Review Paper

# Privacy and security challenges in smart and sustainable mobility

Sara Paiva[1] · Mohd Abdul Ahad[2] · Sherin Zafar[2] · Gautami Tripathi[2] · Aqeel Khalique[2] · Imran Hussain[2]

Received: 7 February 2020 / Accepted: 29 May 2020 / Published online: 6 June 2020


**Abstract**
The current era of computing is witnessing a huge amount of data being generated with every passing moment. This massive data if nourished effectively can open new horizons for the computing world. The modern world is slowly but surely moving towards the automation age where every entity and object is being automated to perform desired tasks without the need of human interventions. This has made the lives of people more convenient and comfortable. Automation has taken over every single field of computing and even beyond. Smart mobility is one such example of automation wherein the users get real time information about the traffic conditions as well as alternate route suggestions in case of traffic jams. Transportation is considered as the backbone of every business. The automated intelligent transportation system (ITS) has completely transformed the way how people, goods and services are transported and is quite important for achieving sustainability. This paper provides an overview of the existing ITS system, concept of smart mobility and existing vulnerabilities in these systems. Their security concerns and scenarios are also analyzed. Furthermore, in this paper the importance and need for securing these intelligent systems is highlighted and future trends in ITS is also suggested. Although ITS and smart mobility technology are already providing convenient transportation and navigational facilities, there is still a huge scope to improve these facilities for the end users. The suggested future trends if integrated in an effective manner can provide exemplary means to provide state-of-the-art navigational facilities and smart mobility in a true sense.

**Keywords** ITS · Smart mobility · Vulnerabilities · Sustainability · Privacy · Security

## 1 Introduction

Smart cities are currently the path being followed by plenty of cities, majorly motivated by cultural, social and environmental sustainability issues. The emergence of information and communication technology (ICT) has increasingly fueled developments and new solutions that empower cities to autonomously and automatically make their processes more efficient. Two important factors contribute to this concept: the citizens themselves and technology. Combining these two factors, countless improvements can be made in a society, with resource optimization and very significant improvements and benefits for citizens. Smart urban mobility is one of the aspects included within smart cities and includes intelligent transportation systems (ITS) that contributes to reducing pollution, traffic congestion (citizens' quality of life), pedestrian and driver safety as well as making the transport network more efficient and easier to manage [1–4]. Authors provided some different interpretations for smart mobility. While one definition focuses on efficient mobility that makes no use of information technology; second one heavily relies on ICT to produce sustainable development with high impact on means of transportation (e.g.

✉ Sara Paiva, sara.paiva@estg.ipvc.pt; Mohd Abdul Ahad, itsmeahad@gmail.com; Sherin Zafar, zafarsherin@gmail.com; Gautami Tripathi, gautami1489@gmail.com; Aqeel Khalique, aqeelkhalique@gmail.com; Imran Hussain, ihussain@jamiahamdard.ac.in | [1]Instituto Politécnico de Viana do Castelo, Viana do Castelo, Portugal. [2]Department of Computer Science and Engineering, SEST, Jamia Hamdard, New Delhi, India.

SN Applied Sciences (2020) 2:1175 | https://doi.org/10.1007/s42452-020-2984-9

eco-vehicles, car sharing) and new solutions that make use of ICT (such as ITS) [5–9]. Technology can certainly be of tremendous benefit for solutions that can help smart mobility in cities. As a process that deals with people—citizens—their collaboration is necessary to implement sustainable solutions that makes their day easier. But while citizens are the first and foremost beneficiaries of smart mobility, the main issue that needs to be achieved is a balance between services to citizens and more political issues that contribute to overall well-being. The services made available to citizens address issues such as increasing productivity, reduced congestion and consequently fewer accidents, better air quality, among other things. The internet of things (IoT) and the internet of vehicles (IoV) will largely contribute to smart mobility but security and privacy will become a major issue when objects start to be connected with one another [10–12]. Security will mainly deal with illegal access to information which is something we are already facing these days with several attacks. On the other hand, smartphones, location and context-aware apps, which are part of some smart mobility solutions, share our location in social networks in ways that sometimes are transparent to some users which makes privacy issues a real challenge [13, 14].

Upcoming sections of this paper will provide detailed background and related study of the proposed study in Sect. 2 followed by identification of vulnerabilities of ITS in Sect. 3. Security approaches and sustainability connected with ITS are detailed in Sects. 4 and 5. Section 6 provides future trends of smart mobility. In Sect. 7 we present open issues and challenges in smart mobility. Finally, in Sect. 8, we present main conclusion of the paper.

## 2 Background of study through related work

With the rapidly evolving automation technology, mobility and navigation systems have also witnessed a complete paradigm shift. Already automated traffic alerts, real time alternate routes options, average turnaround and waiting time of commute etc. parameters are utilized to avoid users waiting in long queues for the limited transportation options. Now directly user can book the transport very easy just with a tap on the mobile phones. Focusing on above discussions this section provides a brief description about the rapidly evolving smart mobility systems. Several smart mobility services and solutions are already arising and becoming usual in many cities: on-demand ride services, ridesharing services, cab sharing programs, bike sharing programs, smart transportation, among so many others [13, 15]. Several cities are implementing mobility solutions to achieve flexibility, efficiency, integration, clean technology and safety. An example of this development and concern is Colombia, which has begun the commencement of traffic data collection to be able to take action to prevent security issues that might start to arise. This collection includes identifying collision points that may exist in cities and being alert for signs that may cause problems at an earlier stage. With these actions, the city is on its way to becoming the first Smart City in the United States, which will serve as an example to encourage other cities to follow suit. In the case of Barcelona, with 1.6 million inhabitants, it has made a bet on its bike-sharing system that is expected to save € 2.5 million per year. The system has a relatively economical annual price for citizens (up to 50 €). In Singapore, the existence of more than 5 million people and almost 1 million motor vehicles made betting on an ITS key to improving citizens' mobility. The Netherlands has long been known for its bet on bicycles as the main means of transport. But in the last 10 years it has led several other projects. One of them changed the way of waste collection reducing to a common truck the collection of organic and recyclable waste which contributed to the reduction of the number of trucks in the street [16]. Helsinki, Finland announced that by 2025 there would be no need for citizens to own their own cars. Instead, they will be able to use an on-demand mobility system that will make use of public and private transport and allow citizens to move as economically and as quickly as possible. Las Vegas is yet another example where self-driving bus pilot have been tested to contribute to the global plan by 2025 for half of the buses on the roads to be electric, with a large majority being secured by China [17].

### 2.1 Motivation

The rapid evolution of societies brings several challenges in terms of the mobility of people and goods, which are reflected in necessary changes at various levels and which serve as motivation for this work. The transport networks are evolving every day to be increasingly equipped with intelligence, an aspect to which we dedicate ourselves in the next section, due to the relevance that it will assume throughout the world in the near future. Digitization, which is also a reality in various sectors of society and business, also in the mobility and transport sector, will apply due to the opportunities and new challenges that it will allow, always with a view to better service for citizens. Accompanied by all these developments, there is also an urgent need to complement research on ITS and the safety aspects that surround it. In fact, security is widely applied to several factors due to the increasing number of attacks that we have seen, as a way for some to improperly take advantage of data that can correspond to personal and even legal damages. Understanding, therefore, the

vulnerabilities of these systems is fundamental in a contribution such as the one we make in this article and which aims to address the aspects of mobility and also the challenges that arise, where security proves to be one of the critical factors. Once the vulnerabilities are identified, we also identify solutions that can be an asset to all academics and companies working in these areas.

### 2.2 Intelligent transportation systems

The evolution of ITS will be a certainty towards the construction of smart cities, as regards citizens' ease of mobility. In order to achieve efficient traffic management, minimize congestion problems, maximize security and efficiently use available infrastructures, these intelligent systems have numerous application domains. There are some common stages in developing an ITS, namely: data collection, data transmission, data analysis and, based on all previous stages, providing information to the traveler. Data collection heavily relies on real-time observation. Information is captured through hardware devices (sensors, cameras, GPS, auto-locators, and so on) that underlie any ITS architecture and allow you to count the number of vehicles, calculate speed limits, weight vehicles, surveillance, etc. [18] All collected information is sent to a central server which stores all collected information for use in subsequent phases. Transmission of data within an ITS system is critical for information to reach citizens in real time. Information output from the data collection system is transmitted to a central server which, after processing, is sent, already processed and with useful information, to the end users of an ITS, the citizens. The information uses several channels to travel this circuit as the use of the internet, SMS, direct communication with the vehicle. Other ways that can be used include Continuous Air Interface Long and Medium Range (CAILM) or dedicated short-range communications (DSRC). Data analysis is centrally done and includes a variety of tasks from clearing out irrelevant data that may have been received, rectifying information or removing inconsistencies. Subsequently, adaptive logic analysis modules are used so that predictive information that may be important and relevant to end users in terms of congested areas, alternative path suggestions, etc. can be extracted. This is some of the information that may be the result of data analysis and is then passed on to end users. But a lot of other information can also be transmitted like calculating travel times, average driving speeds, delays, accidents, route changes, temporary conditions, etc. In addition to the means suggested above, such as the Internet or SMS, notices on the motorways or through the vehicles themselves can be used channels of interaction of an ITS with its end customers [19, 20]. Figure 1 shows the chaining of these phases from the collection of used information and devices to end users, as well as means of transmission.

### 2.3 Related work

The integration of new emerging technologies like wireless sensor networks, big data analytics, embedded systems, World Wide Web etc. has brought significant changes in the day to day processes across domains. The concept of Internet of Things has furthered this change by bringing automation in multiple areas. For the past several years, urban transportation system has seen continuous development and updating. Today, with the advent of technology there is a significant shift from the transportation system to the sustainable and intelligent transportation system with enhanced security, interconnectivity and automation. Ever since the introduction of Intelligent Transportation systems in the 1980's, there has been notable researches and developments in the

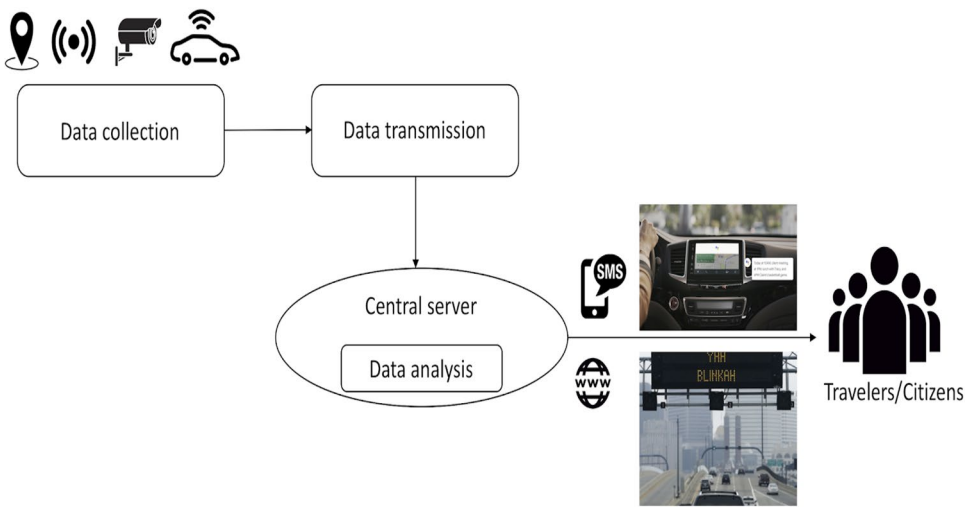


**Fig. 1** ITS stages and flow of communication

field. Some of the earliest works was presented in 1999 [21, 22] that highlighted the study on incident management in ITS. A data driven approach for the intelligent transportation system is presented by authors where the authors [23] have discussed the significance of data in the implementation of an intelligent system for Urban Transportation. An insight into the future prospects of data driven approaches for ITS is also given. Researchers have summarized some of the most significant efforts made in the vehicular communication systems and related technologies [24–26]. The concept of parallel transportation system highlighting both the engineering and social aspects is presented by the authors have further supported their work with experiments and real-world use cases and its applications [27]. The authors have also discussed some of the major categories of ITS like advanced traffic management systems, advanced traveler information system, commercial vehicle operations, advanced public transport system, advanced vehicle control system and advanced rural transport systems. Researchers have discussed the importance of the intelligence gained through several communicating and information sharing vehicles for efficient decision making to improve the transportation system functionalities. The authors have also highlighted the wireless landscapes like WSN that has supported the development and implementation of ITS [28, 29]. Various researchers also have highlighted the impact of location services specifically mobile phone location on the intelligent transportation system [30]. Authors have also discussed the impact of ICT in ITS highlighting the role of modern-day technologies like WSN, Data Analytics, IoT etc. in generating large volumes of data that can be analyzed to achieve a safe and efficient transportation system [31, 32]. A real time traveler information system is presented by various researchers. The work presented uses automatic Vehicle identification for estimating the journey time in real time [33]. Various works focused on the recovery and adaptation of ITS in cases of threats. A study was performed in 10 urban locations to study the resilience of the ITS in unfavorable circumstances and disruptions. ITS have opened new horizons and supported modern day technological concepts for easy implementation [34]. Researchers also have discussed the significance of the mobility data generated through ITS in a smart city domain. The mobility data can be analyzed and visualized to give insights into the urban traffic and people dynamics. The data can further be utilized in making decisions related to traffic control [35]. After focusing on the above discussions its necessary to identify various vulnerabilities on ITS as done in upcoming section.

## 3 Identified vulnerabilities on ITS

Although ITS security has been a major security concern for all researchers, but unfortunately very little attention has been given to assess the impact of various breaches affecting the transportation network. A large number of security vulnerabilities occur within the ITS network of which cyber-physical attacks need to be critically assessed and explored for its various consequences. This section discusses as well as analyzes the various adverse impacts on ITS system due to various security breaches. The various implications and effects are based on real-world analysis of ITS system. ITS is a part of Internet of Things (IoT) and Internet of Vehicle (IoV) through which around 19 billion to 40 billions of "things" are and will be connected [5]. Hence these systems are not only limited to known attacks but are affected by various innovative vulnerabilities. Hence the security aspects require more comprehensive and out of the box thinking. Various stakeholders of ITS include: the manufacturers, road users, legal authorities and service providers which are affected by various security breaches. The recent Yahoo and Equifax attacks resulted in privacy and security concerns for millions of stakeholders [36, 37].

Another vulnerability in the communication ITS due to the high level of heterogeneity. This vulnerability includes the lack of trustworthiness of heterogeneous devices, integrity, and reliability of these devices. Before initiating communication, these devices are required to establish a secure channel for communication. These secure channels are established after establishing trust among the communicating devices. Due to heterogeneity in the devices, privacy cannot be controlled once the communication is started. That is one of the reasons to establish trust among the communicating devices before starting the communication. The degree of trust is inversely proportional to the degree of privacy as shown above in Fig. 2 [23, 38]. In ITS,

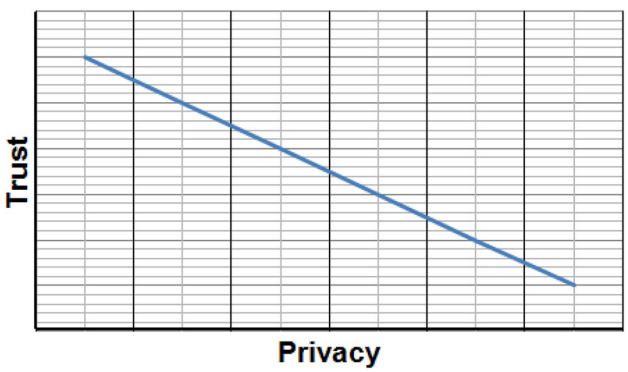


**Fig. 2** Relationship between the degree of trust and degree of privacy

communication among devices is initiated after establishing trust between the devices. Pre-existing trust relationships between devices are required as the IoT network is very dynamic and pervasive in nature. It is important to establish trust among the device at runtime before initiating communication [39, 40]. Trust establishment is also important as it takes care of data or information sharing/privacy preservation based on the trustworthiness of the device. The data or information being shared with other devices is private information and it must not be misused by the other device.

The various attacks on the ITS ecosystems and its consequent effects on the stakeholders can range from compromising the driver's privacy to the hacking of the vehicle. The Location tracking system in ITS can affect the privacy of the stakeholders and also may impose several problems on the road related to the movement tracking of individuals, unauthorized data collection etc. In ITS system, the vehicles send timestamps, position information, pseudo-identifiers and hello beacons periodically for effective communication. Any unauthorized access and leaking of this information can trigger serious privacy concerns where any unauthorized user can use this information to imposes severe consequences. Security attacks on vehicles like compromising the infotainment leaks private information and can extracts the data for further breaches. Further, the ITS vulnerabilities can attack the transportation system by interfering with the safety operation, efficiency, security, reliability, and drivers' behavior. Any in-vehicle hacking attempt like controlling the engine, brakes, steering wheel etc. can result in serious damages by compromising road users' safety. Road user's privacy is also affected by tracking attack that deteriorates malware installation. These attacks lead to monetary losses for road users, transportation operators, cause government distrust and increase vehicles' energy consumption. In another case any false recommendation (Bad-Mouthing attack) by any ITS node/vehicle can also results in security concerns and fake information generation. Thus, ITS attacks not only affect traffic safety but also make the drivers state traumatic resulting in impulsive behavior.

These attacks on the ITS systems can be broadly categorized into seven groups based on the kind of vulnerability it imposes on the ITS ecosystem. Firstly, it hampers the basic safety aspects of the road, driver and the vehicle itself. Secondly, it affects the fine-grained security aspects that includes compromising vehicles availability, compromising driver's privacy by tracking driver's trajectories, its fingerprinting driving pattern and eavesdropping passengers' communication, thus making vehicle a malicious node in the ITS network that leads to very high (VH) risks levels. Thirdly, the various attacks on the ITS ecosystem-imposed reliability questions on the whole system. Further the legal aspects of the attacks including the legal rights in case of hacking, road accidents due to unauthorized control etc. needs to be addressed scrupulously. Another category includes the operations. Operation group takes control of vehicle and compromise its critical components. It also leads to monetary loss of road users and system operators, increase travel time that causes delay, and disables crippled services. Risk exposures associated are marked as Very High (VH), High (H), Moderate (M), Low (L), and Very Low (VL). In operation group, taking control of vehicle operations results in Very High and High risks. Increase in travel time and delay are assessed as very low types of risks. Apart from this the overall system efficiency and the driver's behavior is also adversely impacted.

This section has detailed various attacks, affects and it's grouping risk levels on ITS system but there are no clear specifications of defining privacy and setting its boundaries. Privacy degree is dependent on various factors that include preferences of user, environmental settings, it's applications, regulations of a country and ambiguity in functioning. Since ITS system utilizes IOT system, traffic monitoring system, autonomous and non-autonomous mechanisms hence it sometimes deals with integrity, sometimes provide security but violate the privacy of the users also security and privacy contradict each other in specific scenarios. Various security approaches taking into mind a universal business model needs to be adopted. Upcoming section lists the various security approaches adopted for ITS for reducing the effects of various shortcomings listed in this section.

## 4 Security approaches

Above section has highlighted upon various vulnerabilities existing in ITS systems. Figure 3 shown below comprises security approaches towards the above-mentioned vulnerabilities. In ITS, the major points at which security mechanisms must be employed are at data collection (performed by IoT devices, sensors, actuators etc.), data transmission (through wireless transmission over the network) and data analysis (performed by computing resources at servers).

In this section, security approaches are discussed to ensure that the above-mentioned vulnerabilities shall be prevented in ITS.

1. *Secrecy* Confidentiality/Secrecy of information (data) transmitted shall be ensured by employing confidentiality mechanisms such as encipherment etc. It is imperative to maintain confidentiality of the data gathered through different sensors and IoT devices situated at multiple areas of interest. Strong crypto-

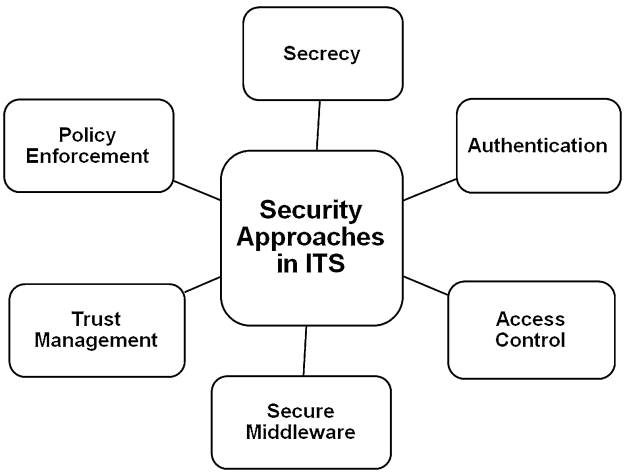


**Fig. 3** Security approaches in ITS

graphic mechanisms can be used to provide an intricate security model of such sensitive information.

2. *Authentication* Entity authentication and channel authentication can be provided by employing robust device identity mechanisms. Hijacking of IoT devices or tampering with sensors or other devices must be prevented to ensure authentication.
3. *Access control* Access control rules and policies must be defined to ensure authorized access to both devices and data. A hierarchical access control mechanism must be devised to ensure isolated access privileges to the individuals in order to ensure privacy and security of the data and other participating individuals.
4. *Privacy preservation* Privacy is most important concern in this type of network especially ITS. Privacy shall be preserved by ensuring compliance to regulations of the intended geography. Privacy shall not be compromised on the cost of computation. However, accurate recommendation about traffic sometimes may exploit privacy preservation to an extent.
5. *Policy enforcement* Proper guidelines and compliance from the regulatory organization must be enforced in establishing communication among different heterogeneous vehicles.
6. *Trust management* Due to heterogeneity in the devices, privacy cannot be controlled once the communication is started. That is one of the reasons to establish trust among the communicating entities before starting the communication. Trust Management model is used to prevent security threats/attacks and routing attacks to increase the reliability of the communication in the network. It also increases the efficiency of computing resources and the robustness of the network.
7. *Secure middleware* Security of middleware used in the data collection, data transmission and data analysis must be ensured from any kind of tampering, hardware faults, damages due to exploitation or even hijacking. It's important that any security approach applied on ITS must be sustainable enough for further computing as discussed in section below.

## 5 Need for sustainable mobility

Effective and Efficient Transportation and mobility is a prime concern in businesses as well as daily chores of lives. It is imperative to devise novel approaches and techniques which provides energy efficient, convenient and sustainable transportation and mobility. The ability to commute in difficult terrains or providing effective mobility which is climate resilient can be a major step forward in achieving smart mobility in actual sense. The whole economy is in a way dependent on transportation. Whenever there is a slight hindrance in transportation, the economies are directly and adversely impacted with it. Therefore, there is an emergent need for sustainable, effective and convenient measures to achieve smart transportation and mobility. Technology has to reach people beyond the social and economic barriers, only then the target of Sustainable Development Goals (SDG) will be met in a more inclusive manner. This penetration of technology to the remotest areas is also vastly depended on the effective mobility. With better transportation and mobility, state-of-the-art facilities which are till now limited to people living in urban and sub-urban areas can be provided to rural and remote areas. These facilities include effective healthcare, sanitation, clean drinking water, education and other forms of livelihoods. In order to achieve all these, there is a need of region-specific approach or a generalized approach for achieving sustainability. However, in either cases its necessary to define clear goals and follow a systematic approach to achieve those goals.

### 5.1 Benefits of sustainable mobility

There are several benefits that are directly related to achieving sustainable and energy efficient mobility. Some of the most crucial ones are given below:

1. Much Reduced Air and Noise Pollutions
2. Saves time by providing real time updates on traffic conditions
3. Better traffic management
4. Seamless connectivity even in cases of natural disasters and other extreme calamities.
5. Improved reachability
6. Integration of small business with the larger ones.

7. Providing better facilities to rural and suburban masses.
8. Improves economy and livelihoods.
9. Facilitates better governance.

Next section highlights upon the future trends in smart mobility.

## 6 Future trends in smart mobility

There is a huge scope of improvement in the existing ITS ecosystem. With the technologies like block-chain, there can be a more secure and privacy preserved ITS. The immutable structure and hash-based coding make it very difficult to tamper data secured through the block-chain. Every chain of the block-chain is linked to the previous one, which means that even if the intruder tries to tamper one block, he has to traverse back to each and every block of the chain which is practically a near impossible thing. Since ITS involve data collection and integration from a variety of devices and entities, block-chain can be an ideal candidate for securing such data.

The smart mobility plays a crucial role in leveraging the way we commute and do transportation. It is estimated that on an average, an individual spends more than 35 h a year stuck in traffic jams. With the help of smart navigations and real time traffic updates, this precious time can be saved. Transportation is a necessity of life; user needs some kind of transportation in our daily chores of lives as well as in the businesses. The ability to receive real time updates and options for alternate routes, navigational systems are already helping the consumers. However, with the scale of data generated in a typical ITS, there is a huge scope for improvements. The big data generated through the entities of ITS can be used to discover deeper insights and take much better decisions. Furthermore, since ITS is a highly dynamic network which needs alteration of the topology with respect to the traffic conditions and several other factors like emergency on road, accidents etc., there is a need for a dynamic network management system which can handle such complexities. Software defined networking (SDN) is one such technology which can handle dynamic network updating requests with ease [41]. This is because of the inherent feature of SDN that separates the data plane and the control planes which means that the control of network routing, topologies, traffic management and monitoring can be handled through an automated software rather than being dependent of the hardware like routers, switches or gateways. The limiting issues and challenges in the existing mobility frameworks of the ITS can be overcome using SDN to a much larger extent.

Another crucial technology that can be proved to be crucial for ITS is the software defined storage (SDS). The SDS is a fairly new technology developed with an aim to provide need based, easy to manage, scalable and agile storage options. The storage can be dynamically managed with respect to the changing needs of the organizations. The dynamic storage is very crucial in ITS where there is a sudden change in traffic conditions. In cases of sudden traffic change, more information is being generated and a different scale of processing is required. The existing ITS systems are harnessing the power of artificial intelligence and deep learning to come up with automation models which works well in different traffic conditions. However, with block-chain, SDN and SDS technologies, the ITS Ecosystems can take a totally new dimension and can be expanded to provide state-of-the-art services to the consumers [42, 43].

## 7 Open issues and challenges in smart mobility

The modern-day enabling technologies like Cloud, Fog/Edge, Artificial Intelligence, IoT plays an important role in realization of smart mobility. In ITS, real time analysis and decision making are highly crucial. In such situations, Fog/Edge computing frameworks come handy. Such frameworks enable the processing of data very close to its source thus minimizing network latencies and cost of uploading data of the cloud storage for analysis. This makes the whole system much faster and more efficient. However such technological solutions have their own inherent limitations and challenges like [44–46]:

1. *Processing capabilities* although the Fog/Edge computing solution facilitates processing of data very near to its point of generation, these systems have constrained capacities and processing capabilities restricting them to process large amount of data or do complex computations.
2. *Energy consumption* the Fog Computing paradigm uses very high amount of energy for processing the data and creation of fog nodes for communications
3. *Security issues* both Fog and Edge computing frameworks are vulnerable to security breaches. Due to the constrained processing and storage capacities, no strong security mechanism can be deployed on these systems. This makes them an easy prey for the malicious attackers and hackers. These systems are generally prone to DDoS, Side Channel and Eavesdropping attacks.
4. *Limited user involvement* the prime aim of the fog and edge systems is to enable an automated working

mechanism with minimum or no human interventions in ideal situations. This is to ensure faster processing and delivering near real time solutions. However, this can lead to severe problem in case of network outage, external attacks, natural calamities etc.

On another hand, the emergence and popularity of smart cities concept has led to the fast adoption of technological interventions across all aspects of smart cities including the smart mobility domain. Over the years researchers have raised concerns about the issues and challenges associated with development and adoption of Intelligent transportation system. The authors in [47, 48] have discussed the various concepts related to the privacy aspects for designing a trustworthy Intelligent Transportation System. A relationship between the technical aspects of ITS and the various threats associated with ITS is identified by presenting a matching between the various ITS functionalities like Traffic Surveillance, Vehicle Surveillance, Inter-Agency Coordination, PaymentSystems, One-WayMobile Communications, Two-WayMobile Communications, Stationary Communications etc. and the privacy concepts like Isolation, Provenance-ability, Traceability, Availability, Integrity, Confidentiality etc. Further the authors have highlighted how the various threats and privacy issues can be addressed.

There are several inherent and external issues and challenges associated with widespread adoption of smart mobility technology on a global scale. Some of these include:

1. *Lack of underlying infrastructure* The underlying infrastructure constitute the backbone of the smart mobility network. Several smaller economies are not capable of creating the required infrastructure need to adopt smart mobility solutions.
2. *Fear of technology failure* The general public is not well versed with the technological advancements around the globe. Due to several cyber threats and crimes in past, the older generation prefer to use conventional modes of transportation rather than relying on smart mobility solutions. Personal Safety and security are of prime importance while adopting new technologies like smart mobility solutions.
3. *Lack of standard operating rules and regulations* Even today with exponentially expanding technological advancements, there is no standard set of rules and regulations available which can govern the smart mobility solutions. Several localized mechanisms which exists, fail to compliment the complexities of smart mobility.
4. *Interoperability* The synchronization of legacy mobility systems with smart mobility solutions poses an intricate challenge. To the best of our knowledge there is no single solution available which is truly interoperable and provide smart mobility solutions
5. *Heterogeneity* The diverse nature of information generated from sensors and corresponding use cases makes smart mobility a more challenging task. Urban mobility solutions pose unique challenges which are fundamentally different from rural and semi-urban mobility solutions.
6. *First and last mile connectivity* This is one of the most prominent challenge to be addressed by the smart mobility solutions. It is often observed that the first and last mile connectivity problems are not addressed in generalized legacy mobility solutions.

In order to harness the true potential of smart mobility, it is imperative to address all these limitations and challenges in future researches by devising novel and sustainable mechanisms.

## 8 Conclusions

With growing mobility in this internet era various transportation infrastructures must be designed to move people and goods seamlessly faster in a convenient way in both urban and inter-urban environments. Intelligent transportation systems are the heart of smart mobility era which needs to be more competitive, cohesive and secure. Smart cities are currently the path being followed by plenty of cities, majorly motivated by cultural, social and environmental sustainability issues. The emergence of Information and Communication Technology (ICT) has increasingly fueled developments and new solutions that empower cities to autonomously and automatically make their processes more efficient. Two important factors contribute to this concept: the citizens themselves and technology. Combining these two factors, countless improvements can be made in a society, with resource optimization and very significant improvements and benefits for citizens. Intelligent transportation system requires intelligent infrastructure to process the real-time information for business requirement. Various technological innovations of remote sensing, advanced analytics, integrated scheduling etc. will become the backbone of ITS incorporating smart mobility. As stated, that around 53% of population of world is a part of urban area and by 2050 this growth will be up to 67% so ITS will be sooner the heart of smart city environment. So, the equation of smartness is clear: no smart city without smart mobility and no smart mobility without ITS. Trust Management models are utilized in ITS to establish trust and ensure secure communication among the devices. They will also calculate trust value for other devices to

prevent security threats/attacks and increase reliability of the communication in the network. This will also increase the efficiency of computing resources and the robustness of the network.

## Compliance with ethical standards

**Conflict of interest** The authors declare no conflicts of interest.

## References


1. Hoh B, Gruteser M, Xiong H, Alrabady A (2006) Enhancing security and privacy in traffic-monitoring systems. IEEE Pervasive Comput 5(4):38–46
2. Papadimitratos P, Fortelle AL, Evenssen K, Brignolo R, Cosenza S (2009) Vehicular communication systems: enabling technologies, applications, and future outlook on intelligent transportation. IEEE Commun Mag 47(11):84–95
3. Sobral T, Galvão T, Borges J (2019) Visualization of urban mobility data from intelligent transportation systems. Sensors 19(2):332
4. Staricco L (2013) Smart mobility: opportunità e condizioni. J Land Use Mob Environ 6(3):342–354
5. Dimitrakopoulos G, Demestichas P (2010) Intelligent transportation systems. IEEE Veh Technol Mag 5(1):77–84
6. GEOTAB (2018) What is smart mobility? Last accessed on 30 Aug. https://www.geotab.com/blog/what-is-smart-mobility/
7. Mimbela LEY, Klein LA (2000) Summary of vehicle detection and surveillance technologies used in intelligent transportation systems. Federal Highway Administration s (FHWA) Intelligent Transportation Systems Joint Program Office. Available at https://www.fhwa.dot.gov/ohim/tvtw/vdstits.pdf. Accessed 1 Feb 2020
8. Papa R, Gargiulo C, Russo L (2017) The evolution of smart mobility strategies and behaviors to build the smart city, pp 409–414. https://doi.org/10.1109/mtits.2017.8005707
9. Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media Inc, Sebastopol
10. Thierer A, Castillo A (2015) Projecting the growth and economic impact of the internet of things, vol 15. Mercatus Center, George Mason University, Fairfax
11. Carlson M, Yoder A, Schoeb L, Deel D, Pratt C, Lionetti C, Voigt D (2014) Software defined storage. Storage Networking Industry Association, working draft, pp 20–24
12. Hubaux J-P, Capkun S, Luo J (2004) The security and privacy of smart vehicles. IEEE Secur Priv 2(3):49–55
13. El Faouzi NE, Leung H, Kurian A (2011) Data fusion in intelligent transportation systems: progress and challenges—a survey. Inf Fusion 12(1):4–10
14. Gerdes RM, Winstead C, Heaslip K (2019) CPS: an efficiency-motivated attack against autonomous vehicular transportation. In: Proceedings of ACM 2
15. Tubaishat M, Zhuang P, Qi Q, Shang Y (2009) Wireless sensor networks in intelligent transportation systems. Wirel Commun Mob Comput 9(3):287–302
16. Ganin AA, Mersky AC, Jin AS, Kitsak M, Keisler JM, Linkov I (2019) Resilience in intelligent transportation systems (ITS). Transp Res C Emerg Technol 100:318–329
17. Schoettle B, Sivak M (2014) A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia
18. Zhao Y (2000) Mobile phone location determination and its impact on intelligent transportation systems. IEEE Trans Intell Transp Syst 1(1):55–64
19. Kelarestaghi KB, Heaslip K, Fessmann V, Khalilikhah M, Fuentes A (2018) Intelligent transportation system security: hacked message signs. SAE Int J Transp Cybersecur Priv 10:10. https://doi.org/10.4271/11-01-02-0004
20. Tam ML, Lam WH (2011) Application of automatic vehicle identification technology for real-time journey time estimation. Inf Fusion 12(1):11–19
21. Nunes BAA, Mendonca M, Nguyen XN, Obraczka K, Turletti T (2014) A survey of software-defined networking: past, present, and future of programmable networks. IEEE Commun Surv Tutor 16(3):1617–1634
22. Thereska E, Ballani H, O'Shea G, Karagiannis T, Rowstron A, Talpey T, Zhu T (2013) IOFlow: a software-defined storage architecture. In: Proceedings of the twenty-fourth acm symposium on operating systems principles. ACM, pp 182–196
23. Ming Y, Shen X (2018) PCPA: a practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks. Sensors 18(5):1573
24. Dötzer F (2005) Privacy issues in vehicular ad hoc networks. In: Proceedings of international workshop privacy enhancing technologies, pp 197–209
25. Ozbay K, Kachroo P (1999) Incident management in intelligent transportation systems. Norwood, MA: Artech House Publishers, pp 1–248. https://digitalscholarship.unlv.edu/ece_fac_articles/103
26. Viechnicki P, Khuperkar A, Fishman T, Eggers W (2015) Smart mobility, reducing congestion and fostering faster, greener, and cheaper transportation options. Deloitte University Press, New York
27. Elmaghraby A (2013) Security and privacy in the Smart City. In: 6th Ajman international urban planning conference AIUPC, United Arab Emirates
28. Miyajima C et al (2007) Driver modeling based on driving behavior and its evaluation in driver identification. Proc IEEE 95(2):427–437
29. Darabseh A, Al-Ayyoub M, Jararweh Y, Benkhelifa E, Vouk M, Rindos A (2015) Sdstorage: a software defined storage experimental framework. In: 2015 IEEE international conference on cloud engineering. IEEE, pp 341–346
30. Zhang J, Wang FY, Wang K, Lin WH, Xu X, Chen C (2011) Data-driven intelligent transportation systems: a survey. IEEE Trans Intell Transp Syst 12(4):1624–1639
31. Figueiredo L, Jesus I, Machado JT, Ferreira JR, De Carvalho JM (2001) Towards the development of intelligent transportation systems. In: Proceedings of the ITSC 2001. 2001 IEEE intelligent transportation systems (cat. no. 01TH8585). IEEE, pp 1206–1211
32. Fink WG (1995) Intelligent transportation systems. In: IEEE 1995 microwave and millimeter-wave. monolithic circuits symposium. Digest of papers. IEEE, p 3
33. Kelarestaghi KB, Zhang W, Wang Y, Xiao L, Hancock K, Heaslip KP (2017) Impacts to crash severity outcome due to adverse weather and other causation factors. Adv Transp Stud 43:31–42
34. Qu F, Wu Z, Wang F-Y, Cho W (2015) A security and privacy review of VANETs. IEEE Trans Intell Transp Syst 16(6):2985–2996
35. Ishtiaq Roufa RM et al (2010) Security and privacy vulnerabilities of incar wireless networks: a tire pressure monitoring system case study. In: Proceedings of the 19th USENIX security symposium, Washington, DC, pp 11–13
36. Selyukh A (2017) Yahoo hack likely breached 3 billion accounts, all that existed in mid-2013: the two-way: NPR. https://www.npr.org/sections/thetwo-way/2017/10/03/555016024/every-yahoo

-account-that-existed-in-mid-2013-was-likely-hacked. Accessed 7 Jan 2019
37. Newman LH (2019) Equifax officially has no excuse. Wired. https://www.wired.com/story/equifax-breach-noexcuse/. Accessed 7 Jan 2019
38. Wang FY (2010) Parallel control and management for intelligent transportation systems: concepts, architectures, and applications. IEEE Trans Intell Trans Sys 11(3):630–638
39. Kreutz D, Ramos F, Verissimo P, Rothenberg CE, Azodolmolky S, Uhlig S (2014) Software-defined networking: a comprehensive survey. arXiv preprint arXiv:1406.0440
40. Kim H, Feamster N (2013) Improving network management with software defined networking. IEEE Commun Mag 51(2):114–119
41. McKeown N (2009) Software-defined networking. INFOCOM Keynote Talk 17(2):30–32
42. Crosby M, Pattanayak P, Verma S, Kalyanaraman V (2016) Blockchain technology: beyond bitcoin. Appl Innov 2(6–10):71
43. Zyskind G, Nathan O (2015) Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE security and privacy workshops. IEEE, pp 180–184
44. Parikh S, Dave D, Patel R, Doshi N (2019) Security and privacy issues in cloud, fog and edge computing. Procedia Comput Sci 160:734–739
45. Roman R, Lopez J, Mambo M (2018) Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Gener Comput Syst 78:680–698
46. Shi W et al (2016) Edge computing: vision and challenges. IEEE Internet Things 3:637–646
47. Kalloniatis C, Kavroudakis D, Polydoropoulou A, Gritzalis S (2019) Secure and privacy-aware intelligent transport systems and their role on smart cities development (no. 19-05814)
48. Kalloniatis C, Kavroudakis D, Polidoropoulou A, Gritzalis S (2019) Designing privacy-aware intelligent transport systems: a roadmap for identifying the major privacy concepts. Int J Appl Geospat Res IJAGR 10(1):73–91