Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions

Preprint *in* IEEE Access · June 2019

DOI: 10.1109/ACCESS.2019.2922236

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2019.DOI

Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain based Solutions

TALAL ASHRAF BUTT[1], RAZI IQBAL [1], KHALED SALAH[2], MOAYAD ALOQAILY[3], YASER JARARWEH[4]

[1]College of Computer Information Technology, American University in the Emirates, Dubai, UAE
[2]Department of Electrical and Computer Engineering, Khalifa University, UAE)
[3]Gnowit Inc., Ottawa, ON, Canada
[4] Duquesne University, 600 Forbes Ave, Pittsburgh, PA, USA

ABSTRACT The Internet of Things (IoT) paradigm has integrated the sensor network silos to the Internet and enabled the provision of value-added services across these networks. These smart devices are now becoming socially conscious by following the Social Internet of Things (SIoT) model that empowers them to create and maintain social relationships among them. The Social Internet of Vehicle (SIoV) is one application of SIoT in the vehicular domain that has evolved the existing Intelligent Transport System (ITS) and Vehicular Ad-hoc Networks (VANETs) to the next phase of Intelligent by adding socializing aspect and constant connectivity. SIoV generates massive amount of real-time data enriched with context and social relationship information about vehicles, drivers, passengers and surrounding environment. Therefore, the role of privacy management becomes essential in SIoV, as data is collected and stored at different layers of its architecture. The challenge of privacy is aggravated because the dynamic nature of SIoV poses a major threat in its adoption. Motivated by the need to address these aspects, this paper identifies the challenges involved in managing privacy in SIoV. Furthermore, the paper analyzes the privacy issues and factors that are essential to be considered for preserving privacy in SIoV environments from different perspectives including privacy of a person, behavior and action, communication, data and image, thoughts and feelings, location and space, and association. Additionally, the paper discusses the blockchain based solutions to preserve privacy for SIoV.

INDEX TERMS Privacy Management, Blockchain, Social Internet of Vehicles, Internet of Vehicles, Social Internet of things, Internet of things.

I. INTRODUCTION

THE need of efficient transportation systems has surged a lot due to the increasing number of vehicles on roads. The rise of metropolitans has made it more challenging to manage the traffic and tackle issues posed by heavy traffic. There are various issues involved, however, traffic congestion, unreliable public transport, traffic accidents due to road conditions are the key issues that crucial to be addressed. Furthermore, the smart city paradigm requires efficient traffic management system for city administrations and novel applications for vehicle owners. Therefore, the importance of technical and original solutions is paramount for the provision of smart services to both road authority and drivers.

Traditionally, the transport management solutions are based on using Vehicular Ad-hoc Networks (VANETs) by provision of different applications and services e.g., automatic tolls, on-demand services, connectivity, to name few. The Internet of Vehicle (IoV) paradigm [1] advances the technology further by leveraging the data availability and enhanced connectivity enabled by Internet of Things (IoT). Furthermore, this paradigm has evolved to Social Internet of Vehicles (SIoV) [2] by enabling the smart behaviour of vehicles as advocated by Social Internet of Things (SIoT) [3]. This evolution allows the vehicles to create and manage social relationships between them based on their owners, context and application requirements. For example, two vehicles travelling towards the same destination will be able to create social relationships among them to share the traffic related information regardless of the distance between

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

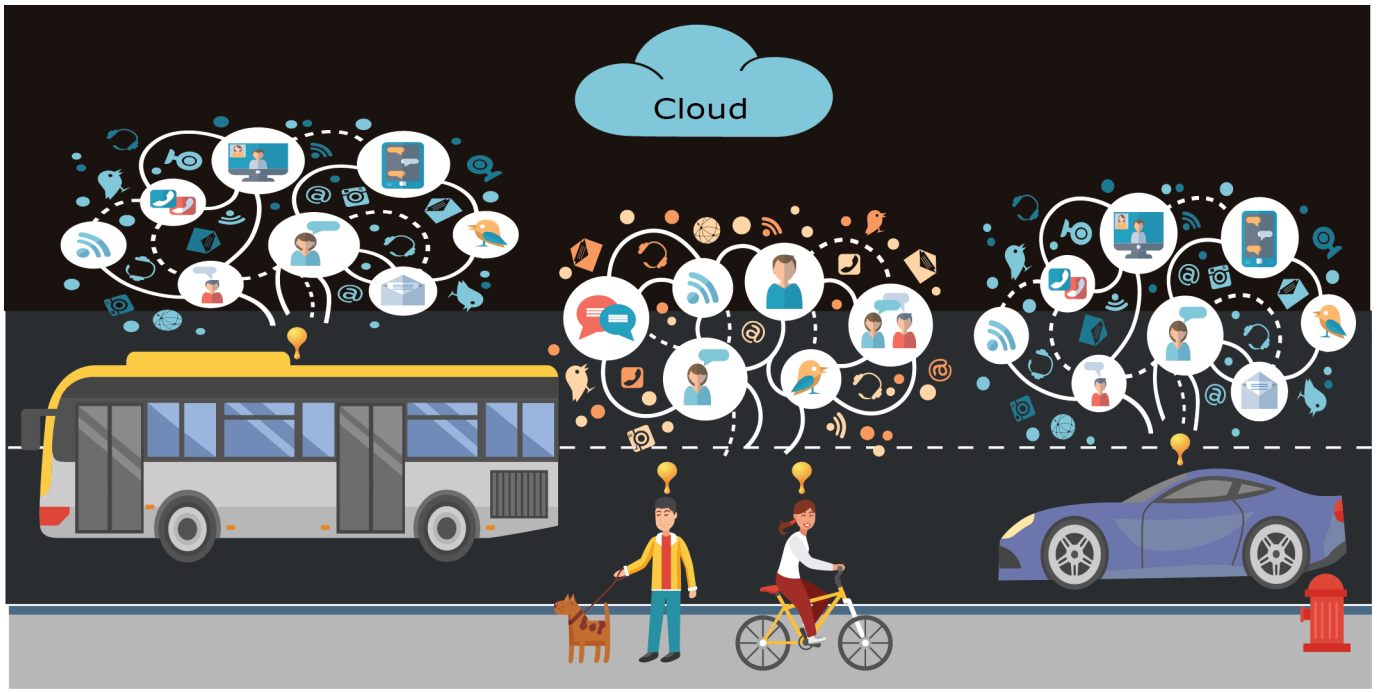


FIGURE 1: SIoV environment and data

them. A vehicle can even create new social relationships autonomously to gather the required data for its applications. For example, several vehicles travelling to the same station through different routes can form social relationships among them to share road conditions even when their owners have no existing relationship. The web of social relationships enables the discovery of potential partners, because trust of existing social relationships can be used to create new relationships when the data is required for a value-added service. For example, if an application requires information to help a driver to select a route where he can find a petrol station with minimum waiting time, then the vehicle can develop new social relationships with the vehicles on the route based on its existing relationships to get reliable information. SIoV enables several new traffic management applications that can work efficiently by exploiting the web of these relationships [4].

The increased data availability, connectivity and autonomy of vehicles in SIoV pose major threat to the privacy of its users [5]. The users of SIoV includes diverse vehicles, passengers, bicyclers, and pedestrians share multivariate data such as sensors' readings, audio, video and messaging as shown in Figure 1. The root cause remains the urge of the involved entities to collect data for different applications [6]. For example, a vehicle might create new social relationships to get congestion information from other vehicles that are travelling to the same destination, however, the vehicle can use the collected information for marketing as well. In this scenario, the privacy can be further violated if the vehicle shares this information to other entities that can benefit from the data without notifying the users involved. Similarly, the increased data availability to all entities is a requirement of SIoV, but an unaccounted data usage and its distribution raise many privacy violation flags. The uninterrupted connectivity fosters novel applications, but also exposes the vehicles to attackers because of inherent security issues in diverse communication technologies. Furthermore, the autonomy of vehicles to create relationships by sharing data, without the involvement of the users, is a serious concern for privacy violation.

The inherent risk of privacy violation comes from many different factors. First, the type of data that is being collected by different entities in a network can determine the way privacy of someone can be violated. In SIoV, different applications require variety of data including the vehicles statistics data, details about the driver and passengers, and social relationships information about the vehicles. These data are used, shared and reused depending on the requirements of applications. The data can be gathered from multiple sources even when it's not required. This unmetered data collection is a big challenge to protect privacy of the SIoV users. Secondly, even in the case of reliable applications, the gathered data is stored in devices to be reused, which poses another threat of data to be reused without the consent of a user. Finally, the security of the diverse communication technology involved in SIoV can be compromised by even a single link in the chain.

The weak privacy protection in SIoV is a grave risk for a user privacy and thus will lead to low adoption of the technology. There are several ways that compromised pri-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

vacy can affect users. For example, the location information about a certain individual can be used for tracking without a consent. Furthermore, the tracking information over a period can reveal the frequent destinations and activities of a certain user. In a worst-case scenario, this information can even be used to predict the future destinations of an individual. This situation is further aggravated in case of SIoV where the social relationship information can even expose your social contacts and their data. These kinds of information are vital for marketing and advertising companies to target their right customers. However, the main issue remains that the individual being tracked had no knowledge about how and where his data is being used. The goal of privacy protection is to offer a transparent system where a user should get full knowledge and control of his data.

Novel SIoV applications offer great benefits to its users but better privacy protection holds the key for its wide acceptance. There are several traditional privacy preserving solutions in VANETs e.g., using pseudonyms for anonymization of users and data, differential privacy, zero-knowledge proofs, secure multi-party computation, and encryption, etc. However, SIoV is a complex system that needs to ensure users' privacy preservation across different levels. Furthermore, the social relationship management and sharing of this relationships information with the other entities located at different layers of SIoV architecture is essential for the efficiency of the system, but it exacerbates the situation in case of a privacy leak.

As mentioned earlier privacy in SIoV is of outmost importance as breach in the privacy can cause serious inconvenience to the vehicular entities on road. Finn [7] categorized privacy into seven different types and one of the major contribution of this paper is to analyze the privacy in SIoV architecture in the light of these seven aspects. Several examples are provided for distinct scenarios at each layer of the SIoV architecture to understand the effect of these seven aspects of privacy on overall SIoV system.

Blockchain technology is an emerging trend in computing domain when it comes to securing shared information among distinct entities of a network. Blockchain can play a vital role in privacy management in SIoV. For example, authentication and authorization of accessing data in SIOV can be accomplished easily, in a trusted, secure, and decentralized manner, with complete openness, traceability and visibility to all stakeholders or actors within the built blockchain network using this technology. Furthermore, the sharing and storage of vehicular data while on the road can be made selective and restricted by smart contracts to only certain vehicles. One of the objectives of this paper is to summarize and review existing work found in the literature related to privacy management using blockchain for SIoV underlying networks and services

This paper emphasizes the privacy protection of the SIoV. The main contributions of the paper are:

1) Analyses the SIoV layered architecture from seven privacy aspects available in the literature and highlights the privacy issues in its architecture.
2) Presents the different challenges to preserve privacy in SIoV.
3) Presents the blockchain technology based solutions that can be employed for user privacy preservation in SIoV.

This paper covers the privacy perspective of SIoV in Section II by discussing the existing efforts and privacy types. Section III emphasizes the challenges to manage privacy in SIoV environments. Section IV scrutinizes each layer of SIoV architecture to analyze the privacy issues and mentions the existing privacy management schemes. Section V presents the trending blockchain-based solutions to manage privacy in SIoV, and the paper is concluded in Section VI .

II. PRIVACY PERSPECTIVE OF SIOV

A. PRIVACY TYPES AND THREATS

The future of transportation will be Connected Vehicles in Smart cities. There are few studies in the literature that analyze the privacy issues related to vehicular networks and Internet of Things as illustrated in Table 1. However, there is still a gap in the literature to analyze the privacy threats by taking into account the socializing aspect of SIoV and new trends in architecture such as Fog computing.

As this paradigm has shifted from the development to the deployment phase, privacy has multifarious aspects that need to be protected for SIoV users [15]. SIoV applications collect varied data about the vehicles and drivers that can be leaked to infringe the privacy of its users. It's essential to understand the types of users' privacy that need to be protected in SIoV. Traditionally, the privacy is categorized in four types [16] including privacy of a person, his behaviour, his data and communication. However, a more fine-grained definition and categories of privacy advocates seven types of privacy [7]. The new types of privacy include privacy of a person's location, association, and thoughts and feelings. Figure 2 presents the seven dimensions of privacy in SIoV environment.

a: Privacy of the person

Privacy of the person is related to keeping the physicality of a person private, e.g., keeping the operations, attributes and state of the persons' body private and should give full right to the person to disclose this information solely based on his preferences. This type of privacy is considered extremely important in SIoV systems as it might reveal information about the drivers and passengers in the vehicle including their body structures, health conditions to other entities of the network that might use this information to create an impression of the drivers and passengers of that vehicle.

b: Privacy of behaviour and action

This type of privacy encompasses keeping person's behaviours and actions private including their habits, political

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

TABLE 1: Existing related reviews of Privacy Management

Related efforts	Domain	Privacy types	Cloud	Fog	Social Aspects
[8], [9]	VANETs	General data	No	No	No
[10]	Ad Hoc Networks	Identity, data and location	No	No	Partially
[11]	VANETs	Identity, data and location	No	No	No
[12]	IoT	Identity and location	Yes	No	No
[13]	VANETs	Identity and location	No	No	No
[14]	VANETs	Identity, data, community and location	No	No	Partially

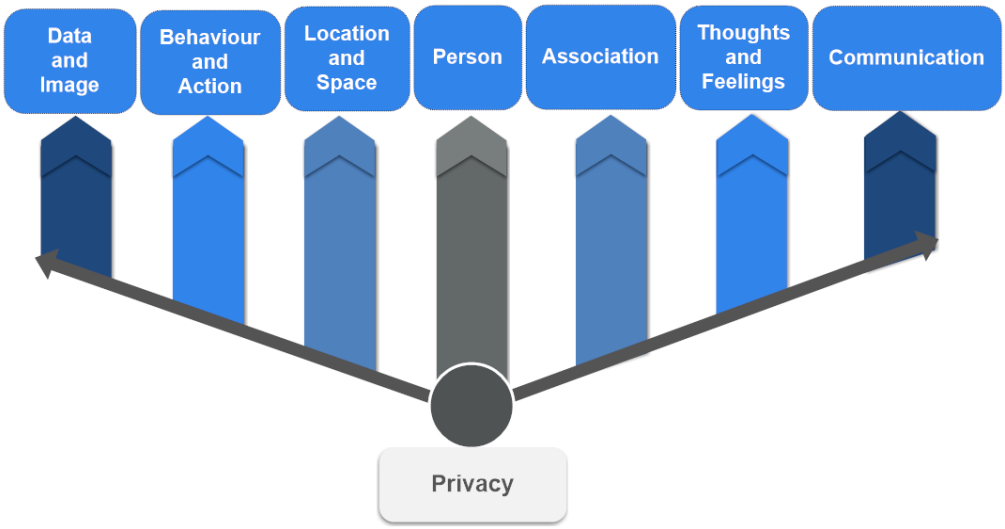


FIGURE 2: Privacy perspectives in SIoV

activities, personal interests and religious practices. This type of privacy in SIoV systems covers the ability of the entities to behave in private, public, semi-public spaces without being monitored or controlled by others including the authorities unless and until the actions and behaviours of a person are harmful to others. The monitoring of the behaviours and actions of the entities of SIoV system can be through CCTV cameras installed on the roads for traffic surveillance. Although such practices help in improving the traffic conditions on the road, drivers should be clearly informed about the data collected by the authorities.

c: Privacy of communication

Privacy of communication includes keeping personal communications, e.g., telephonic conversations, emails, covert chats or face-to-face discussions private. Advent in technology and utilization of several communication media requires privacy of communication to be strictly implemented, especially in SIoV systems where wireless communication technologies, e.g., Wi-Fi, Cellular and Dedicated Short Range Communication (DSRC) are used for transmitting information between different entities of the system. However, if proper security measures are not taken, this wireless communication can be intercepted by the hackers to steal sensitive private information of the entities including name, address, id, car insurance details and social relationships etc. The most applicable solutions these days are the use of learning technologies such as AI and Deep learning to secure vehicular communications [17] [18] [19].

d: Privacy of data and image

Privacy of data and image or multimedia is concerned about protecting the user generated varied data. The aim of this privacy is to verify that the user data is not automatically made available to undisclosed and hidden parties. For example, a vehicle can generate a multitude of data readings and images,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

that is shared by safety applications to a gateway device, need to be protected to be unknowingly shared to other entities that can use the data for undeclared purposes. The user is supposed to get control of his data and its usage. Enabling a substantial degree of control will build the confidence and trust of users and improve the acceptance of a system.

e: Privacy of thoughts and feelings

This type of privacy preserves the right of users to share their thoughts and feelings. The novel SIoV applications might be interested to find the thoughts or feelings of a user. For example, it is helpful for a safety application to know about a driver's feelings to plan better precautions. However, it is a right of individuals to think freely whatever they want. Therefore, any information shared about the thoughts and feelings of individuals is a threat to their privacy. This type of privacy is unique compared to the privacy of behaviour, because it's not mandatory that all the thoughts will be rendered by an individual's behaviour.

f: Privacy of location and space

All the users of a system have the right to be untracked in public or semi-public spaces. The privacy of location and space make sure that a user is not unwillingly identified, monitored or tracked by the system. In SIoV, the vehicles mostly share the information about the location to different applications and other vehicles, which required to be controlled and managed appropriately. It must be ensured that the information about a user's location and space is only shared with the relevant entities for a specific time to avoid tracking. The users should have the right to control the level of disclosure of information related to their current location and space.

g: Privacy of association

This privacy ensures liberty of individuals to associate and socialize without being monitored or supervised. This form of privacy is directly associated with the idea of SIoV, where the different levels of associations are being created between individuals and vehicles. The disclosure of a vehicle's location can violate the privacy of an individual, but leak of its social connections' information violates the privacy of association. Moreover, this kind of privacy violation even allows an infringer to infer information about the associates of a user. The social relationships information is vital in SIoV and increases its potential by enabling novel applications, however, a user should get a control of choosing which application can get access to its contacts and who can use that information.

III. PRIVACY MANAGEMENT CHALLENGES IN SIOV

SIoV is a special form of ITS where vehicular network entities including vehicles, Road Side Units (RSUs), drivers, passengers and pedestrians are expected to socialize with each other to enhance the qilaity of experience [20]. Vehicular network entities like vehicles and RSUs socializing with each other without human interventions might raise privacy concerns that require thoughtful review before distributing this information to other entities of the network. As the SIoV system is highly dynamic in nature, preserving the privacy of the entities in such a system depends upon several factors like architecture, context-awareness, user preferences, social relationships, communication technologies, goals, applications, security, and other environmental factors. This section provides an overview of the challenges involved in managing the privacy of SIoV system.

A. ARCHITECTURE

SIoV is currently in its emerging phase and requires extensive research when it comes to developing a generic architecture. Due to the nature of SIoV network, it endorses the current architecture of VANETs and IoVs. These vehicular networks provide both centralized and decentralized architectures [21]. A centralized architecture in vehicular networks follows the approach of a traditional social network in which information is processed, computed, stored, and analysed at the central cloud server. The data dissemination in centralized architecture is not necessarily in real-time and hence allows delay-insensitive apps. In decentralized architecture, however, the information is processed, computed, stored and analysed locally at object level and hence they have full control over information sharing. Such decentralization of information allows delay sensitive apps to be utilized in highly dynamic mobile environment like vehicular networks. The privacy in SIoV networks heavily depends on the type of architecture to be utilized for SIoV. A centralized architecture might be more information rich and be able to store and process a large amount of data, however, a single breach in server might expose user private information at large. Similarly, a decentralized architecture might ensure more privacy by providing privacy control to the users, however, it might limit the data accessibility and ultimately applications of SIoV system.

B. DATA AND SERVICE MANAGEMENT

Data and services management of SIoV is an easy task to handle especially with the privacy concerns. The data exchange or service provision of SIoV require computing, storage and communication infrastructure to allow for sensing, storing, aggregating, analyzing, processing and delivering various types of data and services. This will also include massive amount of data (i.e. big data) to be transferred and processed among vehicles and surrounded things. As such, the management side of this crowded and critical infrastructure have brought new and interesting challenges related to data processing, storage and networking for future smart cities [22] [23].

C. CONTEXT-AWARENESS

SIoV is highly mobile in nature as vehicles in SIoV are expected to move at a rapid pace and are expected to change their context in a quick manner [6]. Context in SIoV is related

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

to a situation at a certain point of time that might include vehicle locations, surroundings, neighbours and preferences. For example, a vehicle at one stage might require traffic information of a certain area, however, if the information is not provided at the right time, the vehicle might not require this information at the later stage due to change in its credentials. Context-awareness plays a vital role in preserving the privacy of entities of SIoV as the entities might agree to provide their personal data in the context of one situation, however, the same entities might not agree to provide the same data in the context of another situation. For example, a vehicle might agree to provide its location coordinates to a navigation app in order to navigate, however, the same vehicle might not agree to provide its location coordinates to a navigation app when itsit's not planning to navigate through that app. In this case, navigation app collecting the location coordinates of the vehicle without its consent would be considered as privacy breaching.

D. USER PREFERENCES

Advent of equipping the vehicular entities with the Internet has enabled these entities to share information with each other to enhance the overall road experience in vehicular networks. Although this information sharing would greatly benefit the transportation systems in smart cities but at the same time entities would have privacy concerns as their private data could be gathered, analysed, and utilized without prior notice. Most of the entities would like to control the sharing of their private information by clearly articulating their privacy preferences. For example, in modern vehicles, manufacturers would like to collect information from vehicle sensors for diagnostic purposes. However, most of the time, the process of collecting this information is automated, e.g., no vehicle owner interventions required. Such preprogramed systems collecting user information without considering user privacy preferences would result in privacy breaching and hence user preferences are considered an important factor in designing a privacy preserving model for SIoV systems.

E. SOCIAL RELATIONSHIPS AND TRUST

Social relationships are extremely important when it comes to information sharing amongst the trusted entities in a SIoV environment [24]. Rapid change in the topology of the SIoV network has an immense impact on the relationships of the vehicles with their peer vehicles and infrastructure, e.g., a vehicle on a highway at a certain instance might have 2 neighbours that might change when the vehicle takes an exit from the highway. A Vehicle might have a good or bad social relationship with its neighbouring vehicles depending upon its previous interactions with those neighbours, hence, Trust plays a key role in maintaining the social relationship amongst the vehicular entities in SIoV. A vehicle trusting its social contact might be willing to share its personal data with that contact without worrying about its privacy, however, a vehicle might be reluctant to share its personal data with a vehicle that it does not trust fearing about breaching of its privacy. In SIoV network, a new social relationship also requires entities to share their personal data to improve the trust between entities. For example, a vehicle requiring traffic information on upcoming junction from RSU which it has never communicated before, might have to share its current location, driver information and vehicle speed etc that enables RSU to share the traffic information and hence a new relationship is formed. However, this information is formed on a trust that RSU will not share the information gathered from the vehicle to other entities of the vehicular network without consent from the vehicle. Nevertheless, considering the amount of vehicular entities in a SIoV network, maintaining social relationships and hence ensuring the privacy of each entity might be a challenge that requires a system with extensive storage, secure communication and enhanced computing capabilities.

F. ENVIRONMENT

Open environment of SIoV poses several challenges associated to distributed control, proper use of communication, security, privacy, means of communication and lack of policies. Environment can form an ambiguity in the privacy management mechanism due to several parameters like scalability, system complexity, road types, traffic conditions, mobility patterns, and kind of communication [25]. Elevated scalability of SIoV system can affect the privacy of the entities of the system. Rising number of vehicles on road intensifies related factors with each entity of the system, for example, ids, names, sensor readings, manufacturers, messages, social relationships and travel history. More the data feed to the system, higher chances of breaching the privacy. For example, if a vehicle is storing only its current location and if this vehicle is compromised, only the current location of the vehicle will be exposed, however, if a vehicle is storing its id, manufacturer details, sensor readings, social relationships, reputation of its neighbours, travel history, messages, vacant car parking details and other vehicular details, the attacker can steal all the information from the vehicle by performing various security attacks. Furthermore, with open environment, vehicles are free to make new connections by sharing their personal information with other vehicular entities, however, this information in an open environment might be compromised due to lack of a strong security. Hence, it's a challenge to secure the private data of the vehicles in an open environment.

G. SECURITY

Security plays a critical role in designing privacy preserving mechanism for SIoV system [26]. Entities of SIoV are closely connected to each other in order to share information to enhance road experience, however, compromise of a single entity of the network might result in dreadful consequences. In a traditional SIoV system, entities are connected through a wireless medium that is susceptible to attacks. These attacks include, Denial of Service (DoS), impersonation, masquerading, eavesdropping and Sybil attacks etc. Veracity of commu-

nication protocols is of supreme importance in SIoV systems and hence the privacy of the system is directly proportional to the security of the system. For example, if a hacker attacks a RSU and gets full control over it, he/she can compromise a large amount of data being received by the RSU sent by vehicles on road as several vehicles might be sending personal details to this RSU for getting the traffic information at the next junction. Similarly, if vehicular communication is not secure, a hacker can eavesdrop the communication between vehicles and RSU using a transponder and later sell this personal information of vehicles, driver and passengers including their names, contact details, social media ids and images to the advertisement companies for making money. Hence security is of utmost importance when it comes to SIoV systems, however, implementing encryption techniques for securing vehicular communication requires high processing power, swift computations and brisk communication that is still a challenge in SIoV systems.

H. COMMUNICATION TECHNOLOGIES

Communication Technologies guarantee the seamless connectivity in SIoV. Vehicular networks utilize various communication technologies like Wi-Fi, Cellular Networks, Wi-Max, Bluetooth, ZigBee, DSRC and wired networks to connect various entities [27]. Socializing in SIoV requires sharing of vehicle details and sometimes personal details of drivers and passengers etc. Information transfer using these communicating technologies, requires ensuring the privacy of the transmitting data. In SIoV systems, mostly entities are expected to communicate with each other using wireless communication that makes privacy preservation quite challenging due to objects' visibility, network scalability, high mobility, anonymity of entities and enormity of data. For example, RSUs are comprised of numerous distinct sensors for collecting data like, vehicle speed, traffic congestion, and temperature etc. Each sensor is required to gather information for specific purpose, e.g., law enforcing agencies use vehicle speed to monitor traffic violations. However, if service providers (communication technology providers) start using this information in addition to providing this information to law enforcing agencies, it would be considered breach of privacy as service providers are not allowed to view and use this information meant for law enforcing agencies. However, with SIoV, enormous data is being collected, processed and stored that requires a mechanism to ensure that data is not being view or utilized at any level of communication. Designing such a mechanism to ensure privacy is a challenge due to the nature of SIoV and the amount of data being generated by SIoV system.

I. MOBILITY

SIoV network is highly mobile in nature that is comprised of entities changing locations at a rapid speed [28]. Changing topologies make it difficult to preserve the privacy of the entities of SIoV system as privacy preserving algorithms might require sufficient time to compute, process, analyse, communicate and store the information at both entities and cloud level. With entities travelling at a high speed and changing neighbours instantaneously, system would require high speed processing units, brisk computing capabilities, fast communicating devices and large storages to implement privacy preserving algorithms. Furthermore, mobility would require entities to share their information using wireless communication technologies that are considered vulnerable to security attacks and hence prone to leaking private information of the entities to attackers.

J. HETEROGENEITY AND INTEROPERABILITY

One of the key challenges in SIoV is managing the heterogeneity of the entities. In a vehicular network in general, vehicles from several manufacturers are present on a road at a particular instance. Each vehicle might be equipped with different sensors that would gather distinct data for performing various operations for the vehicle. In order for these disparate vehicles to communicate with each other, they should follow certain standards. For example, a vehicle sharing its location in coordinates (X, Y) format should be able to translate the location of another vehicle sharing its location coordinates in (X, Y) format. Hence, the location coordinates should be standardized in (X, Y) format. Interoperability is a key advantage of vehicular network in a way that it allows diverse vehicles to exchange information with each other. Vehicular entities might have varied level of constraints, e.g., some vehicles might have high processing On-Board Units (OBUs) but others might not have. Similarly, some vehicles might be able to provide road information using high speed cellular networks, but others might be able to communicate only through low speed Wi-Fi networks [29]. In order for distinct vehicular entities to exchange information with each other, standards are required that enable these entities to communicate, operate, and function regardless of their make, model, manufacturer, or industry applications. Similarly, in order to manage privacy of the vehicular data, a standard privacy policy is required that must be followed by all the vehicular entities to enable strict management of personal data. Designing a privacy policy for all the vehicular data is currently a challenge as data on the road to be shared or not is still subjective and hence require standard procedures to be followed by all the manufacturers of vehicles, law enforcing agencies, infrastructure manufactures and service providers etc.

IV. PRIVACY ISSUES IN SIOV AND RELATED SOLUTIONS

This section scrutinizes the layered SIoV architecture as shown in Figure 3 and analyzes it for the inherent SIoV privacy threats. Figure 4 illustrates the holistic view of the privacy concerns in SIoV. Furthermore, this section highlights the exiting privacy management schemes available in the literature as illustrated in Table 2.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

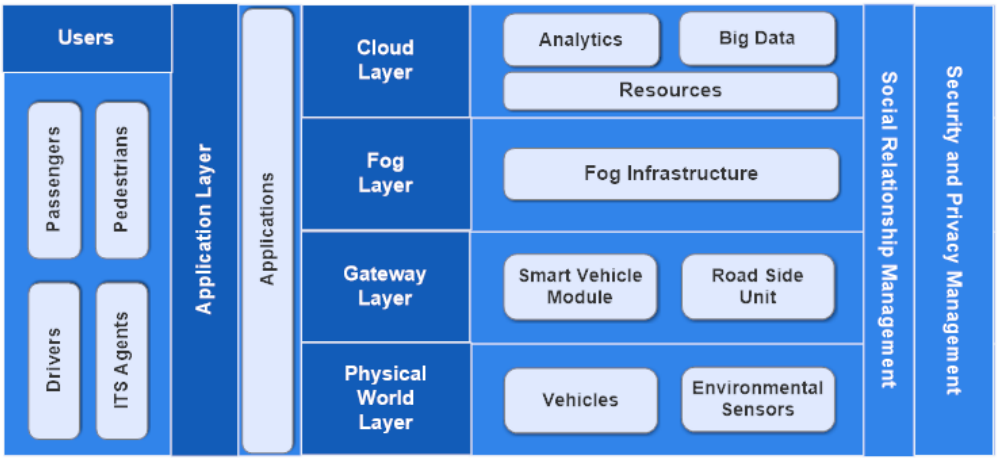


FIGURE 3: SIoV Layered Architecture

TABLE 2: Applicability of existing Privacy Management schemes in SIoV

Privacy Preserving Method	Physical layer	Gateway layer	Fog layer	Cloud layer	Application layer
Anonymity	T-closeness [30]	Pseudonyms [31]	Short-term identifiers [32]	Revocation [33]	
Minimization		Discarding raw data [34]	Cooperative deanonymity [35]	Secure storage [36]	Minimal permissions [37]
Differential Privacy	Noisy readings [38]	Location obfuscation [39]	Noisy data aggregation [40]	Aggregating public data [41]	
Encryption	Private key storage [42]	WPA2 [43], Private Service Discovery [44]	Role-based access control [45]	Homomorphic encryption [46]	
Query based		Reducing granularity [47]		Hiding usage patterns [48]	Query Privacy [49]

A. PHYSICAL WORLD LAYER

The physical world layer of SIoV architecture is comprised of physical entities including vehicles, sensors, drivers, passengers, pedestrians and their smart devices etc. It is a base layer that provides interface to the overall SIoV architecture. One of the major responsibilities of this layer is to sense data through vehicle sensors, and smart devices carried by drivers, passengers and pedestrians. Furthermore, this layer helps in utilizing the complex architecture of various technologies with varying characteristics by providing electrical and mechanical interfaces. For example, On-Board Unit (OBU) provides a mechanism for the drivers to connect to various peripherals of the vehicle using Bluetooth technology, e.g., driver's smart phone can connect to vehicle's speakers etc. Physical world layer is considered the hub of data as it is closest to the mechanics of the entities of SIoV network, e.g., accelerometer can measure the speed of the vehicle which can be used to perform various actions like alarming driver about high speed of the vehicle. As this layer is responsible for gathering data from vehicle, drivers, passengers and pedestrians etc., privacy preserving becomes highly desirable at this layer of the architecture.

a: Privacy of a person

Privacy of a person in the physical layer of SIoV architecture deals with the person's data including gender, body dimensions and health conditions etc. Advancements in wearable technologies has enabled smart devices like smart watches and smart activity trackers to monitor various parameters of person's body, e.g., blood pressure, pulse rate, and heart rate etc. This information is normally stored in the profile of the person either within the device or on the cloud. Sev-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

eral applications like Apple CarPlay allow these devices to communicate with vehicular interfaces that allows vehicle's OBU to read, analyse and store this information. Based on the analysis of this information, various vehicular applications provide information about nearby places of interest. For example, if driver's smart watch is connected to vehicle's OBU and the smart watch sensors detect sudden drop in the blood pressure of the driver, it can communicate this information to vehicle's OBU that can warn driver about his health condition along with providing routes to nearby hospitals. Although this information is quite beneficial in most of the cases, however, if vehicle's OBU is sharing this information with car manufacturers that are selling this information to car insurance companies, it would create a highly undesirable situation for the driver of the vehicle on his next renewal of insurance policy.

b: Privacy of behaviour and actions

Privacy of behaviour and actions in physical layer of SIoV architecture deals with behaviour and actions of entities including, speed, routes and travel details etc. Vehicle navigation systems are quite advanced these days and are capable of storing and communicating substantial information. This information is expected to be private to vehicle owners in most of the cases and if this information is shared with any third-party including vehicle manufacturers, it would be considered breach in privacy. For example, smart vehicles these days can sense that a driver takes the same route from home to office every day, and if a pre-installed application in the smart vehicle gathers this data and sends it to advertisement companies, they can advertise about the nearby shopping malls selling their products by sending notifications to the driver. This process of sending driver private information to other entities without the consent of the driver is highly unethical and would be considered infringing the privacy of behaviours and actions.

c: Privacy of communication

Privacy of communication in physical layer of SIoV architecture deals with keeping communications like conversations, emails, phone calls and chats etc private. Smart vehicles these days are equipped with cutting-edge multimedia technologies including high quality cameras, mic and speakers etc. High quality mics have made it possible for speech recognition applications to take voice commands from the drivers even without physical interaction with infotainment systems and performing various actions like navigation, playing songs, turning on-off air conditioner, sending messages and making phone calls etc. The mics in smart vehicles are normally always turned on looking for keywords like "Hey Siri" (in-case of Apple CarPlay), "OK Google" (in-case of Android Auto) etc. Once these phrases have been identified by infotainment systems, they are ready to take voice commands to perform further actions. Allowing infotainment systems to keep mics "always-on" has the fear of recording the conversation in the vehicle and transmitting this information to third-parties that is considered violating the privacy of communication of drivers and passengers.

d: Privacy of data and image

Privacy of data and image in physical layer of SIoV architecture deals with data of the entities of SIoV system. Vehicles' manufacturers are equipping vehicles with several sensors that are used to monitor the overall performance of the vehicle. The OBUs are gathering the data from various sensors, analysing it and communicating this information to the manufacturer for diagnostics purposes. For examples, coolant temperature sensor also known as master sensor since OBU takes input from this sensor to perform various functions, including, Activating and deactivating the Early Fuel Evaporation, Start-up fuel enrichment and Advancing spark etc. Some manufacturers are using the input of this sensor to diagnose the problems in the vehicles. However, if OBU is sharing the data of master sensor with the manufacturers for the vehicles that do not have major problems without the consent of the driver, it might be considered breach in the privacy as the collected data can reflect the overall performance of the vehicle. Furthermore, if this collected data is shared with the car insurance companies, they can tailor their policies for that particular vehicle which is ethically incorrect.

e: Privacy of thoughts and feelings

Privacy of thoughts and feelings in physical layer of SIoV architecture deals with thoughts and feelings of the drivers, passengers and pedestrians etc. Advancements in Brain Computer Interface (BCI) have now enabled humans to control devices through their thoughts. At the same time, machines are now able to read human thoughts and feelings to react appropriately. As BCI technology is an amalgam of human and machine learning, hence it can be manipulated. BCIs are now capable enough to be incorporated into the vehicles in a way that vehicles can measure the stress level of the drivers using skin conductivity and heart rate metrics. Based on this data, smart vehicles can analyse how stressful a driver is feeling at a particular instance and react appropriately. However, this analysis of human thoughts and feelings might give machines a lot of control over human thoughts and hence people might be judged based only on their thoughts and feelings instead of actions and behaviours. For example, if a vehicle informs authorities about the stress level of a driver on a highway and authorities try to approach the driver to assist but instead driver becomes more stressed thinking of authorities approaching him because of traffic violation might result in a serious consequence on highways, e.g., accident. Hence, a comprehensive framework is required to employ privacy of thoughts and feelings through machines.

f: Privacy of location and space

Privacy of location and space in physical layer of SIoV architecture deals with the right of an individual to move independently in public and private spaces without being monitored. In SIoV system location and space of an individ-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

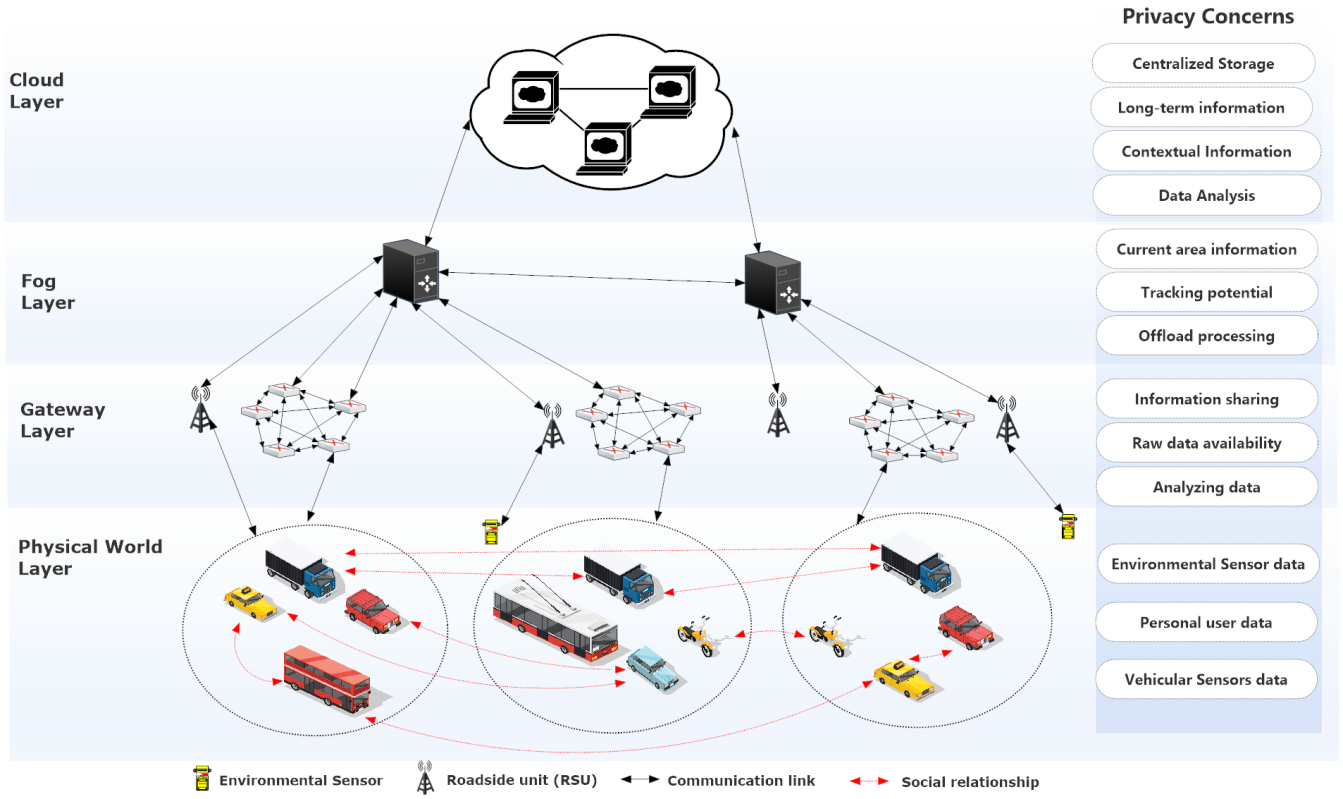


FIGURE 4: Holistic view of SIoV Architecture

ual has a significant importance as vehicles are expected to be on roads most of the times and infrastructures can gather their information anonymously. For example, a speed monitoring camera installed on a highway is meant to measure speed of the vehicles and to inform authorities about speed violations. However, if the same speed camera starts taking pictures of the drivers and the passengers inside the car and sends this information to infrastructure manufacturers that are third party private companies that further share this information (pictures of drivers and passengers, location of the picture taken, time of the picture taken etc.) with their partners, it would be considered serious breach in privacy of location and space of drivers and passengers of the vehicles.

g: Privacy of association

Privacy of association in physical layer of SIoV architecture deals with the freedom of an individual to associate with any group, e.g., religion, country, club or political party etc without being monitored. In SIoV systems with several cameras installed on roads, privacy of association can be challenging. For example, CCTV cameras installed at the car parking of a shopping mall can capture the pictures of the vehicle including stickers on them that can provide more details about them, e.g., a vehicle having a sticker of a particular football club can be recognized through these cameras and later on can be approached by advertisers to market their products related to that football club. Similarly, these cameras can identify the details of the cars, e.g., manufacturer, model and type etc., and can be approached by third party vendors for products related to that particular vehicle model. Capturing these details without informing individuals and then sharing (selling) this information to third parties is considered infringement of privacy. Table 3 presents the categorization of various SIoV entities and their parameters in distinct privacy types as devised by Rachel et. al. [7].

B. GATEWAY LAYER

The gateway layer of SIoV architecture is responsible for facilitating the physical-world layer towards the cloud and fog-based infrastructure. This layer collects the data from the physical world layer and forwards it to the fog layer of the architecture. Gateway layer specifically deals with the modules in smart vehicles that have required communication protocol stacks to directly talk to the fog layer. Furthermore, vehicles and environmental sensors not capable of direct communication with fog layer can use RSU or neighbouring smart vehicles to exchange information with the fog layer. While this layer facilitates in forwarding information to fog layer, it bears a huge responsibility of keeping the data private that would help in strengthening the trust of SIoV entities on the system.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

TABLE 3: Categorization of SIoV entities into Privacy types

Privacy Type	Vehicle	Infrastructure	Driver	Passengers	Pedestrians
Person			Health Conditions	Body Dimensions	Gender
Behaviour and Actions	Routes, Speed	Road Monitoring	Driving Habits	Seating Habits	Road Crossing
Communication	Diagnostic Logs	Entities correspondences	Entities correspondences	In-Vehicle Conversations	Phone calls
Data and Image	Sensors' readings	Sensors' readings	Call logs	Playlists	Video recordings
Thoughts and Feelings			Stress levels		
Location Space	GPS coordinates	Area Information			
Association	Manufacturer	Vendor	Religion	Relationships	Ethnicity

a: Privacy of a person

Privacy of a person in the gateway layer of SIoV architecture deals with the person's data like gender, body dimensions and health conditions etc. including drivers, passengers and pedestrians. RSUs in SIoV system are considered central entity as they can provide several services to peer RSUs, vehicles and pedestrians. These services include, Internet, notifications from law enforcing agencies, event details from local city office, traffic details and facilitation to emergency vehicles. Due to providing these services, RSU are considered the hub of information for vehicular entities and RSU sharing this information to other entities without consent of the entity will result in infringement of privacy. For example, consider a scenario where RSU is providing internet services to passengers waiting for the bus on a bus stop. A passenger using this internet service is downloading the blood report of his/her recent blood test from a hospital portal. If a RSU eavesdrop on this information through the internet service its providing to the passengers, it will be violation of privacy of person.

b: Privacy of behaviour and action

Privacy of behaviours and actions in the gateway layer of SIoV architecture deals with the behaviours and actions of drivers, passengers and pedestrians in SIoV system. Public transportation is considered a vital entity of SIoV system as it can be a source of gathering information from several entities at a single instance, e.g., passengers etc. Hence, a breach in the privacy of such information can be disastrous for a system as it might result in loss of trust of passengers in the public transportation system. For example, consider a scenario in which group of passengers are using the same bus daily to travel to their work place. A camera installed in the bus gives a live feed of the passengers inside the bus to the nearby RSUs using DSRC as bus is not directly connected to the internet. If this RSU operating at the gateway layer of SIoV architecture instead of sharing this feed with law enforcing agencies, starts sharing this information with advertisers that can target these passengers to advertise their products based on their appearances (wearing glasses, dressing sense and looks etc.), actions (passengers using their watches, handkerchief, and brushing their hair etc.), behaviours (socializing with other passengers, sleeping, reading billboards on roads etc.) will be considered infringement of privacy of behaviours and actions.

c: Privacy of communication

Privacy of communication in the gateway layer of SIoV architecture deals with communication of entities of SIoV including conversations, chats, email and phone calls etc. by gateway module. SIoV system does not only include regular vehicles, infrastructures and public transport but also incorporates emergency vehicle like police cars, fire trucks and ambulances etc. These emergency vehicles are normally connected to their peer vehicles and central offices through radio communications to exchange various information which is normally considered sensitive and not meant to be shared with general public. Consider a scenario in which a police car is chasing a criminal and enters a region where radio signals are unreachable, however, police car wants to communicate with central office to update them about the current situation. In the absence of the radio signals, police car can communicate this information to nearby RSU through DSRC that can facilitate in transferring this information to the required central office. The information transmitted by police car to RSU might be very sensitive that includes in-vehicle communications, phone calls, and radio calls. However, if this information is leaked by RSU to a person that is ineligible to receive this information, e.g., criminals, it might result in disastrous situations. Hence, there are chances of infringement of privacy of communication in such cases at gateway layer.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

d: Privacy of data and image

Privacy of data and image in the gateway layer of SIoV architecture deals with the data and image of the entities of SIoV gathered, analysed, stored or communicated through gateway modules like smart vehicle module and RSU etc. The gateway modules can facilitate in communicating the gathered information between physical world and fog layers. Hence, privacy violation at gateway layer can be hazardous as data coming from physical world layer can be shared with other entities without consent. For example, a bus with several passengers is a hub of data of the passengers that might include personal information of the passengers like name, gender, date of birth, nationality, occupation, contact details and at times citizen id etc. A bus in case of no internet connectivity wants to share this information with the cloud (for storage purposes), communicates with RSU using other means of communication like DSRC or Wi-Max and RSU is supposed to share this information with Fog and Cloud layer. However, if RSU shares this information with third party advertisers that are keen to send their product details related to people in the age group of 18-25 years would consider this information extremely useful as this information contains, date of birth and contact details. RSU by sharing this information with advertisers without the consent of the passengers would be violating the privacy of data and image.

e: Privacy of feelings and thoughts

Privacy of feelings and thoughts in the gateway layer of SIoV architecture deals with the feelings and thoughts of the drivers, passengers and pedestrians. Rapid growth in development of medical sensors has enabled measuring the feelings and thoughts of the human beings. For example, its possible to detect if a person is feeling angry, sad or happy based on readings from cardiac and electrodermal activities, facial expressions and postures etc. These feelings and thoughts of a person are considered extremely private as they are not even depicted through behaviour and actions at times, hence, sharing of this information without the consent of the person would result in serious violation of privacy. With devices being able to measure feelings and thoughts of the person, strict policies are required to ensure privacy. For example, imagine a scenario in which a vehicle equipped with various medical sensors that are able to measure the feelings of a driver, e.g., sad, happy and angry etc. The vehicle with the consent of the driver is storing this information locally and at times in the cloud (in user medical profile). Since the consent of the driver is taken before storing this data, no violation occurs. However, if vehicle wants to store this information in the cloud and does not have internet connectivity, it might request nearby RSU to facilitate it in connecting to the cloud. For this purpose, all the data is stored in the cloud through RSU. However, if RSU starts sending this data to a third-party cloud or even worse to a public cloud, a serious breach of driver's privacy would occur. To avoid such breaches in privacy at the gateway layer of SIoV architecture, strict privacy policies are required with necessary implementations.

f: Privacy of location and space

Privacy of location and space in the gateway layer of SIoV architecture deals with the location of the entity at a particular instance of time. Vehicles these days are equipped with GPS chips that are capable of getting the location coordinates. This information is then utilized by applications like navigators to assist in navigating on roads. OBU in vehicles can collect information from various vehicular sensors to provide useful information to the applications, e.g., combining time stamp with locations can provide information about nearby cinemas and suitable movies times etc. However, leaking such information can cause serious inconvenience to the entities of the SIoV system. For example, if a vehicle wants to communicate with nearby RSU to get the latest traffic information at the next junction at a specific time of the day, it might have to share its location and time with RSU which in return provides the required information. However, if RSU shares this information with nearby cinemas and they start sending movies' information to the driver of that car who might not be interested in movies would be annoyed by such information. Similarly, if RSU starts sharing information of nearby police cars to all the vehicles in the area, it might not be a desirable situation for the authorities who don't want other vehicles to know the location of their cars. Such cases would be considered violating the privacy of location and space at gateway layer of SIoV architecture.

g: Privacy of association

Privacy of association in the gateway layer of SIoV architecture deals with the relationship of the entities with each other, their religious practices, association of political parties or connection with any group. These association of the entities are truly private to themselves and they are free not to share this information with anyone. However, sharing this information with others without the knowledge of the entities would be considered breach in the privacy. For example, in SIoV, social relationships of entities are believed to be of high importance as they can provide a lot of information about the entity itself, e.g., a vehicle parked in the parking of a religious place can reveal the driver's religious association. RSU acting as gateway module for transferring such information between physical world layer and fog layer providing this information to others without prior knowledge to the entity would be considered infringement of privacy. For example, a RSU knowing the owner information for the vehicles (a person owning more than one vehicle) sharing this information with the insurance companies that are providing family cars insurance would be breaching the privacy of association of the owner as insurance companies can then advertise their policies based on such information.

C. FOG LAYER

Fog layer implements the concept of fog computing to provide a distributed edge-based infrastructure to support real-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

time and near real-time SIoV applications. The basic idea behind fog layer is to extend the cloud-based architecture at the edge of a network to provide diverse services. This layer is composed of fog nodes that may follow multi-level hierarchy to offer more granular coverage of services. The fog nodes can be of diverse capabilities that range from a simple smart phone to specialized servers. The fog layer targets to meet the scalability requirements of the future networks where millions of vehicles will generate massive amounts of data and will request for services. Beside traditional cloud-based data sharing services, the fog layer also offers support for services such as assistance for complex processing, and location-based connection management. The fog layer receives a multitude of raw and pre-processed data from the smart gateways that are further processed and stored in different fog nodes to enable different services. In SIoV, this layer will also receive the information regarding the social relationships of vehicles. The type and amount data received at this layer have potential of being useful for many business models and thus prone to many privacy threats.

a: Privacy of a person

The privacy of a person can be violated at this layer by exposing the raw or pre-processed data about the person such as health status, etc., to undeclared entities. There are several factors that play role in such violations. First, the type of specific data received about the person and level of granularity of the data determines the value of the data. For example, if details about a health of a truck driver are being recorded by a safety application to avoid any accidents in case of an unexpected scenario, then that information is also shared to a fog node as well to avoid major mishap. This shared health information can be very specific about the driver and thus has potential to privacy infringement. Secondly, the frequency of the sent information at the fog layer can determine the type of health issue a person is facing by detecting a pattern of the received data. For example, if a driver is a smoker and his blood pressure and sugar level readings are being sent to the fog layer for some period then this information can describe any ongoing disease of the driver that he doesn't want to share. There are several novel applications that can offer convenience to the user by consuming this data. However, the leakage of this data provides enough information about the person to different companies such as hospitals and insurance companies. Finally, the duration for which these data are remained stored at the fog layer also increases the chances of information leakage. Although the fog layer is a temporary point to store data, it depends on the service provider to decide the period for which a fog node will store the received data based on the demand of different applications. Beside the benefits of information availability at fog layer, the storage of health-related information for even few minutes increases the probability of privacy violations.

b: Privacy of behavior and action

The privacy of a person's behaviour, action, thoughts and feelings can be violated at the fog layer in SIoV by recording and using the shared driver's status such as stress level, and a vehicle's route and speed details even receiving such information from it. The fog nodes can collect different details about a vehicle by just using its traversal across different nodes. For example, the speed of a vehicle can be determined by the number of fog nodes it is passing through. The speed information combined with the time can reveal the behaviour of the person at different time of a day. This analysed information about the behaviour of a driver can be useful, in case of a driver whose speed pattern is not consistent according to the determined norms, for many safety applications. Furthermore, the movement of the vehicle could also determine the current route of the vehicle that will be useful for advertising of targeted information.

c: Privacy of communication

Privacy of communication can be breached at the fog layer by multiple factors such as unsecure communication technologies and rouge fog nodes. Smart vehicles and other gateway nodes use variety of communication protocols such as Wi-Fi, DSRC and mobile networks to communicate with the fog layer that are prone to plethora of security attacks. A compromised communication link between a vehicle and a fog node will leak all the data communicated. This issue even exists in communication technologies that employ encryption. For example, a smart vehicle serving as a gateway layer communicating through locally available Wi-Fi encrypted channel can leak all private data because its WPA2 encryption is susceptible to attacks [50]. Other important factor that can cause threat to privacy at fog layer is the presence of rogue fog nodes. The rogue fog nodes present them as legitimate part of the SIoV architecture to trap its users to connect and share information with them. An authentic fog node can also become rogue, in case of an attacker is able to control it. All the shared data by the connected vehicles and other entities can be used by an attacker by further analysing the collected data. Furthermore, a fog node can orchestrate man-in-the-middle attacks by tampering the received data before forwarding it to the cloud that can even disable the functionality of SIoV applications. It can also launch further attacks to violate the privacy of other users in SIoV. The issue to control rogue fog nodes is difficult due to many reasons: sometimes other vehicles take the responsibility to act as fog nodes to offer flexible infrastructure and to reduce the cost, and fog nodes are dynamically created and terminated by using SDN and NFV technologies.

d: Privacy of data and image

Privacy of multimedia can be compromised at fog layer because it receives the images and videos from vehicles and other devices to be further processed. There are several sources such as vehicles and stand-alone video camera sensors that generate multimedia data at gateway layer and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

then send that data to be further processed to fog nodes. This offload of processing is done to mitigate the demand of real-time applications and for the sake of applying several advanced algorithms based on the system that can't be hosted at the relatively constrained vehicles. For example, an ambulance carrying a patient will need essential processing aid to perform complex graphic processing related to the patient. This support of the fog nodes comes with the price of sharing private data related to the patient that opens a door to many privacy threats. Another reason could be to use the multimedia data with other context information to create value-added services. For example, an autonomous vehicle can share pre-processed video content generated by a its camera to a fog node that uses the data receives from multiple sources in the area to enable a safety application. This data becomes useful in situations where a single camera perspective might not be adequate to provide an overall picture of a context such as a ball can be seen on the road by a camera, but a street camera in the vicinity can also show whether a running child might suddenly appear from the street. In some scenarios, the data is shared by vehicles to fog nodes for further processing before passing it to the cloud. The chances of privacy infringement increase sharply with the longer retention of that data at the fog layer. For example, a lorry with multiple cameras on it to provide different views to aid a driver and eventually to share this real-time processed video with its company's base. However, the processed video data of its cameras is valuable for many safety applications in the vicinity of a fog node, so the lorry also shares this information with its fog node. Beside its value for specific safety applications, this information is vulnerable to privacy violations.

e: Privacy of thoughts and feelings

Privacy of thoughts and feelings can be violated at fog layer based on the leakage of information related to a specific person. In case the privacy of a person is violated along with the details of his actions then more information about the person's behaviour, thoughts and feelings can be determined. For example, if a driver begins rush driving as soon as he starts smoking then the vehicles in the neighbourhood can be alerted with a caution by a fog layer-based application whenever the cigarette smoke is detected and reported by the vehicle. This information recorded and analysed at fog layer can generate value for many applications. However, the information at fog layer used without the consent of a user will be considered as a privacy violation.

f: Privacy of location and space

The fog layer is capable to determine the location and space of vehicles in SIoV and this capability makes it vulnerable for privacy of location and space violations. The distributed nature of fog nodes requires vehicles in SIoV to coordinate with them to enable several applications. Therefore, a vehicle will coordinate and share its information with multiple fog nodes during its journey depending on the area covered by each fog node. However, the collected information of the vehicle by different fog nodes can determine various information about the vehicle such as its location, speed, and the places where the vehicle has stayed or parked. This shared information becomes valuable for many companies for targeted campaigns and might be misused by unknown or known entities. For example, the fog layer can determine that a vehicle has been to a clinic and will have high probability to visit a medical store now, or a vehicle parked at a sports stadium is the best target for sport's equipment advertisements. Furthermore, the docking of a vehicle at a fog node is an important piece of information for local businesses that can be a target of deliberate or accidental privacy leakage.

g: Privacy of association

Privacy of association has a multifaceted threat in a SIoV because of its reliance on social relationships of vehicles. Many SIoV applications rely on exploiting different available social relationships between vehicles, drivers and passengers to dynamically build trust and consume shared information to enable various services. However, this information can be misused to get more details about an individual by using statistics of its most recent social contacts. For example, two vehicles in SIoV that are travelling to the same destination even on different routes will create a social relationship together. If the first vehicle has recently visited a new theme park in the destination's neighbourhood then the probability that the second vehicle will be interested to visit that park increases. Therefore, fog nodes can exploit the social relationship information to make a gold mine of the collected information of vehicles. Moreover, the privacy violation of location and space also impacts the privacy of association by divulging the spaces where a vehicle has been to and stayed or park. This information of location and spaces can determine the details of the association of people related to vehicle in terms of religious places, sports events and political protests. For example, a sports fan who is travelling to a football match between two counties will explain the association of the driver and passengers with any of the two teams.

D. CLOUD LAYER

Cloud layer provides a centralized hub that receives processed or pre-processed data from fog layer. The received data at cloud layer can be further processed and classified based on the cloud-based applications before storing it for long-term at cloud infrastructure. The powerful and flexible cloud infrastructure enables it to perform complex computations on the massive amount of diverse data sent by millions of vehicles. Therefore, this layer holds the key in the provision of value-added services by utilizing available system-level information. In SIoV, the cloud layer also receives information about the social relationship information created and shared by vehicles. Furthermore, the cloud layer is capable of extracting interactions of different vehicles that are reported by fog layer to infer social relationships between different vehicles. There are several threats to privacy at cloud layer

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

because the availability of enormous amount of multifarious data.

a: Privacy of a person

Privacy of a person can be violated at cloud layer by using the data related to the health condition of drivers, passengers or pedestrians. The data can come from multiple sources to the cloud layer. In the most common case, the health-related data is shared by a vehicle based on the policy agreed between the driver and the other parties. Some insurance companies require such kind of data to be recorded and reported to their cloud servers in order to get better insurance policies. This kind of terms can also be required by a road authority. Once the health-related data is received at the cloud layer, it becomes susceptible to plethora of privacy threats. The health-related data can also be gathered by public transport systems and reported to the cloud layer. For example, a city administration can decide to collect variety of data about its passengers using sensors and video feed to tackle an epidemic by identifying cough related symptoms. This collected information has potential for privacy of a person violation, because each passenger is identified with a smart travel card chip. This information is useful for companies from healthcare domain.

b: Privacy of behaviour and action

There are several threats for privacy of behaviour and action of individuals at cloud layer, because long-term records of speed, incidents, and accidents of vehicles are available at this layer. Different data mining algorithms can be employed at cloud to dig deeper about the behavior of the person by analyzing his actions. For example, the driving speed of a person at different times of a day can determine a pattern that can predict the future behaviour of the person in a particular situation. This data can be useful for a road authority to ensure the safety of other drivers on the road. However, the privacy can be violated if the user has not provided his consent for such kind of analysis. Moreover, the privacy can be further violated if the analyzed behaviour information is shared with a third party without being transparent to the user. Similarly, the long-term date of the selection of routes by a driver can be analyzed to get information about the user preferences that can be used for advertisement agencies to target the customers with a particular behaviour.

c: Privacy of communication

Privacy of communication can face several threats where attackers can exploit the weaknesses of underlying communication technologies and protocols. Fog nodes and cloud user applications use different interfaces to push and request data and services from the cloud. There are varieties of communication technologies such as Wi-Fi and cellular technologies can be used by fog nodes to send data to the cloud layer. For example, a vehicle can act as a fog node will use any available communication technology to push the collected data towards the cloud. Any weak link in communication between fog and cloud will allow an attacker to sniff and record the data that has potential to leak privacy. This kind of security related privacy issue can be mitigated using strong encryption. Moreover, the security vulnerabilities of other protocols and infrastructure such as DNS and HTTPS can increase the risk of privacy infringement. The user applications interface with cloud by consuming web services. The web services rely on DNS to locate a cloud server. If a DNS infrastructure comes under attack then there is a high risk that the user will share private information with an unreliable counterfeit server. For example, once a vehicular cloud-based application is guided to a bogus cloud server by a DNS server, it can blindly share the requested user personal data with the server. Digital signatures can offer a solution to this issue.

d: Privacy of data and image

The cloud layer stores massive amounts of multimedia content that increases vulnerability to privacy of multimedia in case these are used without the consent of a user. All the cloud users fully rely on cloud layer to use their data transparently. However, the data can be misused intentionally or unintentionally as the multimedia content is stored at cloud layer for a long-term basis. For example, the cloud will retain all sent images and video sent by a smart car for post-processing. These data and images are mostly stored unencrypted and are susceptible to many attacks from the system users and outside attackers. Once the data is leaked, the attacker can apply different machine learning algorithms to detect people and places from the images and can use the personal user data for malicious activities. The homomorphic encryption [51] offers solution to this issue by enabling the processing of encrypted data. However, this technique is still in its early phases and yet to be realized in diverse practical scenarios.

e: Privacy of thoughts and feelings

Privacy of thoughts and feelings can be violated at cloud layer by analysing different data about incidents about a user. The long-term unencrypted storage of diverse users and vehicles related data increases the risk of this kind of privacy infringement. Long-term data can draw a better picture of the user in terms of his thoughts and feelings. For example, the video recordings of a vehicle that span over few weeks could be analyzed to detect the mood of a driver during different times. This information can predict the driver thoughts and feelings by understanding his spoken words and analyzing his facial expressions with respect to the previously learned knowledge base. This kind of information can be valuable for safety applications to reduce the chances of accidents by applying different methods. However, the privacy can be violated when the thoughts and feelings information are also shared to advertising companies to identify and target certain types of customers.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

f: Privacy of location and space

There are many ways that privacy of location and space can be violated at cloud layer by using the location information of vehicles collected through multiple sources. The cloud layer is the centralized place where all location related data from fog nodes, environmental sensors and vehicular GPS sensors will be collected over a long period of time. This location data can be used to track a vehicle and further data can be generated based on the spaces a vehicle has visited. For example, a vehicle can be tracked, and his most visited places can be recorded even when the vehicle is not sharing its location information with the cloud. This is possible through the fog nodes data in the vicinities where the vehicle has travelled. Furthermore, the privacy can be further violated by predicting where the user can be on a certain day and time by using machine learning techniques on available big data.

g: Privacy of association

Privacy of association is susceptible to be infringed based on the fact that long-term data of individuals is available at the cloud layer. The data of a vehicle available at the cloud layer can be used to deduce the different associations of its driver and other passengers. For example, the multimedia data can be analyzed to learn about the associations such as religion, school of thought, favourite sport and team, etc. This is possible by analyzing the appearance and dressing of the driver and its passengers. Furthermore, the history of places visited by the vehicle can also help to infer fine details such as the kind of club, pub and political protests visited by the passengers of the vehicle. The privacy of association will be violated if this information is processed without users' consent, used by variety of applications, or shared with companies. The privacy of association can be further infringed if the cloud uses one vehicle's deduced information to predict about another user who has also visited a certain place.

V. BLOCKCHAIN BASED PRIVACY MANAGEMENT SOLUTIONS

Blockchain has become one of the most emerging technologies these days, with considerable impact, potential and growth. Blockchain is the underlying technology of bitcoin but is now seen as a platform to store records and transactions in a highly secure, trusted, transparent and traceable manner [52]. Also with the feature of smart contracts, as found in blockchain platforms as Ethereum and Hyperledger, blockchain can offer open execution in which the execution outcome can be validated and agreed on by the majority of the mining nodes within the blockchain network. Smart contracts can hold rules and terms to be executed by participating parties including owners and providers of privacy information, with restrictions and access control to only legitimate users that may include SIoV vehicles. For example, with blockchain and smart contracts, authentication and authorization of accessing data can be accomplished easily, in a trusted, secure, and decentralized manner, with complete openness, traceability and visibility to all stakeholders or actors within the built blockchain network. Data access permissions or privileges can be automated and given by only owners and providers of data. Moreover, governance for access to shared data can be voted on by multiple stakeholders. Furthermore, the sharing and storage of vehicles data while on the road can be made selective and restricted by smart contracts to only certain vehicles. Such restriction can be made static or dynamic. Dynamic selection can be made based on reputation of vehicles. Reputation logic can be coded within smart contracts logic, and aggregate reputation scores can be computed and shared with all members of the SIoV and blockchain networks.

In this subsection, we summarize and review existing work found in the literature related to privacy management using blockchain for SIoV underlying networks and services. Fig. 5 shows a classification of the most popular blockchain-based approaches for managing privacy information for nodes, vehicles and consumers within a SIoV ecosystem.

The authors in [53] proposed Blockchain-based approaches that provide authentication and secure data exchange among vehicles and nodes within an SIoV environment. A secure data exchange algorithm is proposed to assure accurate information communication between SIoV nodes. The algorithm consists of two parts: (1) Registration of vehicles with the regulatory authority (RA). The RA assigns a pseudo-identity (PIDi) and public key (PKi) to each vehicle (Vi). The PIDi and PKi pairs are digitally signed by the RA, and are stored as a single transaction (TBi) in the identification public ledger. The issued PID, PTRi and the private key SKi are stored within the Vi. (2) Secure Data exchange, where Vi sends messages conditionally to the Stationary Unit (Si). Vi is authenticated when it comes within the range of Si. This message contains PIDi and PTRi encrypted with SPKi, where SPKi is the public key of stationary unit. The stationary unit decrypts the message using the private key of the stationary unit, whether Vi is a trusted vehicle or not which is done by verifying the blockchain. When the PIDi is found in blockchain and it corresponds to PTRi, Si authenticates it to be a part of Sn and joins the group of authenticated vehicles to receive the Group key.

A secure, automated and privacy-shielding protocol for charging of smart electric vehicles was introduced in [54]. The proposed protocol is based on Blockchain technology, which allows consumers to find the nearest and cheapest electric charging station without divulging the customer identity. Privacy attributes such as position and identity of the customer in the decentralized and distributed network is never revealed. The customer requests a bid for tariffs and different charging stations within a definite region, of the vehicle, send the bids for tariffs based on the amount of energy requested. A Blockchain-based public ledger (which serves to be an immutable storage of records and transactions) is utilized for transparency in verification of bids. None of the participants in the network (i.e., all available charging stations within the network and other vehicles in the network range) learn about

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

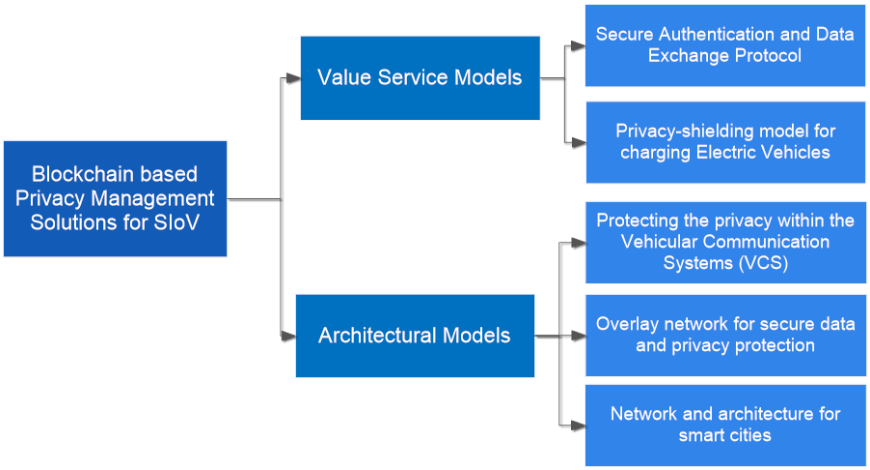


FIGURE 5: Classification of Blockchain-based approaches for SIoV privacy management

the exact position of the Electric vehicle (EV) requesting a bid, no participant except the requesting EV and the selected station know about price or quantity of energy purchased, and EV's cannot be tracked over time. All participants are anonymous, i.e., they are only identified by an ID in the blockchain. This model has 3 primary phases. The exploration phase includes details on the amount of energy spent, a period of time and geographic region chosen is published by EV. In the bidding phase, only charging stations participate in this phase and privacy of EV is not impacted and bids are publicly made available in the blockchain. In this stage, the EV has not accepted any offer from the bids and the blockchain assures the contractual binding after publishing it in the chain, i.e., if the EV decides on a particular station, the latter has to offer the requested energy at the bid's price. In the evaluation phase, the EV privately decides on bids off the blockchain. No information about this decision is leaked to the outside network. A hash value is published on the blockchain as a part of the privacy commitment of the system. Finally, in the charging phase, only the EV and the selected charging station are involved and communicate directly without any interference of other nodes in the decentralized network.

A Blockchain-based solution for large-scale system failures and malicious attacks caused due to wireless communication techniques in the Vehicular Communication Systems (VCS) has been proposed and studied in [55]. The paper presents a secure inter-vehicular communication method using visual light and acoustic side channels that is highly resistant to attacks and third-party influence. Cryptographic techniques are employed to verify the location and identity of the communicating vehicle, and the system employs a public key blockchain infrastructure for enhancing interoperability between untrusted vehicles and manufacturers. The paper describes a handshake protocol for a key establishment which is based on the TLS 1.2 (Transport Layer Security) and establishes a symmetric encryption and authentication keys, when verifying the vehicle's identity with the certificate issuing authorities. The side-channels (visual and audio) provide improved security to the transmissions and are useful for communicating messages between vehicles and, in maintaining the inter-vehicle distance in a vehicular cluster. This blockchain based system solves problems of various traditional, signalling and physical attacks such as RF channel jamming and key compromising which is handled by integrating blockchain with the side channels. The proposed technique secures the vehicle-to-vehicle communication and facilitates using side-channels for attributable, secure, small throughput and exchange of key information between vehicles. The identity of vehicles is authenticated by using digital certificates and visual identity techniques. Due to its verifiable and immutable nature, blockchain is employed in this model to stabilize and secure the inter-vehicular communications.

The authors in [56] presented a decentralized, privacy-preserving blockchain based architecture for smart vehicle ecosystem. The proposed solution forms an overlay network where automobile manufacturers, smart vehicles, and service providers interact with each other. The design of the system is based on LSB (Lightweight Scalable Blockchain) due to its low overhead nature. Nodes in the network are clustered, with only the cluster heads (CHs) are responsible for managing and performing its core functions on the blockchain and these Cluster heads constitute the Overlay Block Managers (OBM). Transactions are broadcasted to and verified by the OBMs, thus eliminating the need for a third party. Each vehicle is decked with in-vehicle storage to store sensitive data. The vehicle owner has the complete rights to define the data which is to be supplied to the third parties in exchange for services and those data which should be private to the in-vehicle storage. Each vehicle is equipped with a Wireless Vehicle Interface (WVI), and local storage. The in-vehicle storage is used for storing private and personally identifiable attributes of the user. Single signature transactions are produced by the vehicles which contain a hash of the data stored

in the in-vehicle storage. This transaction is sent to OBM with which the vehicle associated and the hash is stored in the blockchain.

A blockchain-based, secure, social vehicle network architecture for a smart city was presented in [57]. The proposed architectural design allows vehicles to discover and share their resources to design a vehicular network which works together to provide value-added services. In this model, there are two special nodes; namely, the controller node for providing the necessary and requested services, and the vehicle node or the miner node which handles request/response requisitions. The proposed Blockchain-based solution improves trusted services among network nodes by providing distributed and shared records of all services and resources. For every new registration of the vehicle, the transport authority provides trusted details to the revocation authority, where the latter has the authority to decide the nature of the nodes i.e., which node must be a controller or a miner and also provides the information of the ordinary and miner nodes to the distributed blockchain vehicle network. Each controller node has a hash, a random-pseudo number for authentication, Merkle root, and time-stamp containing details required to afford requested services and computes the data at the individual level and shares the information to other nodes in the distributed network. Every message or communication is secured with a public-private key encryption technique in which private and sensitive information attributes including identity, location, ownership are protected and encrypted.

VI. CONCLUSION

Traditional Intelligent Transport Systems are being revolutionized with the paradigm of Internet of Vehicles with the employment of a system that increases connectivity between smart vehicles and sensor devices. This paradigm is further evolved into Social Internet of Vehicles (SIoV) by the feature of social consciousness that enables the smart devices to engage in by developing relationships based on their application requirements. The value of SIoV has potential to open new avenues for novel applications by using the vast amount of sensor data that is further augmented by the information of context and social relationships. This paper describes the privacy aspects of SIoV by emphasizing the ways privacy can be violated. The paper explains that the value-added data can be a reason of privacy infringement because the data is collected, analyzed and stored at various entities in SIoV architecture. Each layer of the SIoV architecture is scrutinized by this paper to dig deeper and find the core reasons of different privacy violations. Furthermore, it discusses the privacy in IoV architecture in the light of 7 privacy aspects by highlighting the effect of each aspect on each layer of IoV architecture. Several scenarios have been discussed for each layer to provide ease of readability.The paper also discusses existing Blockchain-based solutions general IoT networks and finally provides state-of-the-art blockchain-based privacy preservation solutions for SIoV. The paper is expected to set a foundation for proposing privacy management solutions for highly dynamic environments like vehicular networks. Several key areas are still to be explored in privacy domain for vehicular networks especially in social relationship management, trust management, and overall information management.

REFERENCES

[1] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3701–3709, 2018.

[2] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," IEEE access, vol. 3, pp. 343–357, 2015.

[3] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer networks, vol. 56, no. 16, pp. 3594–3608, 2012.

[4] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social internet of vehicles: Architecture and enabling technologies," Computers & Electrical Engineering, vol. 69, pp. 68–84, 2018.

[5] M. Aloqaily, V. Balasubramanian, F. Zaman, I. Al Ridhawi, and Y. Jararweh, "Congestion mitigation in densely crowded environments for augmenting qos in vehicular clouds," in Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications. ACM, 2018, pp. 49–56.

[6] H. Vahdat-Nejad, A. Ramazani, T. Mohammadi, and W. Mansoor, "A survey on context-aware vehicular network applications," Vehicular Communications, vol. 3, pp. 43–57, 2016.

[7] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in European data protection: coming of age. Springer, 2013, pp. 3–32.

[8] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in International Workshop on Privacy Enhancing Technologies. Springer, 2005, pp. 197–209.

[9] R. Akalu, "Privacy, consent and vehicular ad hoc networks (vanets)," Computer law & security review, vol. 34, no. 1, pp. 37–46, 2018.

[10] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 3015–3045, 2017.

[11] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," IEEE communications surveys & tutorials, vol. 17, no. 1, pp. 228–255, 2014.

[12] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," Security and Communication Networks, vol. 7, no. 12, pp. 2728–2742, 2014.

[13] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," IEEE Transactions on Intelligent Transportation Systems, no. 99, pp. 1–17, 2018.

[14] X. Wang, Z. Ning, M. C. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," IEEE Communications Surveys & Tutorials, 2018.

[15] A. A. Alkheir, M. Aloqaily, and H. T. Mouftah, "Connected and autonomous electric vehicles (caevs)," IT Professional, vol. 20, no. 6, pp. 54–61, 2018.

[16] R. Clarke, "Introduction to dataveillance and information privacy, and definitions of terms," Roger Clarke's Dataveillance and Information Privacy Pages, 1999.

[17] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," IEEE Networking Letters, 2019.

[18] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," Ad Hoc Networks, 2019.

[19] S. Otoum, B. Kantarci, and H. T. Mouftah, "Detection of known and unknown intrusive sensor behavior in critical applications," IEEE Sensors Letters, vol. 1, no. 5, pp. 1–4, 2017.

[20] M. Aloqaily, I. Al Ridhawi, B. Kantraci, and H. T. Mouftah, "Vehicle as a resource for continuous service availability in smart cities," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2017, pp. 1–6.

[21] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions," IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2377–2396, 2015.

[22] M. Aloqaily, B. Kantarci, and H. T. Mouftah, "Fairness-aware game theoretic approach for service management in vehicular clouds," in 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall). IEEE, 2017, pp. 1–5.

[23] M. Aloqaily, I. Al Ridhawi, H. B. Salameh, and Y. Jararweh, "Data and service management in densely crowded environments: Challenges, opportunities, and recent developments," IEEE Communications Magazine, April 2019.

[24] N. B. Truong, T.-W. Um, and G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy social internet of things," Innovations in clouds, internet and networks (ICIN), Paris, France, 2016.

[25] X. Wang, Z. Ning, X. Hu, E. C.-H. Ngai, L. Wang, B. Hu, and R. Y. Kwok, "A city-wide real-time traffic management system: Enabling crowdsensing in social internet of vehicles," IEEE Communications Magazine, vol. 56, no. 9, pp. 19–25, 2018.

[26] L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, "A secure mechanism for big data collection in large scale internet of vehicle," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 601–610, 2017.

[27] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I. Humar, "Cognitive internet of vehicles," Computer Communications, vol. 120, pp. 58–70, 2018.

[28] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," IEEE Wireless Communications, vol. 22, no. 6, pp. 122–128, 2015.

[29] B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu, "Cloud-assisted safety message dissemination in vanet–cellular heterogeneous wireless network," ieee systems journal, vol. 11, no. 1, pp. 128–139, 2017.

[30] Z. Tu, K. Zhao, F. Xu, Y. Li, L. Su, and D. Jin, "Beyond k-anonymity: protect your trajectory from semantic attack," in 2017 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 2017, pp. 1–9.

[31] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "Slotswap: Strong and affordable location privacy in intelligent transportation systems," IEEE Communications Magazine, vol. 49, no. 11, pp. 126–133, 2011.

[32] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in vanets," in 2010 IEEE Wireless Communication and Networking Conference. IEEE, 2010, pp. 1–6.

[33] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Efficient certificate revocation list organization and distribution," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 595–604, 2011.

[34] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens, "Pretp: Privacy-preserving electronic toll pricing." in USENIX Security Symposium, vol. 10, 2010, pp. 63–78.

[35] ETSI, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," European Telecommunications Standards Institute (ETSI), Technical Specification (TS) 102 941, 06 2012, version 1.1.1.

[36] Q. Wang, K. Ren, S. Yu, and W. Lou, "Dependable and secure sensor data storage with dynamic integrity assurance," ACM Transactions on Sensor Networks (TOSN), vol. 8, no. 1, p. 9, 2011.

[37] C. Spensky, J. Stewart, A. Yerukhimovich, R. Shay, A. Trachtenberg, R. Housley, and R. K. Cunningham, "Sok: Privacy on mobile devices–itâĂŹs complicated," Proceedings on Privacy Enhancing Technologies, vol. 2016, no. 3, pp. 96–116, 2016.

[38] G. Ács and C. Castelluccia, "I have a dream!(differentially private smart metering)," in International Workshop on Information Hiding. Springer, 2011, pp. 118–132.

[39] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," arXiv preprint arXiv:1212.1984, 2012.

[40] C. Dwork, A. Roth et al., "The algorithmic foundations of differential privacy," Foundations and Trends® in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014.

[41] C. Culnane, B. I. Rubinstein, and V. Teague, "Privacy assessment of de-identified opal data: A report for transport for nsw," arXiv preprint arXiv:1704.08547, 2017.

[42] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless communications, vol. 17, no. 1, pp. 51–58, 2010.

[43] N. Cheng, X. O. Wang, W. Cheng, P. Mohapatra, and A. Seneviratne, "Characterizing privacy leakage of public wifi networks for users on travel," in 2013 Proceedings IEEE INFOCOM. IEEE, 2013, pp. 2769–2777.

[44] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, "Privacy, discovery, and authentication for the internet of things," in European Symposium on Research in Computer Security. Springer, 2016, pp. 301–319.

[45] O. G. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in 2008 International Conference on Intelligent Sensors, Sensor Networks and Information Processing. IEEE, 2008, pp. 249–254.

[46] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe," SIAM Journal on Computing, vol. 43, no. 2, pp. 831–871, 2014.

[47] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," Journal of systems and software, vol. 84, no. 11, pp. 1928–1946, 2011.

[48] C. Devet, I. Goldberg, and N. Heninger, "Optimally robust private information retrieval," in Presented as part of the 21st {USENIX} Security Symposium ({USENIX} Security 12), 2012, pp. 269–283.

[49] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in Proceedings of the 2008 ACM SIGMOD international conference on Management of data. ACM, 2008, pp. 121–132.

[50] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017, pp. 1313–1328.

[51] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: theory and implementation," ACM Computing Surveys (CSUR), vol. 51, no. 4, p. 79, 2018.

[52] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[53] A. Arora and S. K. Yadav, "Block chain based security mechanism for internet of vehicles (iov)," in Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT). [Online]. Available: http://dx.doi.org/10.2139/ssrn.3166721

[54] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," Computer Science-Research and Development, vol. 33, no. 1-2, pp. 71–79, 2018.

[55] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," arXiv preprint arXiv:1704.02553, 2017.

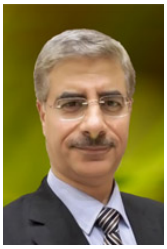
[56] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, 2017.

[57] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-vn: A distributed blockchain based vehicular network architecture in smart city." JIPS, vol. 13, no. 1, pp. 184–195, 2017.

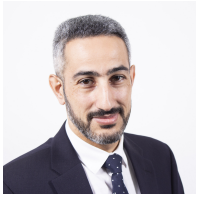
TALAL ASHRAF BUTT is currently working as an Assistant Professor at the American University in the Emirates. He holds a PhD in the domain of Internet of Things from Loughborough University, UK. Before joining the American University in the Emirates, he worked as a part of 5GIC (5G Innovation Centre), the UK Government's funded initiative at the University of Surrey to develop 5G technologies. At 5GIC, he gained experience of working in a testbed team that owned the state-of-the-art mobile testbed and successfully developed and demonstrated novel research ideas. Dr. Butt is a reviewer of IEEE journals and is passionate about next generation networks and protocols.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2922236, IEEE Access

RAZI IQBAL (M '12, SM '18) received the master's and Ph.D. degree in computer science and engineering from Akita University, Akita, Japan. He is an Associate Professor with the College of Computer Information Technology, American University in the Emirates (AUE), Dubai, UAE. Prior to joining AUE, he served as the Chairman of the Department of Computer Science and IT, Director of the Office of Research, Innovation and Commercialization and Research Scientist. His current research interests include short range wireless technologies in precision agriculture, transportation, and education. Dr. Razi serves as an Editor and Reviewer for several peer-reviewed journals and currently a senior member of the IEEE a member of the IEEE Computer and Computational Society.



KHALED SALAH is a full professor at the Department of Electrical and Computer Engineering, Khalifa University, UAE. He received the B.S. degree in Computer Engineering with a minor in Computer Science from Iowa State University, USA, in 1990, the M.S. degree in Computer Systems Engineering from Illinois Institute of Technology, USA, in 1994, and the Ph.D. degree in Computer Science from the same institution in 2000. He joined Khalifa University in August 2010, and is teaching graduate and undergraduate courses in the areas of cloud computing, computer and network security, computer networks, operating systems, and performance modeling and analysis. Prior to joining Khalifa University, Khaled worked for ten years at the department of Information and Computer Science, King Fahd University of Petroleum and Minerals (KFUPM), KSA.



MOAYAD ALOQAILY (M '12, SM '18) received the M.Sc. degree in electrical and computer engineering from Concordia University, Montreal, QC, Canada, in 2012, and the Ph.D. degree in electrical and computer engineering from the University of Ottawa, in 2016. He was an Instructor with the Systems and Computer Engineering Department, Carleton University, Ottawa, Canada, in 2017. He has been with Gnowit, Inc., since 2016. From 2017 to 2018, he was an Assistant Professor with the Computer Engineering Department, College of Engineering and Technology, American University of the Middle East (AUM), Kuwait. He is currently an Assistant Professor of computer engineering with the Faculty of Engineering, Canadian University Dubai, United Arab Emirates. His current research interests include connected vehicles, intelligent transportation systems, cloud and edge computing, vehicular cloud computing, 5G networks, and wireless communications/networks. He is actively working on different IEEE events. He is a Professional Engineer Ontario (P.Eng.).

YASER JARARWEH received his Ph.D. in Computer Engineering from University of Arizona in 2010. He is currently an associate professor of Computer Science at Jordan University of Science and Tech. He has co-authored several technical papers in established journals and conferences in fields related to cloud computing, edge computing, SDN and Big Data. He is a steering committee member and co-chair for CCSNA 2018 with Infocom. He is the General Co-Chair in IEEE International conference on Software Defined Systems SDS-2016 and SDS 2017. He is also chairing many IEEE events such as ICICS, SNAMS, BDSN, IoTSMS and many others. Dr. Jararweh served as a guest editor for many special issues in different established journals. Also, he is the steering committee chair of the IBM Cloud Academy Conference. He is associate editor in the Cluster Computing Journal (Springer), Information Processing and Management (Elsevier) and others.