Using Trusted Platform Module (TPM) to Secure Business Communciation (SBC) in Vehicular Ad hoc Network (VANET)

Irshad Ahmed Sumra, Halabi Bin Hasbullah
Computer and Information Sciences Department
Universiti Teknologi PETRONAS, Malaysia.
isomro28@gmail.com

***Abstract* — Safety of human life during journey is one of most important objective of intelligent transportation system (ITS). Potential safety and non -safety applications of vehicular ad hoc network (VANET) also provides safety of human lives and also comfort passengers during their journey. Comfort applications are also provided entertainment services to users and make journey more enjoyable. Comfort applications provide opportunities for business parties to setup their business near the highway. So in this paper, we are presenting the secure business communication (SBC) model and explain the components of proposed model. TPM is a security hardware module and it is used inside the smart vehicle. TPM is a core component of proposed SBC model and it will ensure secure communication between user and business parties in VANET. The core objective of secure business communication (SBC) in VANET is to serve the end users through potential applications of VANET.**

Keywords- Intelligent Transportation System (ITS), Comfort applications, secure business communication (SBC) Trusted Platform Module (TPM),

I. INTRODUCTION

One specially designed form of these networks is known as the Vehicular Ad Hoc Network (VANET). The VANET is considered to be a subset of MANET (Mobile Ad hoc NETwork) and in VANET, the vehicles are the nodes which travel in patterns that are more regular and fast. However, VANETs possess unique features which are quite different from MANET [1]. Safety application is the most important application of vehicular network because it is directly related to users and due to human life saving factor, its priority is high as compare to non-safety application. The main purpose of safety application is to provide safety of vehicles and its passengers from road accidents. Non safety applications are used to comfort passengers during their journey and to improve the traffic system. Comfort applications are also provided entertainment services to users and make journey more enjoyable. These applications should not interfere with other safety related applications of network. Both types of applications use wireless medium for communication which is called DSRC. Dedicated Short Range Communication (DSRC) [2] is a frequency spectrum and it is used for vehicle-vehicle and vehicle-roadside wireless communication. These applications provide opportunities for business parties to setup their business near the highway such as announcement of services; Parking availability and toll collection are some of the non-safety application of vehicular network [3]. There are great opportunities for Business parties to establish their business and more journey more enjoyable for end users. Govt. authorities give more benefits for business parties to invest their money in this field. Business parties also consider the user requirements while their journey and provide those services which is more necessary for end users. Services provider also consider this important point while providing service, safety application will not disturb through these business services. Figure 1. Shows the basic architecture of VANET.

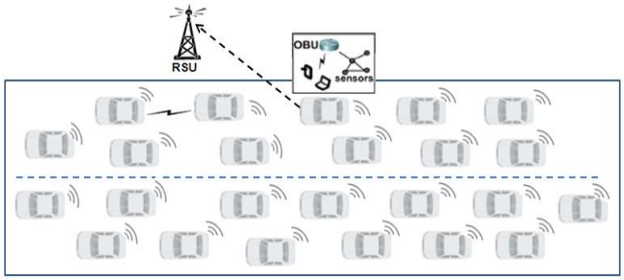

Figure 1. Basic architecture of VANET

Table 1. Provides the detail of safety and non-safety applications in DSRC communication channels. Total seven channels used for applications and four channels are dedicated for non-safety application in DSRC frequency spectrum.

This paper is divided into three sections; Section II provides list of non-safety applications in VANET. Section III discuss in detail the proposed secure business communication (SBC) model for vehicular network and this model is consisting of four modules. Govt. Authorities, Business parties (service providers), TPM and end users are four basic modules of SBC model. TPM plays a key role to ensure the secure business communication between user and business parties in VANET. Conclusion and future work is described in the last Section IV.

II. VANET NON-SAFETY APPLICATIONS

Here is provided the detail descriptions of non-safety applications in VANET [4].

- *Parking Slot Services*

Finding an appropriate parking place near shopping malls, restaurants and sport complexes is a difficult task. This application provides information regarding empty parking slots in a specific geographical area. It provides the

safety of your vehicle and save your time by finding an appropriate parking place in the shopping malls, restaurants and sport complexes.

- *Toll Collection Services*

Toll collection is the time consuming task on the highway where hundreds of vehicles pass through a toll collection point. VANET makes it easier as one can pay the toll without stopping his/her vehicle. The vehicle passes by the toll point and the toll collection point scans the Electrical License Plate (ELP) of the vehicle and issues the receipt message. The toll amount, time and location are mentioned in the receipt message.

- *Services offering Messages*

It provides services in a specific range and passes messages to near users about the restaurant, shopping mall, gas station, and hotel while traveling on the highway. Stationary gateway will be developed for sending such kinds of marketing information (restaurants, shopping mall) to highway users.

- *Map Download Services*

It is type of portal that provides valuable information about a certain area where you are driving. Maps are available and can be downloaded from mobile hotspots area or home station about the specific location. This service is very helpful for the tourist to find some tourist places in specific region.

- *Entertainment Service*

During your journey if you are interested to watch any movie or favorite program you can ask for ES of his favorite movies or any other program. These types of VANET applications make your journey more enjoyable than in the past.

Table 1. DSRC Channels with VANET Application Types

Frequency Band	**Channels**	**Channel Types**	**Application Types**
5.855 -5.865	CH 172	Safety of life, Accident avoidance(V2V)	Safety Application
5.865-5.875	CH 174	Service Channel	**Non Safety Application**
5.875-5.885	CH 176	Service Channel	**Non Safety Application**
5.895-5.905	CH 180	Service Channel	**Non Safety Application**
5.905-5.915	CH 182	Service Channel	**Non Safety Application**
5.885-5.895	CH 178	Control Channel	Safety Application
5.915-5.925	CH 184	Public safety, High power and long range	Safety Application

III. PROPOSED SBC MODEL

Figure 2 explains the proposed SBC model for business communication in future vehicular network. Proposed model consist of three modules and it is necessary these three modules work properly and serves end user and makes their journey more comfortable.

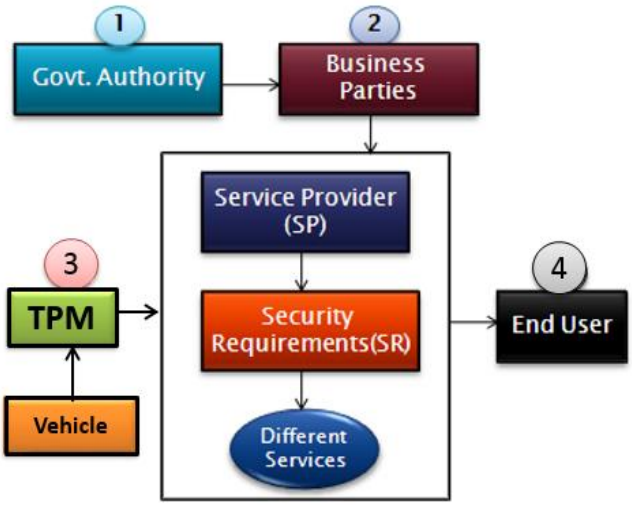

Figure.2 Proposed SBC Model

1. Govt. Authority (GA)

Govt. authority (GA) is the first module of business model it is responsible for providing authentication services for users using secure public and private keys, whether permanent or temporary based on the type of services on highway. GA provides these keys for secure communications between vehicles and infrastructure. Private Trusted Authority (PTA) is also the part of government authorities. Different types of service providers serve various types of users and applications that are heterogeneous. PTA ensures secure communications between users and different types of service providers by using the keys which involve key distribution and key management. PTA defines their own rules for key generation to serve users. Typically, one key is assigned to one particular service session. Most government will make use of VANET to serve certain criminal cases; i.e. authorized parties (such as police, law enforcement agencies) may use private information to find the criminal person. Govt. authority also gives the license to service provider to facilitate the users. Service provider established their own business setup and defines their own policies to serve the users.

2. Business Parties

a) Service Provider (SP)

Prepaid and Postpaid Packages are two types of business services offered on roads and highways [2]. In prepaid package, users pay money to service provider (SP) before taking any particular service and billing is fixed on the monthly bases. For postpaid services such as telephone

and Internet, users send request to SP for particular service which is authenticated at the entry points of the highway.

b) Security Requirements

A user has a dynamic behaviour and changes his/her behaviour according to the information received from other users or from the roadside unit (RSU). There are two types of users which are given below.

Trusted User: Trusted Users (TUs) are those who perform their task properly in the network. The behaviour of a trusted user may change upon receiving messages from other vehicles or from the RSU. When a trusted user receives an accident warning or traffic jam message, the user is expected to change his/her behaviour, that is, slow down his/her vehicle or change route. Figure 4, describes the situation in which vehicle C sends a warning message to other vehicles (D, E). As a result, the users of vehicles D and E slow down their speeds and may take an alternative route due to the accident warning message.

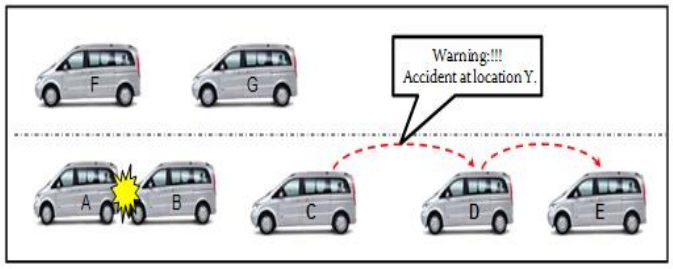

Figure 4. Trusted User Behaviour

Non-Trusted users (Attacker): Attackers are those who intentionally create problems for users in a network by launching different types of attacks (passive or active). In a vehicular network, they become more prominent because they can potentially change a critical message or broadcast a wrong message to other vehicles.

Malicious user (MU): A malicious user [14] has the potential of becoming an active attacker who would begin initiating various and possibly high intensity attacks in the network. A few such high intensity attacks are the Sybil attack, Denial of service attack (DoS) and sending false messages in network. Figure 5, presents an entire scenario where node X is the attacker who can wreck a message's integrity or change what is said in the message. The original message, for example, might read "Parking slot available" but when the attacker, vehicle X, receives the message from the node A, he/she alters the message content and transmits the altered message which reads "No empty parking slot:!!!" to other vehicles in the network. Because of the new message, the other vehicles (B, E and F) have to change their plans accordingly.

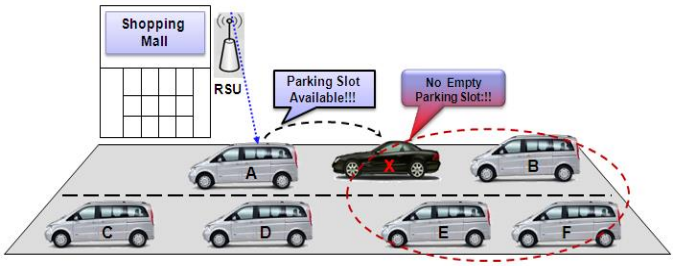

Figure 5. Attacker sending wrong non-safety messages

As stated before, malicious programs can also be sent by the attacker directly to a user or the malicious program is downloaded by a user from an infected RSU while their software is being updated. In another attack, the attacker changes the message that is exchanged in the communication of V2V or V2R. There are two cases possible for this situation:

- Falsify Transaction Application Request: A malicious user sends an application transaction request to the business transaction component close to the RSU but the request is false. The attackers usually use this type of request in applications that are non-safety related. Figure 6 presents a scenario where node X is an attacker who transmits false message request "Toll collection" to the RSU and that RSU is not dealing such kind of services in network.

- Forge Response: A forge response happens when an RSU acts unexpectedly in response to a user's communication with it. As can be seen in Figure 6, user B attempts to communicate with an RSU; he/she tries to send his/her personal data to take some service but instead, the RSU replies with a forge response. It just refuses the message and claims that it contains incorrect data.

Business parties should meet these security requirements while serve the user during their journey. So here we are discussing some security requirements which are necessary for business transactions [3, 4,15].

- *Confidentiality* is an important security requirement in vehicular communication. Confidentiality is requiring for all business application and also personal data need to protect for financial transaction

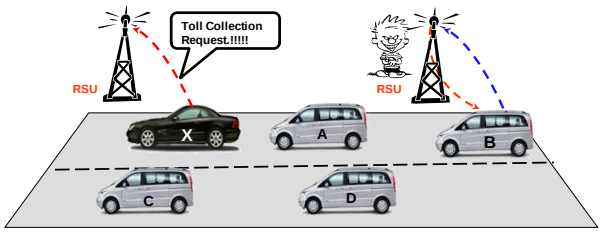

Figure 6. Message tampering attack

- *Data integrity*: While communicating with an RSU and using non-safety applications, if an attacker changes the content of the messages then it would be business lost. For example, in a toll collection application an attacker changes the content of the users' information (vehicle Id, Location), and then the users are not able to pay the toll during their journey.
- *Authentication:* Authentication is the key security requirement and it ensures that all vehicles in a network which are involved in communication are authentic. Authenticity of user is the key security requirement in vehicular network and it is directly concern with who is sending safety and non-safety messages into network. VANET applications serve only authentic users and hence User Authentication must be done.
- *Availability:* Availability is one of the hot research topics in vehicular communication. The purpose of a vehicular network is to serve the users. Business parties establish their network along highway, but when user makes communication with server, it could be busy and user could not serve. It is business losses and other business party takes benefits from this problem.
- *Privacy:* Privacy is also major factor in non-safety applications. User information (driver name, location, vehicle ID) is some of the privacy information and user do not open this privacy information while making monetary transaction.
- Access Control: In a vehicular network, it is necessary for an authorized party to define the network policies, roles and privileges of the vehicles in order to access the network. Access control policies can be implemented in non-safety applications and some applications are free and some applications require payment for using that particular service in network. So, the administration can define some policies for RSU and if a user meets the basic requirement of these policies, it can access all services in that area of network.
- Real Time Guarantee: The dynamic number of users, high mobility of vehicles and dynamic topology of a network are some of the very important factors in a vehicular network. Safety and non-safety both types of applications are time sensitive applications and users need the right information at the right time.

c) Difference Services

Here we are giving the detail of some of the important services which will be provided in future vehicular network [5].

- *Toll Collection Services*
- *Parking Slot Services*
- Internet Access *Services*

3. TPM-Trusted Platform Module

A smart vehicle has an important role to perform the secure communication in a network and smart vehicle is a combination of several mechanical components with the ability to perform computations. Security is provided by both the hardware and software working together; however, the most important role in a smart vehicle is played by the hardware. For secure communication in VANET, the role of these security hardware modules is very prominent and has achieved the maximums level of security in VANET. Event Data Recorder (EDR) Tamper Proof Device (TPD) and Trusted Platform Module (TPM) are some of the security modules which are used in VANRT for secure communications. Trusted computing is a relatively new technology which has gained popularity recently, and the Trusted Computing Group (TCG) [16, 17] has been the main proponent of this technology. The main aim of TCG is to enhance security in computer networks by using a security hardware module (called the Trusted Platform Module). The cost factor is lower as compared of TPD and it has many functional components that perform the cryptographic capabilities. SHA-1 Engine, RSA and Random Number Generator (RNG) are the key modules that perform the cryptographic functions. Figure 7 shows the basic architecture of the TPM and smart vehicle [7, 8, and 9].

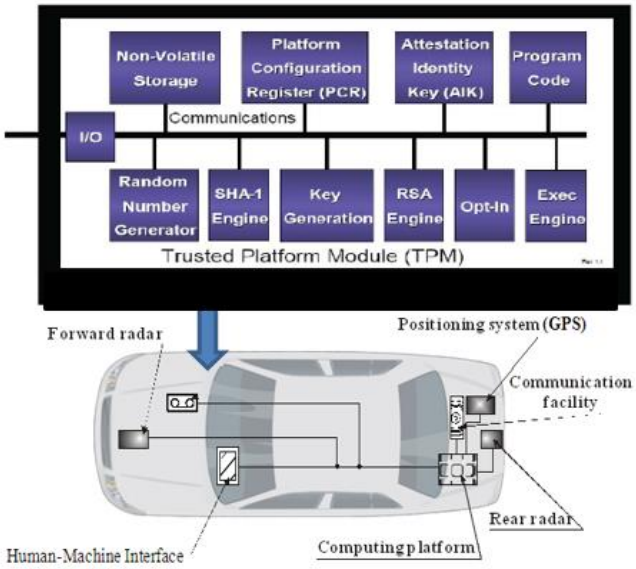

Figure 7. TPM with smart vehicle [12]

Endorsement Key (EK): The Endorsement Key (EK) [12,18] is a 2048-bit key pair, the public key being the PUBEK and the private key being the PRIVEK. The EK is actually generated by the manufacturer and put into the TPM prior to its placement in a platform, as it is used during validity testing for the TPM. The PRIVEK serves as the main private key for the TPM. As such, its exposure outside of the TPM would invalidate the TPM's entire security

capability. Thus, it remains shielded at all times. Any computation done with the PRIVEK must be done inside the TPM. The PUBEK does not present a security concern. However, if it is associated with some kind of personal information such as a platform identifier (e.g. the EK or an AIK, which will be explained shortly), it can become personally identifiable information. This is a major privacy concern, so the association of PUBEK with personal information should be controllable by the user.

Attestation Identity Key: An Attestation Identity Key is a 2048-bit RSA key that aliases the EK. It is used for signing data that is generated internally to the TPM but may be available outside. The EK cannot be used for this due to security reasons and privacy concerns. A "virtually unlimited" number of AIK can be generated by the TPM [13, 19].

4. End User

End user is the last module of business model and purpose of this model to provide entertainments services and makes their journey more enjoyable. With passage of time user requirement will be change and service provider upgrade their system and meet end user requirements in future vehicular network.

IV. WORKING MECHANISM OF SBC

There are two different scenario are given below to describe the working mechanism of proposed SBC model in VANET.

- **Scenario One: Internet Access (ISP)**

The scenario one in Figure 8 shows vehicle A sending a request for access to the Internet while on the road, then the authentication and billing servers both authenticate the user with his/her billing information. Upon receiving the authentication, the server of ISP collects other data such as the speed, location and travelling direction of the vehicle making the request. If all of the requirements are satisfied by the user of the vehicle, the server of ISP allows the user to access the road services that have been requested. Another vehicle, C, could also send a request for some other service, which would require the same procedure to be followed in order to provide the service requested. While communication in network, TPM ensure the user personal information and also provides security from attacker.

1. User (A) send message (MSG) to ISP and this message contains all users' informations with security TPM key.
2. ISP server check the user information (location, valid TPM security key).
3. ISP check the user information and if information is valid and meet the ISP requirement and policies.
4. Then ISP is allow to take services from ISP server.
5. Start the communications between user (A) and ISP server.

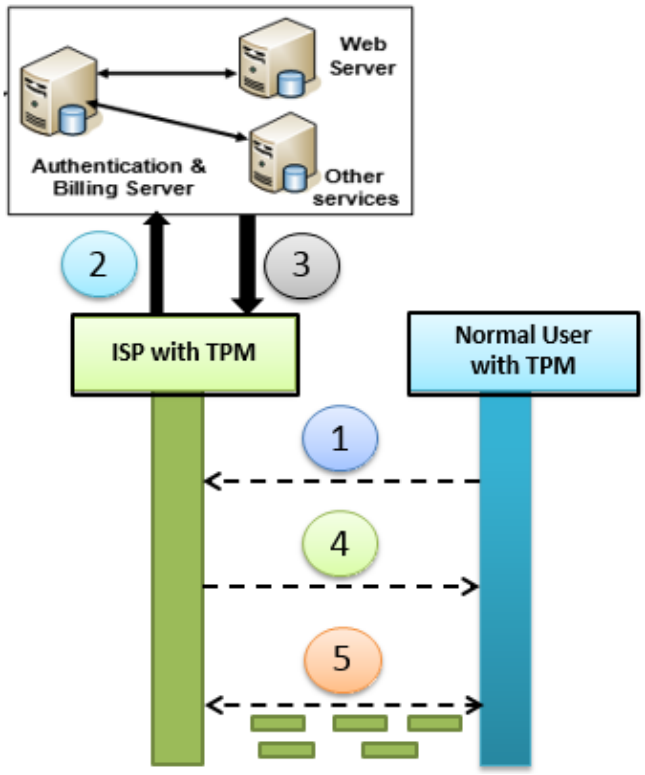

Figure 8 Authentication in Business Communication

- **Scenario Two: Toll Collection Center (TCC)**

Toll collection is a time consuming task on the road. VANET makes it easier as one can pay toll without stopping vehicle. One such toll collection mechanism is whereby vehicles pass from the toll point to another toll collection point which has a Electrical License Plate (ELP) scanner that scans plate numbers and issues the receipt message. Toll charge, time and location are included in the receipt message . Each vehicle has a TPM module and send request to toll collection centre (TCC) and pays required amount. Scenario two explains in Figure 9,where the vehicles (A, D, E) send request to toll collection center for payment of their toll charges.

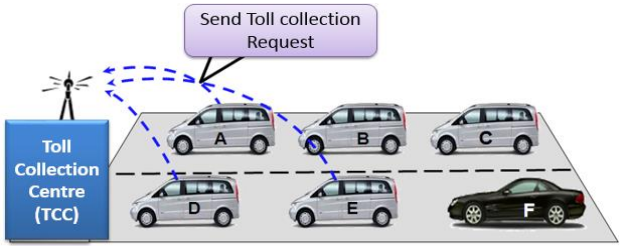

Figure 9 Vehicles send request to toll collection centre (TCC)

V. CONCLUSION AND FUTURE WORK

VANET potential applications directly focus on user's life on the road by sending some safety messages and non-safety messages. In propose model it is explained three modules of business model and explain the relationship of each modules. For successful implementation of business model every module plays their role accurately and serves the end users. Security and privacy is most important factors for real implementation of business model. More study is require to define some business polices for service providers.

REFERENCES

[1] M. L. Sichitiu and M. Kihl, "Inter-Vehicle Communication Systems: A Survey," *IEEE Commun. Surveys Tutorials*, vol. 10, no. 2, pp. 88–105, 2nd Quarter 2008.

[2] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, R. Herrtwich "Design of 5.9GHz DSRC-based vehicular safety communication",Wireless Communications IEEE Vol. 13, No. 5. (2006), pp. 36-43.

[3] Y. Qian, and N. Moayeri, "Design of Secure and Application Oriented Vanets"Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE ,11-14 May 2008, Singapore.

[4] Mishra, B., et al. *Security in vehicular adhoc networks: a survey*. in *Proceedings of the 2011 International Conference on Communication, Computing & Security*. 2011. ACM.

[5] M.Raya, J.Pierre, Hubaux, "Securing vehicular ad hoc Networks", journal of computer security,vol.15, issue no.1 January 2007, pp: 39-68.

[6] Antonios Stampoulis (antonios.stampoulis@yale.edu), Zheng Chai: A Survey of Security in Vehicular Networks.

[7] M. Ghosh, S. Goswami, "IntelligentTransportation using VANET"Access date, 20 auguest 2012,http://pcquest.ciol.com.

[8] J.-P. Hubaux, S. Capkun, J. Luo, "The security and privacy of smart vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49–55, 2004.

[9] M. Raya, J. P. Hubaux. "Security aspects of inter-vehicle communications", in Proceedings of Swiss Transport Research Conference (STRC), Ascona, Switzerland, March 2005.

[10] M. Raya, P. Papadimitratos and J.P. Hubaux, "Securing Vehicular Communications," IEEE Wireless Communications Magazine, vol. 13, no. 5, Nov 2006, pp. 8-15.

[11] F. Kargl, T. Nowey, C. Mletzko, "Towards a Security Architecture for Vehicular Ad Hoc Networks," in Proceedings of the First International Conference on Availability, Reliability and Security (ARES), April 2006.

[12] P. Papadimitratos, V. Gligor, J.-P. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," in Proceedings of Fourth Workshop on Embedded Security in Cars (ESCAR), 2006.

[13] T. Leinmüller, E. Schoch, C. Maihöfer, "Security requirements and solution concepts in vehicular ad hoc networks," in Proceedings of the 4th Annual Conference on Wireless on Demand Network Systems and Services, pp. 84–91, 2007,

[14] G. Guett, C. Bryce,"Using TPMs to Secure Vehicular Ad-Hoc Networks(VANETs)", IFIP 2008, WISTP 2008, LNCS 5019, pp.106-116.

[15] G. Guette, O. Heen, "A TPM-based architecture for improved security and anonymity in vehicular ad hoc networks," Vehicular Networking Conference (VNC), 2009 IEEE , vol., no., pp.1,7, 28-30 Oct. 2009

[16] Samara, G.; Al-Salihy, W.A.H.; Sures, R., "Security issues and challenges of Vehicular Ad Hoc Networks (VANET)," New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on , vol., no., pp.393, 398, 11-13 May 2010.

[17] MA. Moharrum, AA. Al Daraiseh,"Toward Secure Vehicular Ad-hoc Networks: A Survey", IETE Technical Review Journal, Vol 29, issue 01, pp 80-89, Year 2012.

[18] S. Kinney,"Overview of the TPM Architecture", Trusted Platform Module Basics using TPM in Embedded Systems, ch. no.03, pp.26.

[19] A. Reza Sadeghi, "Trusted Computing-Special Aspects and challenges", Lecture Notes Horst-Gortz-Institute(HGI) for IT-Security, Ruha-University Bochum, Germany.2007.

[20] S. Kinney,"Endorsement Key (EK)",Trusted Platform Module Basics Using TPM in Embedded Systems , chapter No.04, , pp No.32.

[21] E.Gallery,"An overview of trusted computing technology", Trusted Computing, Ch no.3, pp.31-32. IEE professional application of computing series 6.