Internet of Vehicles (IOV): Evolution, Architectures, Security Issues and Trust Aspects

Indu, Sibaram Khara

Abstract*: The incessant progression in technology in the field of communication and connectivity has given a paradigm shift leading vehicular Ad-hoc network (VANET) towards internet of vehicle (IOV). This paradigm shift is a result of merging the concept of VANET with internet on things (IOT). Clearly IOT is one of today's tempting technologies and effective VANET is the need of Time. However, to date the concept for internet of vehicles is not fully developed to be deployed as there are various security and trust related issues associated IOV which needs attention. So, in this paper the state of art of IOV is discussed with emphasis on motivation, IOV architectures, security, trust establishment techniques, trust models comparison. Finally, the security challenges for IOV are discussed and future aspects of IOV are envisioned.

***Index Terms*: Internet of Vehicles (IOV); Vehicular Ad-hoc Networks (VANET), Motivation, Internet of Things (IOT), Challenges, IOV architecture, Security, Trust, Trust models.**

I. INTRODUCTION

The automotive technology is continuously growing making remarkable achievements to improve comfort and safety. Every new model of cars introduces bunch of attractive features to improve road safety. Some popular features are high-resolution touch screens, inbuilt 4G Long Term Evolution (LTE) Wi-Fi hotspots, smart phone connectivity, obstacle detector cameras to avoid any collision, lane centering sensors in cars Ford Fusion, Toyota Prius, Lincoln MKZ . But vehicle are still prone to accidents due to high speed, bad weather (rain, fog), human errors, carelessness etc. However this scenario is going to be changed soon as connected vehicles are encouraged by both automotive industry as well as government. In fact the communication between vehicles has now become with the development of VANET. Some foreign car manufacturers for e.g. General Motors have introduced 4G LTE -connected vehicles in 2015 and predicted fully autonomous vehicle by the end of this decade. The LTE connectivity has laid a leading path for the concept of Internet connected vehicles Internet of vehicles is an extension to the concept of VANETs. VANETs serve as a base for the vehicular communication and enhance driving experience by improving various factors like safety, security, infotainment and robustness. Despite increasing traffic safety and driving assistance, VANETs could not gain industrial interest commercially. Various researchers had contributed in exploring its concept but still due to many security and privacy related issues, it has not reached to the deployment stage.

However considerable amount of research in this field has recently shifted from conventional VANET to Internet of Vehicle (IOV)[1]. This shift was realized through merging VANET with the concept of internet on things(IOT)[2]. Clearly internet on things is one most tempting technology these days. However, till now the potential architecture, security framework and trust models for internet of vehicles have not been defined clearly. This paper is dedicated to fill these gaps. The paper is organized as below: Section 2 explains the basic concept and component of IOV network. Section 3 discusses various layered architectures and benefits of IOV network. Section 4 discusses the need of IOV security, security challenges in IOV network and highlights consequent approaches (Encryption and trust based) to achieve security. Sections 5 present the definition and properties of trust in IOV scenario, respectively. Additionally it includes trust establishment approaches and trust models for IOV network. Section 6 presents systematic literature review of the existing trust models. Section 7 includes the performance comparison of trust models. Section 8 provides the conclusion of the review.

II. BASICS CONCEPT OF IOV

The Internet of Vehicle (IOV) is an emerging cyber-physical system that integrates VANETs [3], IOT [4], and the mobile cloud computing. In the IOVs, vehicles are considered as smart objects or nodes, which are equipped with the Internet and wireless networks that enable the smart vehicles to collaborate with each other for data sharing and communications. The smart vehicles also interact with the roadside units[5] and other road users, such as pedestrians and cyclists, to share and gather information on roads and their surrounds. Fig:1 shows the basic concept of IOV. The immense potential benefit that the IOV can offer results into the rapid growth of the IOV market. Gartner forecasts that about one of five vehicles will have some form of a wireless network connection by 2020 [6]. According to a report by Business Insider, there will be over 380 billion connected cars on the road in next five years [7]. Some car manufacturers, such as Mercedes, BMW, and Tesla have already released smart cars with self-driving features. Besides this, the companies such as Google and Uber, are also trying to pioneer the self-driving car. However, the rapid expansion of IOVs also brought some new security challenges.

Revised Manuscript Received on March 20, 2019.

Indu, Research Scholar Galgotias University (GU), Greater Noida, U.P. , INDIA .
Dr. Sibaram Khara, Galgotias University (GU), Greater Noida, U.P., INDIA.

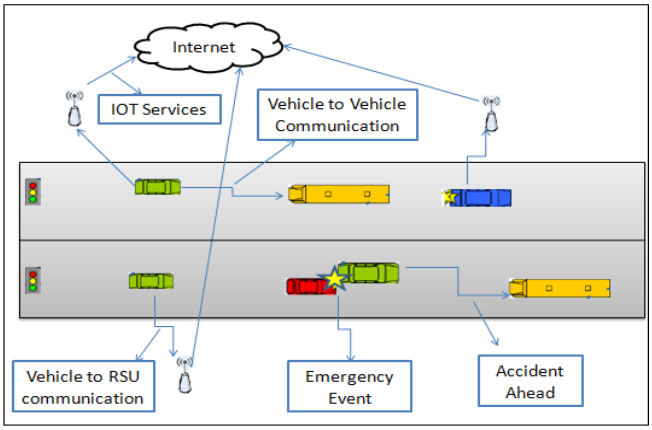

Fig 1: Basic concept of IOV scenario

Since millions of vehicles and IoT devices are interconnected to provide safety in the road, malicious attackers may find IOVs an attractive target for attacks.

Any individual malicious attacker can attack in the IOV environment. Adversaries can exploit the weakness of IOVs, such as insecure communication channels, and can trigger malicious information that causes traffic accidents. Such attacks on a wide scale IOV system can create a massive havoc in the traffic system. Attackers can also use this medium as a means of launching a targeted attack on high-rank officials or military personnel. Indeed, different attacks have been set up in vehicular systems like malware infection affecting the brake and engine of vehicles[8]. Besides that, a large network of compromised smart vehicles can be used to create a strong IOT botnet to take down the Internet. Reliability of the data transmitted (trustworthiness) can also be dubious since the attacker can alter the data transmitted between IOV entities.

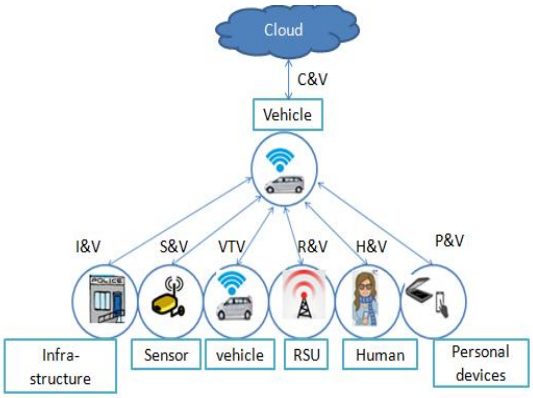

Fig 2: Components of IOV network

A.Components in IOV network

The communication in IOV network includes the following components: Vehicle, Roadside units (RSU), infrastructure, sensors, personal devices and humans which results in seven direct interactions with vehicle as shown in fig2.

Infrastructure and vehicle interaction (I&V)-

I&V interaction allows the vehicle to communicate with the nearby police station, hospital, fire station, gas station in emergency. Moreover cars can communicate with home, office to switch on the devices like AC, blower etc before you drive home.

Sensor and vehicle interaction (S&V)-

In S&V interaction, vehicle will talk to the sensors on signs on bus stops, traffic lights, even with the sensors embedded in the roads to get traffic updates and necessary rerouting alerts. Additionally in vehicle sensors senses the events in its vicinity and provides alert to the vehicles regarding collision avoidance, lane departure. Besides that there are some car engine sensors like massive air flow sensor fuel temperature sensor, engine speed sensor etc.

Vehicle to Vehicle interaction (VTV)-

In V2V interaction, one car will talk to other car directly to exchange the information (regarding passenger in vehicles, brake status, speed, position of vehicle) and driving alerts within a particular range.

RSU and vehicle interaction (R&V)-

In R&V interaction, vehicles can interact with the fixed roadside infrastructures that are connected to the internet and can provide various entertainment related facilities.

Human and vehicle interaction (H&V)-

H&V interaction allows the vehicle to easily communicate with the pedestrian or bicyclists on the way to convey its intention on which people act in turn.

Personal devices and vehicle interaction (P&V)-

In P&V interaction the vehicles communicate with smart devices like phones, laptops, personal digital assistant present in vehicle to collect the information or to access the media of your phone.

Cloud and vehicle interaction (C&V)-

The cloud is the central hub where all of information will pass through. Vehicles have limited computation and storage resources which are not sufficient for emerging applications

Table 1: Comparision of Architectures

Study	Layers	Security	V2V	V&R	V&I	V&P	V&S	R&P	D2D
Liu Nanjie[9]	three	security as service (SAS)	√	√	√	√	×	×	×
F. Bonomi [5]	four	cross layered security (CLS)	√	×	√	×	×	×	×
Wan et al. [10]	three	cross layered security(CLS)	√	√	×	×	×	×	×
Kaiwartya et al. [11]	five	security plain	√	√	√	√	√	×	×
Sejin chun et al. [12]	two	not specified	√	√	×	×	×	×	×
Gandotra et al. [13]	three	not specified	×	×	×	×	×	×	√
Juan and Sherali [14]	seven	security as layer	√	√	√	√	√	√	√

like location based services, in-vehicle entertainment, as they require computation and big storage. Vehicle to cloud interaction provides proficient support to these applications. In vehicle to cloud communication, any node in the network can directly communicate/ call to cloud based services (CBS). CBS may include application related to multimedia, entertainment, data security, communication etc. In this interaction the node can access cloud via various protocols including but not limited to HTTP, HTTPS, RPC (Remote procedure call) and direct API calls (Application programming interface calls). These days direct API calls are used in most application. Application scenario of API calls can be understood by scenario I and Scenario II.

Scenario I: when a node reaches a foreign territory having different language then it may call translation API provided by provided by cloud service provider for using Google. API calls can also be placed by nodes to translate the sign boards and traffic signals.

Scenario II: A moving vehicle can identify objects in its view and report them online using cloud API of object detection. This scenario can be used to identify the theft, to identify the type of vehicle on road like truck, bike etc, to detect the pedestrian, stop signs on roads and taking driving decisions according to the situation. Besides these there is interaction between different RSUs or RSU and cloud which mainly enhance the range of communication connecting all vehicles with each other in IOV network

III. IOV ARCHITECTURES

The design of layered architecture for a worldwide network which includes various other networks is quite challenging. It needs the identification and efficiently grouping of elements of different networks having similar function as a single layer. Liu Nanjie[9] proposed three layer architecture named "Client-Connection-Cloud" system. F. Bonomi [5] proposed four-layered architecture (end points, infrastructure, operation, cloud) for IOV. Wan et al. [10] presented an architecture consisting of three layers (vehicular, location and cloud). Kaiwartya et al. [11] designed five layers architecture (perception, coordination, artificial intelligence, application and business). Sejin chun et al. [12] designed a two layers fog computing architecture for IOV based on publish/subscribe model. Gandotra et al.[13] the proposed three layers architecture for device to device communication in which first layer is used to represent the network area where devices are connected to one another. The second layer is responsible for IP connectivity and roaming. Finally, the third layer deals with the selected application like IOV, smart homes etc. Juan and Sherali [14] proposed a seven layers architecture which provides a transparent connection among various network elements and data propagation in an IOV environment.Table 1 presents a comparative study of IOV architectures depending upon the no. of layers, security and communications supported by them. These architectures mainly support following interactions: Vehicle to Vehicle (V2V), Vehicle and Roadside (V&R), Vehicle and Infrastructure (V&I), Vehicle and Person (V&P), Vehicle and Sensor (V&S), Roadside and Personal (R&P) device and Device to Device (D2D). Device refers to smart phones, tablets, headphones, smart watches etc. From Table 1.1, it is clear IOV architectures are layered models with almost general layers with similar objectives. Most of these models[5], [9], [10], [12], [13] includes less layers which could not provide detailed elaboration of the actual protocols and functioning of each layers, Additionally these models supported interaction between one or two technologies where as model [11], [14] includes large no of layers which results in reducing the complexity of each layer. Moreover models with large no layers supported interactions among maximum technologies.

A. Architectural benefits of IOV

Few years back the vehicles had nothing to do with internet. But this scenario is changing rapidly. Now-days, in most of the models of cars the smart phones can be easily paired with car radio via Bluetooth resulting in attending calls, playing music etc. Similarly internet is wirelessly connected in modern cars resulting in controlling them remotely.

Additionally IOV model architecture enables the V2X communication (x=vehicle/ RSU/ Infrastructure/ personal devices/ Sensor/ Human) providing great benefits to the driver:

Increased *comfort* – V2I can remotely allow the driver to access their home devices like switch on air conditioning systems/ blowers before driving home

Better Convenience - V2P enables Car entertainment system to be connected with driver's cell phone and via phone to your media collection at home.

Increase *safety and efficiency*- V2V and V2R communication increase the driving safety by utilizing collisions preventions, traffic jams, accidents information provided by nearby vehicles, or road infrastructure or the cloud to save the travel time.

IV. SECURITY CHALLENGES IN IOV

IOV are self-organizing vehicular networks connected with internet and have highly dynamic topology. Due to internet connectivity nodes are more vulnerable to threats. The information provided by the nodes may be subjected to risk of malicious activity for e.g. tempering, stealing, eavesdropping, malicious routing, and other security related issues, which may cause catastrophic consequences such as accident taking toll of precious life. This way the security of entire network is compromised. Besides security, Safety in IOV network is of prime concern as innocent human lives are constantly at risk. In contrast, none of the other traditional networks includes life safety as their prime concern. Also except security issues, there are some unique security challenges because of the distinctive characteristics of IOV like high mobility, short time connection and frequent disconnections. These unique characteristics, presents security challenges such as position detection, data protection, trust group formation, and certificate management. To handle these security challenges of network there is a need to define security schemes for IOV. But deployment of a comprehensive security schemes for IOV is also quite challenging in practice.Besides enormous advantages, IOV introduces various security challenges. Trustworthiness of Traffic information disseminated by other vehicles or infrastructure – IOV enables the malicious users may broadcast traffic jam/ accident ahead warnings to clear his own route and gaining time, at the cost of others. IOV enables the hackers to remotely control the automatic braking system by sending fake V2X messages to a vehicle, or by altering the safety-critical communication inside the vehicle. Anyone can misuse internal networks of vehicles via standard onboard device interfaces and moreover update ECU firmware. IOV has enabled Automated Vehicle Identification which allows the vehicle to recognize itself for accessing to a toll payment or parking. Lack of security in IOV network may support the hackers in stealing the personal data like payment details. Above examples illustrates that IOV makes the vehicle openly connected to external networks like internet and making it accessible remotely by hackers or malicious users. So besides safety there is also a need of security and privacy to protect them from attacks in which malicious users may take partial or full control of vehicle by stealing data.

A. Security schemes for IOV network

Security approaches for IOV network includes encryption based security schemes and trust based security schemes.

Encryption based security schemes:

Encryption based schemes are divided into two categories:(1) symmetric encryption scheme (SES) and (2) public-key encryption scheme(PES). SESs share the single key for encrypting as well as decrypting purposes whereas PES uses different keys, one for encryption and other for decryption.SES provides the benefit of quite computational complexity. Due to low computational complexity, the SESs are fast as compared to PES. Since delay in reception of safety related messages sometimes make them meaningless, so to reduce delay SES are better for achieving security in IOV networks. But SES suffers from some problems: (1) the algorithm for key exchange SES is too complex that SES is less scalable for IOV. (2) Authentication code used for authentication increases the communication load, which in turn requires more storage space, resulting in extra power consumption and (3) Confidentiality problem related with key[15]. In IOV, nodes are moving freely on roads and thus can be compromised easily causing security threat to the whole network. Considering the above stated issue generally PESs are being preferred into IOV network In contrast with SES, PESs are more scalable and don't suffer from complicated key management algorithms. Moreover node authentication can be conveniently achieved to guarantee the security of the whole network. Most commonly used Public key encryption algorithms for IOV are the Rivest, Shamir and Adleman algorithm (RSA) [16] and Elliptic Curve Cryptography algorithm (ECC)[17]. But PES has high computation complexity. In nutshell, both SES and PES have their own advantages; however none of them can fully solve IOV network security issues. Encryption schemes are considered as the hard security solutions which provides the security by achieving non repudiation, data integrity and confidentiality, node authentication etc. as shown in fig 3 (a). Like binary solutions, in the hard security solutions nodes either pass the security check or fails. But hard security solution can detect the continuously changing behavior of nodes in which a node acts as a good node for some time and pass the security check and thereafter may turns into bad node due to selfish intentions. Thus the hard security schemes are not able to achieve the reliability and trustworthiness of nodes as well as the information sent by them.

Trust based schemes:

Trust based schemes are mostly used to handle soft security measures which purely depend on node's behavior for e.g. reliability of information disseminated by nodes, assessment of information received from nodes, controlling malicious activities and threats etc as shown in fig 3 (b).

Since security of data is highly dependent on trustworthiness of nodes, So trust based security schemes are more suitable to secure IOV network.

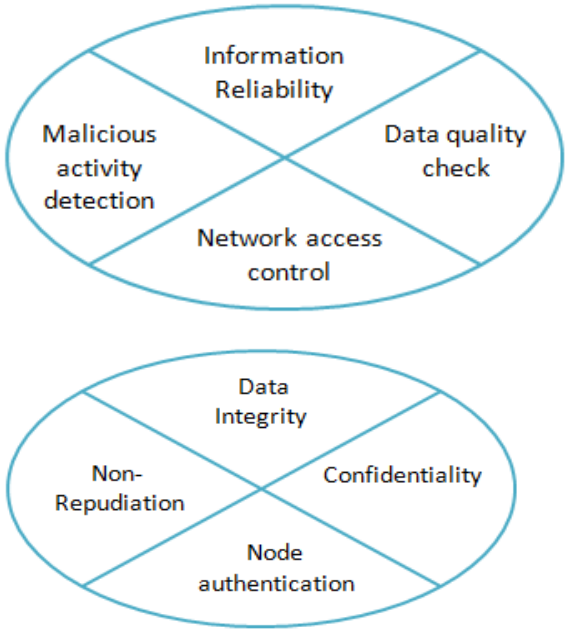

Fig 3: Security scheme measures

V. TRUST CONCEPT AND DEFINITION

Whenever we talk about security of information, the trust comes in the scenario. As we see in human relationship, when secret information is shared with a person then the security of that information (that it will not be disclosed) depends on the trustworthiness of the person with whom it is shared. The same concept applies to the vehicles in IOV network. When a message is forwarded from one vehicle to another then its security (that it is authentic, neither generated nor tempered by any malicious node) depends on the vehicles. Thus to impose the security in IOV network it is necessary to maintain trust between nodes. According to [18] Trust can be defined as:

"Trust is a relation among various entities that is established based on the observations of past interactions."

Basically the trust signifies the relation between two nodes or entities established to perform a particular action. One of these two nodes is called trustor (which makes trust belief that other node will perform in expected manner) and other node is trustee (which maintains the trust by acting in the expected manner). An entity is considered as trusted if it constantly behaves in the expected manner for any purpose. Applying this concept of "trust" in the context of IOV network means that all the entities of the network (vehicles, RSU, infrastructure, sensors, and personal devices) behave in an predictable manner like trusted information is shared among different entities in network. Formally trust can be measured in terms of probability that trustee will perform the task in predictable manner As we know the probability values ranges from 0 to 1 thus Values of trust variable (T) will also vary from 0 to 1 where T=0 signifies the complete TRUST and T=1 signifies compete DISTRUST. Trust can simply be represented as T(A,B, S), which means that A trusts B in situation S.

A. Characteristics of trust

Trust has different properties according to the nature of the network in which it is established. The properties of trust for highly dynamic IOV network can be summarized as below:

1. **Dynamicity:** The trust variable should be dynamic rather than being static. It should be calculated and modified continuously.
2. **Subjectivity:** Trust in IOV network is subjective in nature. Here subjectivity means that different nodes in the network may have different opinion about the same node.
3. **Time dependent:** Trust depends on perception of a node towards other node. Since the perception may change with time thus the trust may also change (Either grow or decay) with time.
4. **Asymmetric:** Trust between two entities follows asymmetric property. It means that it is not necessary that two nodes will have equal trust on each other for example if a node P trusts other node Q then it is not necessary that node Q will also trusts node P.
5. **Context dependent:** Trust between two nodes may also depend on context. For example node P may trust the node Q for forwarding but not for unselfishness.
6. **Transitive:** Trust in IOV is generally transitive in nature. Transitivity means that if a node M trusts the node N and the node N further trusts the node O then node M will trust node O also. But to maintain transitivity in trust, the trustor should trust in a trustee as well as in its recommendations.
7. **Composability:** Trust information about any node obtained from different available paths can be compiled and composed together to attain a single opinion value.

B. Trust establishment approaches in IOV network

Trust in IOV network can be established by using two approaches one is Infrastructure based approach and other is self organized approach [19].

Infrastructure Based Trust establishment approach:
In this approach the trust is established in the accordance with the infrastructure and is static over time (trust in security infrastructure is not lost). This approach mostly makes use of certificates. The presence of RSU is necessary in infrastructure based approach for communication[6]. The infrastructure based trust is of two types: centralized trust and distributed trust.

- **Centralized trust:** The centralized trust establishment approach includes a centralized trusted authority (CTA) which is responsible for calculating the value of trust variable (T) for each node in the network. But the Limitation of this approach includes the fact that the centralized trust authority must be present in active mode at all the time. In case the CTA fails then the whole

- network will be affected. Moreover this technique is not suitable for dynamic environment as it is quite difficult for each node to contact CA each time.
- **Distributed trust:** In distributed trust establishment approach the each node in the network is itself responsible for calculating and maintaining the value of trust variable (T) for any target.

Some infrastructure based trust models are Roadside-unit Aided Trust Establishment model (RATEM) introduced by Wu et al. [20], Long-Term Reputation scheme (LTRS) proposed by Park et al. [21] , Reputation-based Global Trust Establishment scheme (RGTES) proposed by Li et al.[22] and Trust and Reputation Infrastructure-based Proposal (TRIP) introduced by Gomez et al.[23]. But since infrastructure-based trust establishment schemes are based on strong assumptions and have some issues for e.g. high cost of maintenance, single failure point etc. So the recent trust models are based on self-organized trust.

Self Organizing Trust establishment approach:

For extremely dynamic network like IOV there is a need of a modified form of trust establishment. In self organized trust approach decisions concerning trust to other nodes are made autonomously and are based on partial information gathered from unknown nodes that came into contact for very small duration only. The self organizing trust establishment approach is characterized by two properties.

- It does not include any trusted third party like online infrastructure.
- It does not include any global knowledge shared among the participating entities.

The above properties of self organized approach make the trust dynamic. Self Organized trust approach is further divided in three types depending on the source of information [6][7]:

- **Direct self organized trust:** Direct trust relies on direct information obtained about other nodes from the previous encounters with them.
- **Indirect self organized trust:** Indirect trust depends on data collected from other directly trusted nodes. Thus indirect trust may be viewed as transitive attribute.
- **Hybrid self organized trust:** Hybrid trust is combination of both direct and indirect trust. It uses both locally stored information as well as trust information exchanged with other nodes.

Some self organized trust models are novel Trust and Reputation Management Framework based on the Similarity (TRMFS) introduced by Yang [24], Inter-vehicular Communication trust model based on Belief Theory (ICBT) proposed by Bamberger et al.[25], Situation-Aware Trust (SAT) model by Hong et al.[26].

C.Classification of IOV trust models

Trust models in IOV network are divided into three types, entity-Based models, data based models, and combined/ hybrid models.

- Entity based models: As name suggests, these models are responsible for trust computation and evaluation of entity i.e. vehicles for IOV network. If the received data was sent by a trustworthy entity, then it is considered as trustworthy.
- Data based trust models: These trust models are responsible for trust computation and evaluation of data received from other entity rather than the trust computation of entity itself.
- In hybrid trust models is responsible for the computation of trustworthiness of entity as well as data. In this model the trustworthiness of data received from any entity is evaluated by using the trustworthiness of that entity.

VI. SYSTEMATIC LITERATURE REVIEW

The trust management of IOV is still not matured field as limited work is reported to achieve security with IOV platform in literature till date. So In this study a systematic review of literature on Trust models in both networks VANET and IOV is presented following the four basic steps: 1. Resource identification, 2 Studies selection, 3. Information Extraction, 4. Information analysis.

1. Resource Identification

This step involves the recognition of appropriate keywords related to the topic of whose literature review is to be done. Here the resource identification is done by conducting a Google scholar search with a keyword “Trust models in VANETs”. Based on above search 75 articles were found. These articles were kept in LIST1. Similarly another search was conducted using a keyword “Trust models in IOV”. Based on this search 8 articles were found. These articles were kept in LIST 2.

2. Study Selection

Trust models for different networks (VANET and IOV) are selected to prepare final list depending upon particular selection criteria which includes, year, publisher, citation etc.. Selection of studies is followed by following rules.

- Trust models published only in five databases are considered i.e. IEEE, Science Direct, Wiley, ACM and Springer. However, the study is not strictly restricted to the abovementioned databases only. Some articles from other databases with high citations are also considered.
- Second criterion follows the year of publication of articles in which studies published in last 15 years i.e. between 2004 and 2018 are considered.
- The third criterion refers to the articles accepted in conference. In this criterion, the conference articles having citations more than a set threshold i.e. 8 considered.

Following the aforesaid rules, a final list was prepared which included 17 studies published in different databases. The table 2 presents the details of final list.

***3.* Information Extraction**

In this step, key details of the articles selected in final list are obtained which includes network type (VANET or IOV), Class of trust model (Entity based, data Based, combined) , demographics of the article (the year of publication, citations

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

etc). Table 3 shows the details of information extracted from the articles selected in list including the network type, class of trust model, year of publication etc.

Table 2: Number of Articles selected from different databases

	IEEE	Sci. Direct	ACM	Springer	Wiley	others	Total
LIST 1 (Trust models in VANET)	21	7	9	15	8	15	75
LIST 2 (Trust models in IOV)	0	0	0	1	0	7	8
Final Articles List	7	1	1	5	1	2	17

Table 3: Detailed summary of trust models selected in Final list

No.	Author	Trust Model	Network	Class	Year	Publisher	Citation
1	Gerlach et al. [27]	Sociological trust model	VANET	Entity Based trust model	2007	IEEE	75
2	Minhas et al.[28]	A multifaceted approach	VANET	Entity Based trust model	2011	IEEE Journal	50
3	Gomez et al.[23]	TRIP	VANET	Entity Based trust model	2012	Elsevier	114
4	Golle et al. [29]	Detecting and correcting malicious data in VANET	VANET	Data-based trust model	2004	ACM digital library	548
5	Raya et al.[30]	On data centric	VANET	Data-based trust model	2008	IEEE Conference	328
6	Lo and Tsai [31]	ERS	VANET	Data-based trust model	2009	Springer	67
7	Ding et al. [32]	Reputation-based model	VANET	Data-based trust model	2010	IEEE Conference	37
8	Wu et al. [33]	RATE	VANET	Data-based trust model	2011	IEEE Conference	9
9	Gurung et al. [34]	Real time message cntent validation (RMCV)	VANET	Data-based trust model	2013	Springer	15
10	Shaikh and Alzahrani [35]	Intrusion-aware model	VANET	Data-based trust model	2013	Wiley	11
11	F. Dotzer [36]	Vars: VANETs reputation system	VANET	Combined trust model	2005	*IEEE Inter. Symposium*	169
12	Wei and Chen [37]	RSU and beacon-based trust management (RaBTM)	VANET	Combined trust model	2012	Springer	12
13	Chen and Wei [18]	**I.** A beacon-based trust management (BTM)	VANET	Combined trust model	2013	IEEE Journal	23
14	Merrihan Badr Monir et al. [38]	Categorized trust based msg reporting scheme for VANET	VANET	Combined trust model	2013	springer	10
15	Shu Yang et al [39]	Trust-based anomaly detection scheme	IOV	Data-based trust model	2016	Hindawi	4

16	Fangyu Gai [40]	RTM system for Social Internet of Vehicles	IOV	Entity Based trust model	2017	Hindawi	2
17	Fangyu Gai[41]	Ratee-Based Trust Mgmt. System for IOV	IOV	Entity Based trust model	2017	Springer	2

4. Information analysis

In this step the Articles selected in the FINAL LIST are analyzed in two ways: (1) on the basis of the network for which they are modeled, (2) on the basis of the concept used in each model i.e. Methods used to model the trust, type of trust model, the advantages and limitations of the trust models, trust metrics used, properties of trust models. Each of the trust models is summarized below. Out of 17 trust models published in final list only 4 were combined trust models, 8 were data-based trust models and rest 5 papers were entity based trust models which forms 23.5%, 47.1% and 29.4% respectively as shown in table 4 and figure 4.

Table 4: Class wise analysis of trust models

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Combined trust model	4	23.5	23.5	23.5
	Data-based trust model	8	47.1	47.1	70.6
	Entity Based trust model	5	29.4	29.4	100.0
	Total	17	100.0	100.0	

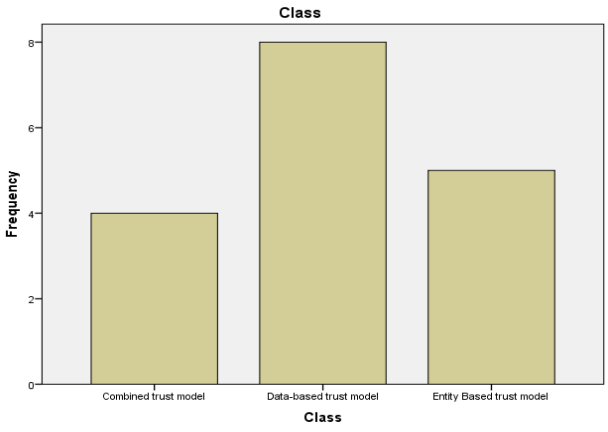

Fig4: Class analysis of Trust models in final list

As the result shows that maximum numbers of trust computation models (47.1%) are focused on data- based trust reason being easy to implement in any type of network. Then the entity based trust models are at second level (29.4%) reason being these trust models are quick in making decision as they only need to recognize who has sent the message. Least trust computation models are focused on combined trust models (23%). Although combined trust models provides the advantage of improved reliabilities; but they also have the limitation that they increase the computation complexity which further affects the efficiency of models.

From the analysis of trust models on the basis of the network for which they are modeled, it is clear that out of 17, Only 3 of them are proposed for IOV network where as the rest 14 trust models are proposed for VANET and which forms 17.6 and 82.4% respectively as mentioned in table 5 and fig 5.Moreover out of 3 trust models proposed for IOV network, one is entity- based and rest two are data based mdels. From Analysis it is clear that none of the trust model has been proposed for combined trust computation in IOV network. In IOV network combined trust computation makes lot of sense due to the ad-hoc nature of network, both data and entity based properties are available which makes the trust computation better and more reliable. Analysis on basis of year of publication suggests that from year 2004 to 2013 there has been gradual increase in trust based computation for providing security in VANET.

Table 5:Analysis of trust models on the basis of their class.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	IOV	3	17.6	17.6	17.6
	VANET	14	82.4	82.4	100.0
	Total	17	100.0	100.0	

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

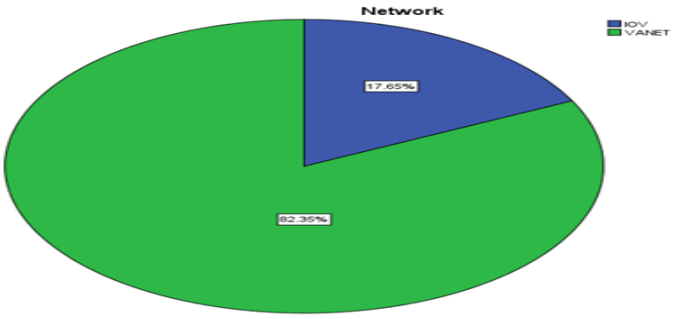

Fig5: Network Class analysis of Trust models in Final list

After 2013, the interest of researchers inclined toward IOV. Table 6 and fig 6 provides the yearly summary of Final list.

Entity based models for VANET

In entity-based model, a message is considered as trustworthy if its sender is trustworthy. In this field, Gerlach et al.[27], Minhas et al.[28], and Gomez et al.[23], proposed a sociological trust model, multifaceted approach to model trust and trust & reputation infrastructure-based trust model respectively. The sociological trust model[27] works on trust as well as confidence tagging principle. In this model various trust foams are recognized which includes namely situational (situation dependent) trust, dispositional (depend on own belief of entities) trust, system (system dependent) trust and process of belief formation (information evaluation considering all forms of trust). This model provides a benefit of location privacy preservation for the vehicle. The limitation of this model is that it has not provided any formalization to join different trust forms collectively.

Table 6: Year wise summary of trust models in final list,

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 2004	1	5.9	5.9	5.9
2005	1	5.9	5.9	11.8
2007	1	5.9	5.9	17.6
2008	1	5.9	5.9	23.5
2009	1	5.9	5.9	29.4
2010	1	5.9	5.9	35.3
2011	2	11.8	11.8	47.1
2012	2	11.8	11.8	58.8
2013	4	23.5	23.5	82.4
2016	1	5.9	5.9	88.2
2017	2	11.8	11.8	100.0
Total	17	100.0	100.0	

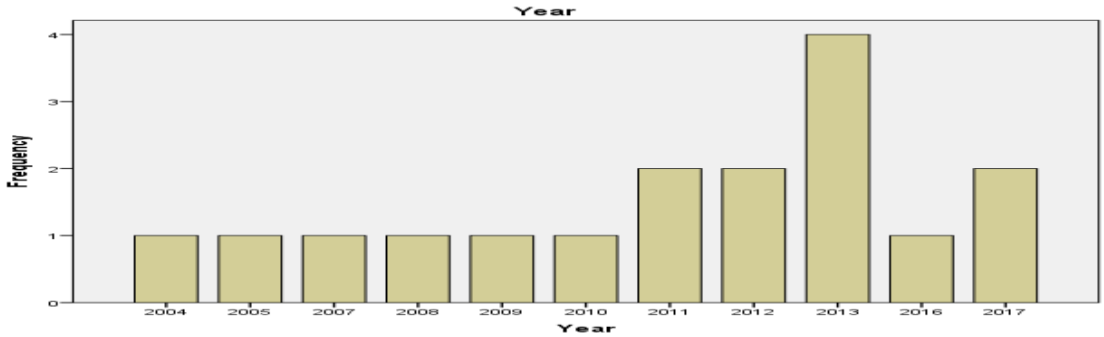

Fig6. Year wise analysis of trust models included in final list.

Multi-faceted approach[28] models the trustworthiness by integrating role- and experience-based trust into the priority-based trust model. Its role-based trust utilizes some pre-defined roles by the identification of agents whereas experience-based trust utilizes the data obtained from direct interactions. This trust model provides the benefit of satisfying several key properties like decentralization, privacy concerns, task specific, location/time specific, scalable, and system-level security. Limitation of this multi-facet model is that it has not addressed the robustness of model. Secondly this model has not considered the situation in which agents fail to report events. TRIP[23] was an efficient trust model to recognize and differentiate malicious or self- centered nodes in extremely dynamic and distributed networks not having central authority. This trust models enables the vehicles to decide the authentication of incoming traffic warning by assessing the trustworthiness of the sender's entity and consequently to accept and reject the warning. It only considers the traffic warning coming from vehicles having good reputation score reliable to accept. It was the first model that provides trust computation from behavioral perspective rather than the identity-based one. TRIP provides the benefit of accurate and fast trust computation. Besides that it is Light weight and scalable model. Limitation of this model is that it has not considered the privacy and identity management issues and actual overhead introduced by this approach.

Data-based trust model for VANETs

In data-based trust model, the trustworthiness of message sent by an entity is evaluated. In this field, Golle et al.[29] Raya et al.[30], Lo and Tsai[31], Ding and Jiang[32],Wu et al.[33], Gurung et al.[34], and Saikh and Alzahrani[35], proposed model for detecting and correcting malicious data, on data centric trust model, Event based reputation system (ERS), Reputation-based trust model, RATE, RMCV, intrusion aware trust model respectively.Golle[29] et al proposed a sensor-driven technique to identify inaccurate data and its source. The approach is based on utilizing sensor data, collected, shared and propagated by nodes in the neighboring region. This sensor data is then processed by each node to check its validity using a VANET model. In case of any inconsistency, an adversarial model is used to detect and correct malicious information on the basis of best explanation of errors. Assumption made for this model is that a vehicle always trust the information gathered by its own. It only checks the validity of information received by other neighboring node. Raya et al.[30] introduced a data-centric trust to secure highly empherical and data-centric vehicular network where node encounters with each other for very small duration. This approach uses the Dempster-Shafer Theory to estimate trust levels of data reports. This trust establishment technique withstands against attackers and quickly takes accurate decisions in time-critical manner. Lo and Tsai[31] presented an Event-dependent reputation system (ERS) for filtering out dissemination of bogus warnings by malicious attackers using cooperative event observation mechanism. In this system, each vehicle stores and manages the traffic events which are encountered by it or about which it is aware from any received messages. If these events has earned the sufficient credits on event intensity and reliability then only that event will be broadcasted by that vehicle. The event intensity and reliability are evaluated via event repuatation and event confidence thresholds.Ding et al.[32] Proposed reputation model which is also event-based to separate out the fake warning. Vehicles play different roles in this model i.e event participator, event reporter, and event observer. Each role has different mechanism for evaluating the reputation value. In the role of vehicle as event reporter, the reputation value is calculated using detection as well as standard frequency for that event. In the role of vehicle as event observer, the reputation value of event will be calculated by observing the succeeding behavior of Event reporter. Wu et al.[33] presented RSU Aided Trust Establishment scheme (RATE) which is completely data-centric. For calculating the trustworthiness of data, RATE employs the use of ant colony optimization algorithm along with the direct observed data with feedback information. When an event is detected, vehicles produce observations and their corresponding confidence. RATE scheme provides the benefit of mitigating the attacks launched by malicious nodes S. Gurung et al.[34] presented a real time message content validation (RMCV) model that is an information-oriented trust model. With this model every vehicle evaluates large amount of messages without depending on any infrastructure. RMCV considers various factors that have direct impact on the message trustworthiness. These factors include resemblance and conflicts in message content and resemblance in message routing path. This model does not make any assumptions in architecture. Shaikh et. al.[35] presented an intrusion-aware model with 3 phases of working state. First and second phases include the calculation of confidence value and trust value respectively where as third phase is responsible for taking decision on the message. The confidence value depends on the location and time closeness as well as on location and time verification. This model The message decision process is done in two steps: (1) Initially the system selects the message with higher trust value, (2) System accepts that message only if its trust value is higher than the minimum threshold; otherwise, rejects the message. The advantage of these models is that it is simple and decentralized due to which it can easily be implemented in the vehicular networks. Moreover model is robust and detects false location and time information.

Combined trust models for VANETs

Combined trust model performs computation of data trust utilizing entity-based trust. combined trust model is focused on finding out the trustworthiness of messages sent by a vehicle depending upon the opinions/recommendations provided by other vehicle nodes. In this field, F. Dotzer presented VANET reputation system (VaRS)[36], then chen & wei proposed two models RaBTM[37] and BTM[18],

Merrihan Badr Monir et al.[38] proposed Categorized trust based msg reporting scheme for VANET

VANET Reputation System (VaRS)[36] is a distributed reputation dependent. VARS uses trust (both direct and indirect) and opinion piggybacking for confidential decisions. In this method three areas are defined clearly: (1) event area (where the event is encountered), decision area (where trust of event related messages are determined) and distribution area (defines the distribution range of messages). When the message is forwarded from one node to other, it is

appended with the opinion of forwarding node about its trustworthiness. RSU and beacon-based trust management model (RaBTM)[37] allows both on board units and roadside units to build entity based trust by verifying the plausibility of both event messages as well as beacon messages. RaBTM aims to prevent internal attack to send false messages and to propagate message opinions quickly.

Beacon-based trust management (BTM)[18] is hybrid model that obtains entity trust from beacon based messages and data trust from both event related messages as well as beacon based messages. Entity trust is computed from beacon messages using cosine similarity where as data trust is obtained by utilizing both direct as well as indirect event trust. Categorized trust based message reporting scheme[38] is mixture of both experience as well as Role based trust. Nodes are evaluated according to their connections for event reporting duration and assigned with a category according to their trust values and confidence value.

Trust models for IOV

IOV network is in developing stage so not much trust models has been proposed by researchers. Moreover following the selection criteria only 3 articles are selected out of which two are entity based trust models and one is data-based trust model.Shu Yang[39] proposed cluster based trust management scheme to detect malicious vehicles. Cluster based detection involves two essential components (1) Cluster-based trust component (builds trust in time fashioned manner to reflect any dynamic situation) and (2) central reputation component (evaluates trust of a node from a long-term perspective). These two components work by uploading the evidence and proving the reputation. The functions of cluster based trust components are Affinity propagation based clustering (works iteratively) and mutual supervision. For evidence evaluation, the intelligent vehicles observe, evaluate and collect evidences regarding the qualities of each other and thereafter report them to the central authority computes reputation globally.Fangyu Gai[40] presented trust Management scheme for Social Internet of Vehicles. This model is nothing but the further extension of Ratee-Based Trust Management scheme. This model is also ratee based in which each ratee node stores the reputation information of its own provided by rater during the past interactions. This model also includes the Certification authority server and public key cryptography to avoid any alteration in the trust information by the ratee. This model used four factors to estimate trust value namely: Cookies number (no. of cookies received by any node), Relationship factor (indicates the relationship between two nodes), Object type (OBUs or RSUs), Centrality (indicates how much a node is central to other node). Fangyu Gai[41] et al. et al. presented a Ratee-Based Trust Management System (RTMS). In rate based trust management scheme there are four essential components: CA server (Centralized Authority), Cookies (Digital Certificates), Relationship management (Global/ centralized trust management), Local trust management. In RTMS trustworthiness of vehicles is computed in dual manner using both cookies and digital certificates. The rater stores the trust of given node in his Local trust. Cookies in RTMS contain the feedback value of transaction between two nodes and other service related information. Cookies are stored at CA for removal of Man-in –middle attack or trust forging. Relationship management module (RMM) is utilized to establish trust between two nodes. Comparison of cookies value based on trust computation is done by RMM.

As for calculating trust in RTM, trust value must be stored at Ratee (Local storage). After evaluation of cookies, trust values are also updated to local storage of the rate using local trust management (LTM). There are two problems associated with this model: 1) Cold start problem (This model does not mention how to trust a node initially and what trust value should be given initially to any nodes), 2) Scalability problem (this model does not define the no. of nodes).

VII. PERFORMANCE COMPARISON OF IOV TRUST MODELS

This section presents the performance analysis of trust models for IOV. For this purpose two trust models for IOV proposed by Fangyu Gai et al.[40] (Trust Management System for Social IOV) and Shu Yang[39] (Trust Management Scheme with Affinity Propagation) are compared on the basis of common parameters i.e. Reputation, Success rate and transaction Growth. In both models Trust is computed using rater id, ratee id, relation between rater and rate, time, transaction numbers and feedback value and The trustworthiness of any node is computed using the equation mentioned below

$$Tij = (1 - \beta - \alpha)\ Centralij + \alpha\ \varphi dirij + \beta\ \varphi indirij$$

where α represents weight assigned to the direct trust & β represents weights assigned to the indirect trust

We evaluated the trust models for trust estimation using the MATLAB environment [**32x**]. To validate the performance of the network, we utilized the random way point mobility model [xx]. All the simulations are run at-least 50 times and the simulation parameters used in our experiments are summarized in Table below.

Parameter	**Values**
Simulation Area	100*100 km^2
Simulation time	50-500 Seconds
Evaluation metrics	Transactions, Reputation, Success Rate
Routing Algorithm	AODV
Trust Computations	Ratee, Affinity Propagation

No of Nodes	1000
Communication range	250 meters
Vehicle length	600 cm
Communication interval	1000 ms

Transaction growth: Fig 7 shows the comparison of both models for transaction growth. The result demonstrates that in Ratee based system trust evaluation (per transaction) is linear in nature. However in affinity propagation model as the time increases, the number of transaction between nodes grows exponentially. Although the transaction growth in affinity propagation model is better initially however in long term the transaction growth in rate based system is better due to linear nature of transaction growth.

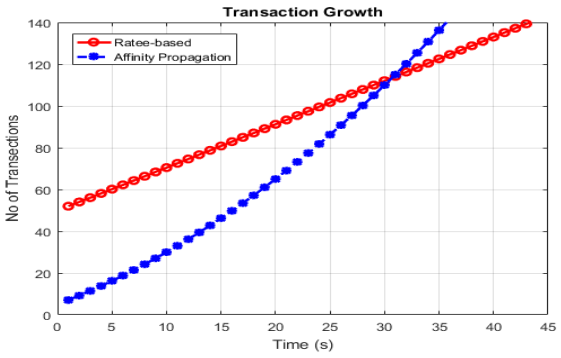

Fig 7: Transaction Growth

Reputation/ Trust Propagation: Reputation or trust of anomaly node in ratee based and affinity propagation model is shown in fig 8. As in affinity propagation model, the identity of node is propagated in environmental context utilizing identity situation and behavior. So the reputation or trust degree of anomaly node rapidly degrades in affinity propagation model. However in Ratee based system there is lag between node trust values calculations due to the presence of centralized mechanism. So Ratee based system lag fast reputation propagation when anomaly node is present in the network. Thus it can be said that as compared with rate based model, the reputation or trust propagation is better for affinity propagation model.

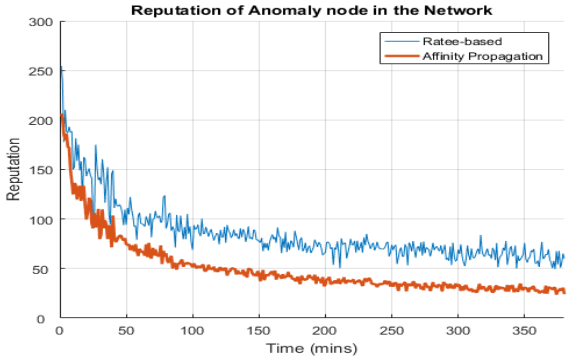

Fig 8: Reputation of Anomaly in the network

Transaction Success rate: Transaction success rate for rate and affinity based propagation is represented by fig 9. Due to better trust propagation, affinity propagation model provides better success rate than rate based trust model in long term.

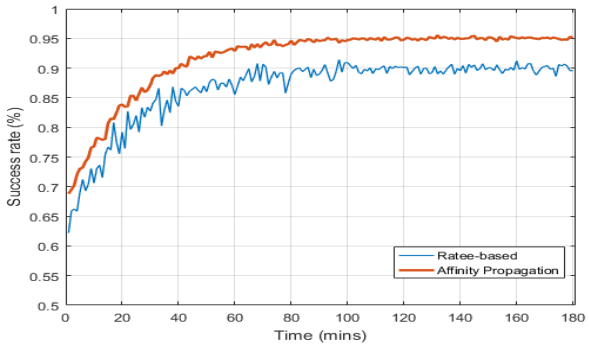

Fig 9: Transaction success Rate

VIII. CONCLUSION

The trust models differentiate the trusted entity and data from malicious ones that prevents the entities and data to be misguided and misused respectively. This study has presented a systematic review of articles related to the management of trust in VANETs and IOV network. This paper has contributed towards (1) discussion about basic concept of IOV, (2) explanation for the need of security in IOV, (3) discussion and comparison of various architectures of IOV, (3) clear definition of trust, its types and mechanism in context of IOV (4) analysis existing trust models in field of VANET and IOV. The analysis concludes that most of the existing trust models are proposed for VANET. Thus literature is rich in trust models for VANET where as the literature on trust models for IOV are quite less. Moreover the trust models proposed for IOV network are either entity based or data based. A hybrid trust model has not been proposed by any researcher till now. Moreover trust models for IOV were evaluated for trust estimation using three parameter i.e. Transaction growth, Reputation/ Trust Propagation, Transaction Success rate in the MATLAB environment. The results suggests affinity propagation model is better than rate based trust model in terms of success rate and trust propagation whereas the rate based model is better than affinity propagation model in terms of the transaction growth. From evaluation results it can be there is a scope of designing the trust model that is better than these existing trust models for all the three parameters. So our future work is focused on
designing the model which is better than existing trust models for almost all trust evaluation parameters

REFERENCES

1. M. Nitti, R. Girau, A. Floris, and L. Atzori, “On adding the social dimension to the Internet of Vehicles: Friendship and middleware,” 2014 IEEE Int. Black Sea Conf. Commun. Networking, BlackSeaCom 2014, pp. 134–138, 2014.
2. M. R. Palattella et al., “Standardized protocol stack for the internet of (important) things,” IEEE Commun. Surv. Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013.
3. Y. Toor, P. Muhlethaler, A. Laouiti, and A. La Fortelle, “Vehicle Ad Hoc networks: applications and related technical issues,” IEEE Commun. Surv. Tutorials, vol. 10, no. 3, pp. 74–88, 2008.

4. S. Vashi, J. Ram, J. Modi, S. Verma, and D. C. Prakash, "Internet of Things (IoT) : A Vision, Architectural Elements, and Security Issues," no. 1, pp. 492–496, 2017.
5. F. Bonomi, "The Smart and Connected Vehicle and the Internet of Things," Synchronization Telecommun. Syst. 2013, pp. 1–53, 2013.
6. P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi, "Trust Issues for Vehicular Ad Hoc Networks," VTC Spring 2008 - IEEE Veh. Technol. Conf., pp. 2800–2804, 2008.
7. J. Zhang, "A survey on trust management for VANETs," Proc. - IEEE Int. Conf. Adv. Inf. Netw. Appl. AINA, pp. 105–112, 2011.
8. M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1557–1568, 2007.
9. L. Nanjie, "Internet of Vehicles: Your next connection," Huawei WinWin, pp. 23–28, 2011.
10. J. Wan, D. Zhang, S. Zhao, L. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions," IEEE Commun. Mag., vol. 52, no. 8, pp. 106–113, 2014.
11. O. Kaiwartya et al., "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," IEEE Access, vol. 4, pp. 5356–5373, 2016.
12. D. Rj et al., "Fog," 2016 IEEE 8th Int. Conf. Cloud Comput. Technol. Sci., pp. 90–93, 2016.
13. P. Gandotra, R. Kumar Jha, and S. Jain, "A survey on device-to-device (D2D) communication: Architecture and security issues," J. Netw. Comput. Appl., vol. 78, pp. 9–29, 2017.
14. J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero Ibáñez, "A seven-layered model architecture for Internet of Vehicles," J. Inf. Telecommun., vol. 1, no. 1, pp. 4–22, 2017.
15. V. Vijayalakshmi and L. Arockiam, "I nternational J ournal OF E ngineering S ciences & M anagement R esearch A STUDY ON SECURITY ISSUES AND CHALLENGES IN IoT I nternational J ournal OF E ngineering S ciences & M anagement R esearch," vol. 3, no. 11, pp. 34–43, 2016.
16. T. R. neema megha, Stalin Shalini, "RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p," in IEEE International Conference on Computer, Communication and Control (IC4), 2015, 2015.
17. R. Singh and S. Miglani, "Efficient and secure message transfer in VANET," in IEEE International Conference on Inventive Computation Technologies, ICICT 2016, 2017, vol. 2.
18. Y. chih wie Yi- Ming Chen, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," J. Commun. Networks, vol. 15, no. 2, pp. 153–163, 2013.
19. Z. Huang, S. Ruj, M. Cavenaghi, and A. Nayak, "Limitations of trust management schemes in VANET and countermeasures," in IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, 2011, pp. 1228–1232.

A. Wu, J. Ma, and S. Zhang, "RATE: A RSU-aided scheme for data-centric trust establishment in VANETs," in IEEE 7th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2011, 2011.

B. C. Z. S. Park, B. Aslam, ", 'Long-term reputation system for vehicular networking based on vehicle's daily commute routine,' in Proceedings of the 2011 , pp. , January 2011.," in IEEE Consumer Communications and Networking Conference (CCNC '11), 2011, pp. 436–441.

20. W. S. X. Li, J. Liu, X. Li, "RGTE: a reputation-based global trust establishment in VANETs," in Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13), pp. 210–214, IEEE, September 2013," in 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13), 2013, pp. 210–214.
21. F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 934–941, 2012.
22. N. Yang, "A similarity based trust and reputation management framework for VANETs," Int. J. Futur. Gener. Commun. Netw., vol. 6, no. 2, pp. 25–34, 2013.
23. W. Bamberger, J. Schlittenlacher, and K. Diepold, "A trust model for intervehicular communication based on belief theory," in Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust, 2010, pp. 73–80.
24. Hong, D. Huang, M. Gerla, and Z. Cao, "{SAT:} Building New Trust Architecture for Vehicular Networks," in The Third International Workshop on Mobility in the Evolving Internet Architecture, 2008, pp. 31–36.
25. Matthias Gerla, "Trust for Vehicular Applications," 8th Int. Symp. Auton. Decentralized Syst., 2007.
26. U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile Ad Hoc vehicular networks," IEEE Trans. Syst. Man Cybern. Part C Appl. Rev., vol. 41, no. 3, pp. 407–420, 2011.
27. P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," Proc. first ACM Work. Veh. ad hoc networks VANET 04, vol. pp, no. NLE-PR-2006-19, pp. 29–37, 2004.
28. M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," IEEE 27th Conf. Comput. Commun., pp. 1238–1246, 2008.
29. N.-W. Lo and H.-C. Tsai, "A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks," EURASIP J. Wirel. Commun. Netw., vol. 2009, no. 1, p. 125348, 2009.
30. Z. Qing Ding, Xi Li, Ming Jiang, "Reputation-based trust model in Vehicular Ad Hoc Networks," in IEEE international conference on Wireless Communications and Signal Processing (WCSP), 2010.
31. S. Z. Aifeng wu, Jianqing Ma, "RATE: A RSU-Aided Scheme for Data-Centric Trust Establishment in VANETs," in 7th IEEE international conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2011.
32. E. B. Sashi Gurung, Dan LinAnna Squicciarini, "Information-Oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks," in Network and System Security, 2013, pp. 94–108.
33. R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks," Secur. Commun. Networks, vol. 7, pp. 1652–1669, 2014.
34. F. Dötzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad-hoc network reputation system," Proc. - 6th IEEE Int. Symp. a World Wirel. Mob. Multimed. Networks, WoWMoM 2005, no. 1, pp. 454–456, 2005.
35. Y.-M. C. Yu-Chih Wei, "Reliability and Efficiency Improvement for Trust Management Model in VANETs," in Human Centric Technology and Service in Smart Space, springer, 2012, pp. 105–112.
36. M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A Categorized Trust-Based Message Reporting Scheme for VANETs," in Advances in Security of Information and Communication Networks, springer, 2013, pp. 65–83.
37. S. Yang, Z. Liu, J. Li, S. Wang, and F. Yang, "Anomaly detection for internet of vehicles: A trust management scheme with affinity propagation," Mob. Inf. Syst., vol. 2016, 2016.
38. F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the Ratee : A Trust Management System for Social Internet of Vehicles," vol. 2017, 2017.
39. F. Gai, J. Zhang, Z. Peidong, and X. Jiang, "Ratee-Based Trust Management System for Internet of Vehicles," in Part of the Lecture Notes in Computer Science Springer book series, springer, 2017.