Privacy Enhancing Technologies (PETs) for Connected Vehicles in Smart Cities

Sohrabi Safa, N., Mitchell, F., Maple, C. & Azad, M. A.

Original citation & hyperlink:
Sohrabi Safa, N, Mitchell, F, Maple, C & Azad, MA 2020, 'Privacy Enhancing Technologies (PETs) for Connected Vehicles in Smart Cities', Transactions on Emerging Telecommunications Technologies, vol. (In-Press), pp. (In-Press). https://dx.doi.org/10.1002/ett.4173

DOI 10.1002/ett.4173
ESSN 2161-3915

Publisher: Wiley

Privacy Enhancing Technologies (PETs) for Connected Vehicles in Smart Cities

Nader Sohrabi Safa[a], Faye Mitchell [b], Carsten Maple [c], Muhammad Ajmal Azad [d], Muhammad Dabbagh [e]
School of Computing, Electronics and Mathematics, Coventry University, United Kingdom[a,b]
WMG, University of Warwick, Coventry, United Kingdom[c]
College of Engineering and Technology, Derby University, United Kingdom[d]
Department of Computing and Information Systems, Sunway University, Malaysia[e]

Abstract

Many Experts believe that the Internet of Things (IoT) is a new revolution in technology that has brought many benefits for our organisations, businesses, and industries. However, information security and privacy protection are important challenges particularly for smart vehicles in smart cities that have attracted the attention of experts in this domain. Privacy Enhancing Technologies (PETs) endeavor to mitigate the risk of privacy invasions, but the literature lacks a thorough review of the approaches and techniques that support individuals' privacy in the connection between smart vehicles and smart cities. This gap has stimulated us to conduct this research with the main goal of reviewing recent privacy-enhancing technologies, approaches, taxonomy, challenges, and solutions on the application of PETs for smart vehicles in smart cities. The significant aspect of this study originates from the inclusion of data-oriented and process-oriented privacy protection. This research also identifies limitations of existing PETs, complementary technologies, and potential research directions.

Keywords: Privacy, Internet of Things, Data Protection, Privacy-Enhancing Technology, Information Security

1. Introduction

Privacy as a multi-dimensional concept encompasses legal, philosophical, and technical concepts [1]. The United State of America supreme court defined individual privacy as the "right to be let alone" in 1834 [2]. The Council of Europe explained privacy as a human right in Article 8 of the European Convention for the protection of human rights and fundamental freedom [3]. More recently, the General Data Protection Regulation (GDPR) emphasises that personal data should be processed in a manner that ensures appropriate privacy and security of personal data. This includes protection against unauthorised or unlawful processing and accidental loss, destruction, or damage of personal data, using appropriate technical or organisational measures.

IoT can be applied on various application domains such as smart cities, smart vehicles, smart health, smart education, smart infrastructure, smart grids, and smart toys. Privacy is important in all of IoT applications, but the emphasis will be on different aspects of the individuals' privacy depending on the context of an application [4]. Patients' sensitive information about illnesses and diseases in smart health, information regarding individuals' attendance at their homes in smart homes, and information about the amount and type of energy people may use in smart grids are just few examples to demonstrate that privacy protection in IoT is a context-based subject. Privacy in smart vehicles involves information about passengers, destinations, vehicle positions and situations, owners of the smart vehicle, energy consumption, and so on. Today, it is hard to protect individuals' privacy in environments in which large amounts of information is collected, processed, and stored by different technologies. A clear definition of privacy is necessary in this

regard; Nissenbaum [5] believes that we should define privacy in its own specific context, considering social norms. For example, information about patients' medical data should only be collected by medical professionals and not be shared outside the health environment, the movement patterns of drivers or vehicle owners should not be disclosed to any party other than the person himself or the data owners. The collected data in context of smart vehicular network should remain private, enable data centre to employ systems that perform analytics in a completely privacy-preserving way. Any use of such data outside of the particular environment is a privacy violation.

A privacy violation not only influences negatively an individuals' reputation, revenue, and intellectual property but also, in the worst-case scenario can cause bankruptcy and risk of life as happened in Ashly Madison privacy breach [6]. Privacy violations in Google, Facebook, and many other internet-centered companies that generate revenues from collecting, processing, and selling personal data of their users have attracted the attention of the general population and regulators. Legal experts and law enforcement agencies created the GDPR in Europe with more emphasis on an individual's right to privacy [7]. Choice, notice, access, and security of information are four principles that should be supported by technology to protect the privacy of individuals. The collection of personal data is lawful, limited, and occurs with the consent of the individuals (collection limitation). Personal data should be collected accurately, completely, and kept up-to-date only for the purposes that have been determined beforehand (data quality). The purpose of data collection should be specified in advance (purpose specification) and the use of data should be limited to that purpose (use limited). Personal data should be adequately protected (information security). The data processing and controller responsibility must be available (openness). Individuals have the right of rectifying, view, delete, complete, and amend their personal data (individual participation). The data controller must be accountable for complying with these principles (accountability). All PETs should be able to support the above privacy criteria [8]. However, the adoption of these principals in the domain of smart vehicles and smart cities is a tough task because of the nature and uncertainty of the conditions.

PETs refer to specific methods that support individuals' privacy based on the law of data protection. PETs protect the privacy of personally identifiable information (PII) that provide by applications or services [4]. PETs try to eliminate personal data without the loss of functionality of the information system. In simple words, PETs help users of technology to be assured about the confidentiality and integrity of their information by service providers [9]. In this study, we will focus more on different technologies that can support individuals' privacy, taxonomy, challenges, and solutions in the domain of IoT.

In this article, we present privacy protection taxonomies in common areas of IoT and smart vehicles. The type of privacy, attacks, and the source of data attacks also will be explained in this paper. We will discuss privacy protection technologies, including approaches, strategies into system design, cryptographic techniques to protect individuals' privacy, and information security. Privacy protection in IoT, its challenges, variety of privacy, and attacks are explained in Section 2. Section 3 presents different privacy protection approaches in smart vehicles. More specific privacy challenges in the domain of IoT and smart vehicles are highlighted in Section 4. Section 5 presents the conclusion and future research directions.

2. Privacy in the Internet of Things

The large scale, ubiquitous, pervasive connectivity, and interoperability found in IoT systems increase the risk of information security and privacy violation [10]. Although, an information security breach can cause privacy violation (and these two have some overlap), however information security and privacy protection are different subjects. A privacy threat is the possibility of the exposure of sensitive data to a person, enterprise, and even an artificial intelligence which are not authorized to possess those data [11]. Wrong data in the wrong entity's hand or too much data in the hands of the right entity is a privacy violation based on privacy principals [12].

Experts have acknowledged that for many years, developers and producers of IoT devices have neglected to consider information security and privacy protection considerations in the design and development of smart objects [13]. There are many challenges in terms of privacy protection in different application domains of IoT, particularly in the connection between IoT and smart vehicles. We have identified these challenges and possible solutions in this study.

2.1. Challenges in Smart Cities

The Internet of Things Strategic Research Agenda (SRA) identified six vertical domains for the IoT applications – smart cities, smart buildings, smart health, smart transport, smart living, and smart energy. Unification of these vertical applications can refer to smart life [14]. We have serious challenges in all of these domains. Companies claim that personal data is anonymised before being used for marketing, but, we have evidence showing the risk of re-identification and the use of the information without an individuals' consent. A recent study, which has investigated 1,100,000 credit cards, has proven the possibility of re-identification of 90% of individuals when knowing only four spatiotemporal points - where the individuals have been at which point of time [15]. This shows that we still need more sophisticated approaches for anonymization of data in IoT systems.

There are a variety of different IoT systems in a smart city; interconnectivity and interoperability among them increase the risk of information security and privacy violations [16]. Although, protocols in different layers of IoT systems can protect information and privacy, but mobile providers can track individuals through their smart mobile, cell towers, and hot spot locations. They can read unencrypted user's traffic and the third party can eavesdrop on the wireless channel [17].

Traffic in public hot spots is not necessarily encrypted, therefore, it can be monitored by nodes in the system, the access point, and even people in the vicinity of the system. Cheng, Wang [18] showed that personal privacy leakage happens when people use free WiFi in airports through HTTP protocol, resolution queries and profiled advertisements. This leakage can be decreased by using encrypted wireless communication (WPA2) or SLL/TLS. But, we still have privacy leakage when using these protocols [19]. Privacy of Metadata is another concern in this domain; information regarding who communicates with whom, when and for how long should be kept confidential. This shows that anonymous communication is important in IoT systems. Unfortunately, anonymous communication protocols cannot always guarantee the privacy of communication and attacks such as timing and traffic correlation attacks can compromise privacy of individuals [20].

Resource constraint is a key challenge in this domain that we have discussed it in several parts of this article. Different solutions have been presented to overcome this challenge. In [21], the researchers have presented a solution in line with VANET framework that proposes limiting the time frame related with the individual parts of the process. To this end, this article recommends that the resource-intensive ciphertext-policy attribute-based encryption (CP-ABE) task should be simplified under partitioning it into subtasks. This can be achieved by a machine-learning technique (decision tree) in a manner that significantly influences the completion times of all subtasks. An approach based on particle swarm optimization (PSO), called task-distribution PSO (TD-PSO), is proposed to perform the CP-ABE task distribution on a VANET. The performance of this approach is evaluated by comparison with a genetic algorithm (GA), followed by a comparison of these two solutions with the optimal solution proposed by the linear programming (LP) method. Results show that the TD-PSO approach consumes less overhead than the GA. The encryption part of this process plays important role in privacy protection in this domain [22].

2.2. Variety of Privacy

Privacy protection is a difficult task in an environment such as IoT in which we have pervasive connectivity and various actuator or smart objects that collect, process, and store individuals' information. Finn, Wright [23] have classified the privacy of individuals into seven types of privacy: privacy of the person, privacy of thoughts and feelings, the privacy of behaviour and action, privacy of personal communication, privacy of association, privacy of data and image, and privacy of location and space. Eckhoff and Wagner [24] believe that these varieties of privacy have some overlap – communication with the individuals always includes individuals' association, this means that communication and association are in the same category; they have considered this in the category of social life privacy. Image, audio, and video can be in media privacy. They also considered privacy of thought and feeling in body and mind privacy.

2.3. Attacks and Privacy

The Internet is a vast environment; attackers in this environment are knowledgeable and experts who use different and novel approaches to achieve their targets such as collecting sensitive information and private data [25]. The attacks can be categorised as active or passive, local or global, external or internal [26]. The attackers' ability and capability in terms of knowledge and available information, the employed algorithms, their resources such as computational power and network recovery influence their attacks. Attackers usually use four sources of data to violate privacy: public data, observable data, leaked data and repurposed data [13]. Public data refers to individuals or the government's data that is available to the public. These kinds of data contain statistical or private data that have been published. The attackers can correlate different sources and extract more private data. Observable data is the data that can be collected through eavesdropping on wired or wireless communication. This is an active attack in which attackers need to be in a location where the communication can be overheard. Repurposed data is the data collected for a particular purpose that is then repurposed for another purpose. For example, a service provider can collect locational data of a customer to provide better services in the future, but this data could be stored in the profile of the customer and could then be used to track them at different times. Repurposing data without users' consent is a privacy violation based on GDPR. Leaked data come from misuse of authorised access, security vulnerability, social engineering, and software flaws. Perfect protection of private data is hard to achieve, but a combination of privacy technologies is an effective way to mitigate privacy violations [27].

In this study, we have focused more on the research studies which have been presented during the last ten years. Our resources are from high-quality publications in Science Direct, IEEE, Emerald, Springer, and many other scientific databases in this domain. We have reviewed about one hundred papers in this domain. The keywords such as smart city, information security, privacy protection, connected vehicles, privacy-enhancing technologies, security attacks, privacy violations and so on have been used in the searches. We have restricted the scope of this study by methods, techniques, and approaches that can protect information and privacy in smart cities and connected vehicles. Figure 1 shows the taxonomy of subjects in a concise form.

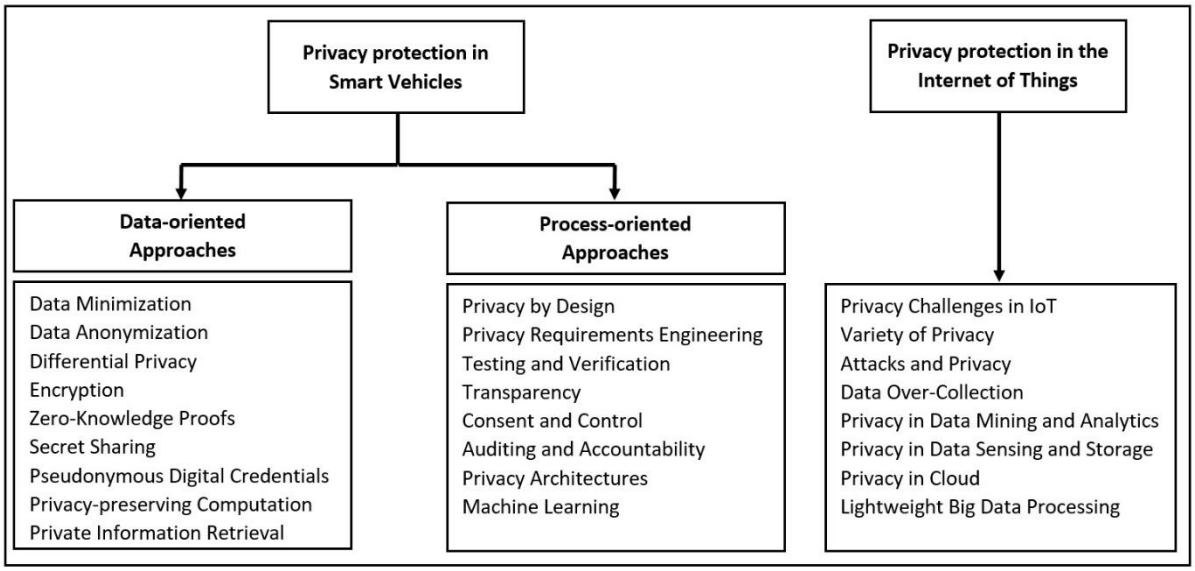

Figure 1: Classification of Subjects

3. Privacy Protection Approaches in Smart Vehicles

The applications of IoT are increasing every day; it is necessary we have a clear road map about how we want to protect individual's privacy. Anic, Budak [28] have defined six important objectives in privacy protection – anonymity, pseudonymise, unlinkability, unobservability, undetectability, and identity management. Anonymity refers to the lack of identification of an object in a group; An object should not be linked to other entities by an attacker in our dataset (unlinkability); hackers should not be able to distinguish whether a subject of their interest exists; anonymity of all involved entities besides undetectability are necessary for unobservability; using pseudonyms instead of real name enhances privacy protection, and identity management refers to managing identities using other technique such as pseudonyms to protect privacy. Looking above these techniques and approaches helped us to understand that these techniques change the data or focus on processes that protect the privacy and identities of individuals. Hence, we have categorised privacy-enhancing technologies based on data, process, and user entities. Data-oriented, user-oriented, and process-oriented privacy protections will be explained in the next sections.

3.1. Different Aspects of Privacy Protection Based on Data

A variety of methods such as data anonymisation, minimization, encryption, and so on have been presented by experts to protect individuals' privacy, focusing on the data. We explain these approaches in this section.

3.1.1. Data Minimization

The GDPR emphasis on adequate, relevant, and limited data collection with individuals' consent. Data minimisation also is one of the principals in privacy by design [29]. The IoT systems usually collect data for a particular task or purpose; however, in many cases, sensors collect more data and this causes risks for an individuals' privacy. For instance, cameras that are used for facial recognition to identify criminals, also capture unrelated information such as an individual's locations, or two persons holding hand that violate individual's privacy (relationships between individuals should be kept confidential). It has been mentioned that data minimisation can effectively decrease the risk of privacy invasion [30].

3.1.2. Data Anonymization

Data anonymisation refers to the process in which we remove personal identity information or encrypt the data to protect individuals' privacy [31]. Anonymisation also refers to converting clear text into nonhuman

readable and irreversible form. Data anonymisation is a technique that provides a secure data transfer across a boundary, between two departments or two organisations while reducing the risk of unintentional disclosure. De-anonymisation is the reverse process in which anonymised data are converted to re-identify data in our dataset [32].

K-anonymity is an approach to protect privacy which produces a dataset with the scientific guarantee that the individual's data cannot be re-identified from at least k-1 individuals whose their data appear in the release. Quasi-identifier are data that are not themselves unique identifiers, but it can be combined with other data to create a unique identifier and refer to an individual or entity. In the process of re-identification, several quasi-identifiers can be combined and create personally-identifying information. For instance, the combination of Post Code, gender, and date of birth can identify 87% of the American population which is a significant risk to privacy [33]. Suppression and generalisation are two common methods in k-anonymity approach.

3.1.3. Differential Privacy

Differential privacy is a mathematical approach to protect an individual's privacy in a dataset. Dwork, McSherry [34] showed that it is possible to publish information from a dataset without revealing some amount of private information. Differential privacy helps experts to provide accurate statistics from the dataset while ensuring high level of privacy. Differential privacy guarantees any disclosure is likely regardless of whether or not an item is in the dataset [35, 36]. In other words, the result of a query should be almost the same regardless of whether the dataset contains an individual's information or not.

3.1.4. Encryption

Encryption protects privacy by encrypting the individuals' data and information. In symmetric encryption, two parties need to share an encryption/decryption key, while the public-key is needed for encrypting data or message and a private-key is necessary for decryption [37, 38].

Identity-based encryption is a useful approach in which the system uses the identity of the user such as name or email address (as public-key) for encrypting the message [39]. The recipient does not need the pair of public/private key for decryption. This approach can be used for the recognition of private service discovery.

Attribute-based encryption is another useful cryptography approach; the private-key and the ciphertext depend on the user's attribute. The recipient can decrypt the message if his key's set of attributes fit the ciphertext [40]. One of its applications is in smart health where you can encrypt data for several groups of recipients who share common attributes such as doctors, nurses, and patients.

Homomorphic encryption (HE) is an approach that allows a system to perform computations on encrypted data; the result of the computation on encrypted data is the same as if they had been performed on the plaintext (decrypted data) [41]. For instance, HE can be used to calculate tax, currency exchange, and shipping on a transaction in a cloud without exposing the unencrypted data. HE can be used to securely chain together different services without declaring original data. HE has been applied in smart metering, voting system, recommendation system, private information retrieval, genomic test, and collision-resistant hash function to increase security and privacy [42].

3.1.5. Zero-Knowledge Proofs

Zero-Knowledge Proof is a cryptography method that helps us to protect information and privacy; it can be used for authentication, showing that an entity knows the password without revealing it; one party proves its knowledge about a fact or a value to another party [43]. In this process, the honest verifier who follows the protocol properly will accept the fact (knowing the secret in possession of prover) by an honest prover.

Completeness, soundness, and zero-knowledge transfer are three important characteristics of this process. Many companies use this approach alongside other approaches for authentication. It can be applied to show the steps in a protocol or process have been done correctly (honest behaviour). This approach has been already used in smart meter and electronic toll pricing [44].

In authentication, one party tries to prove its identity to another party through some secret information (a password), but the second party should not be able to learn anything about the password. A zero-knowledge password proof is a special kind of zero-knowledge proof of knowledge that addresses the limited size of the password.

Ethical behaviour is another application of zero-knowledge proofs, in which, we use cryptographic to enforce honest behaviour while protecting privacy. Indeed, we know that a user should act honestly to be able to provide valid proof. This approach can be used in nuclear disarmament.

3.1.6. Secret Sharing

A secret is distributed among several participants and cryptography is applied to increase the privacy of the message in secret sharing [45]. Shamir's Secret Sharing is a cryptography algorithm that divides a secret into several parts and every participant will receive his/her part; some parts of the secret or all of them are needed in order to reconstruct the secret. In this approach, we divide secret S into n pieces of data s_1, s_2, s_3,…, s_n in the way that:

1) Any combination of K pieces can help to reconstruct the secret (K<=n)
2) K-1 or fewer piece of secret leaves the secret completely undetermined.

Therefore, secret sharing provides both confidentiality and reliability. Secret sharing uses for data aggregation in a smart city, and participatory sensor networks [46].

3.1.7. Pseudonymous Digital Credentials

The identity of the originating entity is an important issue in the domain of information security and privacy protection. A sender of a message or a request should be identified in an IoT system. Anonymous digital credentials prove the identity of an entity without revealing its identity. In a blind signature, the system signs messages without reading their contents [47]. In this way, the authority testifies the message authors' identity while the signature does not contain the identity. Blind signature verifies the message was sent by legitimate cars in smart vehicles without disclosing vehicle identity [48].

Users can obtain credentials from authorities in anonymous credentials in the process in which transactions cannot be traced and identify users. Anonymous credentials are used in attribute-based credentials where revocation and de-anonymisation have been added [49]. Attribute-based credentials used in smart cities, help users authenticate with cloud providers without disclosing their identities [50].

Pseudonyms are used for long-term communication where the system needs to check the validity of an entity and not its identity; the certificate authority can link pseudonyms to user identity. This technique allows for privacy protection in smart vehicles where driver's location privacy is protected but the driver's actions are accountable in traffic [51].

3.1.8. Privacy-preserving Computation

Multi-party computation (MPC) or secure multi-party computation is a cryptographic approach when several parties jointly compute a function based on their inputs and keep these inputs private [52]. In this process, adversaries or eavesdroppers that can send and receive data cannot access the data. This approach is based on some game assumptions in which different individuals play over a distance without requiring

the trust to other players. Confidentiality and unlinkability are the most characteristics of this technique. One of the applications of MPC is in the health systems where the system computes the results of genomic tests when the system protects the patients' genomes and test sequences [53].

3.1.9. Private Information Retrieval

Private Information Retrieval (PIR) is a cryptographic approach in which PIR allows a user to retrieve information from a database on a server without disclosing which item is retrieved [54]. PIR provides undetectability, unlinkability, and confidentiality in an IoT system. This approach has been used to hide access patterns to data stored in the cloud [55].

3.2. Different Aspects of Privacy Protection Based on Process

In Auditing and Accountability, Privacy Architecture, Privacy by Design, Privacy requirements Engineering, testing and Verification, Transparency, and Consent and Control, the focus is more on the process of privacy protection in an IoT system. We explain them in the following subsections.

3.2.1. Privacy by Design

The consequence of privacy violation can be very unpleasant and even cause suicide such as what happened in Ashly Madison. As we mentioned before, GDPR also emphases more on privacy protection [13]. Unfortunately, experts and developers of smart devices in the domain of smart homes, smart health, smart toys, smart appliance, and so on have neglected to consider privacy considerations in the design stages of smart objects for many years. Experts believe that privacy should be taken into account throughout the entire engineering process. It is acknowledged that privacy by design when used alongside the other privacy protection approaches can mitigate the risk of privacy violations. Cavoukian [56] have mentioned seven principles for privacy by design:

1) Privacy protection should be a default setting
2) The privacy should be embedded into the design
3) Full functionality plus full privacy protection
4) The entire lifecycle of data should be protected (data collection, storage, process, share, destroy)
5) Visibility and transparency are important
6) Individual's privacy is respectful
7) Proactive privacy protection instead of remedial action

End to end privacy protection and data minimisation are examples that can be considered in the design of a health system [57].

3.2.2. Privacy Requirements Engineering

Privacy Requirement Engineering is a prerequisite of privacy design; this process can be started with data minimization and functional requirement analysis considering vulnerability, risk, and attacks associated with the system, and finally implementation and testing [58]. Hoepman [59] have proposed two groups of privacy design strategies – data focus, and process focussed. Data hiding, minimisation, aggregation, and separation refer to data focussed strategy, and controlling, demonstrating, informing and enforcing refer to the process focused privacy strategy.

Users trust a system when they think the system protects their private information. Users' desire for the protection of personal information is an important factor when they communicate. Experts recommend that we should consider privacy protection during system design instead of system implementation [24]. PriS is a security requirement engineering approach that considers privacy requirements from the first step of system development process. Pris considers privacy protection as requirement goals that should be part of

business process and place in the system architecture. PriS is a holistic approach from organisational goals to privacy protection [60].

3.2.3.Testing and Verification

Privacy testing and verification is an important step to guarantee that a system fulfills the defined privacy requirements. Privacy requirements refer to privacy objectives and GDPR considerations that determine the capabilities, and functionality of a system in terms of privacy protection. Privacy requirements should be actionable, traceable, measurable, and testable [61]. Privacy testing approaches are proposed to find information leaks and system weaknesses through different testing methods such as Black-box testing, taint checking, analysis of information flow based on sensitive program input and output [62].

3.2.4.Transparency

Many devices in our vicinity collect data about individuals and transfer them through the Internet for further processing [61]. The GDPR emphasises that individuals should be aware of what data about them is collected, where this data is stored, how it will be processed and shared, how long the data will be kept and how it will be protected. Transparency in privacy protection creates trust and improves individuals' collaboration in our society [63]. Trust of smart objects is a controversial issue for people and experts. Algorithmic transparency is an effective approach that explains the steps of data processing in IoT systems [64]. An explanation of algorithmic transparency in an understandable language improves the level of perceived privacy in smart cities, smart vehicles, smart health and so on.

3.2.5.Consent and Control

Consent is an important element for both users who use smart devices such as smart sports equipment, smart health devices, smart toys, and individuals whose their information are collected by the smart objects in smart cities, smart homes, smart grid, etc [65]. Users of smart devices and individuals whose their information are collected by smart objects should agree with data collection, process, the period that the data will be kept and another process that relates to their data [66]. Unfortunately, people are not able to control these processes in many cases, or even review the privacy policies that have been created by agents or companies; it is difficult to give users control over their data for deleting and updating of the data. Users' privacy setting is an approach that allows individuals to control the flow of data and some of the other processes in this regard [67].

3.2.6.Auditing and Accountability

There are two views about the accountability of privacy in IoT environments. First, to keep smart devices accountable in terms of individuals' data collection and compliance with GDPR. Second, to put individuals under surveillance in order to account for their misbehaviours [68]. Logging and auditing help experts to investigate whether smart objects comply with privacy policies or not. Auditing determines that how and how often privacy violation has been occurred by smart objects or actuators [69].

3.2.7.Privacy Architectures

Privacy architecture is an important part of Privacy by Design (PbD).It encompasses feature and privacy principles into the basic design of information processes and information systems. Privacy architecture is different from security architecture; they must be coordinated and combined. For instance, data minimization and anonymity are important to be considered in the privacy domain, but they are not necessary in information security, although they can be considered.

Table 1 lists privacy protection approaches. They are classified into two main categories of data-oriented and process-oriented approaches.

Table 1: Privacy Protection Approaches

Data-oriented approaches	Process-oriented approaches
Data Minimization	Privacy by Design
Data Anonymization	Privacy Requirement Engineering
Differential Privacy	Testing and Verification
Encryption	Transparency
Zero-Knowledge Proofs	Consent and Control
Secret Sharing	Auditing and Accountability
Pseudonymous Digital Credentials	Privacy Architectures
Private Information Retrieval	

3.3. Privacy and Security overlap

Confidentiality, integrity and availability of information have been mentioned in many resources as the three main pillars in information security [70]. Privacy refers to the protection of information about an individual or a group; they can choose which information about themselves can be shared with others. The content and boundaries of what is private are different in different countries [57]. Privacy is a context-based concept. There is a strong intermix between information security and privacy protection when we discuss about patients' privacy, relationships privacy, address and place privacy, etc. Although some of privacy protection approaches such as encryption (homomorphic encryption, attribute-based encryption, identity-based encryption, etc.) safeguard both privacy and security, some of the other approaches such as pseudonym, de-identification, auditing and accountability, differential privacy, and transparency emphasise more on privacy protection. The line between conceptual and security-related privacy is not clear in the domain of IoT [24]. For instance, a smart camera that captures and transfers the image of individuals for policing, capture his/her companion and information leakage in such system have more negative consequence on individuals, privacy; this is a challenge that should be addressed in terms of privacy protection as well.

3.3.1. Information Leakage

Information leakage refers to the transfer of data or information to unauthorised parties. Hacking, attacking, insider threats (employees intentional and unintentional) etc., are resources for information leakage [71]. Side-channel attacks are another source of information leakage in which attackers gain information from the implementation of a computer system instead of bugs or flaws in an algorithm or a software. Technical knowledge of the internal processes and operations help attackers in side-channel attacks [72].

Application of web technologies and software as a service have a high potential risk of side-channel attacks even when the system transfers data and information using encryption. Table 2 shows several types of side-channel attacks.

Table 2: Different types of Side Channel Attacks

Attacks	Description
Cache Attack	Attackers monitor cache in share physical system that made by the users in a cloud service or virtualised environment.
Timing Attack	Measurement of the time to respond to certain queries can leak from a system. Attackers use this information to compromise information security. In cryptography, attackers analyse the time taken to execute cryptographic process, detecting the time for each operation and use the results of the analysis to compromise the system.
Power-monitoring Attack	Attackers focus on power consumption of devices during computation to compromise the system.
Electromagnetic Attack	Electronic magnetic radiation can be used to develop cryptographic key. This can be a source of attackers in cases in which experts use electromagnetic for encrypting secrets.
Differential Fault Analysis	The secrets are disclosed by injecting faults in a computation.
Cold Boot Attack	Attackers have access to computers and able to retrieve encryption key from DRAM and SRAM in running operation system.

Cache-based vulnerabilities in CPU has attracted attention of experts recently. Spectre and Dubbed meltdown attacks are threats that allow hackers to leak memory contents and the operating system [73].

3.3.2. Protocol and Network Security

Applying cryptographic protocols in which encryption algorithms such as hash functions are used, plays an important role in securing confidential communication. For instance, the flaw in 6LOWPAN stack can reveal user activities in the system from information that comes from header of message [74]. An improperly developed protocol increases the risk of a privacy violation in some attacks such as eavesdropping. To decrease the risk of privacy violation in an IoT system, the system should be designed in a privacy-aware manner [1]. Developers of protocols should always check the entire protocol stack to prevent any risk of information security and privacy violation.

3.3.3. System Security and Access Control:

The security of the systems or sub-systems in an IoT environment plays an important role in privacy protection. For instance, hackers can compromise the privacy of individuals when they spy on the events and habits of family members through the control of devices in a smart home; this is a problem in security of the system. This can compromise the privacy of individuals when they use intelligent vehicles, wearable devices, autonomous systems, sensor networks, and many other smart objects [75].

Study of Uluagac, Subramanian [76] show that the sensory interfaces of smart objects pose privacy challenges; this study revealed that the sensory channel of the cyber-physical system can cause privacy violation. The sensors such as LiDAR in smart vehicles can affect driving decisions [77]. Access control prevents access to the system and its databases, but it cannot prevent misuse of authorized access; attribute-based encryption besides access control can improve the security and privacy of a system.

4. Privacy Challenges

The IoT contains several basic technologies such as information, communication and computation technologies. In addition, large scalability, high granularity, and diversity of data have the potential of information security breaches and privacy violations. Cloud computing, data analytics and mining, sensor

technology, and big data have created new challenges in this domain. We explain these challenges in the next subsections.

4.1. Data Over-Collection

Data over-collection refers to data that is collected by a smart object such as smartphone, where the data contains information that is more than the data that is needed for a particular function [1]. The information that is collected by a camera to increase the security of people in different parts of a city can reveal the model of their cars, his or her companion at a particular time and their relationships, items that they carry or buy, cloths style, locations, and so on, that may be irrelevant to the original purpose of data collection. Current technologies are not able to conceal irrelevant information from the data collection process and protect the privacy of individuals completely [78].

Many applications have been designed to help individuals with their health, financial activities, environmental monitoring, etc. These applications can have access to data resides in our mobiles, tablets and other smart devices that we use. This enables them to transfer more information about individuals than they really need [79]. Therefore, it is necessary to design effective technologies to overcome data over-collection issue in smart environment.

4.2. Data Mining and Analytics

Government agencies, companies, contractors, business partners, are all interested in collecting individuals' information and analysing this information to provide better services and extend their markets. They use different approaches and devices to achieve this target. The IoT has provided an appropriate approach for them [80]. The volume of this data is increasing significantly; the big data is not only a challenge in terms of analysis and process but also in terms of information security and privacy protection. Data analytic approaches help companies to identify new potential customers in which it may disclose individuals' information without their consent. Cameras, sensors, and smart devices capture individuals' information and try to improve their databases, creating a relationship with other data resources to complete and identify people [81].

Data analytics is an approach that many companies use to draw a complete picture of their customers or clients and potential new customers. Data analytic refers to quantitative and qualitative techniques and processes used to gain more benefits in businesses and enhance productivity [82]. Data can be used to produce classifications that identify the patterns of customers' behaviour, attitudes and their perception of people [83]. Data analytics have been applied in the domain business market economy. We heard recently that experts can feed social networks and even influence political tendency and election process in a country such as the United State of America [84]. Preventing unauthorized processing on an individuals' information and influencing their behaviour in a particular direction is a serious challenge in this regard. Data anonymization and using data analytic algorithms on encrypted data are solutions that experts have presented in this regard. However, data analysis on encrypted data is very time consuming, difficult and unsuitable for online data analytic [85].

It has been acknowledged that information security and privacy violation is an important issue in the domain of connected autonomous; in particular, when the systems connect to roadside systems or cloud for data analysis and decision making. To mitigate these concerns, Aloqaily, Otoum [86] introduces an automated secure continuous cloud service availability framework for smart connected vehicles that enables an intrusion detection mechanism against security attacks and provides services that meet users' quality of service (QoS) and quality of experience (QoE) requirements. In another study, Rathee, Sharma [87] has used a particular data block that helps autonomous vehicles to reduce congestion by allowing recent

information to be obtained by the vehicles instantly; the presented blockchain does not allow malicious users mislead or disrupt normal communication and real-time management of the systems.

4.3. Data Sensing and Storage

IoT systems are able to collect data through different smart objects, actuators, wireless sensors and so on. The collected data is usually transferred into a database or cloud storage. We are faced with a huge volume of data in some applications of IoT [88]. Auto-tiering storage is used as an efficient approach to store this data based on the policies established by organizations. The mismatch between these organisational policies and unverified storage causes several security vulnerabilities for auto-tiering technology. For instance, auto-tiering relocates the storage based on the rate of the access requests (high request or rarely request); less security is considered for the data which seldom requested and located at a lower tier of the database. Another challenge refers to the security of log files in this system; transaction logs contain a list of activities on the database. These transactions should be kept securely for further investigations if it is necessary [89]. The rollback attack and collision attack have been mentioned as other flaws in auto-tiering technology.

4.4. Cloud and Smart Vehicle Challenges

Smart health-care, smart citizens, and smart governance are examples of IoT systems that make extensive use of cloud computing due to its useful facilities. Although the integration of IoT and cloud computing has attracted the attention of experts in this domain, information security and privacy protection are still a controversial issue in this domain [90].

Resource constraint is a serious challenge that negatively influences information security and privacy protection in the domain of smart vehicles. An interesting model has been presented by [91] that shows how a cloud environment can be formed by individuals' vehicles, where each vehicle offers its resources as a service, using a 5G network [92]. The key factor in this approach is network slicing that allows managing the congestion between the sender and receiver. In another study, [93] have discussed about intra-vehicle resource sharing model to provide a range of cloud services such as on-demand entertainment and speech recognition for driver assistance. The proposed solution forms nearly low-latency vehicular service cloud (VSC) on-the-fly as per the need of vehicular users [94].

Multitenancy is another concern in the cloud IoT. Multitenancy is one of the differences between locally managed computing and cloud computing in which some of the tenants can share resources and delegate the management of the data and process to the cloud service provider [95]. In this scenario, the cloud service provider can provide a shared environment and even a shared database. This raises some concerns about information leakage and data breach. To overcome these challenges, Taha, Talhi [96] have presented Attribute Based Encryption (ABE) with a mechanism that can overcome resource constraints. The other concerns that originate from multitenancy issues are malware propagation, unauthorised connection monitoring, and man in the middle attacks [97].

4.5. Lightweight Big Data Processing

Big data and IoT are two concepts that strongly have interwoven due to the nature of IoT. The data which have been collected in different IoT systems such as smart traffic control, smart grid, smart cities, wireless sensors and so on usually are stored in NoSQL databases [98]. We need to perform both batch and real time processing in these kinds of systems. The real-time data processing must be performed concurrently with continuous input data, analysis, and flows of output in a small amount of time, which requires a high-performance system. [99] have proposed a big data analytic framework to overcome these challenges in smart cities. However, the majority of the proposed solutions have neglected or are unable to support information security and privacy considerations through a variety of IoT systems [100]. Information security and privacy protection in such real-time systems need high-performance systems that utilize

lightweight encryption approaches to deal with the resource-constrained environment and high computational costs.

5. Conclusion

The IoT is a new revolution in many domains such as smart cities, and smart vehicles, but information security and privacy protection are still two serious challenges to be addressed in these domains. Privacy protection is a context-based concept; we need to use different approaches to protect individuals' privacy in this complicated environment. The recent research in this domain show we have many challenges. Privacy Enhancing Technologies have attracted the attention of experts recently and help them to overcome these challenges, but as there is limited research in this domain this has encouraged us to start a study.

We have tried to present a comprehensive view of the approaches, techniques, and methods that help experts to improve information security and privacy protection in smart cities and smart vehicles. We explained that although information security and privacy protection are two different subjects, they have remarkable overlap. The significant aspect of this study points to technologies and techniques that support GDPR. We have classified these technologies into data-focused and process-focused approaches. This research shows a broad range of subjects for research by experts in academics and practitioners; we have serious challenges in privacy protection, particularly in IoT and smart vehicles domain that we have mentioned them in this article. Working on the taxonomy of attacks in smart vehicles and IoT can be considered for the next step in this research. We believe that this research sheds light on academics and practitioners in this domain.

References

1. Sookhak, M., et al., *Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges.* IEEE Communications Surveys & Tutorials, 2018: p. 1-1.
2. Warren, S.D. and L.D. Brandeis, *The Right to be Alone.* Harvard Law Review, 1890. **4**(5): p. 193-220.
3. Europe, C.o., *European convention on human rights*

1987.

4. Lavranou, R. and A. Tsohou, *Developing and validating a common body of knowledge for information privacy.* Information and Computer Security, 2019. **26**(5): p. 668-686.
5. Nissenbaum, H., *Privacy is Conttexttual Integrity.* Washington Law Rev., 2004. **79**(1): p. 119-158.
6. Brumen, B., R. Ivančič, and I. Rozman. *A comparison of password management policies*. in *2016 Portland International Conference on Management of Engineering and Technology (PICMET)*. 2016.
7. Union, C.o.t.E., *General Data Protection Regulation*, in *5419/16* C.o.t.E. Union, Editor. 2016: Brussels.
8. Da Veiga, A. and N. Martins, *Information security culture and information protection culture: A validated assessment instrument.* Computer Law & Security Review, 2015. **31**(2): p. 243-256.
9. Coss David, L. and G. Dhillon, *Cloud privacy objectives a value based approach.* Information and Computer Security, 2019. **27**(2): p. 189-220.
10. Maple, C., *Security and privacy in the internet of things.* Journal of Cyber Policy, 2017. **2**(2): p. 155-184.
11. *Privacy*, second, Editor. 2018, Stanford Encyclopedia of Philosophy.
12. Misra, S., M. Maheswaran, and S. Hashmi, *Security Challenges and Approaches in Internet of Things*. 2017: Springer.
13. Romanou, A., *The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise.* Computer Law & Security Review, 2018. **34**(1): p. 99-110.
14. Vermesan, O., et al., *Internet of Things Strategic Research Roadmap*. 2011.
15. de Montjoye, Y.-A., et al., *Unique in the shopping mall: On the reidentifiability of credit card metadata.* Science, 2015. **347**(6221): p. 536-539.
16. Al-Turjman, F., H. Zahmatkesh, and R. Shahroze, *An overview of security and privacy in smart cities' IoT communications.* Transactions on Emerging Telecommunications Technologies. **n/a**(n/a): p. e3677.
17. Cimmino, A., et al., *The role of small cell technology in future Smart City applications.* Transactions on Emerging Telecommunications Technologies, 2014. **25**(1): p. 11-20.
18. Cheng, N., et al. *Characterizing privacy leakage of public WiFi networks for users on travel*. in *2013 Proceedings IEEE INFOCOM*. 2013.
19. Georgiev, M., et al., *The most dangerous code in the world: validating SSL certificates in non-browser software*, in *Proceedings of the 2012 ACM conference on Computer and communications security*. 2012, ACM: Raleigh, North Carolina, USA. p. 38-49.
20. Johnson, A., et al., *Users get routed: traffic correlation on tor by realistic adversaries*, in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013, ACM: Berlin, Germany. p. 337-348.
21. Bany Taha, M., et al., *TD-PSO: Task distribution approach based on particle swarm optimization for vehicular ad hoc network.* Transactions on Emerging Telecommunications Technologies. **n/a**(n/a): p. e3860.
22. Taha, M.B., C. Talhi, and H. Ould-Slimanec, *A Cluster of CP-ABE Microservices for VANET.* Procedia Computer Science, 2019. **155**: p. 441-448.
23. Finn, R.L., D. Wright, and M. Friedewald, *Seven Types of Privacy*, in *European Data Protection: Coming of Age*, S. Gutwirth, et al., Editors. 2013, Springer Netherlands: Dordrecht. p. 3-32.

24. Eckhoff, D. and I. Wagner, *Privacy in the Smart City-Applications, Technologies, Challenges, and Solutions* IEEE Communications Surveys & Tutorials, 2018. **20**(1): p. 489-516.
25. Safa, N.S., et al., *Information security conscious care behaviour formation in organizations.* Computers & Security, 2015. **53**(0): p. 65-78.
26. Parra-Arnau, J., D. Rebollo-Monedero, and J. Forné, *Measuring the privacy of user profiles in personalized information systems.* Future Generation Computer Systems, 2013(0).
27. Porambage, P., et al., *The Quest for Privacy in the Internet of Things.* IEEE Cloud Computing, 2016. **3**(2): p. 36-45.
28. Anic, I.-D., et al., *Extended model of online privacy concern: what drives consumers' decisions?* Online Information Review, 2019. **43**(5): p. 799-817.
29. van Rest, J., et al. *Designing Privacy-by-Design*. 2014. Berlin, Heidelberg: Springer Berlin Heidelberg.
30. Tudor, V., M. Almgren, and M. Papatriantafilou, *The influence of dataset characteristics on privacy preserving methods in the advanced metering infrastructure.* Computers & Security, 2018. **76**: p. 178-196.
31. Gkoulalas-Divanis, A., G. Loukides, and J. Sun, *Publishing data from electronic health records while preserving privacy: A survey of algorithms.* Journal of Biomedical Informatics, 2014. **50**: p. 4-19.
32. Kohlmayer, F., et al., *A flexible approach to distributed data anonymization.* Journal of Biomedical Informatics, 2014. **50**: p. 62-76.
33. Sweeney, L., *k-Anonymity: A Model for Producing Privacy.* International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002. **10**(05): p. 557-570.
34. Dwork, C., et al. *Calibrating Noise to Sensitivity in Private Data Analysis*. 2006. Berlin, Heidelberg: Springer Berlin Heidelberg.
35. Dwork, C., et al., *On the complexity of differentially private data release: efficient algorithms and hardness results*, in *Proceedings of the forty-first annual ACM symposium on Theory of computing*. 2009, ACM: Bethesda, MD, USA. p. 381-390.
36. Azad, M.A., S. Bag, and F. Hao, *PrivBox: Verifiable decentralized reputation system for online marketplaces.* Future Generation Computer Systems, 2018. **89**: p. 44-57.
37. Saxena, A.K., S. Sinha, and P. Shukla. *A new way to enhance efficiency & security by using symmetric cryptography*. in *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*. 2017.
38. Azad, M.A., et al., *TrustVote: Privacy-Preserving Node Ranking in Vehicular Networks.* IEEE Internet of Things Journal, 2019. **6**(4): p. 5878-5891.
39. Wu, D.J., et al. *Privacy, Discovery, and Authentication for the Internet of Things*. 2016. Cham: Springer International Publishing.
40. P, P.K., S.K. P, and A. P.J.A, *Attribute based encryption in cloud computing: A survey, gap analysis, and future directions.* Journal of Network and Computer Applications, 2018. **108**: p. 37-52.
41. Emmanuel, N., et al., *Structures and data preserving homomorphic signatures.* Journal of Network and Computer Applications, 2018. **102**: p. 58-70.
42. Wang, C., et al., *Toward Privacy-Preserving Personalized Recommendation Services.* Engineering, 2018. **4**(1): p. 21-28.
43. Kannan, B. and K. Mala, *Zero Knowledge Proofs: A Survey*, in *Algorithmic Strategies for Solving Complex Problems in Cryptography*, B. Kannan and M. Rajakani, Editors. 2018, IGI Global: Hershey, PA, USA. p. 111-123.
44. Jawurek, M., M. Johns, and F. Kerschbaum. *Plug-In Privacy for Smart Metering Billing*. 2011. Berlin, Heidelberg: Springer Berlin Heidelberg.
45. Kursawe, K., G. Danezis, and M. Kohlweiss. *Privacy-Friendly Aggregation for the Smart-Grid*. 2011. Berlin, Heidelberg: Springer Berlin Heidelberg.

46. Framner, E., et al., *Making secret sharing based cloud storage usable.* Information and Computer Security, 2019. **26**(5): p. 647-667.
47. Schaub, F., et al. *V-Tokens for Conditional Pseudonymity in VANETs*. in *2010 IEEE Wireless Communication and Networking Conference*. 2010.
48. Petit, J., et al., *Pseudonym Schemes in Vehicular Networks: A Survey.* IEEE Communications Surveys & Tutorials, 2015. **17**(1): p. 228-255.
49. Camenisch, J., et al., *Concepts and languages for privacy-preserving attribute-based authentication.* Journal of Information Security and Applications, 2014. **19**(1): p. 25-44.
50. Avgerou, A., et al., *On the Deployment of Citizens' Privacy Preserving Collective Intelligent eBusiness Models in Smart Cities* International Journal of Security and Its Applications 2016. **10**(2).
51. Eckhoff, D. and C. Sommer, *Driving for Big Data? Privacy Concerns in Vehicular Networking.* IEEE Security & Privacy, 2014. **12**(1): p. 77-79.
52. Bogetoft, P., et al. *Secure Multiparty Computation Goes Live*. 2009. Berlin, Heidelberg: Springer Berlin Heidelberg.
53. Jha, S., L. Kruger, and V. Shmatikov. *Towards Practical Privacy for Genomic Computation*. in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. 2008.
54. Devet, C. and I. Goldberg. *The Best of Both Worlds: Combining Information-Theoretic and Computational PIR for Communication Efficiency*. 2014. Cham: Springer International Publishing.
55. Devet, C., I. Goldberg, and N. Heninger, *Optimally robust private information retrieval*, in *Proceedings of the 21st USENIX conference on Security symposium*. 2012, USENIX Association: Bellevue, WA. p. 13-13.
56. Cavoukian, A. *The 7 Foundational Principles* 2009 [cited 2009; Available from: www.ipc.on.ca.
57. Lu, Y. and R.O. Sinnott, *Semantic privacy-preserving framework for electronic health record linkage.* Telematics and Informatics, 2018. **35**(4): p. 737-752.
58. Deng, M., et al., *A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements.* Requirements Engineering, 2011. **16**(1): p. 3-32.
59. Hoepman, J.-H. *Privacy Design Strategies*. 2014. Berlin, Heidelberg: Springer Berlin Heidelberg.
60. Kalloniatis, C., E. Kavakli, and S. Gritzalis, *Addressing privacy requirements in system design: the PriS method.* Requirements Engineering, 2008. **13**(3): p. 241-255.
61. Amato, F. and F. Moscato, *A model driven approach to data privacy verification in E-Health systems.* Trans. Data Privacy, 2015. **8**(3): p. 273-296.
62. Enck, W., et al., *TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones*, in *Proceedings of the 9th USENIX conference on Operating systems design and implementation*. 2010, USENIX Association: Vancouver, BC, Canada. p. 393-407.
63. Janic, M., J.P. Wijbenga, and T. Veugen. *Transparency Enhancing Tools (TETs): An Overview*. in *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*. 2013.
64. Diakopoulos, N. and M. Koliska, *Algorithmic Transparency in the News Media.* Digital Journalism, 2017. **5**(7): p. 809-828.
65. Singh, J., T.F.J.M. Pasquier, and J. Bacon. *Securing tags to control information flows within the Internet of Things*. in *2015 International Conference on Recent Advances in Internet of Things (RIoT)*. 2015.
66. Wakenshaw, S.Y.L., et al. *Mechanisms for meaningful consent in Internet of Things*. in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. 2018.
67. Neisse, R., et al. *An agent-based framework for Informed Consent in the internet of things*. in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. 2015.
68. Garg, D., L. Jia, and A. Datta, *Policy auditing over incomplete logs: theory, implementation and applications*, in *Proceedings of the 18th ACM conference on Computer and communications security*. 2011, ACM: Chicago, Illinois, USA. p. 151-162.

69. Wang, C., et al. *Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing*. in *2010 Proceedings IEEE INFOCOM*. 2010.
70. Safa, N.S., et al. *Information security collaboration formation in organisations*. IET Information Security, 2017. **12**, 238 - 245 DOI: 10.1049/iet-ifs.2017.0257.
71. Safa, N.S., C. Maple, and T. Watson, *The information security landscape in the supply chain.* Computer Fraud & Security, 2017. **2017**(6): p. 16-20.
72. Chiappetta, M., E. Savas, and C. Yilmaz, *Real time detection of cache-based side-channel attacks using hardware performance counters.* Applied Soft Computing, 2016. **49**: p. 1162-1174.
73. Sadique, U.K.M. and D. James, *A Novel Approach to Prevent Cache-based Side-Channel Attack in the Cloud.* Procedia Technology, 2016. **25**: p. 232-239.
74. Hennebert, C. and J.D. Santos, *Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis.* IEEE Internet of Things Journal, 2014. **1**(5): p. 384-398.
75. Komninos, N., E. Philippou, and A. Pitsillides, *Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures.* IEEE Communications Surveys & Tutorials, 2014. **16**(4): p. 1933-1954.
76. Uluagac, A.S., V. Subramanian, and R. Beyah. *Sensory channel threats to Cyber Physical Systems: A wake-up call*. in *2014 IEEE Conference on Communications and Network Security*. 2014.
77. Petit, J., B. Stottelaar, and M. Feiri, *Remote Attacks on Automated Vehicles Sensors : Experiments on Camera and LiDAR*, in *Black Hat Europe*. 2015.
78. Li, Y., et al., *Privacy Protection for Preventing Data Over-Collection in Smart City.* IEEE Transactions on Computers, 2016. **65**(5): p. 1339-1350.
79. Damopoulos, D., et al., *User privacy and modern mobile services: are they on the same path?* Personal and Ubiquitous Computing, 2013. **17**(7): p. 1437-1448.
80. Kalloniatis, C., *Incorporating privacy in the design of cloud-based systems: a conceptual meta-model.* Information and Computer Security, 2017. **25**(5): p. 614-633.
81. Lesk, M., *Big Data, Big Brother, Big Money.* IEEE Security & Privacy, 2013. **11**(4): p. 85-89.
82. Cárdenas, A.A., P.K. Manadhata, and S.P. Rajan, *Big Data Analytics for Security.* IEEE Security & Privacy, 2013. **11**(6): p. 74-76.
83. *Assessing Russian Activities and Intentions in Recent US Elections*. 2017, Intelligence Community Assessment. p. 1-15.
84. Jones, J.J., et al., *Social influence and political mobilization: Further evidence from a randomized experiment in the 2012 U.S. presidential election.* PLOS ONE, 2017. **12**(4): p. e0173851.
85. Ren, X., et al., *High-Dimensional Crowdsourced Data Publication With Local Differential Privacy.* IEEE Transactions on Information Forensics and Security, 2018. **13**(9): p. 2151-2166.
86. Aloqaily, M., et al., *An intrusion detection system for connected vehicles in smart cities.* Ad Hoc Networks, 2019. **90**: p. 101842.
87. Rathee, G., et al., *A Blockchain Framework for Securing Connected and Autonomous Vehicles.* Sensors 2019. **19**(14).
88. Stergiou, C., et al., *Secure integration of IoT and Cloud Computing.* Future Generation Computer Systems, 2018. **78**: p. 964-975.
89. Safa, N.S., et al., *Deterrence and prevention-based model to mitigate information security insider threats in organisations.* Future Generation Computer Systems, 2019. **97**: p. 587-597.
90. Moreno-Vozmediano, R., R.S. Montero, and I.M. Llorente, *Key Challenges in Cloud Computing: Enabling the Future Internet of Services.* IEEE Internet Computing, 2013. **17**(4): p. 18-25.
91. Aloqaily, M., et al., *Congestion Mitigation in Densely Crowded Environments for Augmenting QoS in Vehicular Clouds.* Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, 2018: p. 49-56.
92. da Silva Barbosa, F.E., F.F. de Mendonça Júnior, and K.L. Dias, *A platform for cloudification of network and applications in the Internet of Vehicles.* Transactions on Emerging Telecommunications Technologies, 2020. **31**(5): p. e3961.

93. Balasubramanian, V., et al., *Low-latency vehicular edge: A vehicular infrastructure model for 5G.* Simulation Modelling Practice and Theory, 2020. **98**.
94. Atif, Y., et al., *Internet of Things data analytics for parking availability prediction and guidance.* Transactions on Emerging Telecommunications Technologies, 2020. **31**(5): p. e3862.
95. Zou, M., J. He, and Q. Wu. *Multi-tenancy access control strategy for cloud services*. in *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*. 2016.
96. Taha, M.B., C. Talhi, and H. Ould-Slimane, *Performance Evaluation of CP-ABE Schemes under Constrained Devices.* Procedia Computer Science, 2019. **155**: p. 425-432.
97. Rao, M.V., G.V. Murthy, and V.V. Kumar. *Multi-Tenancy authorization system in multi cloud services*. in *2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC)*. 2017.
98. Strohbach, M., et al., *Towards a Big Data Analytics Framework for IoT and Smart City Applications*, in *Modeling and Processing for Next-Generation Big-Data Technologies: With Applications and Case Studies*, F. Xhafa, et al., Editors. 2015, Springer International Publishing: Cham. p. 257-282.
99. IBM, *2018 cost of data breach study: Global analysis*. 2018.
100. Benrazek, A.-E., et al., *An efficient indexing for Internet of Things massive data based on cloud-fog computing.* Transactions on Emerging Telecommunications Technologies, 2020. **31**(3): p. e3868.

Data sharing is not applicable to this article as no new data were created or analyzed in this study.