middleware then forwards access to a relatively idle VM. This can further reduce the workload of sub-VMs

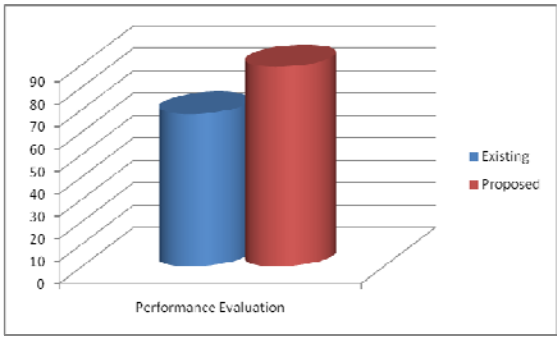

Fig 3. Result Analysis

This Fig 3. shows the comparison growth between existing and proposed work. In the proposed, we introduced encryption to check the certificate authority to ensure the process of vehicle cloud environment

VI. CONCLUSION

We have first introduced the security and privacy challenges that VC computing networks have to face, and we have also addressed possible security solutions. Although some of the solutions can leverage existing security techniques, there are many unique challenges. For example, updating vehicular location and time status. The vehicles have high mobility, and the communication is inherently unstable and intermittent. We have provided a directional security scheme to show appropriate security architecture that handles several, not all, challenges in VCs.

REFERENCES

[1] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle , Security Challenges in Vehicular Cloud Computing, Vol-14 No-1 Mar 2014.

[2] Boyang Wang "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," IEEE Trans. State Key Lab of Integrateed Service Network Xidian Univ, ., Xi'an, China, Jan2014.

[3] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, and I. Khalil, "Datacenter at the airport: Reasoning about time-dependent parking lot occupancy," IEEE Transactions on Parallel Distribution system, 2012.

[4] S. Olariu, M. Eltoweissy, and M. Younis, "Toward autonomous vehicular clouds," ICST Trans. Mobile Communication. Computing volume11, no. 7–9, pp. 1– 11, 2011.

[5] S. Olariu, I. Khalil, and M. Abuelela "Taking VANET to the clouds," Int. J. Pervasive Computing Communication., volume. 7, no. 1, pp. 7–21, 2011, 2011.

[6] G. Yan and S. Olariu, "A probabilistic analysis of link duration in vehicular ad hoc networks," IEEE Trans. Intelligent. Transaction System, vol. 12, no. 4, pp. 1227–1236, 2011.

[7] Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hoc networks," IEEE Wireless Communication., volume. 16, no. 6, pp. 48–55, 2009.

[8] GL. Li, J. Song, F.-Y. Wang, W. Niehsen, and N. Zheng, "IVS 05: New developments and research trends for intelligent vehicles," IEEE Intelligent systems, volume. 20, no. 4, pp.10–14, 2005.

[9] G. Yan, S. Olariu, and M. C.Weigle, "Providing VANET security through active position detection," Comput. Commun., vol. 31, no. 12, pp. 2883– 2897, Jul. 2008, Special Issue on Mobility Protocols for ITS/VANET.

[10] D. Huang, S. Misra, G. Xue, and M. Verma, "PACP: An efficient pseudonymous authentication based conditional privacy protocol for vanets," IEEE Trans. Intell. Transp. Syst., vol. 12, no. 3, pp. 736–746, Sep. 2011.