International Journal of Engineering & Technology, 7 (1.3) (2018) 181-186

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Analysis of Security Issues for the Internet of Vehicles in India

S.Nithyanantham[1]*, Dr.S.Kannimuthu[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore
[2]Associate Professor, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore
**Corresponding author E-mail: s.s.nithyanantham@gmail.com*

Abstract

Internet of Vehicles is a popular one in this decade which plays a vital role in automobile industry. Where most of the vehicles used for public and private are integrated with various sensors and transistors which will be core essential for an intelligent vehicle a steady growth. In vehicles, the quantity of chips will also increase according to the development. The increase in the amount of data formed by these sensors appears to be more dramatic as sensors frequently produce data. It is important to store these data for future reference, analysis and finding valuable information like fault diagnosis information, GPS tracing, auto drive support etc. Inappropriately, the variety of data and volume becomes rapidly extreme. In large scales, the existing analytical techniques fail to work effectively and produces a lot of false positives, which under means their efficacy, when enterprises move to cloud architectures and gather massive data, the issues become more serious

KEYWORDS: *Big data, Vehicle tracking, Vehicle monitoring, IoT, Smart City*

1. Introduction

Internet of vehicles (IoV), a rapidly developing segment, transforms the automobiles which possess incredible new features like car connectivity, advanced driver safety and in-vehicle infotainment and finally puts it as equal with home and office as a consumer space. The seismic change in automotive design has a tremendous impact, which alters the interface of the consumer with their cars and it maintains interest for India.

IoV technology is a dynamic mobile interaction method which communicates between vehicles and public networks which involves Vehicle to Vehicle (V2V), Vehicle to Road (V2R), Vehicle to Human (V2H) and Vehicle to Sensor (V2S).

IoV technology assists to share and gather information about transport, roads and their surroundings. It also highlights the process, figuring, partaking, and security of data platforms. This information helps the system of data platforms. This information helps the system to virtually lead and monitor transport, and give sufficient multimedia and mobile Internet application services. In accordance with the view of network, an IoV system is a three-level "Client-Connection-Cloud" system in Figure 1.

- Client system – client system is the exceptional sensors of a vehicle which collects the vehicle understanding and discovers driving condition and surrounding. It is a widespread communication terminal which attributes intra-vehicle, inter-vehicle and vehicle network interaction. It further involves IoV handling and accomplish of an assured vehicular identity in cyberspace.
- Connection system – it ensures the link to realize interaction and roaming between ad-hoc vehicular networks (VANETs) and other heterogeneous networks.

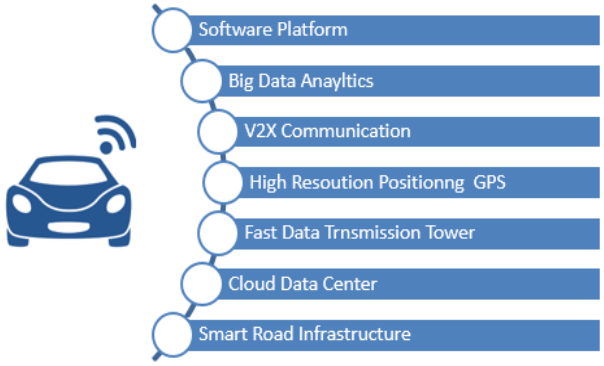

Figure.1. infrastructure technologies will enable car data monetization

- Cloud system IoV is a cloud-based vehicle functioning data platform. This ecosystem covers varied services like Intelligent Transport Systems (ITS), logistics, cargo/passenger transport, hazmat transport, vehicle repair/fitting, vehicle manufacturing, vehicle dealership, vehicle supervision, insurance, emergency rescue, and mobile Internet, which enables a variety of copious sources of information. Cloud system requires operations like virtualization, authentication, real-time communication and bulk accumulation. The transport information collection, computing, scheduling, control management and applications, which are integrated through this system.

The current GPS+GPRS system is only a joint application of the surviving technologies. Many ITS tests are carried out based on this technology. This IoV technology would be unfavorable for strategic priorities and technical inventions of a country.

Automobile designers can leverage Wi-Fi top deliver software upgrades and new features in car. Drivers can avail a mobile de-

vice to remotely monitor their car's destination, gas levels and mileage and the device can receive alerts regarding the functioning of the vehicle and diagnostics. The inbuilt Wi-Fi technology provides hotspots for on-the-go link without depending on cellular service. Wi-Fi is also supposed to play a major role in vehicle-to—everything(V2X) interaction and allow self-driving vehicle, mainly as standards continue to evolve to support Gigabit speeds and beyond.

Large information analysis is the across-the-board analysis and processing data in vibrant functions in vibrant functions in numerous areas, and currently, it has engrossed the attention of the security community due to its challenging capacity to analyse and relate safety linked information diligently and at an unprecedented measure. Distinguishing among ancient information analysis and large information analytics for safety is not forthright. Nevertheless, the data safety community has been leveraging the research of network traffic, system logs and other information sources to recognize the challenges and find numerous accomplishments, for serving more than a decade, and it remains complicated as to how these conformist attend vary from massive information. "Big Data Analytics for Security Intelligence" emphases the safety of the accumulated information.

2. Related Works

Sensors in the car enable to find objects and move around them. The sensed data is processed by artificial intelligence software which judges the behavior of the objects and designs decisions regarding the response of the car. The self-learning competencies of the car enable it to find, respond and learn from new situations.

The vehicle's operation is established on its capability to reply immediately to stimuli and pass verdicts which drive a correct response (i.e.,) the aptness, continuous communication and timeliness in processing the data. Connectivity enlarges which enables the progressive incorporation of a vehicle into a broader ecosystem of additional devices and infrastructure technologies as shown in figure 2. Additional capabilities like smart traffic routing of self-driving vehicles arise which aims in enhancing transport effectiveness.

The dimensions of the technologies intricate occurs to signify, as it has in the past, an augmentation of the ecosystem required to permit this value loop and a sensible shift in power balance among the relevant players. Industry undergoes a fundamental and widespread transformation, due to the impact of the automotive business model. In a scenario, the power lies firmly with software platform givers, and the vehicle is just a conduct that acts on the data provided a powerful functioning system? Here, the majority of value is captured by players in the ecosystem that has the ability to use data provided by the vehicle and its surroundings.

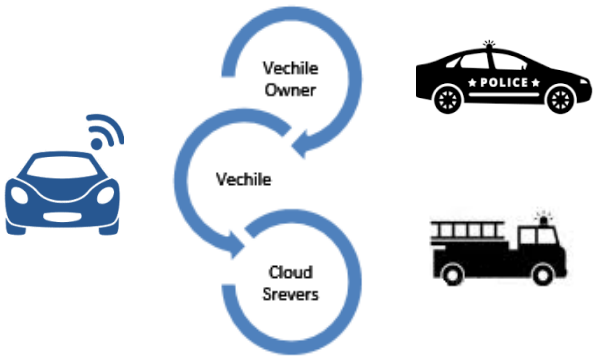

Figure 2. Infrastructure technologies with communication among the vehicles

A. Communication between vehicles and the Vehicle Owners

Few attributes of the vehicle like the vehicle speed and fuel level are directly reported to the users in the vehicles, only when the vehicle is in use. However, to enable the user to receive active updates even when the vehicle is not being used and when the user is away from the vehicle, an on-board processor is useful.

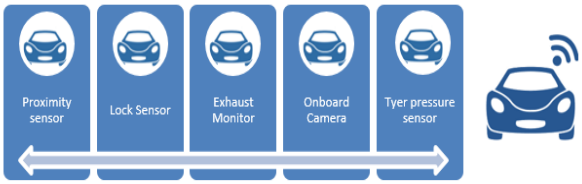

Figure 3: Vehicle to its Owner Communication

The active updates mentioned may involve

a. security alert about the vehicle,
b. damage alert about the vehicle
c. attributes like proximity, tyre pressure and vehicle lock

The sensors and the on-board processors in the vehicle are shown in Figure 3.

B. Communication between vehicles

Communication between vehicles involves the sharing of these data:

1. Proximity between the vehicles
2. Monitoring of the immediate surroundings of a vehicle through onboard cameras.
3. Speed of vehicles within a particular radius of the vehicle under consideration.
4. Tyre burst related accidental information

When a vehicle is on the road or when a vehicle is parked, its proximity to other vehicles in its immediate vicinity can prove to be crucial in avoiding accidents and damage to the vehicles.

Knowing the speed of the vehicles surrounding a particular vehicle can help in giving a warning to the nearby vehicles on the road about a fast approaching vehicle. Thus the vehicle which receives the warning message will alert the driver about the problem next to him.

When a vehicle is on the road or when a vehicle is parked, its proximity to other vehicles in its immediate vicinity can prove to be crucial in avoiding accidents and damage to the vehicles.

Knowing the speed of the vehicles surrounding a particular vehicle can help in giving a warning to the nearby vehicles on the road about a fast approaching vehicle. Thus the vehicle which receives the warning message will alert the driver about the problem next to him.

Figure 4: Vehicle to Vehicle Communication

C. Communication between vehicles and a centralized server

The data monitored from the vehicle is relayed to the nearest communications node via an on-board computer. The node in-turn communicates the data via a satellite to the communications node of the server which monitors breaches. The server stores the data in the database and analyses the data for the breach. It provides a suitable solution to the vehicle through the same channel from which it received the messages which is shown in Figure 1.
To monitor the metrics of the vehicles, a number of sensors are deployed on each vehicle in Figure 5. IoV makes these sensors work in unison to derive reasonable inferences from the data generated. It is not uncommon for automobiles to have sensors in-built [6]. However, with the vast amount of data that needs to be analysed, sensors are to be standardized to have effective results. The metrics of the automobile that need to be monitored are:

- Tyre pressure
- Fuel level
- Speed / velocity reading
- Exhaust gases' contents
- Vehicle lock

Sensors are fixed at their respective positions to continuously monitor the data being generated. All these localized sensors are to be set with threshold values. When breached, all the data regarding the breach are to be sent to a processing and communication device on-board [7].

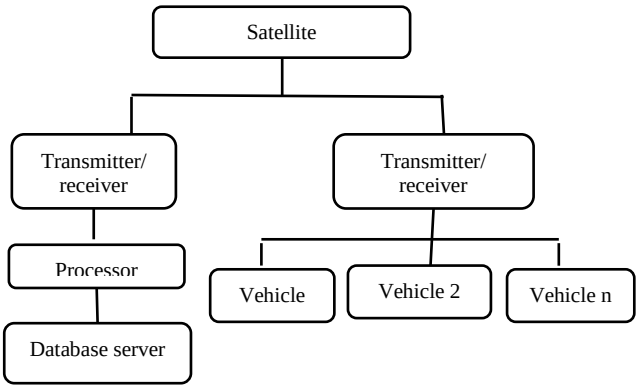

Figure 5: Vehicles to Centralized Server Communication

The processor will basically be a mini computer on board, powerful enough to handle the processing of the incoming data and the communication modules implemented on board.
Use of a raspberry pi processor [8] on board has been tested and proven to be successful and can be extended to vehicle management as well. It offers some significant advantages in terms of power consumption and speed of processing and it is used as a communication device [9].

D. Communication between Server and Third Parties

This mode of communication occurs between the server and the third parties including:

1. Emergency response like ambulance, fire-engine
2. Pollution control
3. Police patrol

Data deemed to be of primary concern are the data regarding vehicular collision, temperature spikes, theft etc. When these data are reported from the on-board processor on the vehicle, to the server, they are forwarded to the respective third parties.
These third parties correspond directly with the vehicle under consideration and take measures to provide necessary assistance. Deciding when the third parties need to be triggered. The centralized server decides Information regarding how to classify the incoming messages is of primal importance and is to be pre-fed into the server's decision making algorithm.
The features of the big data along assured lines-for example, how information is framed, analysed and processed. Once the data is segregated, it can be suited with the suitable big data pattern.

- Analysis type-it verifies whether the data is analysed in real time or batched for later analysis. It gives alert deliberation to choose the analysis type, because it affects several other decisions about products, tools, hardware, data sources and judge able data frequency. A combination of both types may be essential by the use case.
- Fraud detection; analysis must be done in real time or near real time.
- The analysis can be in batch mode, by using trend analysis for strategic business decisions.
- Processing methodology – this technique is involved for handling data (e.g., ad-hoc query, predictive, reporting and analytical). The needs in business controls the suitable processing methodology, a combination of techniques can be involved. The choice of processing methodology helps to identify the appropriate tools and techniques that are to be involved in big data solution.
- Data frequency and size – it determines the quantity and arrival of data. A knowledge regarding frequency and size enables to regulate the storage mechanism, format and the essential pre-processing equipment.
- Data frequency and size is contingent on the sources of information:
  - Demand with social media data
  - Frequent feed, real-time(weather data, transactional data)
  - Time series(time – based data)
- Data type – type of data to be processed-transactional, historical, master data and others. Knowledge of the types of data enables to divide the accumulated data.
- Content format – the format of the incoming data – structured (RDBMS, for example), or semi – structured. The process of the incoming data in the choice of equipment and techniques and defining a solution from the view point of a business perspective is determined by a format.
- Data source – sources of data (where the data is engendered) – web and social media, machine – generated, human – generated etc. recognizing all the data sources enables to examine the scope from the business viewpoint. The figure reveals the most widely enabled sources of information.
- Data consumers – a list of all possible consumers of the data being processed:
  - Business processes
  - Business users
  - Enterprise applications
  - Individual people in various business roles
  - Part of the process flows
  - Other data repositories or enterprise applications
- Hardware – the type of hardware for implementing the big data solution – commodity hardware or state of the art. Knowledge about the boundaries of hardware enables information on choosing big data solution.

It highlights the varied grades for dividing big data. The key categories for defining big data patterns have been identified and pointed in striped blue. Big data patterns, mentioned in the below article, are taken from a combination of these categories.

3. Communication devices in vehicle

Compare to telecom industry, IoV would produce more information. Its requires a terabyte scale(1015) data enabling system for collecting, processing and releasing dynamic processing and releasing dynamic traffic information from varied sources available in the city. To manage the data of this magnitude, cloud computing is preferred –In a cloud outline in following figure 6, the whole smart system incorporates all the systems related with the collection of data and operations, monitoring the condition of traffic on roads, vehicle-by-law and advice, monitoring the signals, combining the systems and announcements related to information.

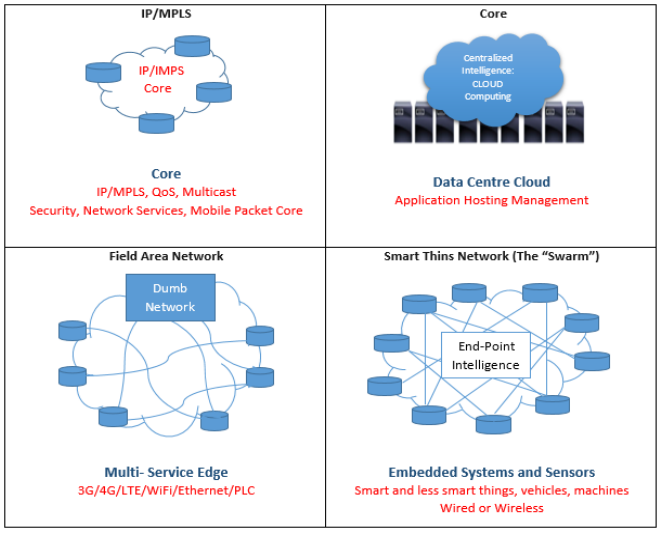

Figure 6 Cloud computing in big data

The integrated decisions are made based on the information shared among these systems. Cloud services which are connected with IoV and ITS are classified under the subsequent three categories as shown in Figure. 7. [14, 15, 16, 18]. The Clear IoV-and-traffic-related computing services are discovered.

- Infra - structure as a Service (IaaS): Uncomplicated IoV and traffic combined computing acts are founded on the cloud framework, which comprises the parameters like vehicle status data storage, area-based vehicle control, vehicle safety control, real-time traffic analysis and bill admittance and settlement. In the meantime, as a core capability, open APIs are given to any third party application developer to enable them to gradually build related application services. Clear IoV and traffic related computing function are discovered depending on the cloud frame work, comprising the vehicle status, data accumulation, area-based vehicle controlling, vehicle safety status control, real—time traffic analysis, admittance billing and finalizing. Open APIs are given as a core capability to any third-party application developers to enable in fastly building the related application services.

- Platform as a Service (PaaS): it compromises a major part in operating the GPS and GID data, proceeding ITS holographic data, cloud accumulation, data mining and analysis, data safety and information security and data buses.

- Software as a Service (SaaS): the resources of basic cloud and third-party services, a manufacturer creates certain applications which helps IoV and ITS from various points (PC browsers and mobile phones). Big data is not an elixir, in the everlasting arms race of attack and defence. The security researchers must walk around fictional methods to contain sophisticated attackers. Big data enables a world where sustaining monitoring in excess of the outcome.

4. Security issues in vehicle devices

The cloud removes geographic distance barriers and enables unique new features - many of which will not be considered until after the deployment of connected vehicles (CV) infrastructure and capabilities. For instance, researchers are working today to leverage the compute capabilities of a group of vehicles to create on demand vehicular clouds that support a variety of use cases. Furthermore, the step towards 5G communications offers exciting new connectivity options for vehicles. There is potential for future cellular technologies such as 5G, when paired with cloud computing, to either replace or augment dedicated short-range communications (DSRC) capabilities to support direct interaction with the cloud.

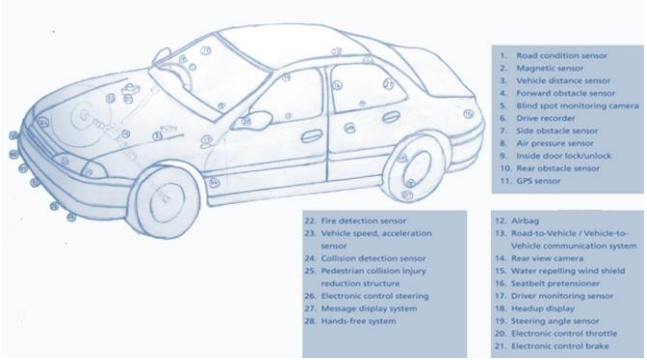

Figure 7. Vehicle sensors

IoT system architects can make use of the cloud to link disparate services, solutions and devices within and even across industries. These connections support data acquisition from myriad endpoints to deliver new value and enable fully threaded autonomous operations. There are exciting new SaaS-based applications and use cases being developed as more organizations understand the pieces of the puzzle and begin to brainstorm new ways of doing things. The same will occur in the CV domain, where companies such as Ericsson are already developing CV cloud solutions that can be deployed on standard cloud infrastructures. An interesting example of cloud connectivity is happening in Eindhoven, where connected cars are participating in a pilot to report acceleration and location data via the cloud for analysis by the traffic authority. Cloud connectivity enables interesting new capabilities for auto OEMs. The potential to collect and analyse data from vehicle operations can support analytics for product updates and future vehicle release.

Researchers have also identified security vulnerabilities within vehicles. For example, in July 2015, wired magazine states that a 2014 Jeep Cheroke, which was rode by a magazine writer was remotely disrupted by two hackers, by turning off the car's transmission. Following this announcement, 1.4 million cars and trucks were recalled by Fiat Chrysler in June 2014, followed by the recall of an additional 8,000 Jeeps (2015 Renegades) due to address remote hacking concerns. Fiat Chrysler is not the only car manufacturer having experienced hacks of their CV ecosystem: in August 2015, researchers managed to take control of a Tesla Model S and turned it off at low speed. Fortunately, Tesla quickly and remotely delivered software updates to fix the issue. In September 2016, a remote attack was discovered through the Tesla Bug Bounty Program Securing the overall ecosystem of CVs that operate within an IoT cloud-connected environment requires coordinated planning and execution across multiple stakeholder communities (e.g., OEMs, suppliers, aftermarket developers, traffic infrastructure developers, traffic management centre operators). This should be achieved through a methodical examination of the

security posture across all transportation participants and components that interact with CVs and CV infrastructure. [10]

The Security issues are increased vehicle miles travelled (VMT) (which could upsurge road congestion and travel times), augmented urban sprawl, and job forfeiture in certain sectors. Google's patent driverless car named Waymo will eradicate all the fatal errors caused by humans, but still it's in research and development phase.

- Marketing automation – a network is formed by mobile customer engagement, geo-location and Apple's iBeacon to know the customer's location, intentions, preference and purchasing styles. This degree of location-based familiarity has to hit the appropriate balance between the privacy of the user and the timely delivery of beneficial goods and facilities to the customers.
- Inventories are convenient to trace – large number of business firms utilize the Internet of Things to decide what their existing inventories occur to be. As an alternative of physical accordance, which implies money and time, appending permits immediate modernizing enabling the organization to have knowledge about ordering new products. This saves time, which is important in today's business world.
- Quite a few major information systems commence to examine the disputes in data, transmitting standards, analytical needs and reactions in technology that are brought to operational analytics and supply chain backgrounds, but very few are designed to cope with IOT. The challenges in data comprises of high input rate, streaming (time-series) data, large small files, and the essential for rapid micro modifications in the functional background. The challenge faced by the prime technology would be the incorporation of the whole thing; big data, cloud, billions of devices (IOT and M2M) and the network fabric.

Security in wireless communications can be a major concern in the concept of Internet of Vehicles (loV). With such an overwhelming number of vehicles on the road, there are a number of links to a number of nodes and all of these connected to a central server. Hackers pose a major threat to this system. The vulnerabilities might lie in any point in the system. Be it the processor on the vehicle, the router or the central server itself. A single loop hole anywhere in signals or the nodes might result in the exploitation and thereby crash the entire system.

Failure of networks: The very concept of IoV requires every vehicle on the road to be installed with a processor and sensor. While this might be a herculean task, a bigger drawback is the load generated by so many vehicles. Unless the servers and the intermediate processes are all able to handle the load efficiently, the existence of such a system might not be of much use. While the concept of IoV may be appealing, realizing the idea is still very hard. With a huge number of vehicles on the road, making sure that all the owners comply with this system is difficult and may involve legal issues. Organizing the infrastructure required, namely the server farms, making the equipment involved internet friendly and having them all work in unison can pose significant challenges. [11]

- Hardware Security: Use of secure boot and software attestation function, trusted platform module, tamper protection, cryptographic accelerator, active memory protection, device identity directly on device (e.g. Intel EPID, physically unalienable function).
- Software Security: Secure boot, partitioned OS, module level authentication, enforcement of approved and appropriate behaviour, secure product development lifecycle
- Network Security: Message and device authentication, Identify and enforce predictably holistic behaviour, access control
- Cloud Security: Secure authenticated channel to cloud, Remote monitoring of vehicle, threat intelligence exchange, OTA updates, credential management
- Supply-chain Security: Authorized distribution channel, track and trace components, continuity of supply, ability to identify uncertified component. [12]

A number of areas of concerns have been raised regarding security and privacy challenges posed by Internet of Vehicles ecosystem. Many of these questions existed prior to the growth of IoV, but they increase in significance due to the scale of deployment of IoV devices and connected world initiatives in Figure 8. [13]

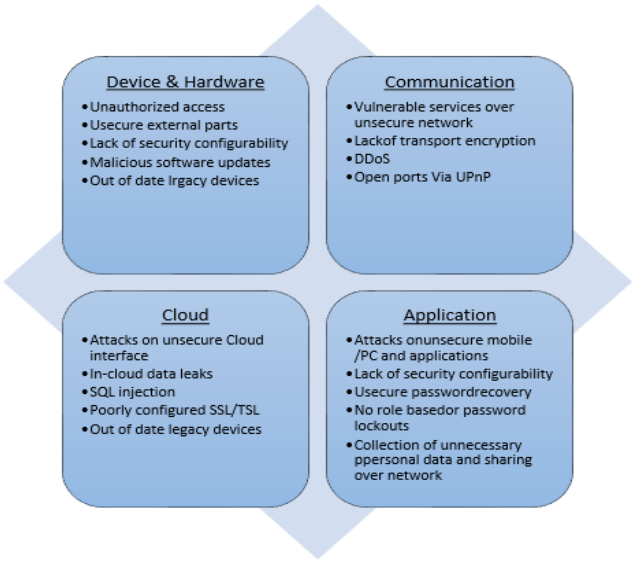

Figure 8. IoV Security and privacy threats

5. Big data for vehicles

Big data has become popular. Academicians and industrial experts use this word. Literature offers varied definitions for this word. Since 2001, the concept of big data prevails, where the threats of increasing data when addressed with 3VS model. 3VS, referred as dimensions of data, represents the increasing volume, variety and velocity of data. Advanced persistent threat (APT) detection and forensics require big data tools. 4.5 APTs function in a low and slow mode: as such they can befall over a protracted period of time while the prey leftovers unaware of the incursion. To notice these attacks, who prerequisite to gather and link big extents of diverse data (including internal data sources and external shared intelligence data) and does long – term historical link to include a posterior data of an attack in the history of network.

Later, the insured firms can avail cars linked to control the performance of the driver and safety. Issues will arise related with ethics and privacy; few drivers may dislike the concept of being monitored through sensors.

Until, drivers who are safe, reliably abide the road rules, ensured dispatched speed limits, could obtain a discount if they evidence their safe discount if they evidence their safe drinking habits with date from linked cars.

In case of any accidents and other occurrences, insurance firms might be competent to avail date from coupled cars to trace what has happened. This could diminish negative assertions which would assist both the insurance firms and the lawful authorities to find out who is rightly at fault.

With these data, insurance firms become competent to be ultimately responsible for one-on-one driving insurance. As an outcome, this could upturn incentives for drivers to drive carefully. This enables more drivers to practice safe driving live out which would really enable the roadways safe for all drivers.

6. Big data analytics on vehicle security issues

The science of logical cognitive unclogged by related visual interfaces is termed as visual analytics. Based on effective computation and storage, human-computer interaction in bog data has gained less attention. It is considered to be one of the basic tools to accomplish the deal of big data analytics, as its aim is to deliver the data effectively to humans. Big data is altering the landscape of security technologies for network monitoring, SIEM and forensics. Big data is not an elixir, in the everlasting arms race of attack and defense. The security researchers must walk around fictional methods to contain sophisticated attackers. Big data enables a world where sustaining monitoring in excess of the outcome of private data is frequently confronted. Consequently, the need to multiply our exertions to edify a modern set of computer scientists and engineers based on privacy worth has risen; there is a need to work with them to enhance the equipment for framing big data systems which tracks generally approved private rules.

Data safety is essential in all firms. Enterprise data is subjected able to leaks by internal stake holders. Steps are taken to propose a risk assessment mechanism which helps the information security manager to be alert of the safety challenges and value the vulnerability in the end client device. Large numbers of legacy safety measures certainly do not function in the manner we expect them to. Especially, as the data size increases, there is an increase in the data variety and data sources. The existing ways struggle with large volumes of information, varied data sources and analysis tools which are not able to cope with data velocity.

Big data methods can take conventional safety analytics to the next level. Each and every data is essential as it has some value in it. We require methods for better identification of trends detect new challenges based on suspicious activity, identify geographic regions seeing similar disproportionate threat activities, global threat features etc.

Availed a challenge of safeguarding/protecting the important data of any firm, the main aim is to comprehend the varied functions carried out in the system, status of the system, controlling the typical behavior of the system and finally reviewing its safety. The managers and data safety officials in business or firms need to comprehend the properties owned by the firms which include web servers, mail servers, file servers, personal computers and all software and application service software. Here the information sets will be big, complicated and dynamic which needs to capture, manage and process the information. The involvement of Big data techniques can lead to entirely new set of safety capabilities. This discovering process will be considered as an auditing of firm information safety. Figure 1 shows the proposed Big data analytics model for implementing enterprise data safety.

Addressed business requirements of Internet of Vehicles vary for commercial vehicles. Improved vehicle positioning, vehicle surveillance and management, analysis of traffic information and other business needs by enabling a centralized storage and managing PB-level massive data in the data center.

Allowing real-time management and controlling by gathering real-time status and news from vehicles for analysis and research. Forming a nimble up-coming data center design comprising storage, network and computing tasks supports future business needs and the growth of IoV enables business development.

7. Conclusion and future work

Management and monitoring of vast number of vehicles is one of the challenges in the real world. The development that's exists in vehicle automation through sensors provides a huge amount of data, there are a lot of controversies and concerns due to its immaturity and prospective security issues. It enhances the efficiency and effectiveness of the detection by collecting and controlling the vehicles through Internet without any malicious intrusion and attack. Yet, there are works to be done to defend the management of vehicles through fault diagnosis and various level sensors to manage the vehicle. In near future, the sensors found in the vehicle need to be stored in huge data storage volumes and those data are considered as sensitive data of vehicle history.

References

[1] Mythili G, Manush Nandan M (2017), "Internet of Vehicles (IoV): The Pathway For Proficient Smart Global Transportation", International Journal of Management and Applied Science, ISSN: 2394-7926, Volume-3, Issue-6, Jun.-2017.

[2] G Geethakumari, Agrima Srivatsava Big Data Analysis for Implementation of Enterprise Data Security IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555, Vol. 2, No.4, August 2012.

[3] Flavio Bonomi," The Smart and Connected Vehicle and the Internet of Things", WSTS 2013, Cisco Systems San Jose.

[4] Goutam Chakraborty, Hiromitsu Watanabe and Basabi Chakraborty.
Prediction in Dynamic System - A Divide and Conquer Approach. IEEE
Mid-Summer Workshop on Soft Computing Methods in Industrial Applications, 2005.

[5] Sanjeev Kumar, Anand Prakash, "Role of Big Data and Analytics in Smart Cities", International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064

[6] Galip Aydin, Ibrahim Riza Hallac, and Betul Karakus , "Architecture and Implementation of a Scalable Sensor Data Storage and Analysis System Using Cloud Computing and Big Data Technologies", Hindawi Publishing Corporation Journal of Sensors
Volume 2015, Article ID 834217, 11 pages, http://dx.doi.org/10.1155/2015/834217.

[7] http://www.intel.in/content/dam/www/public/us/en/documents/case-studies/big-data-xeon-e5-trustway-casestudy.pdf

[8] http://www.ibm.com/smarterplanet/us/en/traffic_congestion/article/traffic-management-and-prediction.html

[9] http://www1.huawei.com/enapp/28/hw-110836.htm

[10] "Observations and Recommendations on Connected Vehicle Security", CSA, Cloud Security alliance, https://cloudsecurityalliance.org/group/internet-of-things/

[11] Patrick Nisch (2011), "Security Issues in Modern Automotive Systems", panisch, http://citeseerx.ist.psu.edu/viewdoc/similar?doi=10.1.1.463.3202&type=cc, pp-1-6.

[12] Arnab Chattopadhyay," Securing Connected Vehicle through Secure Product Development", P&ES, the way we do it, Capgemini, pp.1-6.

[13] Shri Krishan, Vishal Sharma & Pawan Dubey,"IoT Connected world : Security and Privacy", White Paper: Infosys, pp.1-12.

[14] J. Srikanth. "Prevention of Heavy Vehicular Accidents Using Raspberry PI." Asian Journal of Research in Social Sciences and Humanities 6, no. 8 (2016): 417-426.

[15] http://www.iotconnectivitysolutions.com/news/2016/07/14/8391784.htm, July 2016.

[16] http://www.gartner.com/newsroom/id/3185623, Gartner, 2016.

[17] Bhadani, A., Jothimani, D. (2016), Big data: Challenges, opportunities and realities, In Singh, M.K., & Kumar, D.G. (Eds.), Effective Big Data Management and Opportunities for Implementation (pp. 1-24), Pennsylvania, USA, IGI Global

[18] Dr.S.Kannimuthu et all "Certain Investigation on Significance of Internet of Things (IoT) and Big Data in Vehicle Tracking System"