Security and Privacy Concerns in Connected Cars: A Systematic Mapping Study

Prabhat Ram, Jouni Markkula, Ville Friman, Arian Raz
University of Oulu, Oulu, Finland
{prabhat.ram, jouni.markkula, arian.razmifarooji}@oulu.fi; ville.friman@student.oulu.fi;

***Abstract*— Significant strides are being made in research towards security and privacy concerns associated with connected cars. Being a relatively novel research domain, it is crucial to examine the state of the art to formulate future research strategies. The objective of the paper is to aggregate the research progress made in identifying security and privacy concerns in connected cars, and the concomitant solutions. Using systematic mapping study, we reviewed the state of the art to address the research objective. Results indicate that in the last couple of years, there has been an exponential increase in investigation into this research topic. Compromised vehicular communication has received more attention than any other concern, and the popularity has only increased in recent years. A secure system design and infrastructure is the most common solution for all the identified concerns in this paper, but securing communication is the most popular one. Real-world applicability of the devised solutions is debatable, as most researchers have preferred simulations to empirical evaluation. Overall, insecure system design or infrastructure warrants more attention from solution point of view. In this context, the principles of *Prevention by Design* and *Privacy by Design* can be among the most effective strategies.**

Keywords—connected cars; communication; system design; security; privacy

I. INTRODUCTION

Connected cars adopt network technologies to enable economical and effective communication between vehicles [1]. However, security in connected cars can be compromised simply by a malicious audio file [2], and a survey findings suggests that people are wary of using car-related services fearing privacy violation [3]. There is expected to be an increase in the market size of connected cars [4], potentially resulting in a proportional rise in security and privacy concerns. Therefore, it becomes necessary to identify and propose solutions to tackle these security and privacy concerns as early as possible.

Researchers have been addressing security and privacy concerns in connected cars [5]–[8]. However, it is claimed that the focus has mainly been on problem definition and not solutions [5]. It is also argued that most solutions are not empirically validated [9]. To this effect, a mapping study to identify the security and privacy concerns in connected cars and the corresponding solutions, could elaborate on the aforesaid claims and also suggest a way forward. To the best of our knowledge, the domain of connected cars has never been subjected to a systematic mapping study with the above outlined objective. This shortcoming motivates the research questions in Table I.

Using systematic mapping study (SMS), we investigate the state of the art to aggregate security and privacy concerns identified in connected cars and the concomitant solutions. With this study, we are also interested in addressing the claims made about excess focus on problem definition [5], and lack of empirical evaluation of solutions [9]. Lastly, we also aim to identify current research focus, and propose a change in future research strategies, if warranted.

Based on the abovementioned research objectives, our paper is structured across following sections: Section II discusses related work, followed by research methodology in Section III. Section IV presents results from the SMS, with discussion in Section V. Section VI outlines limitations of this paper, followed by conclusion in Section VII.

II. RELATED WORK

Existing secondary studies have investigated the state of the art of connected cars, but with a limited coverage, and sometimes even lacking the rigor of a systematic research method. For example, Kleberger et al. [6] conducted a survey on security in connected cars, focusing on only the in-vehicle network. The authors also provided taxonomy of threats and attacks. They concluded that despite the progress made in studying security features of connected cars, several security issues still remain to be analyzed. They also claimed that most research are interested in just identifying security problems, and not much in presenting solutions for them. In our paper, we lay emphasis on both the concerns and the solutions that have been documented in the state of the art. Additionally, we also attempt to validate the aforesaid claim of focusing on just problem definition.

More recently, Parkinson et al. [10] surveyed the existing literature to identify vulnerabilities and mitigation techniques in autonomous and connected cars. The authors identified several knowledge gaps deserving of future research attention, and concluded that there is a reactive tendency to addressing cybersecurity threat detection. Despite a much broader coverage of security concerns in connected cars, the authors did not report to have adopted a systematic research approach in meeting their research objectives. In contrast, the systematic approach of our paper builds on such existing studies to identify both concerns and solutions.

Our systematic approach is also in contrast to the survey by Othmane et al. [9], which bears close resemblance to the research topic of our SMS. Their survey provided taxonomy for security and privacy issues in connected vehicles. The goal of the survey was to produce an initial repository of threats and solutions to counter those threats. However, the authors did not report

TABLE I. RESEARCH QUESTIONS

ID	Research Question	Aim
RQ1	What security and privacy concerns have been identified in connected cars?	Identify various security and privacy concerns in connected cars for further analysis
RQ2	What solutions have been proposed for the identified security and privacy concerns in connected cars?	Produce a condensed view of the trend and focus adopted by researchers while devising solutions
RQ3	What research focus can be observed from the state of the art?	Derive an overarching focus observed in the state of the art that can help inform our recommendation for future research strategies

to have followed any systematic research method to conduct the survey. In addition, in contrast to our SMS, the authors included several Vehicular Ad-hoc Network (VANET) related primary studies in the survey. VANET differs from connected cars in several ways. In VANET, every participating vehicle acts as a wireless router, facilitating communication among vehicles by creating a network [11], but these networks cannot provide a global and sustainable services to its customers [12]. Vehicles need to evolve into smart objects equipped with multi-sensor platform, better processing power, reliable IP-based connectivity to Internet, and a set of communication technologies [13]. This led to VANET evolving into Internet of Vehicles (or Connected Cars) [11]. Connected cars operate on a combination of vehicle's networking and vehicle's intelligence [12], integrating myriads of objects to create an intelligent network that can offer services for larger cities or even an entire country [11][13]. This distinction between VANET and connected cars is important, as it serves the foundation of our SMS, and distinguishes it from other similar secondary studies.

As highlighted above, most existing studies are inclined towards tackling a single security or privacy concern in connected cars. Scrutiny of the state of the art has been limited to surveys, targeting mainly a specific security concern, such as communication. There appears to be a lack of secondary studies that covers the research topic in a holistic fashion, and that is an overarching aim of our SMS.

III. METHODOLOGY

We followed systematic mapping study guidelines proposed in [14] to answer the research questions, and to classify the supporting evidence at a higher degree of granularity [15], [16]. A research protocol was developed based on [14] to guide the study and reduce the possibility of bias. The protocol specifies study objectives, research questions, search strategy, inclusion and exclusion criteria, primary study selection, and approach for data extraction.

The search process was conducted using digital libraries, viz. IEEE Xplore, ACM Digital Library, Springer Digital Library, Scopus, Elsevier, ScienceDirect, Web of Science, ProQuest, and EBSCOhost Research Databases. The search was carried out in January 2018, using the search string ("Connected Cars" OR "Internet of Things" OR IoT OR "Internet of Cars" OR "Internet of Vehicles" OR "Connected Vehicles" OR "Machine to Machine" OR "Machine 2 Machine" OR m2m) AND (Automobile OR Automotive OR Car OR Vehicle OR Transport OR Traffic) AND (Security OR Privacy in All Text). The first set of keywords needed to be in "Abstract", whereas second and the third set in "All Text". The search produced 13,373 papers, which were reduced to 11,359 after removing duplicate entries.

The papers were subjected to the inclusion criteria that it must be: available online; in English; in journal, conference; focusing on connected cars or its related keywords; and focusing on security or privacy in connected cars. Correspondingly, studies were excluded if a study was: not made available online; not in English; from grey literature (opinion papers, experience reports, patents, text books, etc.); not focusing on connected cars or its related keywords; not focusing on security or privacy in connected cars; focusing on VANET; or focusing on the topic as an indirect reference or in an interpretive capacity only.

One researcher screened all the papers from the result set. Excluding papers from 2017, two more researchers screened all the papers, which were divided between them. Reliability of our analysis was measured by piloting the inclusion-exclusion criteria over 50 random papers. We registered a Fleiss Kappa value [17] of 0.82 between the first and the third researcher, and 0.79 between the first and the fourth researcher. The second researcher acted as the mediator to resolve conflicts. A total of 93 primary studies were selected, which was supplemented by adopting backward snowballing [18]. In snowballing, additional papers are identified either from the paper's reference list (backward snowballing), or from the citations to that paper (forward snowballing). As a result, an additional six primary studies were identified from backward snowballing, increasing the final tally to 99.

The first researcher extracted the metadata, research methods, and results to answer the research questions. Some primary studies were presented at Symposiums and some at Workshops. A definitive distinction between these two could not be made. So, these studies were classified under "Conference", as they both share some characteristics of a conference. Majority of the primary studies involve concept formation, modeling, and artifacts production Developing solutions in the form of aforementioned artifacts is a characteristic of Constructive Research [19]. Constructive research involves artifact creation to solve a domain-specific problem in order to

create knowledge about how a problem can be solved in principle [19].

Extracted results were categorized based on themes constructed from security and privacy concerns reported by the primary studies. These themes were identified based on the "Line of argument" synthesis [14], where inferences are drawn about a research topic from a limited set of studies that focus on part of the issue. Each primary study was analyzed to derive key concepts related to the concerns and solutions. In order to enhance credibility of the identified themes related to security and privacy concerns, we decided to classify them under an existing security and threat taxonomy for IoT [20]. The classification is spread across six categories, viz. *Communication Threat, Identity Management, Embedded Security, Physical Threat, Storage Management, and Dynamic Binding.* Post classification of concerns and solutions, these primary studies were looked at holistically to derive a research focus.

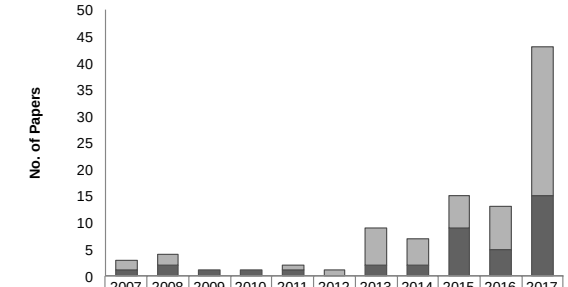
IV. RESULTS

Primary studies details such as research methods, type of solutions and their evaluations will help establish research focus partially, needed to address RQ3. Furthermore, answers to RQ1 and RQ2 will help supplement this research focus enquiry.

A. Overview of the primary studies

The list of 99 primary studies included in this SMS is available online (link). For reference convenience, these primary studies are labeled from S1 to S99.

The chart in *Fig. 1* shows the distribution of the primary studies by year of publication and source of publication. Majority of the primary studies have been published in Conferences (60) followed by Journals (39).



	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Conferences	2	2			1	1	7	5	6	8	28
Journal	1	2	1	1	1		2	2	9	5	15

Fig. 1. Primary studies across year and publication source

Based on the publication year, the earliest study was from the year 2007. Coverage of this specific topic saw an uneven, but declining, trend until 2012. Post 2012, a sharp rise can be seen, and the year of 2017 witnessed an exponential increase in the number of publications. One of the reasons for the increase in interest in connected cars could be due to the predicted rise in its market penetration [4].

Nearly 85% of the primary studies (*N = 84*) used constructive research method to investigate the research topic. Of the remaining primary studies, seven were theoretical in nature, reporting findings based on an extensive understanding of the field, or by reviewing related works. Among these, five are survey studies that review the state of the art of security and privacy concerns in connected cars. One primary study adopted a multimethodological approach, combining literature review with qualitative interviews, to enquire the research topic.

B. Results for the Research Questions

Data extracted from the primary studies, and the subsequent analysis, helped answer the research questions. The granularity and distinct scope of RQ1 and RQ2 helped build up to the research question RQ3, which reveals the focus of the topic in the research community. Results from survey papers are discussed separately, because unlike other primary studies, they do not investigate and discuss a specific security or privacy concern and solutions. These are secondary studies summarising the state of the art. Hence, results from such papers are not considered in answering RQ3.

1) RQ1: What security and privacy concerns have been identified in connected cars?

Majority of the security and privacy concerns identified pertain to security in connected cars, whereas a handful tackle privacy-specific issues. A list of these concerns is presented in Table II. The classification has been adapted from the IoT threat taxonomy presented in [20]. From the original taxonomy, security and privacy concerns identified in this study map only to *Communication Threat*, *Identity Management*, and *Embedded Security* classifications. We did not find any security or privacy concern corresponding to the classification of *Physical Threat* (direct hardware tampering), *Storage Management* (cipher key management to achieve confidentiality and integrity), and *Dynamic Binding* (naming and addressing mechanisms).

TABLE II. SECURITY AND PRIVACY CONCERNS

Threat Taxonomy	Description	Primary Studies	*N*
Communication Threat	Malicious attacks (like DoS) to compromise communication	S1-S6, S9, S12, S13, S14, S17, S18, S20, S23, S24, S25, S26, S27, S33, S35, S36, S37, S39, S40, S41, S42, S43, S45, S49, S51, S53, S55, S58 – S60, S63 – S72, S79, S80, S81-S85, S87, S88, S89, S91, S92, S94, S95	60
Identity Management	Covers authentication, authorization, accounting, and provisioning of device/user/session	S7, S8, S21, S22, S29, S32, S34, S46, S50, S52, S57, S61, S62, S73, S76, S78, S93, S96	20
Embedded Security	Covers threats at physical and MAC layer (like device/data tampering, bus monitoring, etc.)	S10, S11, S15, S16, S19, S30, S31, S44, S48, S56, S74, S86, S97, S99	14

a) Communication Threat

This classification represents malicious activities like Denial of Service (DoS) attacks, network injection, and spoofing that compromise communication [20]. In view of this threat definition, compromise in vehicular communication is the most prominent concern (N = 60) identified in the primary studies. Lack of data integrity [S4, S42, S45], insecure diagnostic sessions [S24, S27], insecure alert messaging systems [S14], and insecure firmware updates [S40, S97] have also been categorized under this threat, as these involve compromises to the communicated data.

Communication compromises have been reported to be caused by malware [S12, S35], malicious users [S2, S36, S39, S49], wireless attacks [S5, S53], and intruders [S9, S83]. However, these are instantiations of multiple overarching or fundamental causes. One of these causes is the operational nature of the connected-cars technology itself. A connected car's high mobility and lack of central authority may render the default security and privacy safeguards ineffective in most cases. Another major cause identified is the insecure system design or infrastructure. A typical connected car is composed of numerous Electronic Control Units (ECUs) [21], interconnected via heterogeneous communication network like Controller Area Network (CAN) [22], where security still remains a glaring omission from the design of CAN [S5, S33, S53]. Insecure communication protocol is the next commonly reported cause for compromises in communication, with consequences like self-propagating worm attacks [S20, S89], cyberattacks, or even privacy-related issues [S35]. Inadequate security or privacy safeguards and insecure system design are two other most reported causes.

b) Identitiy Management

Identity Management relates to undesired access to data or the network, and carries ramifications for both security and privacy of a network. Despite advanced technology supporting communication, authentication still poses a problem [S7, S8, S34], and it can expose a network to all forms of attacks [S8]. For an incident-free authentication, a secure infrastructure is mandatory [S8]. Communication established using public key infrastructure does not offer protection against certain forms of attacks [S34], while the wireless communication medium can be vulnerable to various security threats. Therefore, insecure system design or infrastructure remains a major cause for this concern.

Focusing on concerns affecting privacy, these could emerge in scenarios where private information like location [S21, S38, S46, S75], social credentials [S29], and route information are exchanged. Personal or private details are readily disclosed by the vehicle operator, or are necessary from certain operational standpoint. Inadequate or lack of privacy safeguards here, or even misuse, is how privacy is compromised in connected cars. Insecure system design or infrastructure is a major cause for this concern as well. For example, insecure communication mechanism with RSU [S21, S22], or insecure central server or an RSU [S29, S32] can compromise a vehicle's safeguard against privacy-related attacks.

c) Embedded Security

This classification covers threats across the physical and MAC layer, representing concerns like side channeling, data tampering, lack of secure environment even [20]. The primary studies document several concerns that involved compromised architecture or infrastructure in connected cars, thereby exposing a connected car to every conceivable security and privacy related attacks [S16]. A couple of primary studies investigate insecurity in system design [S44, S56], alluding to the need to address such concerns at a fundamental level. This indicates that the aforesaid concern could be the most fundamental concern. It is also reported that design of connected cars trades security and privacy for functionality [S44], where the in-vehicle network was originally meant to operate in a closed environment [S19]. The underlying insecure system design or infrastructure can be a major cause for introducing security risks in connected cars. Secondly, the constrained system of connected cars impedes its scalability and efficiency [S11, S16]. Also, sensors and sensor gateways used in exchanging sensor data over the network are constrained devices, and secure communication still remains a challenge, as a result [S15]. Other less frequently cited causes for this concern are "operational nature of connected cars", "inadequate security or privacy safeguards", and "malicious or faulty nodes".

In the survey primary studies, [S28] theorizes that insecure system design and architecture, and insecure communication protocols can be a threat to the in-vehicle network. The surveys in [S54, S64, S77] attribute the nature of connected cars and the operational characteristics like the dynamic topology, network scale, non-uniform node distribution, etc., as the causes for attacks on data integrity.

2) RQ2: What solutions have been proposed for the identified security and privacy concerns in connected cars?

Solutions analyzed for the reported security and privacy concerns in connected cars are presented in *Table III*. Multiple primary studies refer to, conceptually, similar solutions for these concerns. We report these solutions as per the threat taxonomy we adopted in reporting the security and privacy concerns.

a) Communication Threat

Trust-based framework [S1, S25, S72], communication management system [S17], certificate or encryption-based authentication [S68, S88], data integrity verification [S4], secure access control [S87, S91], and even artificial intelligence based algorithms [S65] are some of the reported solutions to secure communication. Use of "Secure communication protocol" is another prominent solution, devised using complex mathematical formulae [S23], cryptography [S40], resource-friendly protocol [S43], adaptive communication protocol [S43, S45], or hardware implementation of Advanced Encryption Standard (AES) [S55]. Securing system design or infrastructure by exhaustively describing security relationship among involved entities [S18], implementing security mechanism at the lowest network stack level [S27], modularizing security mechanisms [S37], or by validating salient communication features pre and post transmission [S41] have also been proposed .

Targeting specifically malicious attacks, "Attack or intrusion detection mechanisms" are the most discussed solution (N = 17). Counter-mechanisms involving statistics

TABLE III. SOLUTIONS FOR THE IDENTIFIED SECURITY AND PRIVACY CONCERNS

Solution	Security and Privacy Concerns		
	Communication Threat	Identity Management	Embedded Security
Secure system design or infrastructure	S18, S27, S37, S41, S51	S32, S50	S10, S11, S16, S30, S31, S56
Encryption-based authentication and authorization	S2, S3, S5, S33		S15, S19, S74
Privacy-preserving schemes		S21, S22, S29, S38, S46, S52, S61, S62, S75, S76, S78, S93, S96	
Secure communication protocols	S23, S40, S43, S45, S55, S60, S63, S67		
Data integrity verification	S4		
Attack or intrusion detection mechanisms	S6, S9, S12, S13, S36, S39, S47, S59, S65, S69, S70, S79, S81, S83, S84, S89, S92		
Trust-based mechanisms	S1, S17, S24, S25, S26, S42, S49, S58, S66, S72, S80		
Patching using cellular network	S35		
Secure access control	S87, S91		S44, S48
System-wide secure frameworks	S71, S94, S95	S86	S99
Certification or encryption-based authentication	S68, S82, S85, S88	S7, S8, S34, S57	

and pattern recognition [S6], machine learning [S9], cloud-assisted anti-malware [S12], and community-driven protocols [S36] are some of the focus points for the reported solutions. Four primary studies [S2, S3, S5, S33] propose "Encryption-based authentication and authorization" to tackle the current concern. Trust-based anomaly detection [S49], security at requirements stage [S51], and smart patching through cellular networks [S35] were other lesser-known solutions for this concern. Two primary studies [S20, S53] did not report any solution, as their aim was to demonstrate threats to connected cars caused by malicious attacks or users.

a) Identity Management

Schemes involving cluster authentication [S7], trust certification revocation scheme [S8], and mutual authentication constitute a broader solution strategy of "Certification or encryption-based authentication" for dealing with the threats to authentication.

For privacy associated concerns under the *Identity Management* threat classification, "Privacy-preserving schemes" are the most commonly reported solutions (*N = 13*). These solutions use bit-array encoding [S21], cryptography [S22, S38, S46], *k*-anonymity [S29], or pseudonym-changing scheme [S52] to ensure privacy. Solutions involving a secure system design or infrastructure [S32, S50], system-wide secure framework [S86], and even certificate of encryption-based authentication [S57] appear to be relatively less popular.

b) Embedded Security

The solution of "Secure system design or infrastructure" was the most commonly reported solution for overcoming comrpomised security architecture or infrastructure in connected cars. Solutions proposed involve leveraging safety standards like ISO 26262 [S10], RSU distributed intelligence [S11, S16], Privacy by Design [S16], Security by Design [S56], and a system-deep security model [S30]. A couple of primary studies [S15, S19] recommend low-cost, low-overhead encryption-based authentication and authorization solutions. Only [S44] and [S48] discussed "Secure access control" policies as a potential solution to this concern.

3) RQ3: What research focus can be observed from the state of the art?

Focus here characterizes specific preferences of the research community. In our SMS, we consider research methodology, type of concerns and solutions, and their evaluations to identify these preferences.

From the perspective of research methodology, "Constructive Research" has been used extensively (N = 84) to conduct these studies and develop solutions. Among security and privacy concerns, the focus is on "Communication Threat" (N = 60), followed by concerns related to authentication, authorization, and privacy under "Identity Management" threat classification (N = 20). A secure system design or infrastructure is the most common solution approach to tackle most of the identified security and privacy concerns. However, there appears to be more focus on devising concern-specific solutions. For instance, communication-specific concerns are tackled by solutions that detect malicious activities (N = 17), or by adopting a secure communication protocol (N = 8). Concerning solution evaluation approach, simulation was the most preferred choice (N = 58). Only two studies [S6, S66] relied on empirical findings to propose a solution, 17 reported no specific solution evaluation (five of them were survey results) and the rest used theoretical understandings to carry out the evaluations.

C. Discussion

We discuss our findings based on the research focus

identified in the primary studies. Answers to RQ1 and RQ2 can be found in the following two subsections, and RQ3 has been addressed by both these subsections taken together.

1) Security and privacy concerns

Communication is an integral and common element in most of the identified concerns. Compromised communication is the most frequently reported concern, caused primarily by the operational nature of the connected cars. Focusing on this specific concern, for example, Tbatou et al. [23] recommended solutions that span from securing the external interfaces (such as communication channel) to the security of processing the communicated data. The authors propose deploying safeguards at every level of the connected car network. Ten primary studies identified an insecure system design or infrastructure as the primary cause for threats to communication. Insecurities in communication protocols (CAN, FlexRay) of an in-vehicle network and wireless protocol (IEEE 802.11P) have also been reported to cause this concern. Jaballah et al. [24] report that the inherent insecurity of CAN is due to oversight on the part of industrial community in designing secure connected cars. Therefore, the cause of insecure communication protocol, especially in-vehicle communication, is a direct result of shortcomings in the system design. Inadequate security or safeguards have also been identified as one of the major causes for compromised communication in connected cars. Taken together, we argue that compromised communication has more to do with the systemic issue of insecure system design or infrastructure, and less with the nature of the connected-cars technology.

Insecure system design or infrastructure is also a major cause for the remaining concerns under *Identity Management* and *Embedded Security* threat classification. An insecure architecture or infrastructure is a direct consequence of the default insecure system design [S19], trading system security and privacy for functionality [S44], and lack of security considerations during system design development [S56]. Therefore, without addressing these fundamental issues in totality, effectiveness of protection mechanisms built on top of such an insecure system will prove counterintuitive [25]–[27]. In case of case of a compromised security architecture or infrastructure, deployment of security or privacy safeguards are further challenged by the inherent system constraints of connected cars [S11, S15, S16]. In response to tackling privacy-related concerns classified under *Identity Management*, most primary studies have drawn attention to insecurities arising from an untrustworthy RSU or CA [S22, S29, S32, S38]. An interesting conclusion drawn in [S21] means that even frequency of communication can cause privacy breaches. Existing research suggest that privacy requirements (and security requirements) are given less attention during requirements engineering of a system [28]. Another startling observation made in [29] is that most of the privacy-specific concerns are a result of defects in system design, and not a consequence of merely an intentional attack. These claims and observations favour the argument that privacy-specific concerns may actually be the consequence of an insecure system design or infrastructure.

Among all the documented concerns, "communication" has managed to draw a significant attention, especially in recent years. For instance, 33 primary studies investigated this concern between 2007 and 2016. However, in 2017 alone, 27 primary studies reported on this concern. This emphasis suggests that the security and privacy concerns related to communication in connected cars was drawing, and will continue to draw, attention of the research community for the foreseeable future.

2) Solutions

As claimed in [30], most of the proposed solutions identified in our primary studies are limited to only detecting and mitigating attacks. For instance, the concern classified under *"Communication Threat"* is tackled by developing solutions that propose trustworthy communication. Establishing trust is the central objective of these solutions. However, such solutions involve traditional computing primitives [28], [29], and are ill equipped at tackling insecurities at the system level [30]. Similarly, solutions targeting detection and protection from specific form of attacks or malicious node are limited in their scope. Such a targeted approach can address only the symptom in focus and not the inherent flawed system [27], [31]. Instead, the alternative strategy of *"Prevention by Design"* is needed, where vulnerabilities are tackled in the early stages of system design, and not as a reactive measure [30]. Only one primary study [S51] adopts this strategy, proposing a solution where security is part of the design stage. In case of the rest, trust-based schemes receive the most attention.

The principle of "*Prevention by Design"* is integral to most solutions in response to the concerns related to *architecture* or *infrastructure*. Even the principle of "*Privacy by Design"* is endorsed by [S16] as a safeguard against insecure system architecture. Interestingly, these principles are not adopted in dealing with concerns like privacy under *"Identity Management"* threat classification. Instead, proposed solutions rely heavily on cryptography and pseudonyms. Only a couple of primary studies [S32, S50] argue for the need to address the insecure system design or infrastructure to safeguard privacy. Solution involving informed consent [S50] is made more pertinent by EU's GDPR, which obligates manufacturers and service providers to adopt the principle of *data protection by design and by default* [32]. Going forward, this enforcement may translate into the much-needed prevalent adoption of *"Prevention by Design"* and *"Privacy by Design"* principles.

Among the solutions presented in the surveys [S28, S54], *'Honeypots'* is missing from our findings. This particular solution learns from actual cyberattacks, and

evolves to improve its effectiveness. Largely, the primary studies involving surveys [S77, S98] report solutions that are reactive, similar to several other primary studies discussed before.

Othmane et al. [9] claimed that most solutions in response to the concerns in connected cars are not empirically validated. Judging by the solution evaluation preference highlighted in this mapping study, the claim finds some support. Majority of the primary studies advocate for their solution's effectiveness based on simulations. Considering the mobile and dynamic nature of the connected car network, simulation may be inadequate for solution validation. Simulations may be a convenient evaluation method, but lack of empirical testing raises doubts about a solution's effectiveness and reliability in real-world operational conditions.

A lightweight solution relying on RFIDs and sensors [33], [34] is suited for connected cars, rather than solutions that rely on cryptography. Majority of the proposed solutions are lightweight in nature and use symmetric-key encryption, known for minimal computational overhead [S8]. However, this overhead can be traded for communication delay and vice versa [35]. This tradeoff is worthy of further research, to investigate for a solution that can strike the right balance between adequate protection and optimal performance.

We have presented that insecure system design or infrastructure can be associated with several security and privacy concerns identified in this study. Hence, we argue that solutions should target this fundamental issue, instead of tackling concerns and devising reactive solutions. Such a misalignment also limits the scope of the proposed solution. Security and privacy need to be considered throughout a system's development lifecycle, should be embedded in system's design by default [36], and not left as an afterthought [27]. The reactive solutions involving software-level components (firmware signing, encryption algorithms, etc.) [26], [31], [33] leave the hardware unattended, which can still be susceptible to new attack vectors [27]. Therefore, a long-term view of developing secure system architecture and infrastructure will be a more effective and sustainable approach. In order to achieve this goal, a preemptive and a proactive approach of adopting the principles of *Prevention by Design"* and *"Privacy by Design"* [25], [30], [32], [33], [37] should be a priority going forward.

V. Limitations

Our mapping study adhered to the research protocol that was systematically developed following the well-established guidelines in [14]. However, keywords used for retrieving primary studies can still present a potential limitation. Synonyms used for "connected cars" may be inadequate, as phrases such as "intelligent transport", "intelligent transportation" and "intelligent vehicle", have also been used to convey the technology of connected cars, as shown in some primary studies. This oversight may have cost us some potentially relevant studies.

Based on the guidelines [14], multiple researchers were involved in the study selection, thereby mitigating selection bias to some extent. However, our study has deviated from the said guidelines, as only one researcher was involved in study selection from 2017, and data extraction and data synthesis for the entire set of primary studies. These limitations have been kept in check by involving another researcher to validate the results from each of those steps. Additionally, involving multiple researchers for a systematic mapping study positively impacts the validity of our findings.

VI. Conclusion

Our paper presents results from a systematic mapping study on security and privacy concerns, and concomitant solutions in connected cars. Communication has been a critical topic of concern among researchers, and based on the exponential rise in such enquiries in the last one year, the focus on this concern is expected to continue. We posited that insecure system architecture or infrastructure is the primary cause for all the identified concerns, which is supported by the focus on developing secure system design or infrastructure as a solution characteristic in 13 primary studies. However, the advocated solution is still secondary to solutions that are reactive in nature. Therefore, we propose future research strategies give due consideration to the *Prevention by Design"* and *"Privacy by Design"* principles.

From academic perspective, researchers favour the methodology of constructive research to develop solutions. Supporting the existing literature claim, most of these solutions lack empirical evaluation. There is a need to realign solution evaluation approach, by emphasizing on and adopting empirical assessment of these solutions. Doing so will help in a realistic assessment of a solution's effectiveness in real-life operational conditions.

References

[1] S. H. Yu, P. P. Lindenberg, B. C. Cheng, and H. Chen, "SMILE+: An Efficient Privacy Preserving Missed-Connection Service in IoV Networks," in *Future Information Technology - II*, J. J. (Jong H. Park, Y. Pan, C. Kim, and Y. Yang, Eds. Dordrecht: Springer Netherlands, 2015, pp. 163–172.

[2] L. Reger, "Addressing the security of the connected car," 2014. [Online]. Available: http://blog.nxp.com/automotive/addressing-the-security-of-the-connected-car. [Accessed: 27-Dec-2016].

[3] McKinsey&Company, "What's driving the connected car. McKinsey Insight," 2014. .

[4] M. Lengton, D. Verzijl, and K. Dervojeda, "Internet of Things: Connected Cars. Business Innovation Observatory," 2015.

[5] K. Koscher *et al.*, "Experimental Security Analysis of a Modern Automobile," pp. 1–16, 2010.

[6] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *IEEE Intelligent Vehicles Symposium, Proceedings*, 2011, no. Iv, pp. 528–533.

[7] T. Wollinger, M. Wolf, and A. Weimerskirch, “State of the Art : Embedding Security in Vehicles,” *Eurasip J. Embed. Syst.*, vol. 2007, no. 1, pp. 1–16, 2007.

[8] M. Jenkins and S. Mahmud, “Security needs for the future intelligent vehicles,” *2006 SAE World Congr.*, no. 724, 2006.

[9] L. Ben Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, “A survey of security and privacy in connected vehicles,” in *Wireless Sensor and Mobile Ad-Hoc Networks Vehicular and Space Applications*, 2015, pp. 217–247.

[10] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, 2017.

[11] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, “Internet of Vehicles: Architecture, Protocols, and Security,” *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2017.

[12] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, “An overview of Internet of Vehicles,” *China Commun.*, vol. 11, no. 10, pp. 1–15, 2014.

[13] H. Moustafa, G. Pau, F. Bai, and Y. Zhang, “Guest Editorial,” *IEEE Internet Things J.*, vol. 1, no. 6, pp. 522–524, 2004.

[14] B. Kitchenham and S. Charters, “Guidelines for performing Systematic Literature Reviews in Software Engineering,” *Engineering*, vol. 2, p. 1051, 2007.

[15] D. Budgen, M. Turner, P. Brereton, and B. Kitchenham, “Using Mapping Studies in Software Engineering,” *Proc. PPIG, 2008*, vol. 2, pp. 195–204, 2008.

[16] B. A. Kitchenham, D. Budgen, and O. Pearl Brereton, “Using mapping studies as the basis for further research – A participant-observer case study,” *Inf. Softw. Technol.*, vol. 53, no. 6, pp. 638–651, Jun. 2011.

[17] J. Cohen, “A Coefficient of Agreement for Nominal Scales,” *Educ. Psychol. Meas.*, vol. XX, no. 1, pp. 37–46, 1960.

[18] C. Wohlin, “Guidelines for snowballing in systematic literature studies and a replication in software engineering,” in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE ’14*, 2014, pp. 1–10.

[19] G. D. Crnkovic, “Constructive research and info-computational knowledge generation,” in *Studies in Computational Intelligence*, 2010, vol. 314, pp. 359–380.

[20] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed security model and threat taxonomy for the Internet of Things (IoT),” *Commun. Comput. Inf. Sci.*, vol. 89 CCIS, pp. 420–429, 2010.

[21] R. Charette, “This car runs on code,” *IEEE Spectrum*, p. 3, 2009.

[22] T. Nolte, H. Hansson, and L. Bello, “Automotive communications-past, current and future,” in *2005 IEEE Conference on Emerging Technologies and Factory Automation*, 2005, p. 8.

[23] S. Tbatou, A. Ramrami, and Y. Tabii, “Security of communications in connected cars Modeling and safety assessment,” *Proc. 2nd Int. Conf. Big Data, Cloud Appl. - BDCA’17*, pp. 1–7, 2017.

[24] B. J. W., C. M., M. M., and P. C.E., “Impact of security threats in vehicular alert messaging systems,” in *2015 IEEE International Conference on Communication Workshop, ICCW 2015*, 2015, pp. 2627–2632.

[25] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[26] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” *Computer (Long. Beach. Calif).*, vol. 44, no. 9, pp. 51–58, 2011.

[27] O. Arias, J. Wurm, K. Hoang, and Y. Jin, “Privacy and Security in Internet of Things and Wearable Devices,” *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, 2015.

[28] S. L. Pfleeger and C. P. Pfleeger, “Harmonizing privacy with security principles and practices,” *IBM J. Res. Dev.*, vol. 53, no. 2, pp. 1–12, 2009.

[29] A. Adams and M. Angela Sasse, “Privacy in Multimedia Communications: Protecting Users, Not Just Data,” in *People and Computers XV---Interaction without Frontiers: Joint Proceedings of HCI 2001 and IHM 2001*, 2001, pp. 49–64.

[30] P. Karpati, G. Sindre, and A. L. Opdahl, “Visualizing Cyber Attacks with Misuse Case Maps,” in *International Working Conference on Requirements Engineering: Foundation for Software Quality*, 2010, pp. 262–275.

[31] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, A. Iera, and A. I. A, “A systemic and cognitive approach for IoT security,” pp. 183–188, 2014.

[32] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies (In Press),” *Comput. Law Secur. Rev.*, 2017.

[33] M. Abomhara and G. M. Køien, “Security and privacy in the Internet of Things: Current status and open issues,” in *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, 2014, pp. 1–8.

[34] L. Eschenauer and V. D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” in *Proceedings of the 9th ACM conference on Computer and Communications Security*, 2002, pp. 41–47.

[35] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *J. Comput. Secur.*, vol. 15, pp. 39–68, 2007.

[36] S. Li, T. Tryfonas, and H. Li, “The Internet of Things: a security point of view,” *Internet Res.*, vol. 26, no. 2, pp. 337–359, 2016.

[37] J. Veijalainen, D. Kozlov, and Y. Ali, “Security and Privacy Threats in IoT Architectures,” *Proc. 7th Int. Conf. Body Area Networks*, no. International Conference on Body Area Networks, pp. 256–262, 2012.