Sādhanā (2020)45:88
https://doi.org/10.1007/s12046-020-1320-9

A novel integration of smart vehicles and secure clouds for supervising vehicle accidents on roads/highways

KAMTA NATH MISHRA

Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi, India
e-mail: mishrakn@yahoo.com

MS received 6 October 2017; revised 10 September 2019; accepted 25 January 2020

Abstract. Precluding death percentage from road accidents has always been challenging task for technologists and scientists of this earth. As per the recent reports of world health organization approximately 1.5 million people including children and women are getting sudden and sad demise from road accidents. Approximately 25% of these deaths are because of non-availability of in-time medical aid and the existing automobile automatic communication technology is feeling helplessness. Although, the existing technologies of this earth and their integrations can help to the persons who are trapped in accidents and getting sudden demise. It is the social responsibility of scientists and researchers to work in the direction of developing easily accessible technologies which can provide immediate help on urgent basis to the persons struggling for life on the place of accident. This research work uses secure cloud (SeC) based online cameras called virtual eyes and internet of things (IoT) for developing a flawless and intelligent road traffic accident death prevention system called Intelligent Road Transportation Management and Control System (IRTMCS). The proposed IRTMCS is reliable, economically feasible and innocuous. The implementation and installation of the proposed system in existing vehicles can save the life of millions of people every year. In this research paper, the author has presented an innovative SeCBVE (*Secure Cloud Based Virtual Eye*) based IRTMCS (*Intelligent Road Transportation Management and Control System*) for preventing the deaths of individuals including women and children in road accidents. The implementation of the proposed approach brings us to a juncture where death percentage of persons in road accidents is decreased by 25% and approximately the life of approximately 400,000 (Four Hundred Thousand) persons including women and children can be saved every year by using the proposed system. The proposed approach uses secure cloud (SeC) based online cameras called virtual eye and internet of things (IoT) for implementing an unblemished and smart road traffic accident death prevention system. The proposed SeCBVE based IRTMCS is capable to help the investigators in finding the cause of accident and it will help the judicial system in tracing the culprit on the basis of stored video images. It can be concluded from the results and discussions sections that the proposed SeCBVE based IRTMCS gives promising performance in terms of efficiency, consistency and fault tolerance and it includes all the necessary features which are required for accountable, reliable and flawless road traffic accident death prevention systems (RTADPS). The implementation and installation of the proposed system in existing vehicles can save the life of millions of people every year.

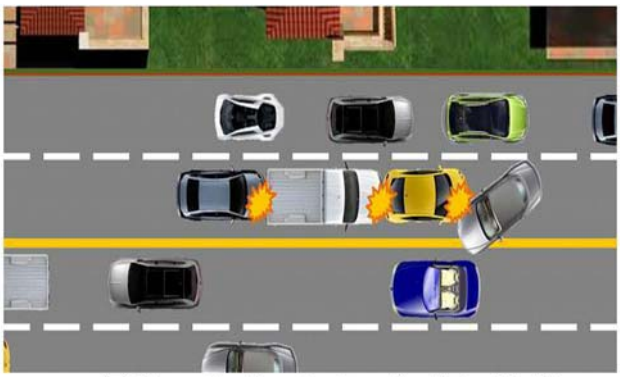
Keywords. Accident death prevention; human machine communication technology; secure cloud based virtual eye; smart vehicles; wireless technologies.

1. Introduction

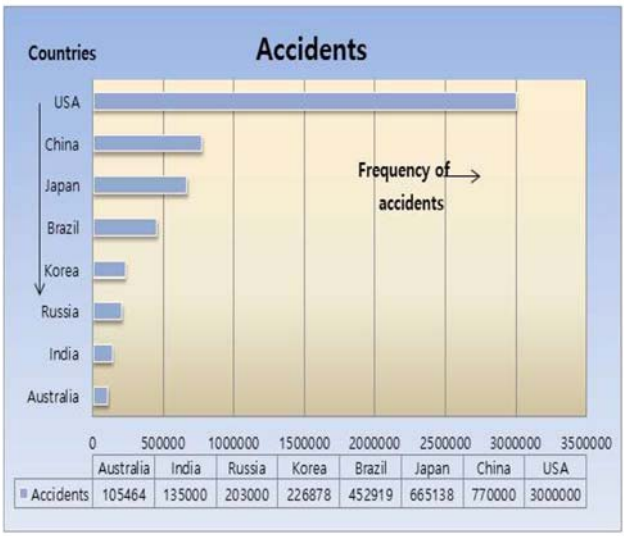
The world is fast transforming scientifically, and by now this earth has achieved a lot in scientific and technology advancements in the area of catastrophe, supervision, data assembly and storage of different types of affair managements [1, 2]. Conversely, the world is facing several calamities where millions of valuable human lives are lost in accidents. The towering rise in measured traffic compactness, road accidents and disasters faced in modifiable constructive management of travel control in metropolitan and rural areas have worried us to build up an elegant solution in these situations [3, 4]. To prevent deaths in road accidents the author has proposed *Intelligent Road Transportation Management and Control System (IRTMCS)* which uses secure cloud (SeC) based online cameras called virtual eyes and internet of things (IoT) for developing a flawless and intelligent road traffic accident death prevention system [5].

In these days the financial system of almost every country is growing at a fabulous speed. The citizens in every division of world are having their own

Published online: 20 April 2020



(a) Current hauling structure of vehicles [8], [9].



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

(b) Statistical information of accidents occurred in developing and developed countries [9], [10].

Figure 1. Current vehicle transportation structure and accidents scenario in developing/developed countries.

motorcycles, cars and other vehicles for journey. It is said about the cars that someone might purchase it for status emblem while others buy it for necessity [6]. We can often see the increasing overflow of cars in every street. On the other side, there are growing numbers of catastrophic vehicle accidents which have become a common phenomenon [7]. Figure 1(a) shows a traffic scenario of current transportation system. According to recent reports, figure 1(a) represents the numbers of accidents that have taken place in cost-effectively unstable countries is presented. Due to the ever-increasing number of accidents, there have been many cases of vehicles accident debates or road fume cases after the occurrence of accidents. Sometimes, these accidents and road fumes take very terrible shape and its consequences can be the death of a person. In figure 1(b) the car accidents statistics of many urbanized and developing countries is presented [8–10].

Whenever an accident occurs, in most of the cases, people expire due to lack of aid or support on time because neither the concerned authorities nor the victim's family members can have the knowledge of the place and the level of emergency in terms of vehicles caught up/scratched, level of injury/causalities of the persons seating in the vehicle, etc. In order to prevent such catastrophe situations, the proposed vehicular *IRTMCS* can be installed on the dash board of each vehicle.

At present, there has been a notable research improvement in this direction. The proposed *SeCBVE* has the ability to store location, driving video, front end, rear end, left side, right side and angular collisions both prior to and after the mishap. In the case of an accident, the proposed *SeCBVE* stores the position of catastrophe as an essential piece of information for the concerned authorities.

The proposed *IRTMCS* is the sphere of ultramodern transportation systems which can use the sophisticated techniques of impending technologies such as superior wireless antenna networks, distributed system architectures, and SeCBVE, which directs and detects several types of automobiles on roads and rail networks for humanizing the safety of passengers. In this research paper the author has presented an *IRTMCS* which can play an exceptionally decisive role in preventing, avoiding, monitoring and controlling accidents that are occurring on a daily basis.

The proposed *IRTMCS* is compatible with upcoming technologies which can integrate the transportation system with virtual and sophisticated wireless technologies and human machine communication technologies. In this research work the author has investigated and explored innovative potential to enhance the agenda of death prevention in road accidents.

2. Theoretical foundations and literature review

The vehicles can be classified into different categories like two wheeler vehicles (cycle, motorcycle), three wheeler vehicles (rickshaw, Auto Rickshaw, three wheeler cycle for differently able persons, three wheeler motorcycle), four wheeler vehicles (Bus, Minibus, Car, Jeep, mini-truck, truck), and more than four wheeler vehicles (heavy duty truck). If an accident occurs on a road then either one of these vehicles will be unbalanced because of certain unknown reasons or two and more of these types of vehicles will collide with each other or one of these vehicles will collide with another steady/moving object [11, 12].

If a vehicle meets an accident then either sudden exponential change in noise density will arise or unexpected change in angular position of vehicle will happen or hasty increase in collective momentum will occur or two and/or more combinations of these three situations together will occur. If any of these situations take place then the proposed cloud computing based technique called *IRTMCS* of

next section can be used for providing instant information to the concerned authorities including medical help and therefore the death toll of accidents can be minimized.

The cloud based computations scheme is internetworking based computation environment where platform, infrastructure and application software products are accessible and the end users can access them as the consumers. Till date several researchers, industry experts and academicians have tried to define the term cloud computing and its characteristics e.g., the researchers Khodadadi [4] and Bhabya *et al* [13] defined it as "Cloud is a parallel and distributed computing system which consists of a collection of inter-connected virtualized computers and these computers are dynamically provisioned as one or more unified computing resources established through negotiation between the service provider and consumers".

Van Bon *et al* [14] have established that a cloud is a gigantic gathering of effortlessly functional and reachable virtualized resources that is passionately reconfigured to fine-tune with a changeable load and it optimizes source consumption. The collections of resources in cloud environment are shared as per pay-and-use approach. Here, guarantees are offered by infrastructure provider as per the pre-defined service agreements. The researcher Miller [15] claimed that clouds are hardware reliant services which offer computation, network and storage capacity with exceedingly expandable communications ability.

A report from University of California, Berkeley reveals that the key distinctiveness of cloud computing are boundless computing resources, up-front commitment abolition and pay for each use [16]. Similarly, the scientist Alger [17] affirmed that cloud is more regularly used to refer as the information technology infrastructure deployed on an IaaS data hub. The cloud computing is now widely used in many industries and it has diversified applications e.g., secretarial applications, consumer liaison supervision, communications and partnership, emails and shared calendars, etc. The cloud computing has many rewards like 24/7 support, pay for each use, scalability, virtualized and bouncing atmosphere [18–20].

3. Proposed Intelligent Road Transportation Management and Control System (IRTMCS)

In each and every part of this world an accident is occurring in every hour. Some of these accidents are catastrophic which frequently kill many people on roads and highways. So, a new scheme is proposed in this research work which is very economical, advantageous and efficient. The author has proposed a *SeCBVE* based *IRTMCS* which can be used in different dimensions and paradigms of transportation for preventing the deaths of persons in road accidents. Further, the proposed technique can have innumerable applications like detecting road accidents, preventing casualties in road accidents, computing the number of road accidents, and broadcasting road accident related information to the phone numbers of concerned authorities including nearest police station, nearest hospital, relatives of driver, and vehicle owner.

The *SeCBVE* based IRTMCS contains an *emergency section button* for sharing the sequence of urgent information and videos to the concerned patrons via an ad- hoc-network and web server in the case of disaster occurrence. In the emergency section a Wi-Fi module and a Bluetooth module connected to their respective interfaces and two processors are used. In special case of emergency if one of the processor stop working then the next processor will perform the tasks of first processor and hence information transmission tasks will be continued in all situations. The preceding ingredient of *SeCBVE* based IRTMCS is data collector section which consists of different modules for acquiring and transmitting data/information like camera modules for back and frontage, LCD module, GPS Module, pressure sensor for accident/catastrophe detection, temperature sensor for shielding the data which could be damaged from disproportionate hotness, closeness sensor for vehicular lane change detection, and speed sensor for measuring the speed of the vehicle.

The emergency section will already have information like vehicle owner's phone number, driver's close relatives phone numbers, vehicle owner's close relatives phone numbers, ambulance common phone number (which is "108" in India) and nearest police station phone number (which is "100" in India) in its database. Within the fraction of seconds of occurrence of accident the driver of the vehicle will press the button of emergency box and immediately the voice calls based information and videos of last few minutes (one to two) will be transmitted to all the concerned authorities and persons including police station and ambulance phone numbers.

Usually, if a person dials phone number "100" or "108" then the call is received at the district headquarter and then the corresponding information about the event is conveyed to the nearest police station of the venue but in the proposed approach the GPS system will automatically search the location of accident, and location of nearest police station for sending videos and recorded information. Here, two processors are used for executing data dispensation duty. The first one is the key processor and the subsequent one is the additional processor. The key processor with the help of additional processor will immediately share the data (video, audio, information regarding the location of incident using GPS) with the smart phone numbers of vehicle owner, driver's close relatives (two to three relatives), ambulance, and nearest police station using ad-hoc network or web-based Wi-Fi server.

If the key/primary processor fails in emergency cases then the additional processor will trigger the circuit to perform the tasks of primary processor. If the key processor does not fail then the secondary processor will assist the

begin

1. The installed cameras of vehicle record the *front*, *rear, left, right* and *inside* videos continuously if once the vehicle's engine is in start state;
2. The emergency button physically present in the vehicle is pressed by driver / person if once the accident occurs;
3. **if** (Emergency Button Pressed)
   {
   Use GPS system and Internet of Things (IoT) of proposed *IRTMCS* for searching the exact location of accident place, phone numbers of nearby police station and hospitals;

   Search the phone numbers of *vehicle owner*, *driver's close relatives* (two to three relatives) from the important phone numbers database;

   if (*key processor is working*)
   {
   Use key and additional processors to make automatic phone calls to concerned authorities and persons in a sequence & convey the message about accident to each one through recorded voice call of 10 seconds;

   Automatically send videos to concerned persons/authorities one after another using key processor and additional processors;
   } ***// end of inner if condition***

   else
   {
   Use supplementary processor to make automatic phone calls to concerned authorities and persons in a sequence & convey the message about accident to each one through recorded voice call of 10 seconds;

   Use supplementary processor and send videos to concerned persons / authorities in a sequence;
   } ***// end of inner else condition***
   } ***// end of outer if condition***
4. **else**
   {
   Continue video recording and storing in video footage database;
   } ***// end of outer else condition***

end.

Figure 2. Algorithm for sending videos to the concerned persons/authorities in the case of vehicle's accident.

key processor in expediting the sending tasks of audio and video information to the corresponding persons and authorities. The algorithm for the proposed *SeCBVE* based *IRTMCS* is presented in figure 2.

Figure 3 depicts full communication details of *SeCBVE based IRTMCS*. Here, it is very clear that the voice signals and video images are continuously taken and stored in video database using front, rear, inner and side cameras immediately after the start of vehicle's engine for recording the pre and post-accident data. Immediately after pressing the emergency button the collected voice signals and video images are processed using key processor and supplementary processor. Further, the voice signals and video images are consecutively sent to the concerned persons/authorities using algorithm of figure 2. In the case of accident, the video recorded using the collectors and the information about the location specified by the GPS module are transferred to the concerned persons/authorities using a Wi-Fi-based server as per the description of algorithm proposed in figure 2. Therefore, the concerned authorities can have a glimpse at the evidence videos received and further they could take immediate corrective measures to save the life of persons who are struggling for life at the place of accident.

In functionality, the main purpose behind the design of such an *emergency section button* in *SeCBVE based IRTMCS* is to immediately share the accident videos with several responsible agencies and persons by excluding the involvement of a third party electronic devices. In addition to sharing the information amongst various agencies/authorities, the proposed approach shares the collision videos of front, rear and angular sides via Wi-Fi network and web servers which can help the concerned authorities to know the exact situation of accident place that is far in remote area.

4. Results and discussions

The cloud computing systems put forward bounty of scalable and flexible rewards to its consumers. The end users can operate from any remote location at all time in a safe manner. With the rising figure of web-enabled devices which are being used in these days (e.g., laptops, smart phones, tablets, etc.) have eased in accessing the information and data of any person. Therefore, in order to guarantee data confidentiality the counter approach of CCMP is being used in the proposed SeCBVE based IRTMCS for completing encoding of data and videos before transferring them to concerned persons/authorities. In the case of cloud services where end user to server and vice versa network communication is essential, the encoding key *'K'* remains the same for whole session.

The objective of this research work is not only to provide immediate medical aid to the persons injured in accident but also to trace the cause of accident and help the concerned authorities in finding the culprit. Usually, it becomes very difficult to trace the mistakes of person/vehicle because of whom the accident happened and therefore instead of sending the injured persons to the hospitals on urgent basis the people of vehicles start quarrelling, blaming and fighting with each other immediately after the occurrence of accident.

If a vehicle meets an accident by hitting another moving or steady object (living or nonliving) then following situations may occur:

S_1: The vehicle has hit one or multiple steady objects.

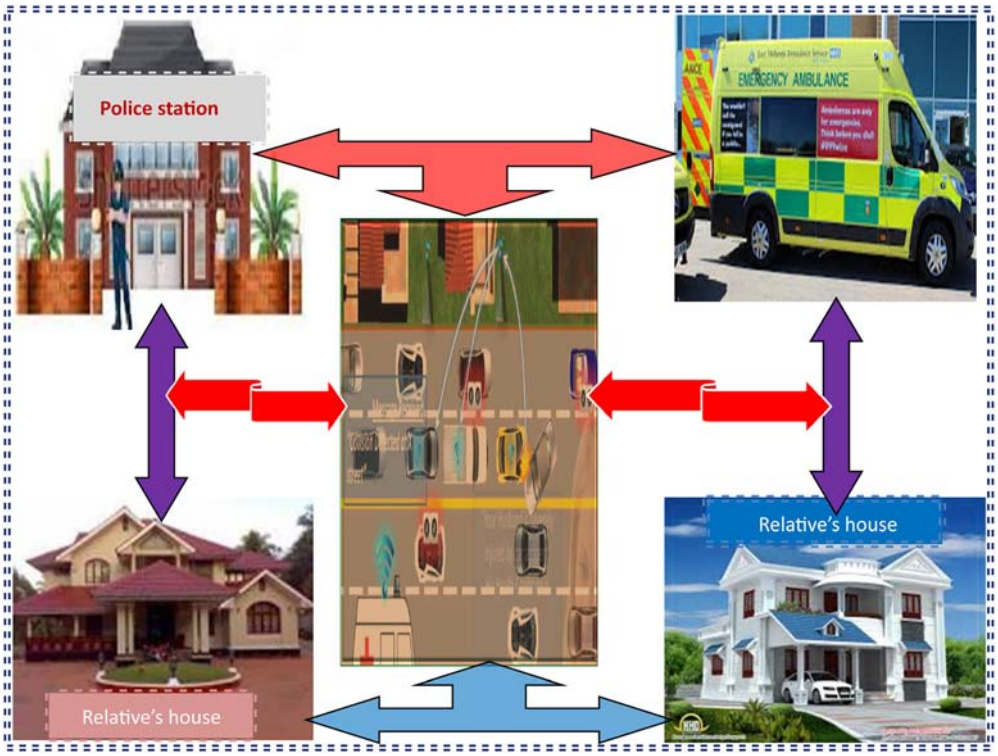


Figure 3. The Proposed SeCBVE based communication between the components of ***IRTMCS*** instantly after occurrence of accident.

S_2: The vehicle has hit one or more moving objects which are also moving either in the same direction or in the opposite direction of vehicle.

In both situations (S_1 and S_2) the combined linear and angular momentums will help in deciding the seriousness level of accident and the transmitted videos will help to the concerned investigation authorities in finding the cause and wrongdoer in the case of accidents occurrences. The linear and angular momentum of vehicles and other objects which are involved in accident can be represented by following equations:

$$Linear\ momentum\ of\ vehicle = M_i \times V_i \qquad (1)$$

where M_i is the mass and V_i is the velocity of *ith* vehicle.

$$Angular\ momentum\ of\ vehicle = J_i \times W_i \qquad (2)$$

where J_i is moment of inertia and W_i is angular velocity of *ith* vehicle.

In many situations it is not possible to decide the offender vehicle on the basis of momentum/angular momentum/videos and therefore in those circumstances the concerned authorities can use the videos and vehicle's momentum (angular and linear) together to conclude about the offending person/vehicle. Hence, the proposed system is helpful in making decisions while detecting and deciding offender vehicle/person and therefore the law enforcement agencies of the country can accordingly punish the offender as per the rules of country.

4.1 *Hardware implementation and system set-up*

The hardware and software components used for designing of *SeCBVE* based *IRTMCS* are: infrared sensors, global positioning system (GPS), Global Systems for Mobile (GSM) communication, Google reverse geo-location API, Google docs API with cloud service integration, five cameras (for recording videos from front, rear, left, right and inner side of vehicle), LCD display, and LPC2148 development board (for fast data transfer). The interconnections of these components provide communication between emergency boxes and other concerned authorities/persons whose information is stored in the cloud database. Therefore, the proposed system is easily transmitting voice signals and video images to the concerned authorities. The structure of each component and interconnected architecture of the proposed SeCBVE based IRTMCS is presented in figure 4.

The inputs given to and the output obtained from each component of the proposed *SeCBVE* based IRTMCS can be represented by a mathematical system which specifies following possessions:

(i) The inputs given to and outputs obtained from each state of IRTMCS processing.
(ii) The numeral of distinct state/stages encountered from starting to the closing stages of processing.
(iii) The interlinks between inputs, outputs and privilege phases.

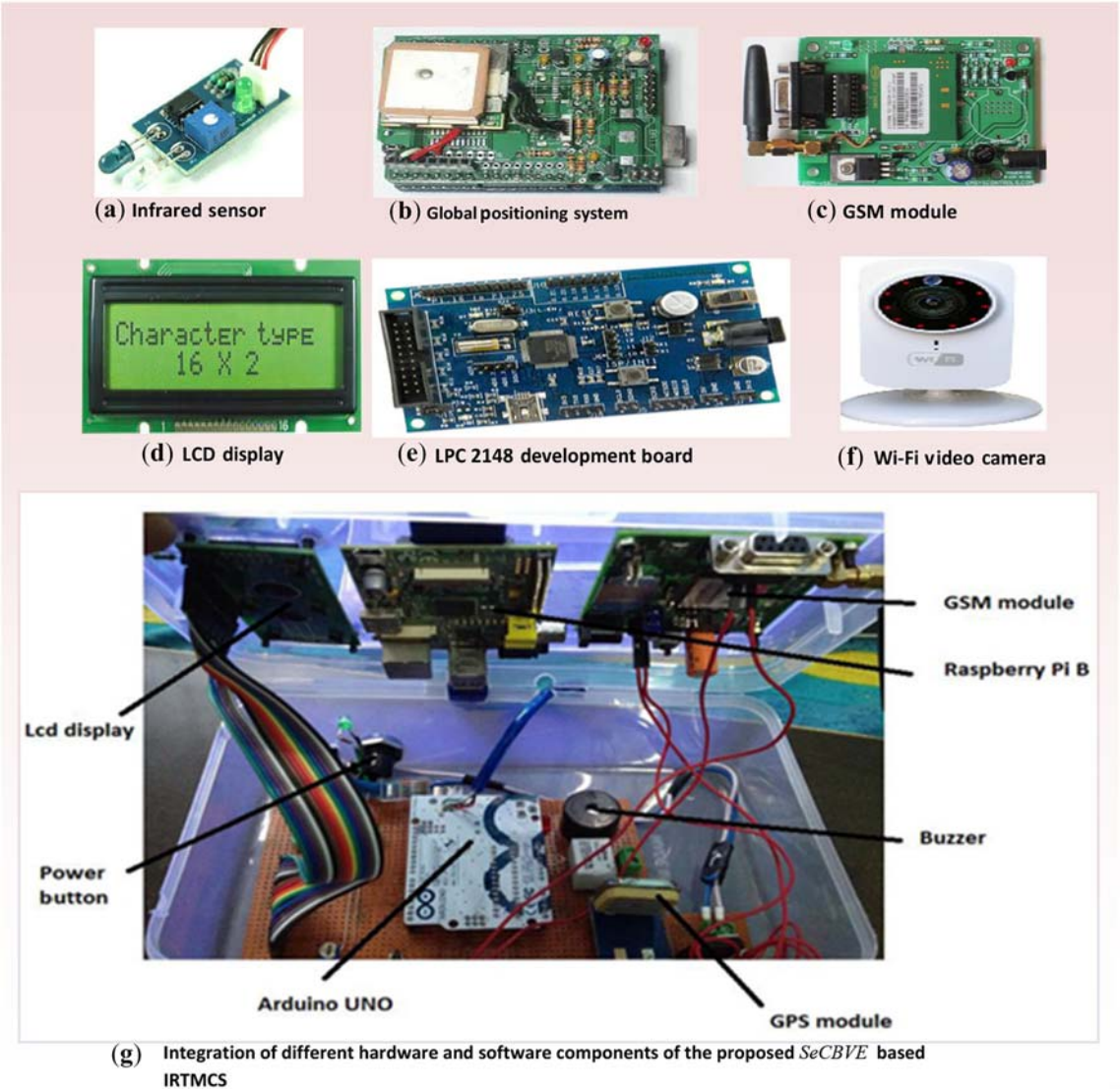


Figure 4. Integration of components and hardware implementation of proposed *SeCBVE* based IRTMCS approach.

(iv) The flow and data handling of different processing states of IRTMCS.

4.2 *Arrangement of IRTMCS components*

The arrangement of different components of SeCBVE based IRTMCS can be represented by Eq.(3).

$$IRTMCS = \left\{S, \sum, Q, T_f, O_f, I_s\right\} \tag{3}$$

The cryptograms of Eq. (3) are defined as follows:

S finite non unfilled set of states

$\sum$ finite non-empty set of inputs given to any component of IRTMCS

Q finite non-empty set of outputs obtained from any component of IRTMCS

T_f state transition function which brings IRTMCS to the subsequent state. The subsequent state is dependent on preceding state

O_f The output function which depends on the state and input elements

I_s the initial/starting sate. The IRTMCS will initiate from this state and it is a subset of 'S' i.e., $I_s \in S$

Now, each state is initially considered as a single processing unit where the authentic processing on the input data is carried out. The output is obtained from each state in terms of recorded voice signals, videos and other images after the completion of processing tasks. The outputs may or may not have some noise disturbances.

4.3 *Integration of IRTMCS components*

The comprehensive mathematical analysis of all the components of IRTMCS presented in figure 4 is described as follows:

4.3a *Set of States ('S')* Every state of SeCBVE based IRTMCS can be accepted as a distinct unit of processing where the inputs and outputs are evidently identified. The processing approved at every state can be denoted by a method which accepts inputs and returns outputs.

4.3b *The input / output sets ('$\sum$'/'Q')* The input alphabet set $\sum$ is the union of all those elements which are specified as input to SeCBVE based IRTMCS at different states. Therefore, it can be said that $\sum$ = {x | x is an alphabet considered as input using a state of *SeCBVE* based *IRTMCS*}

The elements of $\sum$ are video images and voice frequencies in the form of matrices of order$i \times j \times k$ i.e. $\sum = \{x \mid x_{i\times j\times k}$ is a matrix of order $i \times j \times k\}$. If B $\in \sum$, then $B_{1\times1\times1}$ is the simplest ingredient of $\sum$, and it is a real number.

If B $\in \sum$, then [B] = $b_{l,m,n}$ = b(l, m, n) $\forall$ l, m, n $\in \{\mathbb{Z}^+$-0}. At this juncture, $b_{l,m,n}$ is a constituent of matrix B which belongs to the lth row, mth column, nth layer. Further, for element 'b' following condition is necessarily true:

$$b \in \mathbb{Z}^+ \text{ i.e. } b_{l,m,n} > 0.$$

The output alphabet set 'Q' is the union of all individual elements which are received as output after using different states of SeCBVE based IRTMCS. Here, it should be noted that the inputs and outputs might consist of several elements of $\sum$ and 'Q'.

If 'B' $\in \sum$, then the elements of matrix 'B' will be represented by $b_{i\times j\times k}$ whereas $\Sigma = \{x \mid x_{i\times j\times k}$ is a three dimensional matrix} and matrix 'B' will be represented by symbol [B]. Hence, the matrix 'B' can be described as:

[B] = $b_{i\times j\times k}$ $\forall$ i, j, k $\in \{\mathbb{Z}^+$-0} where i, j, k are being used for row, column, and plane correspondingly.

The easiest element of Q will be $B_{1\times1\times1}$ and it is a single element of $\{\mathbb{Z}^+$-0}.

4.3c *The state transition function (T_f)* The state transition function of IRTMCS presented in figure 4 governs the flow control from one state to another state. It also finds the input required flow from one state to next state and the output originated while changeover is taking place. The state transition function 'T_f' can be represented by Eq. (4) as follows:

$$T_f : \sum^{*} \times S \rightarrow S \tag{4}$$

In Eq. (4), $\sum^*$ is the set of all video images and voice signal strings produced by the essentials of $\sum$.

4.3d *The output function ('O_f')* This function displays the output obtained at each state. The output function 'O_f' defined and represented by Eq. (5) as follows:

$$O_f : \sum^{*} \times S \rightarrow Q^* \tag{5}$$

In Eq. (5), Q^* is the set of all video images and voice signal strings obtained by the elements of 'Q'.

The processing tasks carried out by SeCBVE based proposed system are alienated into different algorithms where each of these algorithms can be described by the states of IRTMCS. The authentic values of every tuple for the above mentioned equations (Eqs. (3) to (5)) can be described by Eq.(6) as follows:

$$\begin{aligned} S &= \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\} \\ \sum &= \{\mathrm{FV_{img}}, \mathrm{REV_{img}}, \mathrm{LEV_{img}}, \mathrm{RIV_{img}}, \mathrm{INV_{img}}, \mathrm{VOI_{sig}}\} \\ Q &= \{\mathrm{FV_{img}}, \mathrm{REV_{img}}, \mathrm{LEV_{img}}, \mathrm{RIV_{img}}, \mathrm{INV_{img}}, \mathrm{VOI_{sig}}\} \\ T_f &: S\times^{*} \rightarrow S \text{ and } O_f : S\times^{*} \rightarrow Q^* \end{aligned} \tag{6}$$

In Eq. (6) $FV_{img}$is the video images and voice signals obtained from the front view camera, REV_{img} is the video images and voice signals obtained from the rear view camera, LEV_{img} is the video images and voice signals obtained from the left view camera, RIV_{img} is the video images and voice signals obtained from the right view camera, INV_{img} is the video images and voice signals obtained from the inner view camera of the vehicle, and VOI_{sig} is the recorded voice information signals which are to be transmitted immediately to the concerned authorities/ persons after the occurrence of accident as alert message. Here, each video image is consisting of two things namely video images and voice signals where video images are the collection of two dimensional interconnected moving images and voice signals are representing one dimensional digital values obtained by taking the combinations of zeros and ones.

Now, if 'b' $\in \sum^2$ and 's' $\in$ S then, T_f (s, b) justifies the processing completed on 'b' $\in \sum^2$, at state s $\in$ S. Here, 's' is representing an algorithm. Basically, T_f maps an algorithm and an output in symbol of $\sum^2$ which needs to be executed. In the similar way, the output function 'Q' combines an input and an algorithm to obtain an output. In this way each component of IRTMS is integrated with each other and finally videos and voice signals are transmitted to the concerned persons and authorities.

4.4 *Information flow between interlinked components of proposed IRTMCS*

In this proposed research work the piezoelectric sensor is used for detecting the unusual vibrations during the occurrence of accident. The accelerometer is used to detect the acceleration in different axis and the toppling condition of vehicle during the occurrence of accident. In the proposed SeCBVE based IRTMCS it is considered that the five

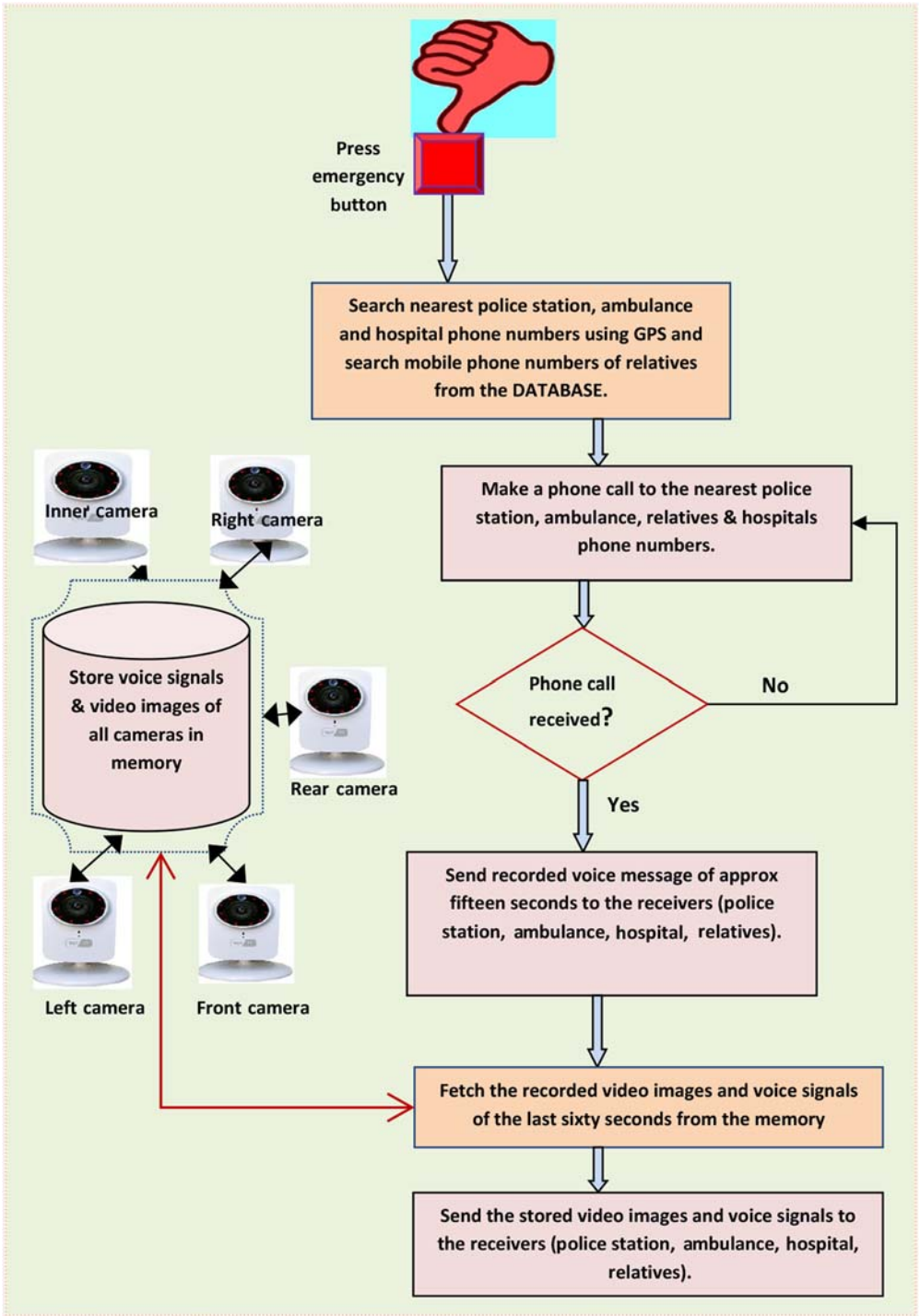


Figure 5. Flow of signals and video information between connected components and concerned authorities of proposed IRTMCS.

cameras (front view, rear view, left view, right view, and inner view) of system start recording video images and voice signals immediately after starting the engine of vehicle and these recorded voice signals and video images are being stored in secondary memory of proposed system. The five cameras are used to record videos images and voice signals before and during the occurrence of accident. The collective outputs of piezo sensor, cameras and accelerometer are given as input to the microcontroller available on the board. The global positioning system (GPS) available in the device calculates the longitude and latitude values for the vehicle. The global system for mobile communication (GSM) module present in the proposed system is being used for sending messages to the

concerned persons and authorities including nearby hospitals, police stations, and other important persons related to the accident. The Nimbits software is to be installed in the proposed SeCBVE based IRTMCS for real time access of cloud data.

The sensors are used to detect the stimuli and microprocessor evaluates the response from sensors to perform action such as initiating message/data transfer. The external interface to the Internet, wifi module and SMS service is also provided by the device. The GPS technology is employed to gather the information of the speed and the location (latitude and longitude) of the vehicle.

The GSM module is used to send messages to the vehicle owner/third party when required. The accelerometer is used to record the acceleration of the vehicle in various planes. This is indicative of abnormal driving. The Raspberry pi+ board is used for interfacing the device with the cloud. The board is connected to the Internet through a Wi-Fi receiver module. The Google API software is used for data logging on the cloud server. Immediately after pressing the emergency button the SeCBVE based IRTMCS interlinked components start functioning and finally the video images and voice signals are transmitted to concerned authorities including nearest police station, ambulance control centre, relatives of accidental vehicle's driver, and nearest hospital. The information and video / voice flow of proposed SeCBVE based IRTMCS is diagrammatically explained in figure 5.

The interpretation of figure 5 reveals that if the concerned authority does not receive the phone then the proposed approach retries to contact the authority and if the concerned authority receives the phone call then the proposed system display fifteen minutes recorded message about the venue and occurrence of accident before sending the recorded video images and voice signals of accident place of approximately sixty seconds. The proposed SeCBVE based IRTMCS uses Information as a Service (IaaS) and Software as a Service (SaaS) features of cloud computing for detecting accidents and forwarding information alerts to the concerned persons / authorities in the real time environment. The internet is providing interface between the vehicle and cloud. The short message service (SMS) is providing interface between user and cloud.

4.5 *Security analysis of proposed SeCBVE based IRTMCS*

There are serious concerns about protecting connected vehicles from hacking and cyber terrorism. Recently, Chinese students hacked an electronic car of Tesla and opened its front and rear side doors while the car was running on the road. Further, United States researchers have demonstrated and confirmed a cyber attack on Ford and Toyota Prius vehicles which affected steering and brake system. But, these incidents were conducted in test environments. Till date no such types of attacks have been reported on roads in real world. The GSMA has developed IoT security guidelines to guarantee the best practice for secure connection based management of IoT devices on any mobile transportation network. An integrated and robust approach to ensure security in reliable environment has been proposed by the author in this research work of secure cloud based smart transportation system.

A finest vehicle may consist of more than seventy five electronics control units (ECUs) which are unified through the network data and control buses. It is general thought that ECUs are hack-able by putting significant effort in generating reverse engineering and carjacking processes. In fact the researchers have been demonstrating in the research labs that attacks could be much more effortlessly crafted tenuously via Bluetooth, Cellular radio or through a malicious smart phone applications [21, 22]. Although, the physical access cannot be granted in these attacks. In order to hack a vehicle the attackers need to have high-level knowledge of vehicle's network architecture. Here, a convincing concern is that a complicated adversary can breach into the vehicular ad-hoc communication network and may inject false information to an in-vehicle network of IRTMCS [23]. Its further consequences may be the system breakdown, shut down of engine, alter the dashboard information and manipulate the data and video images which are to be transmitted to the concerned persons and authorities [21, 22, 24]. Ahead of all, catastrophic incidents could happen where adversarial parties may be able to drive the vehicle up to certain extent through remote access.

As far as the consequences of in-vehicle network security vulnerabilities are concerned, several impacts can be singled out. Mainly these consequences are concerned with transportation's security [25], efficiency, reliability, and behavior of persons and driver seating in the vehicle [26]. The hacking of vehicular network may force severe damages to the vehicle and the persons seating in the vehicle. The safety concerns of vehicular networks have been acknowledged in several studies (e.g., [27]). Taking control of vehicle's engine, brake, steering wheel and throttle [28, 29], to surpass the driver, compromises the safety of the embattled driver and his adjacent passengers of the vehicle. Further, distorting the dashboard and communication system of IRTMCS [28–31] not only compromise the traffic safety but it also leaves an injured driver and other persons of the vehicle in a traumatic state.

Ahead of the mentioned concerns, a malicious attacks and hacking of vehicle communication system may compromise the road users' privacy. The compromise of in-vehicle network may enforce monetary losses for road users and transportation operators. Since, not many studies are existing to scrutinize attacks' consequences on road users and authorities. Therefore, the security attack impacts on transportation network needs further in-depth investigations through simulation models and regression analysis based studies [32, 33].

Table 1. The classification of security related risks which may occur in vehicular network of SeBVE based IRTMCS.

Category of threat	Compromised security attribute that triggers consequences*			Effect on transportation network Item	Explanation	Threat exposures** Impact	Probability	References
	C	*I*	*A*					
Safety			*	Safe-PDO	Property damage crashes.	M	V_H	[27, 28, 34, 35]
			*	Safe-IF	Crashes with a harshness level of injuries and fatalities.	V_H	M	[21, 36–38]
Fine-grained Security			*	Sec-A	Compromise vehicles availability.	VH	V_H	[28, 34]
	*			Sec-PT	Compromise driver's privacy: track driver's trajectories.	VH	H	[21, 37]
	*			Sec-PF	Compromise driver's privacy: fingerprint drivers' driving pattern.	H	H	[29, 39],
	*			Sec-PE	Compromise driver's privacy: eavesdrop passengers' communication.	H	H	[26, 40]
	*	*		Sec-MN	Vehicles become a malicious node in the IRTMCS network.	V_H	M	[41]
Reliability	*	*	*	Relia-D	Originates road users to disbelieve the intelligent vehicle.	L	M	[42]
	*	*	*	Relia-VANET ET	Originates road users to disbelieve VANET future implementation.	M	M	[43]
Operation			*	Oper-TC	Taking control of vehicle and compromise vehicle's critical components including the communication system.	V_H	H	[28, 34, 35]
	*		*	Oper-ML	Monetary loss of road users and system operators.	M	H	[21, 31, 42]
			*	Oper-TT	Increase in travel time and cause delay.	V_L	M	[29, 30, 44]
			*	Oper-DS	Disabled and crippled services.	M	M	[24, 27, 45, 46]
System Efficiency			*	Effic-EC	Sudden increase in Surrounding vehicles' energy consumption.	L	M	[27, 28, 34] [47]
			*	Effic-D	Cause uneasiness to passengers.	L	H	[29, 45, 48]
Driver's Behavior			*	Behav-TE	Disturbing experience that can contribute to an impulsive driver's behavior	H	M	[28, 34]

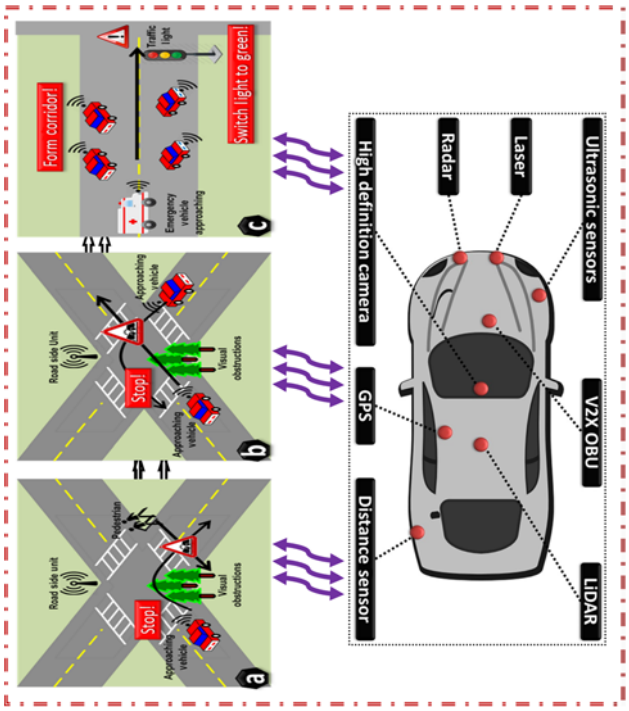


Figure 6. The interaction of IRTMCS components with road traffic communication systems.

The predictable impacts of a compromised in-vehicle network are presented listed in table 2. The impacts hacking and malicious attacks on transportation network can be categorized into seven types namely safety, fine-grained security, reliability, operation, legal exposure, system efficiency, and suspicious behaviors of drivers and persons seating in the vehicle. Further subdivision of these categories include following things:

(i) Taking control of vehicle and compromise vehicle's critical components.
(ii) Financial loss of road users and system operators.
(iii) Increase in travel time and level of tiredness.
(iv) Disabled and crippled services.

The risks associated with each of the adverse impacts of IRTMCS are categorized as Very High (V_H), High (H), Moderate (M), Low (L), and Very Low (V_L) levels. For the case of operation impact-type, an adversary taking control of a vehicle will be counted as V_H while the impact associated with an increase in travel time will be counted as V_L. The risk impact values of each impact-type are marked in table 1.

The three distinctive examples of emerging IRTMCS road safety applications are presented in figure 6. The first example describes about the pedestrian crossing warning application available in IRTMCS where the drivers are informed in the cases of pedestrians crossing the road (figure 6(a)). To implement this feature the sensors are to be deployed on the sidewalks to sense the presence of pedestrians and the equivalent sensory actions are collected at the road side units. These road side units (RSUs) can thus detect and/or predict the happening of potential accidents and these RSUs will notify the same to the incoming vehicle's IRTMCS.

The 2nd example of figure 6(b) is being used for assisting the driver in left turn. In a specific situation visual obstruction, two vehicles may approach for an intersection without seeing each other. The objective of the proposed IRTMCS is thus to help the driver in making a safer left turn at the point of intersection. Lastly, the figure 6(c) is related to the third application in which an impending emergency vehicle (e.g., ambulance, fire fighter or police vehicle) requests the nearby vehicles to provide a clear path by forming a corridor. In this case, the emergency vehicle will be able to interact with the nearby road vehicles through communication system of IRTMCS. Hence, the emergency response time is minimized. Some other examples of road safety and security applications include urgent situation based electronic brake lights advice, indication of stationary vehicles, roadwork related warning, warnings related to intersection collision avoidance, and lane change related warnings [49–51].

The traffic management applications represent the succeeding major class of SeCBVE based IRTMCS applications, whose foremost objective is to improve the management, control and synchronization of traffic flows for providing various cooperative navigation services to the users. In order to build and maintain global traffic map databases these applications depend on the compilation and analysis of the exchanged SeCBVE based IRTMCS messages. The traffic data are usually collected from road side sensors and are wirelessly transmitted to distantly located data centers for the purpose of data analysis and information processing. The collected information includes location-based appropriate information related to drivers, vehicles, and suspicious road events.

After processing and translating the collected data into significant information, these are delivered to the concerned drivers and persons through application service providers which notify them about current and/or future traffic congested jam areas, recommend itineraries, navigate instructions, and notify speed limits.

4.6 *Performance analysis and result comparison of proposed SeCBVE based IRTMCS with existing systems*

The smart vehicles and the linked infrastructure pose significant security challenges that must be addressed in order to encourage the adoption of SeCBVE based IRTMCS technologies and the allied services. These challenges include authentication, privacy and localization, reliability, mobility, low error tolerance, and resolving the conflict interests. The SeCBVE based IRTMCS require to have

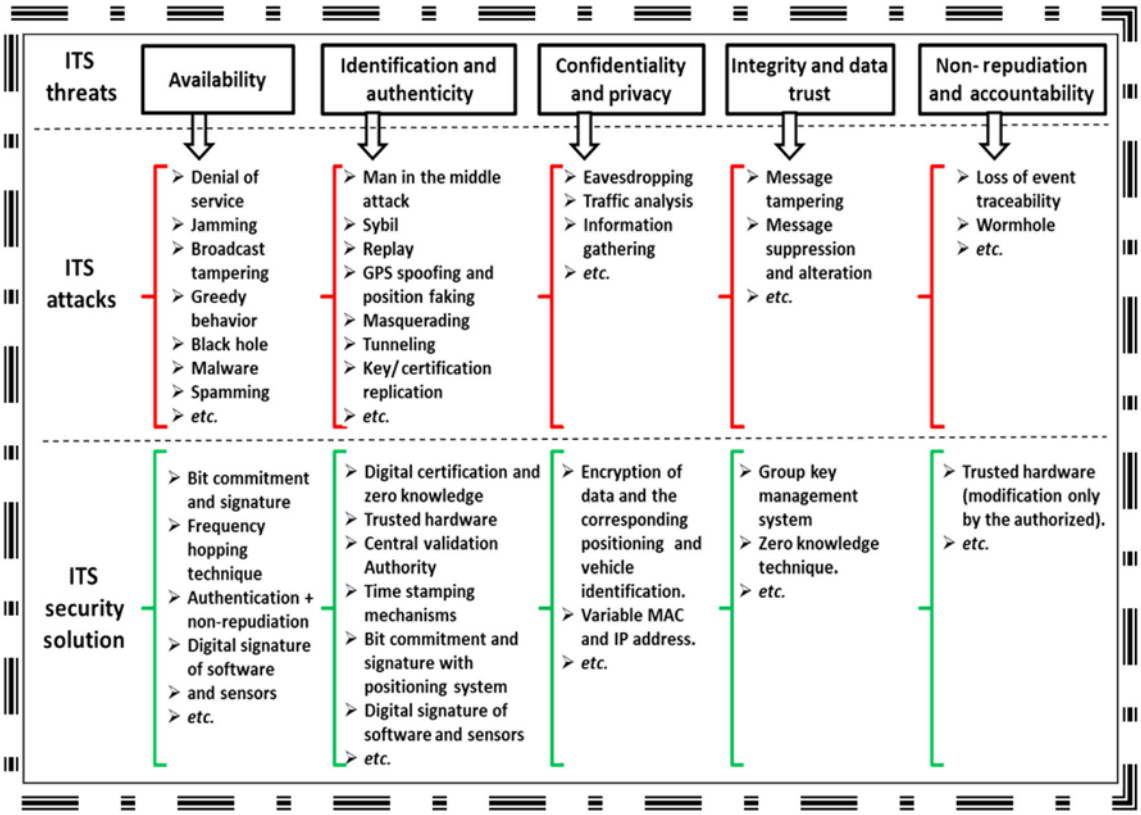


Figure 7. The threats/attacks to SeCBVE based IRTMCS and the corresponding countermeasures.

efficient end-to-end communication between its users and trustworthy authentication of all participating entities to promise the genuineness of exchanged messages. This permits a vehicle to proceed with confidence for a message received which may dictate the need to prevent masquerading and other types of spoofing attacks. In the specific cases where attacks take place, the well-built message authentication and genuineness mechanisms can act as forensic evidence for the purpose of pursuing legal actions.

Many vehicular networks and their applications depend on accurate localization. Hence, it becomes most important to achieve efficient and reliable authentication of all participating attributes of SeCBVE based IRTMCS to promise the high level faithfulness of exchanged messages. The decisive interactions between the components of IRTMCS based vehicular applications involve highly consistent and always available real-time communications which has been provided in the proposed SeCBVE based IRTMCS. The vehicular networks and their applications are self-organized where each and every vehicle in the proposed system interacts with several new entities like other means of transport on a single path just for a moment. By considering safety issues and the involvement of human lives it is necessary that the vehicular networks and the applications must be able to prevent malicious and other types of attacks on urgent basis. Because, a post-attack detection may be of no use if the attack has already resulted the vehicle into an accidental state and passengers are injured seriously.

The vehicle manufacturers, service providers, law enforcement agencies and consumers frequently have incompatible necessities and interests e.g., government's traffic control system and some other service providers including police may need to know the exact location of the vehicle. But, because of some hidden and unfair interests the consumers may reject such an approach of knowing the exact location of vehicle by others. The consumers may require that the recorded matters of by the cameras of the vehicle should only accessible by them (not to any other agency) whereas the investigating authorities would also want access to the incident recordings of the event. These differences are resolved by the proposed SeCBVE based IRTMCS by providing accident related details to vehicle owners, investigating agencies, nearby police station, and nearby hospitals.

The researches on intelligent transportation system (ITS) have attracted a lot of concentration from the research community in the last few decades. [52–55]. The challenges of intelligent transportation systems are being considered as social barrier to the universal adoption of ITS. The ITS technology was mainly intended to improve road safety, traffic efficiency, and safety of passengers. But, several

Table 2. Threat categories and the corresponding actions taken by SeCBVE based IRTMCS.

Sl. no.	Threat categories	Denial of service	Disclosure	Manipulation	Masquerading	Reply	Repudiation
1.	Natural disaster threats	√	×	×	×	×	×
2.	Accidental disclosure	×	√	×	×	×	×
3.	Configuration error	√	√	√	×	×	×
4.	Electrical disturbances	√	×	√	×	√	×
5.	Electrical interruption	√	×	×	×	×	×
6.	Fire	√	×	×	×	×	×
7.	Hardware failure	√	×	√	×	√	×
8.	Liquid leakage	√	×	×	×	×	×
9.	User/operator error	√	√	√	√	×	√
10.	Software error	√	√	√	√	√	√
11.	Telecommunication interruption	√	×	√	×	√	×
12.	Data alteration	√	√	√	√	√	√
13.	Software alteration	√	√	√	√	√	√
14.	Bomb threat	√	×	×	×	×	×
15.	Employee sabotage	√	×	√	×	×	×
16.	Enemy overrun	√	√	√	×	×	×
17.	Fraud	×	×	√	√	√	√
18.	Consumption of resources	√	×	×	×	×	×
19.	Terrorism	√	√	√	×	×	×
20.	Theft	√	√	√	×	×	×
21.	Unauthorized use	√	√	√	√	√	√
22.	Vandalism	√	√	√	×	×	×

threats can affect the functioning of ITS because of its dependability on wireless communications and thus it may lead to accidents. The primary threats / attacks which may affect the intelligent transportation system with their counter measures provided in the proposed SeCBVE based IRTMCS are presented in figure 7 [56, 57].

From security point of view the different attributes involved in SeCBVE based IRTMCS are: the drivers, on-board persons, road side unit (RSU), third party entities, malicious attackers, and videos of accidents. The drivers are one of the most important elements of IRTMCS. The driver will have to take decisions in the cases of accidents, and malicious attacks to ensure the wellbeing of persons seating in the vehicle. The on-board persons refer to all the persons seating in the vehicle at the time of malicious attacks or accidents. The road side units can be further classified into two namely normal road side units (NRSUs) and malicious road side units (MRSUs). The NRSUs will give the actual and correct information to the IRTMCS whereas MRSUs may give misleading information to the IRTMCS. The examples of third party entities are transportation regulatory agencies, nearby hospitals, nearby police stations and the relatives of the driver to whom the messages are to be transmitted automatically. The third party entities can be trusted or semi-trusted, and they are accountable for managing the whole situation after receiving the message and videos of accident. The malicious attackers attempt to breach the security of IRTMCS by using several techniques. These attackers can be categorized into different categories. The threat categories and the corresponding corrective actions taken by the proposed SeCBVE based IRTMCS are presented in table 2.

In the proposed system different components of SeCBVE based IRTMCS are communicating with each other with objective to save the life of persons who are struggling to be hospitalized within in limited period of time. Therefore, overall communication time computation becomes exceptionally important. Table 3 presents the amount of time (in seconds) which is taken by each task/phase of the proposed system in order to complete the communication.

The results of table 3 reveal that the proposed system completes communication with all concerned authorities and persons about the accident within first five minutes of accident occurrence. As per the recent reports of *World Health Organization (WHO)* more than 1.5 million (Fifteen Hundred Thousand) people die every year in road accidents on this earth and approximately 25% of these people are dying because of nonavailability of in time medical aid. Hence, if the concerned authorities and persons take immediate corrective measures after getting information from IRTMCS about the accident then the life of maximum of these 25% persons including women and children who are dying every year in accidents can be saved [16]. Therefore, it can be firmly said that the world wide implementation of the proposed SeCBVE based IRTMCS can save the life of approximately 400,000 (Four Hundred Thousand) persons including women and children every year. Since, every day a large number of new vehicles are coming to the roads. Therefore, the number of accidents and the corresponding death of persons will further increase

Table 3. Time taken by each task/component/phase of SeCBVE based IRTMCS for storing and sending voice signals and video images.

	Component/phase/task name	Properties	Time required for communication
1.	Video cameras	The five video cameras of vehicle capture continuous videos images immediately after the start of vehicle and these videos with voice signals are stored in memory of IRTMCS	Not applicable
2.	Processor 1 (Key processor)	Stores video images and voice signals continuously in the memory, transmits voice calls, voice signals and video images to concerned authority / person, assigns tasks to Processor 2(Extra Processor) and directs / controls Processor 2	Not applicable
3.	Processor 2 (Extra processor)	Helps key processor in executing the assigned tasks including storing voice signals and video images in the memory	Not applicable
4.	Pressings emergency button	A person driving the vehicle or seating in the vehicle can press the E*mergency Button*. If once the *Emergency Button* is pressed then the communication and videos with voice signal transmission system becomes active	Within 5 Seconds (approximately)
5.	Search the location of accident	The GPS of IRTMCS is used to search and display the location of accident instantly after pressing the *Emergency Button*	Within 2 seconds (approximately)
6.	Search the nearest police station's location, ambulance location and their phone numbers	The GPS of IRTMCS with Google search application software is used to search the nearest police station's phone number	Within 2 second (approximately)
7.	Search the location of nearest hospital and the corresponding phone number	The GPS and Google search application software is used to search the location of nearest hospital and the corresponding phone number	Within 1 second (approximately)
8.	Search the phone numbers of driver's relatives and vehicle owner	The database of proposed IRTMCS is used to search phone numbers of vehicle owner, and driver's relatives	Within 1 second (approximately)
9.	Contact the nearest police station/vehicle owner/driver's relatives through recorded voice messages	The automatic phone caller of proposed IRTMCS is used to contact the concerned authority and persons through recorded voice phone calls	Approximately 30 seconds for each phone call
10.	Sending recorded accident videos to the concerned authority/person	The processor1 and processor2 of proposed IRTMCS is used to transmit the recorded voice signals and videos of approximately sixty seconds to the concerned authority and persons	Approximately 30 seconds for each destination

Table 4. Performance analysis of proposed system with other existing system.

Algorithm/technique name	Available features								
	Video cameras available	Parallel processing	GPS based accident location searching	GPS integrated nearest police station phone searching	GPS integrated nearest hospital phone searching	Driver's relatives phone in database	Voice based alert and reminder call available	Video images and voice signals transmission to nearest police station	Video images and voice signals transmission to relatives of driver
1.Nova genesis model for future internet and IoT [2]	√	×	√	×	×	×	×	×	×
2.Intelligent public transport management system [13]	√	×	√	×	×	×	×	×	×
3.Accident detection and reporting system [58]	√	×	√	√	√	×	×	×	×
4.Intelligent transportation systems for smart cities [59]	√	×	√	×	×	×	×	×	×
5.Accident detection technologies and recovery systems [60]	√	×	√	×	×	×	×	×	×
6.Internet of vehicles for safe driving [61]	√	×	√	×	×	×	×	×	×
7.Traffic accidents analyzer [62]	√	×	√	×	√	×	×	×	×
8.Road accident prevention in vehicular ad-hoc networks[63]	√	×	√	√	√	×	×	×	×
9.Intelligent traffic information system [64]	√	×	√	×	×	×	×	×	×
10.Accident detection and reporting system [65]	√	×	√	×	×	×	×	×	×
11.Cloud based authentic accident detection and management [66]	√	×	√	√	√	×	×	×	×
12.Geo-based mechanism for vehicular networks [67]	√	×	√	×	×	×	×	×	×
13.Accident prevention using VANET [68]	√	×	√	×	×	×	×	×	×
14.Proposed SeCBVE based IRTMCS	√	√	√	√	√	√	√	√	√

in the forthcoming years. Hence, the world wide implementation of the proposed SeCBVE based IRTMCS will save the life of millions of people every year and it will be an appropriate tribute to the women and children who lost their life in last many decades.

The performance comparison of the proposed SeCBVE based IRTMCS with other existing *road traffic accident death prevention systems (RTADPS)* in terms of available features and distinctiveness is presented in table 4. The results of table 4 show that the proposed SeCBVE based IRTMCS gives promising performance and it includes all the necessary features which are required for an accountable, reliable and flawless RTADPS.

5. Conclusions

In this research paper, the author has presented an innovative SeCBVE based IRTMCS approach for preventing the deaths of individuals including women and children in road accidents. The implementation of the proposed approach brings us to a juncture where death percentage of persons in road accidents is decreased by 25% and approximately the life of approximately 400,000 (Four Hundred Thousand) persons including women and children can be saved every year by using the proposed system. The proposed approach uses secure cloud (SeC) based online cameras called virtual eye and internet of things (IoT) for implementing an unblemished and smart road traffic accident death prevention system.

The proposed IRTMCS uses two parallel processors (master and slave) for speedy transmission of voice alerts, voice signals and video images of accident to the smart phones of concerned persons and responsible authorizes with minimum communication latency. Therefore, if one of these two processors stops working then the other processor will perform all the communication tasks like sending voice calls based information alerts and video images to specified phone numbers of nearest police station, nearest hospital, relatives of the driver and vehicle owner. The proposed SeCBVE based IRTMCS is capable to help the investigators in finding the cause of accident and it will help the judicial system in tracing the culprit on the basis of stored video images. It can be concluded from results and discussions sections that the proposed SeCBVE based IRTMCS gives promising performance in terms of efficiency, consistency and fault tolerance and it includes all the necessary features which are required for an accountable, reliable and flawless RTADPS.

References

[1] Albeshri A and Caelli W 2010 Mutual protection in a cloud computing environment. In: *12th IEEE International Conference on High performance Computing and Communications (HPCC)*, pp. 641–646

[2] Alberti M A and Singh D 2014 *Developing a Nova Genesis Architecture Model for Service Oriented Future Internet and IoT: An Advanced Transportation System Scenario*, IEEE World Forum on Internet of Things 2014, Seoul, Korea, pp. 6–8

[3] Singh D 2013 Developing an architecture: scalability, mobility, control, and isolation on future internet services. In: *Second International Conference on Advances in Computing, Communications and Informatics (ICACCI),* Mysore, India, pp. 1873–1877

[4] Khodadadi F, Calheiros R N and Buyya R 2015 A data-centric framework for development and deployment of internet of things applications in clouds. In: *Proceedings of the 10th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP 2015)*, Singapore, April 7–9, pp. 1–6

[5] https://en.wikipedia.org/wiki/Traffic_collision Last Accessed 5 July 2017

[6] Ahmed I, James A and Singh D 2014 Critical analysis of counter mode with cipher block chain message authentication mode protocol—CCMP. *J. Secur. Commun. Netw.* 7(2): 293–308

[7] Ahuja R 2011 SLA based scheduler for cloud storage and computational services. In: *International Conference on Computational Science and Applications (ICCSA)*, pp. 258–262

[8] Buyya R, Yeo C S and Venugopal S 2008 Market oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities. In: *Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications* (HPCC 2008, IEEE CS Press, Los Alamitos, CA, USA), Dalian, China, September 25–27, pp. 1–9

[9] Almulla S and Chon Y Y 2010 Cloud computing security management. In: *2nd International Conference on Engineering Systems Management and Its Applications*, pp. 1–7

[10] Mishra K N 2018 A novel mechanism for cloud data management in distributed environment. In: *Data Intensive Computing Applications for Big Data*, pp. 267–291

[11] Security guide for critical areas of focus in cloud computing V3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf. Last Accessed July 2017

[12] Singh I, Mishra K N,. Alberti A, Singh D and Jara A 2015 In: *9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 301–305

[13] Bhayya G and Raghava Rao K 2015 Intelligent public transport management system using embedded technologies. In: *National Conference on Advancements in Embedded Systems and Sensor Networks, India*, pp. 189–193

[14] Van Bon J and Van Der Veen A 2007 *Foundations of IT Service Management Based on ITIL*, vol. 3, Van Haren Publishing, Zaltbommel, pp. 1–317

[15] Miller M 2008 *Cloud Computing: Web Based Applications that Change the Way You Work and Collaborate Online*, Que Publication, London, pp. 1–312

[16] Plummer D C, Smith D, Bittman T J, Cearley D W, Cappuccio D J, Scott D, Kumar R and Robertson B 2009 *Gartner Highlights Five Attributes of Cloud Computing: Gartner Report*. USA, G00167182: 1 5

[17] Alger D 2005 *Build the Best Data Center Facility for Your Business*, Cisco Press, Indianapolis, pp. 1–20

[18] Jaehoon P Jeong and Eunseok Lee 2014 VCPS: vehicular cyber-physical systems for smart road services. In: *Proceedings of 28th International Conference on Advanced Information Networking and Applications Workshops*, pp. 133–139

[19] Hogan M, Liu F, Sokol A and Tong J 2011 *NIST cloud computing standards roadmap—Version 1.0*, Natl. Inst. Stand. Technol. Spec. Publ., pp. 1–63

[20] Mell P, Grance T 2009 *The NIST Definition of Cloud Computing. version 15*, National Institute of standards and Technology (NIST), Information Technology Laboratory, pp. 1–3 Online Available www.csrc.nist.gov

[21] Checkoway S, Damon M and Brian K 2011 Comprehensive experimental analyses of auto-motive attack surfaces. In: *Proceedings of the USENIX Security Symposium*, San Francis-co, pp. 77–92

[22] Woo S, Jo H J and Lee D H 2015 A practical wireless attack on the connected car and security protocol for in-vehicle CAN, *IEEE Trans. Intell. Transp. Syst.* 16(2): 993–1006

[23] Othmane L B, Fernando R, R. Ranchal, Bhargava B and Bodden E 2014 "Likelihood of threats to connected vehicles, *Int. J. Next-Gener. Comput.* 5(3): 1–14

[24] Koscher K, Alexei C, Franziska R, Shwetak P, Tadayoshi K, Stephen C, Damon M, Brian K, Danny A, Hovav S and Stefan S 2010 Experimental security analysis of a modern automobile. In: *Proceedings of the IEEE Symposium Security and Privacy (SP)*, pp. 447–462

[25] Kelarestaghi K B, Zhang W, Wang Y, Xiao L, Hancock K and Heaslip K P 2017 Impacts to crash severity outcome due to adverse weather and other causation factors. *Adv. Transp. Stud.* 43: 31–42

[26] Kelarestaghi K B, Heaslip K, Fessmann V, Khalilikhah M and Fuentes A 2018 Intelligent transportation system security: Hacked message signs. *SAE Int. J. Transp. Cybersecur. Privacy*, 1(2): 1–16

[27] Hoppe T, Kiltz S and Dittmann J 2008 Security threats to automotive can networks-practical examples and selected short-term counter-measures. In: *Proceedings of the International Conference Computer Safety Reliability and Security*, pp. 235–248

[28] Miller C and Valasek C 2015 *Remote Exploitation of an Unaltered Passenger Vehicle,* Black Hat USA, pp. 1–91

[29] Miller C and Valasek C 2013 Adventures in automotive networks and control units. *DEF CON* 21: 260–264

[30] Burakova Y, Hass B, Millar L and Weimerskirch A 2016 Truck hacking: an experimental analysis of the SAE J1939 standard. In*: Proceedings of the Work-shop Offensive Technologies (WOOT)*, pp. 1–10

[31] Higgins K 2019 State trooper vehicles hacked. pp. 1-8 [Online]. Available: https://www.darkreading.com/attacks-breaches/state-trooper-vehicles-hacked-/d/d-id/1322415. Accessed on: Jan. 7, 2019

[32] Jeihani M and Banerjee S 2018 "Drivers behavior analysis under reduced visibility conditions using a driving simulator. *J. Traffic Logist. Eng.*, 6(2): 48–52

[33] Jeihani M, Narooie Nezhad S and Kelarestaghi K B 2017 "Integration of a driving simulator and a traffic simulator case study: Exploring drivers and Australian Shen. *IATSS Res.*, 41(4): 164–171

[34] Greenberg A 2015 Hackers remotely kill a jeep on the highway with me in it, *Wired* 7: 1-20

[35] Yan C, Xu W and Liu J 2016 Can you trust autonomous vehicles: Contact- less attacks against sensors of self-driving vehicle. *DEF CON*, 24: 1-18

[36] Foster I D, Prudhomme A, Koscher K and Savage S 2015 Fast and vulnerable: A story of telematic failures. In*: Proc. Workshop Offensive Technologies (WOOT)*, pp. 1–9

[37] Blum J and Eskandarian A 2004 The threat of intelligent collisions. *Journal of IT Prof.*, 6(1): 24–29

[38] Oka D K, Furue T, Langenhop L, and Nishimura T 2014 Survey of vehicle IOT bluetooth devices. In: *Proc. IEEE 7th Int. Conf. Service-Oriented Computing and Applications (SOCA),* pp. 260–264

[39] Sumra I A., Iftikhar A., Halabi H and Jamalul-lail A 2011 Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET). In: *Proc. IEEE 3rd Int. Cong. Ultra Modern Telecommunications (ICUMT) and Control Systems and Workshops,* pp. 1–8

[40] Sumra I A, Hasbullah H B and AbManan J B 2015 Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey. In: *International Conference on Vehicular Ad-Hoc Networks for Smart Cities*. 2015, pp. 51–61

[41] Jafarnejad S, Castignani G and Engel T 2017 Towards a real-time driver identification mechanism based on driving sensing data. In: *Proc. IEEE 20th Int. Conf. Intelligent Transportation Systems (ITSC)*, pp. 1–7

[42] Tyagi P and Dembla D 2014 Investigating the security threats in vehicu- lar ad hoc networks (VANETs): Towards security engineering for safer on-road transportation. In: *Proc. IEEE Int. Conf. Advances Computing Communications and Informatics (ICACCI), p*p. 2084–2090

[43] Schoettle B and Sivak M 2014 *A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia,* University of Michigan, pp. 1-38

[44] Jafarnejad S, Codeca L, Bronzi W, Frank R and Engel T 2015A car hacking experiment: When connectivity meets vulnerability. In; *Proc. IEEE Globecom Workshops (GC Wkshps),* pp. 1–6

[45] Greenberg A 2013 *Hackers Reveal Nasty New Car Attacks with Me Behind the Wheel*, pp. 1–4.[Online Available]: https://www.darkreading.com/attacks-breaches/state-trooper-vehicles-hacked-/d/d-id/1322415

[46] Miller C and Valasek C 2014 *A Survey of Remote Automotive Attack Surfaces*, Black Hat USA, pp. 1–94

[47] Mishra K N 2020 An efficient palm-dorsa-based approach for vein image enhancement and feature extraction in cloud computing environment. *Unmanned Aerial Vehicles in Smart Cities*, Unmanned System Technologies, pp. 73–94

[48] Gerdes R M, Winstead C and Heaslip K 2013 CPS: an efficiency-motivated attack against autonomous vehicular transportation. In: *Proceedings of the ACM 29th Annual Computer Security Applications Conference*, pp. 99–108

[49] Al-Sultan S, Al-Doori M M, Al-Bayatti A H and Zedan H 2014 A comprehensive survey on vehicular Ad Hoc network. *J. Netw. Comput. Appl.* 37: 380–392

[50] Bhoi S and Khilar P (2014) Vehicular communication: a survey. *IET Netw.* 3: 204–217

[51] Lebre MA, Mouel FL, Menard E, Dillschneider J and Denis R 2015 *VANET applications: Hot Use Cases.* Technical

Report hal-01024271, pp. 1–36. [Available online]: https://hal.inria.fr/hal-01024271. Access 6 July 2015

[52] Pietro RD, Guarino S, Verde N and Domingo-Ferrer J 2014 Security in wireless ad-hoc networks—a survey. *Comput. Commun*. 51: 1–20

[53] Mejri MN, Ben-Othman J and Hamdi M 2014 Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* 1(2): 53–66

[54] Engoulou RG, Bellaiche M, Pierre S and Quintero A 2014 VANET security surveys. *Comput. Commun*., 44: 1–13

[55] Petit J and Shladover S 2015 Potential cyber attacks on automated vehicles. *IEEE Trans. Intell. Transp. Syst*. 16: 546–556

[56] Kelarestaghi K B, Foruhandeh M, Heaslip K and Gerdes R 2019 Intelligent transportation system security: Impact-oriented risk assessment of vehicle networks. *IEEE Intell. Transp. Syst. Mag*. pp. 1–14

[57] Hamida E B, Noura H and Znaidi W 2015 Security of cooperative intelligent transport systems: standards threats analysis and cryptographic countermeasures. *Electronics* 4: 380–423

[58] Amala J 2013 *Accident Detection and Reporting System Using GPS, GRS, & GSM Technology.* A seminar report of Amal Jyoti College of Engineering, pp. 1–21

[59] Balasubramaniam A, Paul A, Hong W-H, Seo H C and Kim J H 2017 Comparative analysis of intelligent transportation systems for sustainable environment in smart cities. *MDPI J. Sustain.* 9: 1–12

[60] Keerthi Ch R, Shanmukh G and Sivaram R 2013 Various accident detection technologies and recovery systems with victim analysis. *Int. J. Adv. Trends Comput. Sci. Eng.* 2(3): 7–12

[61] Singh D and Singh M 2015 Internet of vehicles for smart and safe driving. In: *IEEE International Conference on Connected Vehicles and Expo*, pp. 328–329

[62] Abdullah E and Emam A 2015 Traffic accidents analyzer using big data. In*: IEEE International Conference on CSCI*, pp. 392–397

[63] Gokulakrishnan P and Ganeshkumar P 2015 Road accident prevention with instant emergency warning message dissemination in vehicular ad-hoc network. *PLoS ONE J.* 10(2): 1–36

[64] Al-Sakran H O 2015 Intelligent traffic information system based on integration of internet of things and agent technology. *Int. J. Adv. Comput. Sci. Appl*. 6(2): 37–43

[65] Amin M S, Jalil J and Reaz M B I 2012 Accident detection and reporting system. In: *Proceedings of International Conference on Informatics Electronics and Vision*, pp. 640–643

[66] Gautam R, Choudhary S, Surbhi, Kaur I and Bhusry M 2015 Cloud based automatic accident detection and vehicle management. In: *2nd International Conference on Science Technology and Management*, pp. 341–352

[67] Wang S, Yan Z, Geng G and Zhang Y 2016 Geo-based content naming and forwarding mechanism for vehicular networking over CCN. *Int. J. Internet Technol. Secur. Trans.* 6(4): 291–301

[68] Khandelwal S A, Abhale A B and Nagraj U 2014 Accident prevention and air pollution control using VANET under cloud environment. In: *Proceedings of 3rd International Conference on Recent Trends in Engineering and Technology*, pp. 900–804