Survey on Issues and Recent Advances in Vehicular Public-Key Infrastructure (VPKI)

Salabat Khan, Fei Luo, Zijian Zhang, Mussadiq Abdul Rahim, Mubashir Ahmad, and Kaishun Wu

***Abstract*—Public-key infrastructure (PKI) provides the essential foundation for public-key cryptography, and security is often bootstrapped from a PKI. Standardization bodies, organizations, researchers, and experts reached a consensus that deploying Vehicular PKI (VPKI) can ensure the security and privacy requirements of Cooperative Intelligent Transportation Systems (C-ITS). Given the importance of VPKI, researchers and experts have worked to ensure VPKI meets the high security and privacy requirements of C-ITS. This survey focuses on VPKI schemes designed to securely and privately manage and revoke public-key certificates in three parts. The first part presents evaluation metrics that help to compare the existing VPKI proposals systematically. The second part classifies VPKI schemes and provides an overview of each. The third part focuses on observations made using the evaluation metrics through a systematic comparison of VPKI schemes. Finally, suggestions for future VPKI research are presented.**

***Index Terms*—Revocation, privacy, vehicular ad hoc networks (VANETs), vehicular public-key infrastructure (VPKI), cooperative intelligent transportation systems (C-ITS).**

I. Introduction

CONVENTIONAL transportation systems in many countries are rapidly approaching their peak limit because of a rapid increase in the use of vehicles [1], [2]. A recent study [3] found that more than a billion vehicles are in use worldwide, including commercial and passenger vehicles, with an expected 2 billion vehicles by 2035 [4]. Conventional transportation systems are inefficient and have high maintenance and up-gradation costs. Moreover, the rapid increase in the number of vehicles is correlated with an increase in road casualties and traffic congestion. There is an increasing demand for efficient, reliable, and safe transportation systems to overcome the problems faced by traditional transportation systems.

Cooperative Intelligent Transportation Systems (C-ITS) have attracted industry, researchers, operators, and investors because due to their potential to address the problems of conventional transportation systems [5]–[8]. C-ITS provides a variety of benefits over conventional transportation systems, such as improved driving experience, transportation efficiency, road-safety, support for semi-autonomous vehicles, infotainment applications, and reduction in the risk of road accidents [9]–[12]. C-ITS solutions rely on Inter-vehicle (V2V) communications, Vehicle-to-Pedestrian (V2P) communications, Vehicle-to-Sensors (V2S), and Vehicle-to-Infrastructure (V2I) communications, which are collectively referred to Vehicle-to-Everything (V2X) communications [2], [13]–[15]. The transmission of Cooperative Awareness Messages (CAMs) and Basic Safety Messages (BSMs) (containing speed, location, and hazards) among vehicles and nearby commuters are processed by safety applications to identify potential hazards and critical conditions. Cooperative information (e.g., CAMs/BSMs) sharing and processing can reduce traffic accidents by almost 80% through proactive hazard identification [16], [17]. V2X communication, however, exposes vehicles to various kinds of privacy- and security-related cyber-attacks. If BSMs/CAMs are broadcast and processed without being signed and authenticated, an intruder can easily disrupt the C-ITS, causing additional crashes and fatal casualties. Therefore, anonymous and secure Vehicular Communications (VC) is a prime desire; however, conditional linkability in case of a device compromise is also a mandatory requirement [18].

In recent years, researchers, experts, standardization bodies (e.g., Secure Vehicular Communication (SeVeCOM) [19], IEEE VPKI standards [20]), and organizations (e.g., PRESERVE [21], Car-to-Car Communication Consortium (C2C-CC) [22]) reached a consensus to employ VPKI for conditional privacy-preserving authentication and secure VC. VPKI is a complex system that comprises processes, hardware, and protocols that securely and privately manage vehicles' digital identities. These digital identities are used for authentication and secure vehicular communication. In C-ITS, devices authenticate themselves to the VPKI's Certification Authorities (CAs), and upon successful authentication, are issued digital identities (certificates). Unlike conventional PKI, devices in the VPKI have two kinds of digital identities—long-term

Manuscript received 14 April 2021; revised 23 October 2021, 29 December 2021, 14 February 2022, and 4 April 2022; accepted 21 May 2022. Date of publication 26 May 2022; date of current version 23 August 2022. This work was supported in part by the National Natural Science Foundation of China under Grant U2001207 and Grant 61872248; in part by the Natural Science Foundation of Guangdong Province under Grant 2017A030312008; in part by the Shenzhen Science and Technology Foundation under Grant ZDSYS20190902092853047 and Grant R2020A045; in part by the Project of DEGP under Grant 2019KCXTD005 and Grant 2021ZDZX1068; and in part by the Guangdong "Pearl River Talent Recruitment Program" under Grant 2019ZT08X603. *(Corresponding author: Kaishun Wu.)*

Salabat Khan, Fei Luo, and Kaishun Wu are with the College of Computer and Software Engineering, Shenzhen University, Shenzhen 518060, China (e-mail: salabatwazir@gmail.com; luofei2018@outlook.com; wu@szu.edu.cn).

Zijian Zhang is with the School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100811, China (e-mail: zhangzijian@bit.edu.cn).

Mussadiq Abdul Rahim is with the Department of Computer Science, National University of Technology, Islamabad 44000, Pakistan (e-mail: mussadiq.ar@gmail.com).

Mubashir Ahmad is with the Department of Computer Science and IT, The University of Lahore (Sargodha Campus), Sargodha 40100, Pakistan (e-mail: mubashir_bit@yahoo.com).

Digital Object Identifier 10.1109/COMST.2022.3178081

identities and anonymous short-term identities. The long-term identity is used for acquiring short-term anonymous identities, while anonymous identities are used to sign BSMs/CAMs. Each device has a single long-term identity and a pool of short-term anonymous identities, which are changed frequently to make tracing difficult [23], [24]. The following are some potential applications of VPKI.

- Device authenticity: A VC device needs to verify that the device that is receiving BSMs/CAMs is a legitimate participant of VC. To achieve this, devices attached their Public-Keys (PKs)/digital identities to CAMs/BSMs, which VPKI can ensure [25].
- Data authenticity: To prevent false information (e.g., BSMs/CAMs) propagation in VC, each device needs to attest each message digitally [26]. Devices need VPKI to ensure correct usage of PKs to verify digitally signed messages of other devices [27].
- Data integrity: Unintended modifications to BSMs/CAMs should be prevented, thwarted, or at least detected. Digital signature/message authentication codes are used for ensuring integrity, but they are ultimately reliant on VPKI to manage the PKs of the vehicles [27], [28].
- Privacy-preservation of devices and data: Privacy of devices and their generated information is a prime priority in the VC. Sending V2X messages including identifiers (such as IP address, Station ID, MAC address, etc.) enables tracking of vehicles by cyber-attackers [29]. To ensure the privacy of devices and data, various cryptographic methods such as homomorphic encryption, proxy re-encryption, and multi-party computation are used. All these anonymity techniques require participants to have PK, and VPKI is mandatory to ensure secure and correct PKs management.

For the reader's convenience, Table I lists all the main acronyms and their explanations used in this survey article.

TABLE I
ACRONYMS USED THROUGHOUT THIS ARTICLE

Acronyms	Definitions
AA	Authorization Authority
AAA	Authentication, Authorization, Accountability
BF	Bloom Filter
BK	Butterfly-Key
BSM	Basic Safety Message
CA	Certification Authority
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transportation Systems
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCM	Device Configuration Module
DoS	Denial of Service
GS	Group Signature
IoV	Internet of Vehicles
IVC	Inter-vehicle Communication
LOP	Location Obsecurer Proxy
LTCA	Long-Term CA
LT-certificate	Long-Term Certificate
MA	Misbehavior Authority
OBU	Onboard Unit
OCSP	Online Certificate Status Protocol
PCA	Pseudonym CA
P-certificate	Pseudonym Certificate
PGP	Pretty Good Privacy
PK	Public-Key
PKC	Public-Key Cryptography
PKI	Public-Key Infrastructure
RA	Revocation Authority
RCA	Root CA
RGA	Registration Authority
RSU	Roadside Unit
SDSI	Simple Distributed Security Infrastructure
SK	Secret-Key
SPoF	Single-Point-of-Failure
SPKI	Simple PKI
TA	Trusted Authority
VANETs	Vehicular Ad Hoc Networks
VC	Vehicular Communication
VPKI	Vehicular PKI
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
ZK	Zero-Knowledge

II. RELATED SURVEYS

Despite a large body of work on VC authentications, privacy, and security, there is so far no complete, concrete, and comprehensive survey on VPKI architecture, recent advances in VPKI, and existing open challenges in the VPKI. Hartenstein and Laberteaux [30] presented a list of VC applications, topologies, architectures, protocols, physical channel features, and requirements. They also shed light on the main challenges hindering VC implementation. Willke *et al.* [31] categorized Inter-vehicle communication (IVC), essentially the same application as V2V, into four different classes: General Information Services, Individual Motion Control Services, Safety Information Services, and Group Motion Control Services. Classifications were based on the performance and requirements of VC. Karagiannis *et al.* [32] added to existing survey articles by identifying the basic features, use cases, protocols, specifications, and challenges of Vehicular Ad-hoc Networks (VANETs). They also identified the latest standards, architectures, and ongoing ITS projects and research in 2011 in the USA, Japan, and Europe.

Riley *et al.* [33] discussed VC authentication protocols (group-based and non-group-based protocols) based on symmetric and Public-Key Cryptography (PKC). However, their survey did not cover the security and privacy of VPKI architecture from a VPKI perspective. Zeadally *et al.* [34] filled the routing and security literature gap by presenting a thorough and complete survey on research in the area of vehicular routing, quality of service, broadcasting, and security. They discussed several state-of-the-art VC simulators (e.g., SUMO, VanetMobiSim, and MOVE). Eze *et al.* [35] rendered an overview on the current VC research state, VANETs applications, existing challenges, as well as strategies to implement C-ITS in practice. Whaiduzzaman *et al.* [36] examined the integration of cloud computing with VANETs, vehicular cloud computing feasibility, and its cost-effectiveness when compared to traditional cloud computing. They also investigated privacy- and security-concerns that VANETs and cloud-computing integration can cause. Engoulou *et al.* [37] probed exiting VC architectures, the trade-off between security and privacy, threats, and solutions. Mejri *et al.* [26] explored and investigated various recommended cryptographic strategies and evaluated their efficiency. Gerla *et al.* [38] explored protocols for content dissemination in vehicular

communication. Qu *et al.* [39] classified authentication protocols and compared their trade-offs between privacy and security. Mokhtar and Azab [40] categorized cyber-attacks per network layer in VANETs and provided recommendations for thwarting future cyber-attacks.

Petit *et al.* [41] discussed and compared pseudonym authentication protocols based on PK, identity-based, symmetric-key, and group-signature cryptography. They discussed state-of-the-art standards and identified open VC research challenges. Lu and Li [42] investigated privacy-preserving vehicular nodes and message authentication schemes. They classified these based on each approach's methodology and cryptographic scheme along with potential challenges. Azees *et al.* [43] examined cyber-attacks on security-services (e.g., confidentiality and authentication) and mitigation solutions to thwart them. Bernardini *et al.* [44] summarized cyber-security requirements of advanced cars and classified cyber-threats along with existing countermeasures based on the underlying employed technologies. Khan *et al.* [45] evaluated vehicular PK revocation schemes (e.g., CRL) and classified schemes based on revocation and dissemination mode. Sakiz and Sen [46] conducted a comprehensive overview of existing intrusion/misconduct detection schemes used in VANETs and the Internet of Vehicles (IoV).

Manavi and Tangade [47] proposed a taxonomy of VC authentication schemes along with their pros and cons. Hasrouny *et al.* [48] outlined a classification scheme for VC cyber-attacks with an emphasis on the technical challenges of VC privacy and security. Ferrag *et al.* [23] conducted a detailed survey of privacy-preserving models (e.g., identity privacy, traceability, and location privacy) for mobile and vehicular social networks. Weil [49] discussed the efforts on standardization and the road to SCMS [16], [50]. Asuquo *et al.* [51] cataloged privacy and security requirements, specifications, cyber-attacks, and threat models along with performance evaluation metrics in the location-based services for investigating privacy in VC. MacHardy *et al.* [52] shed light on V2X access technologies. Boualouache *et al.* [24] investigated and compared the pros and cons of Pseudonym Certificate (P-certificate) changing strategies. van der Heijden *et al.* [53] reviewed misbehavior detection algorithms. Lu *et al.* [54] surveyed trust management models, simulators, pseudonym-based authentication, and location privacy strategies.

Manivannan *et al.* [55] reviewed VC authentication proposals of the last decade in their survey article. Masood *et al.* [56] investigated vehicular cloud computing security and privacy issues. Wang *et al.* [57] presented a systematic taxonomy of revocation schemes based on revocation information placement strategies. Malhi *et al.* [58] conducted a multi-disciplinary survey by overviewing various aspects of VC such as security challenges and related requirements, cyber-attacks on VC, and cryptographic mechanisms to ensure security, including highlights on trust models and intrusion detection systems.

From the above discussion and Table II, it is clear that few survey articles either partially reviewed revocation proposals [45], [57] or discussed the VPKI standardization process [48], [49]. The review works carried out in [45], [57] examined revocation proposals without reviewing VPKI proposals. Similarly, survey articles [48], [49] briefly shed light on the VPKI standardization journey without comprehensively covering the state-of-the-art proposals and open research issues. Table II summarizes the existing survey articles and justifies how these survey articles differ from our survey article. No surveys in the literature, however, have presented a comprehensive overview of articles addressing VPKI proposals, architectural and design problems inherited from Internet PKI, the gap left in VPKI schemes, and the recent advanced security features, which are achieved by PKI schemes outside the VC realm. To our knowledge, this effort represents the first survey covering VPKI proposals in detail.

A. Contribution of This Survey

The main contributions of this article are as follows:

- We survey the state-of-the-art VPKI proposals by starting with a comprehensive discussion on the generic VPKI architecture, the VPKI architecture adopted in Europe, and the VPKI architecture adopted in the U.S.
- We present evaluation metrics regarding the trust, security, privacy, availability, and performance parameters to evaluate and compare VPKI schemes. In addition, a set of evaluation metrics are presented to assess and inspect revocation schemes.
- We provide a taxonomy of VPKI proposals based on the credentials management mechanism used by them as well as the classification of revocation proposals based on the data structure and revocation information dissemination method used by them. We also shed light on the strengths and weaknesses of each scheme.
- A detailed and systematic comparison is made among VPKI proposals as well as among revocation proposals using the presented evaluation metrics. Finally, we discuss lessons learned and future challenges in terms of trust, security, revocation, and performance.

III. Background and Overview of VPKI

We first provide a brief history of PKI, its evolution, and the first large-scale deployment. We then discuss a generic VPKI framework, the US and European standard VPKI frameworks, and basic terminologies used in a VPKI system. We further present evaluation metrics for VPKI schemes and proposals complementing the revocation process of VPKI.

A. Evolution of PKI

The initial proposal of networking (Internet) contains no mechanism for binding a meaningless digital identity (e.g., public-key) to a meaningful real-identity (person, organization, devices). Initial digital identities (MAC and IP addresses) can at best authenticate a device, not the person using it. Both kinds of addresses are poorly suited to authenticate a person, organization, or device because IP addresses can change over time, and MAC addresses can be manually modified. Entity (e.g., device, domain server, and Web server) names can be registered by anyone, even without the person offering proof of ownership. Today, it is unimaginable to use these traditional

TABLE II
COMPARISON OF RELATED SURVEYS PAPERS CONTRIBUTION

Survey Paper	Year	Domain	Security Challenges	Privacy Challenges	Attacks	Trust Model	Revocation	Specialized on VPKI	VPKI Challenges
Hartenstein et al. [30]	2008	VANETs applications and architectures.	✓	✓	✗	✗	✗	✗	✗
Karagiannis et al. [32]	2011	VANETs architectures, standards, and projects.	✓	✓	✓	✓	✗	✗	✗
Riley et al. [33]	2011	VANETs authentication schemes.	✓	✓	✓	✓	✗	✗	✗
Zeadally et al. [34]	2012	VANETs routing protocols, quality of service, and security.	✓	✓	✓	✗	✗	✗	✗
Eze et al. [35]	2014	VANETs applications and security challenges.	✓	✓	✗	✗	✗	✗	✗
Wahiduzzaman et al. [36]	2014	Vehicular cloud computing.	✓	✓	✗	✗	✗	✗	✗
Engoulou et al. [37]	2014	VANETs security.	✓	✓	✓	✗	✗	✗	✗
Mejri et al. [26]	2014	VANETs security and cryptographic solutions.	✓	✓	✓	✗	✗	✗	✗
Gerla et al. [38]	2014	VANETs content distribution.	✓	✓	✗	✗	✗	✗	✗
Qu et al. [39]	2015	VANETs security and privacy.	✓	✓	✓	✗	✗	✗	✗
Mokhtar and Azab [40]	2015	VANETs security.	✓	✓	✓	✗	✗	✗	✗
Petit et al. [41]	2015	Pseudonym schemes in vehicular networks.	✓	✓	✓	✗	✗	✗	✗
Lu and Li [42]	2016	VANETs privacy-preserving authentication schemes.	✓	✓	✓	✗	✗	✗	✗
Azees et al. [43]	2016	VANETs security services.	✓	✓	✓	✗	✗	✗	✗
Bernardini et al. [44]	2017	VC security and privacy.	✓	✓	✓	✗	✗	✗	✗
Khan et al. [45]	2017	VANETs revocation.	✓	✓	✗	✗	✓	✗	✗
Sakiz and Sen [46]	2017	C-ITS attacks and detection mechanisms.	✓	✓	✓	✗	✗	✗	✗
Manavi and Tangade [47]	2017	VANETs authentication schemes.	✓	✓	✓	✗	✗	✗	✗
Hasrouny et al. [48]	2017	VANETs security.	✓	✓	✓	✗	✗	✗	✗
Ferrag et al. [23]	2017	Vehicular social networks privacy.	✓	✓	✓	✗	✗	✗	✗
Asuquo et al. [51]	2018	Location privacy in VANETs and mobile networks.	✓	✓	✓	✗	✗	✗	✗
Zachary et al. [52]	2018	V2X access technolgies.	✓	✓	✗	✗	✗	✗	✗
Boualouache et al. [24]	2018	VANETs pseudonym changing strategies.	✓	✓	✓	✗	✗	✗	✗
Heijden et al. [53]	2018	C-ITS misbehavior detection mechanisms.	✓	✓	✓	✓	✗	✗	✗
Lu et al. [54]	2019	VANETs security, trust, and privacy.	✓	✓	✓	✓	✗	✗	✗
Manivannan et al. [55]	2020	VANETs privacy-preserving authentication schemes of last decade.	✓	✓	✗	✗	✗	✗	✗
Masood et al. [56]	2020	Vehicular cloud computing security.	✓	✓	✓	✓	✗	✗	✗
Wang et al. [57]	2020	Revocation in vehicular networks.	✓	✓	✗	✗	✓	✗	✗
Malhi et al. [58]	2020	VANETs security.	✓	✓	✓	✗	✗	✗	✗
Our work	2021	C-ITS public-key management systems.	✓	✓	✓	✓	✓	✓	✓

addresses for authentication and to consider everyone legitimate that on the Internet are whom they claim to be, based on these addresses, such as banks, service providers and their users, and health services.

An infrastructure known as Public-key Infrastructure (PKI) or key management infrastructure appears to be best suited to fulfilling the identity management requirement of open and online communication securely. It provides a vital foundation for applications of public-key cryptography and essential security in open communication networks. The increasing online communication and increasing security requirements have resulted in the deployment of PKI in various communication systems.

Among various deployments, PKI was first introduced in 1988 for use with Internet communications, and since that time, the deployment of PKI on the Internet has been dominated by the X.509 standard [59], commonly known as PKIX. Several other standards, such as Pretty Good Privacy (PGP), Simple Distributed Security Infrastructure (SDSI), and the Simple PKI (SPKI), are also based on certificate-based authentication. The SDSI [60] was started in 1994 to correct some of the perceived issues and complexity of PKIX [61]. In particular, it aimed to build a PKI framework that would not rely on a unique hierarchical naming network but would instead operate on a local naming system. The SPKI [62] project was initiated at about the same time, with aims similar to the SDSI [61]. Later, SDSI and SPKI specifications were merged into the PKIX standard.

PGP [63] was designed by Phillip Zimmerman that is used to sign and encrypt digital files and e-mail. Unlike PKIX, it uses a "Web of Trust" trust model to bind identities to keys. The Web of Trust replaces the PKIX concept of identity binding via a CA with identity binding via many semitrusted paths. In PGP, each user maintains a directory of matching PKs and identities, each of which is granted double trust ratings. The first ratings imply how trusted the binding is between PK and the bound identity, and the second rating implies how trusted a particular binding is to certify and introduce new bindings. When a given binding is in a directory is signed by enough trusted bindings, that binding is considered as a trusted binding. Although PGP is still being used in many applications, it falls short when applied to applications that require strong security and authentication. PKIX is a large and complicated infrastructure consisting of processes, policies, trusted servers, entities, and service providers responsible for secure identity management.

All the processes, entities, and policies play essential roles in managing identities securely, but CAs are primary trust servers, and the integrity and security of the entire system rely on their trustworthiness. The fundamental operations in any generic PKI are certification and validation. Fig. 1 portrays a generic PKIX and its two fundamental operations. During

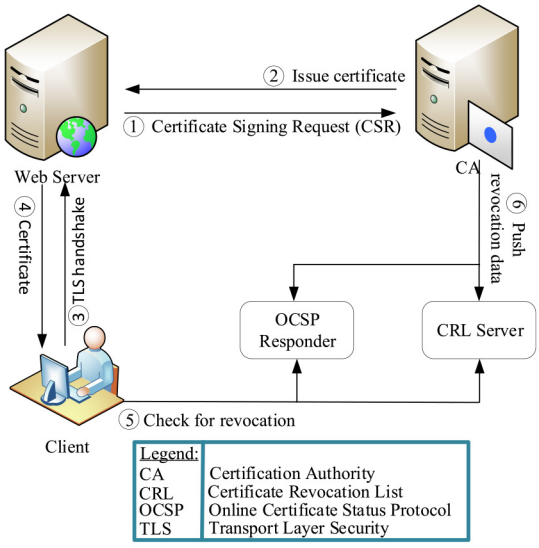

Fig. 1. A high-level overview of a generic PKIX architecture.

the certification step, each server sends a Certificate Signing Request (CSR) to a trusted CA, which then issues a signed certificate upon successful identity verification, as illustrated in step 1 and step 2 of Fig. 1. When a client initiates a connection to the server, the server presents a CA-signed certificate to the client during communication. The client checks the certificate's validity by verifying that it is signed by a trusted CA and not yet revoked by checking its revocation status, as shown in step 3 to step 5 of Fig. 1. CA periodically sends updated revocation data to the CRL server and OCSP responder to prevent revoked certificate usage, as shown in step 6 of Fig. 1.

In PKIX design, CAs are trusted third-parties who receive digital identity certification requests from their clients. They then certify their clients' digital identities by cryptographically signing digital certificates for them after verifying the real-identities of their clients. These digital certificates are electronic identities that bind physical identities to cryptographic keys, which can be further used for secure communications among parties by validating digital identities, which is referred to as the authentication process. Major protocols and systems that require firm protection and authentication leverage PKIX to protect their connections. Even the security of widely adopted and used suits of Internet security protocols is Transport Layer Security (TLS), which also relies on PKIX to secure communication on the Internet.

Although PKIX is the most widely deployed PKI used to secure communication, it faces several challenges when applied to VC as the two application scenarios have a quite different set of requirements in terms of privacy, authentication, delay, revocation, performance, and malicious credential detection. Obscuring real-identities and locations of vehicles is a priority for VC, while PKIX was not designed with privacy as a primary objective. Authentication has two fundamental differences in terms of privacy, as well as authentication rate and mode between the application communication scenarios. In VC, each device needs to authenticate a large number of signed safety messages broadcast by anonymous devices within a strict time limit (e.g., 100 ms $\sim$ 300 ms); otherwise, they become useless. In contrast, each device needs to validate signed messages received from a known server in a client-server and unicast fashion without a strict time limit in Web-based communication. Revocation methods used in PKIX, such as CRL and OCSP fall short in terms of delay and performance when applied to VC because of dynamic network topology and strict real-time requirements. In comparison to PKIX architecture, VPKI malicious credential detection is highly challenging as it needs a significantly larger amount of credential provision (e.g., each device needs $1000 \sim 2000$ P-certificates per year in the VPKI model as compared to one or few certificate(s) per domain in the Internet PKI model) [64]. Also, the complex and anonymous credential provision makes it difficult to detect fake credential issuance and instead requires the development of new malicious credential detection methods. This resulted in efforts to develop a new standard VPKI framework that can meet the VC requirements.

B. Overview of a Generic Vehicular PKI (VPKI)

Zarki *et al.* [65] proposed the first framework that relies on digital signature and PKI for authentication and key management, respectively. The SeVeCOM project [19] initiated security frameworks design for V2X development through extensive security, performance, and privacy requirement analysis. SeVeCOM designed a set of security- and privacy-related principles and requirements for security architecture. SeVeCOM uses the PKIX design where CAs are central trust anchors and uses a hierarchical trust model. However, it suggests privacy by design through the separation of privileges and roles while recognizing that traditional CRL falls short when used for VC.

Fig. 2 shows a generic VPKI architecture for securing VC, which was designed by Bissmeyer *et al.* [66] in the context of the C2C-CC project. Bissmeyer *et al.* [66] discussed and defined roles and specifications for a generic VPKI. As in any generic PKI, a VPKI also includes two fundamental operations: certification and validation. However, certification and validation are carried out at two levels: real-identity and pseudo-identity. Real-identities of devices are certified by Long-Term CA (LTCA) by issuing Long-Term certificates (LT-certificate) upon successful real-identity validation, as shown in step 1 and step 2 of Fig. 2. The LT-certificate is then used by the device to acquire a pool of P-certificates. Similarly, P-certificates are issued by Pseudonym CA (PCA) to devices with a valid LT-certificate. The device after obtaining LT-certificate sends a P-certificates signing request to the home PCA, as shown in step 3 of Fig. 2. This P-certificate request includes the device identity of the LT-certificate, the set of PKs, the current position, and LTCA information. The PCA checks its authority of P-certificate issuance for the requested region. If another PCA is designated for the region, then the signing request is relayed to the designated PCA. The appropriate PCA forwards the request with the encrypted identity of the device, preloading time, and the region to LTCA for verification in step 4.

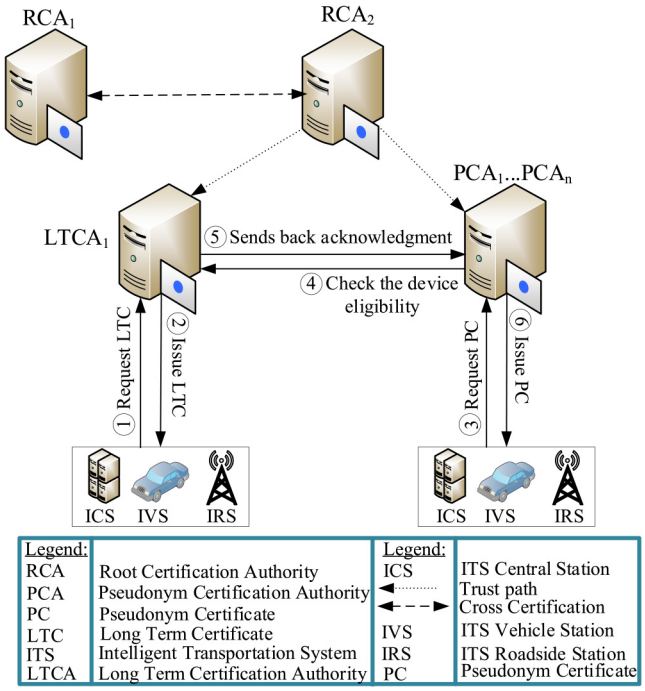

Fig. 2. A generic VPKI architecture source [66].

The LTCA examines the device's eligibility by validating that the LT-certificate is not deactivated and that no P-certificates are issued for the given region. Subsequently, the LTCA replies to the PCA with an acknowledgment and a start timestamp for fresh P-certificates upon successful validation of the device in step 5. The PCA generates a signed set of P-certificates and generates a digest of the P-certificates. The set of P-certificates is relayed to the device in step 6. P-certificates are used in privacy-preserving and secure vehicular communication. P-certificate is validated by checking that a trusted PCA has attested it and the P-certificate is not expired. Although Bissmeyer *et al.* [66] work was the first that introduced privacy by design, yet, P-certificate resolution and revocation are not addressed by this work [67].

The US and Europe designed their security frameworks based on SeVeCOM and [66] specifications–SCMS [16], [50] and ETSI ITS [68] VPKI, which are approved in the US and Europe for deployment, respectively. Next, we shed light on the two flavors of VPKI architectures.

C. U.S. Standard for VPKI

SCMS [16], [50] is a recent VPKI framework whose preliminary prototype has been implemented, tested, and deployed by the US Safety Pilot Model Project [69]; it is expected to be leveraged by the US for connected vehicle projects [70]. Fig. 3 portrays a high-level overview of SCMS, which comprises: 1) SCMS manager, 2) root CA, 3) intermediate CA, 4) PCA, 5) Device Configuration Module (DCM), 6) anonymizer (e.g., Regional Authority (RGA) and Location Obscurer Proxy (LOP)), 7) two linkage authorities, 8) Misbehavior Authority (MA), and 9) devices (e.g., vehicles with Onboard unit (OBU) and infrastructure-based Roadside Units(RSUs)). The lifecycle of a device in SCMS comprises four phases: 1) bootstrapping, 2) credential provisioning, 3) misbehavior reporting, and 4) misbehavior detection, resolution, and revocation. Bootstrapping includes initialization and enrollment, and the lifecycle of a device starts with this step. During initialization, a device obtains all authorities' certificates it requires to enable the device to receive trusted messages. In the enrollment step, each device is assigned an LT-certificate (enrollment certificate) by LTCA (Enrollment CA) upon meeting the SCMS requirements (e.g., performance requirements) and certificate type confirmation. As shown in step 1 to step 5 of Fig. 3, the bootstrapping process involves a device, the DCM, the LTCA, and the certification services.

After enrollment, the device enters the P-certificate provision phase, where the device generates a P-certificates acquisition request by creating butterfly-key seeds using the butterfly-key expansion procedure, signing the request with its LT-certificate, stapling the LT-certificate, and encrypting the request with the PK of RGA. The RGA forwards an acknowledgment to the device and expands the seed by performing butterfly-key expansion after successful validation of the device status. The RGA sends one request per P-certificate along with pre-linkage values to PCA after shuffling with requests from different devices. The PCA generates linkage value from pre-linkage values, inserts it in the to-be-signed P-certificate, and signs the P-certificate. It encrypts the P-certificate along with the private-key reconstruction value using the response encryption PK. After encryption, the PCA signs the encrypted package and sends it back to the RGA. The RGA provides a set of packages for download to the device. P-certificate provision is the trickiest mechanism in which the butterfly-key expansion method and the design ensure the efficiency and privacy of subjects. The process includes a device, RGA, PCA, and two linkage authorities, which is carried out in step 6 to step 10 of Fig. 3.

In SCMS, vehicles have identification certificates beyond the LT-certificate and a pool of P-certificates. Similarly, RSUs have application certificates beyond the LT-certificate. It is important to mention that identification certificates are reserved for V2I communication if needed in the future, while the application certificate is used to sign any over-the-air messages. The removal of misbehaving or compromised devices is carried out in the last phase of a device's lifecycle, which includes reporting, detecting, investigating, and consequently revoking the device if found to be untrustworthy. The revocation process is executed in the reverse order of P-certificate provision. The reporting entity forwards the P-certificate belonging to the offending device to the MA. The MA fetches the hash value of the P-certificate based on linkage values in step 11. The MA forwards the hash value to RGA so that the device's LT-certificate can be added to the blacklist of revoked devices in step 12. The MA also fetches the linkage seed from the two linkage authorities and adds the linkage seeds along with their identities on the CRL to revoke the device's P-certificates in step 13 to step 15.

The design and butterfly-key expansion method ensure that PCA cannot link the set of P-certificates issued for a device.

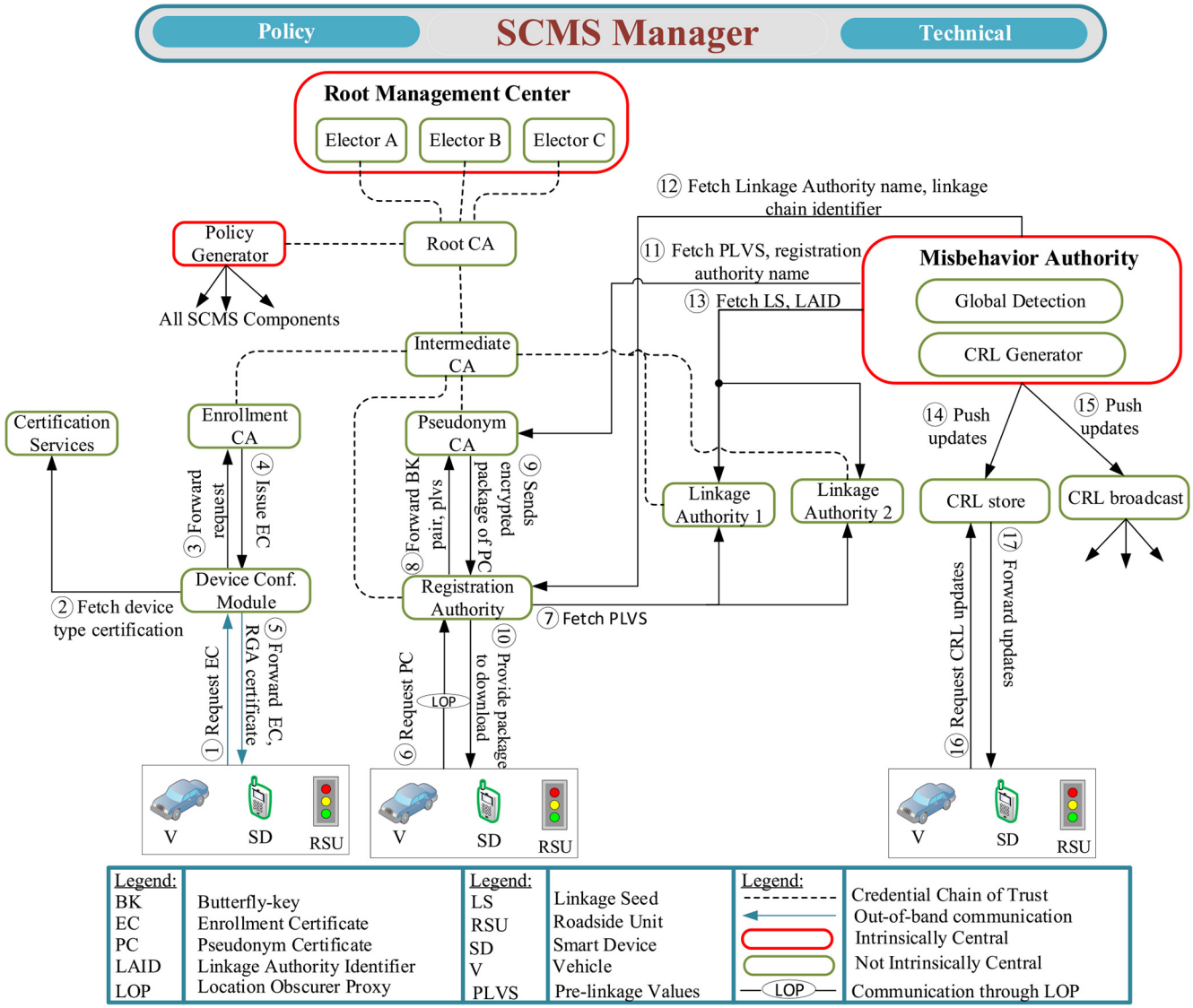

Fig. 3. Overview of SCMS source [50].

In contrast to SeVeCOM recommendations, SCMS relies on CRL but eases CRL issues by introducing a novel linkage-values mechanism per set of P-certificates. However, SCMS revocation faces some new problems. For example, a false misbehavior report may be submitted by a device through LOP, which makes it difficult to identify who submitted the bogus report. Thus, a corrupted device can slow the system by reporting many false misbehavior reports and can cause incorrect device revocation.

D. European Standard for VPKI

ETSI ITS [68] specifies a VPKI architecture for securing C-ITS communications. As shown in Fig. 4, ETSI VPKI architecture is relatively simpler and designed to have low overhead and high scalability while ensuring device privacy. The ETSI VPKI architecture comprises: root CA, Enrollment Authority (EA), Authorization Authority (AA), and C-ITS stations (e.g., vehicles, RSUs, IoT devices). Issuance and revocation of credentials occur at two levels—authority and device. The root CA is authorized to issue certificates to EA (LTCA) and AA (PCA) and revoke them by placing their certificates on CRL.

A C-ITS device (referred to as a C-ITS-station in the European standard) lifecycle starts in the manufacturing stage by generating a canonical identity, a canonical key-pair, a generic profile, and an optional self-signed bootstrap certificate. After the initialization step, the device enters the credential issuance phase, which begins with the enrollment step. In the enrollment step, a device having valid canonical credential contacts LTCA (EA) to obtain a set of LT-certificates (Enrollment Certificate (EC)) as shown in step 2 and step 3 of Fig. 4. The LTCA grants a set of LT-certificates to the device. LT-certificates are used only for entity identification in the system and not for signing safety messages. It is important to note that the LT-certificates are made unlinkable to the canonical identity by inserting pseudo-identities in them during issuance. After successful enrollment, a device (C-ITS station) contacts PCA (AA) for P-certificates (Authorization Token (AT)) issuance. The device is authorized and privileges are granted to use specific services by PCA through issuing

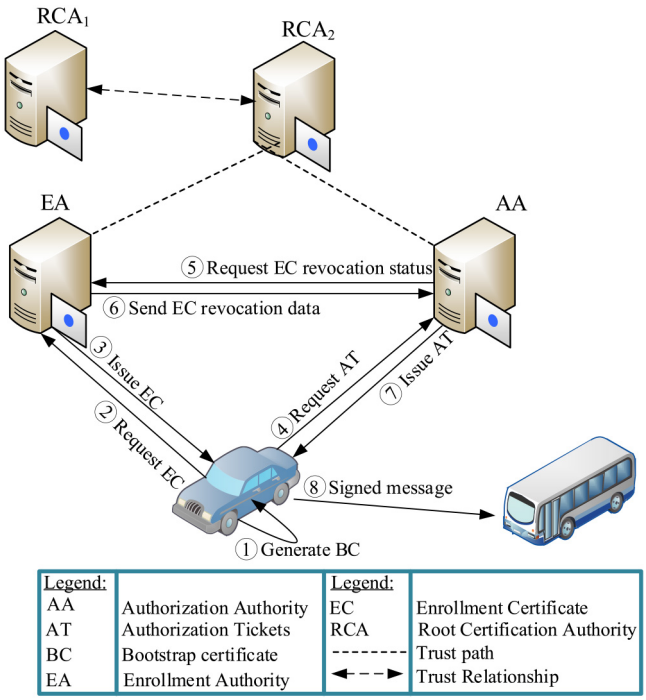

Fig. 4. A high-level overview of European standard VPKI architecture source [68].

P-certificates after successful verification of its LT-certificate. The process of P-certificates acquisition is displayed in step 4 to step 7 of Fig. 4.

As shown in Fig. 4, each device has three types of certificates: bootstrap certificate, LT-certificate, and P-certificates. Communication between devices and authorities is encrypted using authorities' keys. A device lifecycle comes to an end when they are evicted from the framework by denying P-certificates' renewal in case of unusual behaviors by the device. The European standard for P-certificate revocation does not rely on CRL. Instead, LTCA adds corrupted vehicles to the blacklist whenever it gets a revocation request from revocation authorities. When a revoked vehicle requests fresh P-certificates, the LTCA rejects the request by denying the issuance of fresh P-certificates. Although European standard has eliminated CRL successfully, a corrupted PCA can still issue P-certificates to revoked vehicles even without any detection.

E. Basic Terminology

This subsection defines some basic VPKI terminologies used in VPKI frameworks.

1) Digital Certificate: The certificate is an electronic identity document $cert(ID_e, pk_e, \sigma)$ that binds the identity ID_e of an entity e with its public-key PK_e with the help of a digital signature σ from the certificate-issuing party. It is the basic building block of all types of PKIs, which acts as a shell that enables devices to use, communicate with, exchange, authenticate, and store PKs. In VPKI, certificates are generally categorized into two types:

A) Long-Term Certificate (LT-certificate): LTCA issues this class of certificates after successful identity verification. It has an extended period of validity, which is referred to as a Long-Term Certificate (LT-certificate) throughout this article.

B) Pseudonym Certificate (P-certificate): PCA issues this class of anonymous certificates to devices having valid LT-certificates. It has a brief period of validity, which is referred to as a Pseudonym Certificate (P-certificate) throughout this article.

2) Trust Model: Baseline VPKI inherits the PKIX trust model, where CAs are responsible and issuing authorities for certifying digital identities of devices. Standard VPKI adopted the hierarchical CA trust model to create trust relationships among root CAs to their sub-ordinate CAs, enabling users to maintain a small subset of root CAs instead of storing all sub-ordinate CAs certificates.

3) Truststore: Truststore saves certificates of trusted root CAs used to verify a device certificate presented during secure communication. During initialization, it is provided to devices and usually needs software updates for the operating system installed trusted certificates or CRL distribution for PKI installed trusted certificates to add/revoke a certificate saved in the truststore.

4) Keystore: Keystore saves the credential(s) of a device presented to other parties to prove ownership of PK(s) presented during secure communication. It maintains the credential(s) acquired from a trusted CA and is locally updated when either the certificate(s) expires or private-key(s) is leaked.

5) Certificate Chaining/Chain of Trust: Certificate chaining/chain of trust is defined as "certification path" [71] starts with end-entity certificate followed by subsequent one or more subordinate CAs (e.g., Intermediate CA and PCA) certificates. More concretely, it refers to a device's certificate and how it can be linked back to the trusted root CA certificate saved in the truststore. The device's certificate must be traceable to the root of trust it was signed off and ensure that all certificates in the pathldevice, subordinate CA (e.g., PCA), and root CA are valid and properly trusted.

6) Certificate Revocation: Revocation invalidates a certificate acquired maliciously, or its secret-key is leaked from a device before expiration. Revocation is essential in VC and an integral part of any generic VPKI framework.

7) Butterfly-Key Expansion: The P-certificate provision process in SCMS [16], [50] offers an efficient and cost-effective mechanism for devices to acquire arbitrarily large numbers of P-certificate batches with a small-size P-certificate acquisition request message. Each device generates two pairs of caterpillar public-keys/private-keys, (s, S = G.s) and (e, E = e.G.), where S, s are public/private parts of caterpillar signature keys, E, e are public/private parts of cocoon encryption keys, and G is the generator of an elliptic curve group. The device sends the public parts S and E of caterpillar keys to RGA along with two pseudo-random functions, say, f_1 and f_2. The RGA expands S and E to generate β cocoon signature $(S_i = S + f_1(i))$ and encryption $(E_i = E + f_2(i))$ keys by applying f_1 and f_2 on S and E, respectively. Cocoon keys (S_i, E_i) from different devices are shuffled before sending an individual P-certificate acquisition request to the PCA. The PCA generates either an explicit or implicit P-certificate, digitally signs it, encrypts it with E_i, and sends it back to the

RGA. The device validates P-certificates after downloading the packages provided by the RGA.

8) Conditional Linkability: For revocation, VPKI's authorities should be able to trace a device in case the device abuses system's resources or arises a critical situation (i.e., car accidents). If any condition meets, then the resolution of P-certificates of the device becomes necessary to handle the condition properly.

F. Evaluation Metrics for VPKI

We survey the literature on VPKI to list the desired evaluation metrics to evaluate VPKI schemes systematically. We also identify some advanced security features achieved outside the VC realm (e.g., PKIX) or strongly recommended to ensure stout security (i.e., security against a powerful adversary capable of compromising trusted servers, such as LTCA and PCA). The evaluation metrics will help researchers to use them to compare their proposed VPKI solutions to existing VPKI solutions and identify the issues inherited from PKIX and gaps left in VPKI architecture that further need extensive research to fill the gaps.

Trust:

- Limited trust model is the property that no party is entirely trusted for credential issuance and revocation. For example, CA (i.e., LTCA, PCA) and Revocation Authority (RA) (e.g., Misbehavior Authority (MA) in SCMS) are fully trusted for certificate-issuance and cancellation, respectively, in the currently adopted CA model of VPKI architecture.
- Trust flexibility enables clients to decide and select their own root of trust for credential issuance and freely and frequently revisit their trust decision. This property ensures independence of trust.
- Credential issuance transparency is a property that enables clients to audit and verify the operations and behavior of credential issuing parties they are placing trust in.
- Revocation transparency is a property that enables clients to audit and validate the credential revocation process of RA they are placing trust. It ensures that if an RA revoked a credential, all relevant parties should be able to validate the revocation within a predefined and bounded time.
- Trust delegation transparency is a feature that enables clients to know and audit the delegation of trust by a root CA they are placing trust. It prevents root CA from delegating trust to an unknown entity without exposing it to public scrutiny.

Security:

- Malicious credential detection allows monitoring parties to detect malicious-issuance of credentials by CAs (i.e., LTCA, PCA). It is a weaker level of security but still ensures reporting the malicious incidents. It would allow monitoring parties to take countermeasures to ensure the system's security and maintain good reputations in public.
- Malicious credential prevention ensures that only a single issuing authority attested credentials are not enough to be accepted by devices without being witnessed or attested by another party. It is a stronger level of security and is important in safety-related applications such as VC, where terrorists can take down issuing authority to cause life-threatening incidents [72].
- Formal security analysis examines that a given security system is provable secure and formally verified. Security system always has loopholes and formal verification is the only way to detect and fix them systematically.
- Denial of Service (DoS) attacks mitigation ensures verification services in the face of attackers trying to block verification services. This kind of defense is vital against adversaries who want to stop the system from providing credential verification and validation.
- Truststore protection is the property that can defend clients even if the manufacturers, intruders, and administrators try to install private and malicious trusted root CA in the truststore of a device. It is an important feature, especially for safety-related systems where private CA can cause disaster and steal important information.
- Keytstore protection is a property that can defend devices even if attackers physically control them and try to use the credentials saved in the devices' keystore maliciously. It is an essential characteristic in VC, where attackers can physically control vehicles and use the credentials stored in their keystore.

Privacy:

- Device privacy says that a malicious entity should not be able to learn devices' real-identities.
- P-certificate set linkage says that the issuing PCA should not be able to link the set of P-certificates nor link real-identities of devices during credential provision.
- Connection privacy ensures that the verification and validation process does not know about device connection.

Availability:

- Offline verification is a property that enables devices to validate PKs without connecting to verification parties.
- LT-certificate/P-certificate revocation type specifies the method employed by the VPKI proposals to cancel LT-certificate and P-certificate.

Performance:

- Timely key update is the property to ensure a fast update of trusted party keys in the case of key loss and compromise. For example, in both VPKI standards updating Trusted Authority (TA) requires either software update or CRL distribution to update key/certificate of TAs (e.g., LTCA and PCA), which may take days to a week (e.g., first revoking the compromised key and then inserting a new key for the TA).
- Certificate path/chain verification includes verification from the end-entity certificate to the root CA certificate. It includes at least two signature verification operations in the hierarchical CA model adopted by VPKI standards.
- Scalability enables a framework to handle increasing participants and the real-world workload. It is crucial to ensure efficient authentication and secure communication in case of a heavy workload. We define three measures 1) Low, 2) Medium, and 3) High to describe the scalability of proposals. Low measure states that the VPKI proposal

cannot handle the current systems loads; Medium measure indicates that the VPKI proposal can handle current loads but cannot meet system loads in case of future expansion; High measure states that the VPKI framework can handle existing and future loads.

- P-certificate revocation check elimination says that devices do not need to validate that P-certificates being accepted by them are not yet revoked. Although it eliminates revocation status checking latency during authentication, however, it can raise security concerns.

G. Evaluation Metrics for Revocation Proposals

Besides the metrics for VPKI proposals evaluation, we also specify a set of metrics for comparison of revocation proposals. The following are the listed revocation metrics.

- Scalability enables a framework to handle increasing revocation. It is important to ensure efficient checking and distribution in case of a heavy workload. Low, Medium, and High are used to measure revocation scalability as discussed under the performance metric in the previous section.
- Communication overhead measures the bandwidth consumed by information sent with signed messages to validate signatory revocation status.
- Memory overhead measures the storage used by storing revocation information on end devices.
- Validation support determines the type of communication supported by proposals (e.g., online, offline, or both modes) to perform the revocation check.
- Extra connection is a binary measure showing that an additional connection is needed for credential revocation status checking or not.
- Real-time validation is a binary measure to specify the proposal's capacity to offer real-time revocation status validation service to the devices.
- Validation privacy shows if the system employs a server to know which credentials' revocation statuses are validated by devices in a specific region. It can therefore perform region-based tracking of credentials.
- Mapping indicates if the revocation needs a resolution of P-certificate to real-identity in order to revoke misbehaving devices or not.

IV. Existing VPKI and Credential Revocation Proposals

In the first subsection, we review VPKI proposals, and the subsequent subsection covers revocation schemes presented to complement the VPKI revocation process.

A. VPKI Proposals

Several VPKI schemes are proposed to ensure the high privacy and security requirements of vehicular communications. We classify VPKI proposals into four different types: baseline VPKI proposals, hybrid VPKI proposals, registry-based VPKI proposals, and distributed ledger-based VPKI proposals.

1) Baseline VPKI Proposals: SRAAC [73] decoupled the certification process into several certified IVC certification servers to make the certification process blind through distributed magic-ink signature [74] combined with the standard digital signature scheme. The magic-ink signature [74] uses a novel method called "Magic-ink", which offers a method of creating blinded signatures that can be unblinded by the signer if misconduct is identified. In the case of distributed signing, the integrity of magic-ink signature relies on a (t, n)-threshold mechanism, where t and n represent the threshold and the total number of signers, respectively. It enables a threshold number of CAs to sign P-certificates for vehicles blindly. Similarly, the threshold number of CAs must cooperate to map a P-certificate to a vehicle's identity. SRAAC comprises four phases: 1) registration, 2) anonymous certificate-issuance, 3) revocation, and 4) secure IVC. SRAAC involves several challenges, such as a revoked device can use unexpired P-certificates due to the lack of a P-certificate revocation mechanism [33]. Sha *et al.* [75] ensured various privacy levels at the cost of computational and communicational overhead. The protocol in [75] consists of five steps: 1) RSUs' PKs signed by LTCA are temporarily recorded by vehicles, 2) each car sends an authentication query to RSU before sending data or using server offered services, 3) RSU validates the query, 4) the subject receives a challenge from RSU and replies to RSU to solve the challenge, and 5) the subject is validated after successful challenge verification, and the subject is allowed to use services and report data. Reference [75] used the client-server model of PKIX where RSUs work as servers and vehicles as their clients. The RSUs are authenticated by LTCAs, and then RSUs serve as an authentication server as in [73].

Papadimitratos *et al.* [76] designed a security architecture to provide a comprehensive set of security and privacy solutions in the SeVeCom project. Work in [76] also introduced a set of procedures for credential and identity management of vehicles without violating privacy. Schaub *et al.* [77] proposed V-token to ensure blind P-certificate issuance and revocation through blind signature and V-tokens. A V-token comprises a vehicle's identity information and a unique randomization factor encrypted with commonly known PK of resolution authorities. The home LTCA blindly signs a vehicle's V-tokens after verification of the resolution authorities' signature in a blind signature scheme. After acquisition of blindly signed V-tokens, V-tokens are then presented to PCA to obtain P-certificates. The V-tokens are inserted in P-certificates by the PCA after successful verification of the LTCA signature. If P-certificate resolution is needed, the embedded V-token is extracted from the P-certificate in question. A pre-defined number of resolution authorities must cooperate to obtain the resolution information from the V-token.

Shen *et al.* [78] addressed the linkability issue of Chameleon hash signature [79] by leveraging EC-based Chameleon signature and dynamic PKs and proposed a new lightweight privacy-preserving protocol based on the newly designed algorithm. Shen *et al.* [78] protocol comprises the registration, authentication, and tracking phases. In the registration phase, vehicles and RSUs are assigned credentials after successful identity verification. They also handle revocation of devices

when they get corrupted in the tracking phase, where RA resolves the compromised device's real-identity and revokes it from using the system's resources. Copra [67] complemented the ETSI VPKI framework [68] by presenting a generic P-certificates resolution mechanism. Copra operates in two phases. In the first phase, enrolled vehicles are assigned P-certificates, and mappings between P-certificates and real-identities are saved by LTCA. PCA provides linkage identifiers of disputed vehicles to RA, which is forwarded to LTCA for mapping to real-identities.

VeSPA [80] presented a VPKI framework that employs a Kerberized [81] ticket-based authentication process for P-certificate provision. Reference [80] ensured the three AAA (authorization, authentication, and accountability) requirements of VC. Each vehicle has one LT-certificate, which is used to obtain tickets from LTCA for the privacy-preservation P-certificate provision process. Each vehicle is granted a pool of P-certificates per ticket. The authors also provided a performance evaluation and showed that VeSPA is feasible and practically applicable. However, P-certificates are linkable since the entire set is provided per ticket. Also, LTCA can launch timing attacks to reveal the real-identity of vehicles since LTCA issues time-bounded tickets for vehicles [82]. Alexiou *et al.* [83] extended the VeSPA scheme to cross-domains, multi-services architecture, and decouples LTCA and PCA to support multi-services. They computed that the average time for ticket provision is 100.95 ms and 16.46 s for 1000 P-certificate provisions, including verification, storage, and communication with service providers. They also measured 363 ms for multi-domain protocol and concluded dominant latency for distant LTCA services. However, the protocol could not eliminate the privacy concerns of VeSPA.

SEROSA [84] designed a service-oriented privacy-preserving and secure VPKI framework for VC to provide the AAA features along with a set of credential management services in a multi-services ecosystem. Their architecture integrated VPKI with Web services, where LTCA and PCA act as Identity provider (IdP) and Service Providers (SP), respectively. SEROSA [84] comprises 1) federated trust, 2) registration, 3) service provision, and 4) P-certificate resolution and its revocation protocols. First, vehicles get LT-certificates from IdP by registering in the system. Then they query anonymous identifiers to use the service offered by SP. Vehicles' registrations are canceled if their private-key is leaked or they start abusing the system in the final resolution and revocation phase. Reference [85] improved [80], [83], [84] in terms of privacy and performance. Reference [85] anonymized the ticket used for P-certificates provision to thwart tracking of timing by LTCA. They also decreased the issuance and revocation latency of P-certificates. However, [85] still used one ticket to get a set of P-certificates, which raises privacy concerns. Khodaei and Papadimitratos [86] shed light on the performance of VeSPA [80], [85], [87], and SEROSA [84], demonstrating P-certificate issuance time of 817 ms, 1000 ms, 260 ms, and 650 ms per 100 P-certificates, respectively.

Work in [88] addressed vehicle-to-RSU communication use cases of work [66]. Cincilla *et al.* [89] implemented, deployed, and tested a large-scale and fully functional VPKI prototype to examine the scalability-consistency trade-offs of VPKI replicated components. PUCA [90] extended [87], which integrated the C2C-CC [22] P-certificate concepts, REWIRE [91] revocation scheme, CL signature [92], and periodic n-show credentials [93], [94] to make P-certificate issuance blind through cryptographic technique instead of separation of roles. PUCA ensures honest clients' anonymity against corrupted and colluding servers (e.g., PCA) and keeps them anonymous while enabling refilling and revoking of P-certificates.

SECMACE [82] proposed multi-policies VPKI architecture compatible with IEEE 1609.2 standards [20] suits of specifications. The authors defined three different policies: user-defined, oblivious, and universally fixed policy to obtain a ticket, which is used in P-certificates acquisition. In SECMACE, a vehicle lifecycle starts from registration by LTCA after successful authentication through TLS. Similarly, the P-certificate lifecycle is a three-cycle process 1) anonymous ticket provision, 2) P-certificate provision, and 3) P-certificate revocation after resolution. The vehicle lifecycle comes to an end when its LT-certificate is revoked in case of key leakage or found guilty of abusing the system, and then the vehicle is needed to enter a new lifecycle. The experimental results of SECMACE show its practicality and feasibility. Unfortunately, issuing a bundle of P-certificates per ticket by PCA enables the issuing PCA to track the set of P-certificates.

Haidar *et al.* [29], [95] investigated the performance of VPKI P-certificate refilling-related protocols. In the first work [29], they developed a proof-of-concept implementation as well as proposed an optimization technique. In the later work [95], they also quantified the consumed P-certificates while driving and observed that P-certificate usage is indirectly proportional to vehicle speed. They concluded in their works [29], [95] that interaction among devices and VPKI servers is non-negligible while reloading P-certificates.

Gaiduk *et al.* [96] proposed zero-knowledge (ZK) proofs along with an anonymous reputation-based scheme to authenticate and revoke devices while still hiding their real-identities. The scheme simplified VPKI architecture by rendering the LTCA and PCA separation as each device can authenticate itself to LTCA using ZK proof without revealing the real-identity. Work in [96] adopted a reputation-based passive revocation mechanism where a device needs to prove to LTCA that it is holding a reputation score above a system-defined threshold using ZK proof.

2) Hybrid VPKI Proposals: Group Signature (GS) [113], [114] is a concept where a group of users shares a single PK to ensure users' privacy, which is known as Group PK (GPK), and each user is assigned a private-key. These proposals integrate either GS or identity-based cryptography with VPKI architecture to provide anonymity.

TACK [97] presents hybrid VPKI to ensure private and secure IVC. In TACK, each node has Group Secret-Key (GSK) and regional PCA certifies P-certificates for nodes. In TACK, a vehicle lifecycle starts with the assignment of a GSK, which is used later to acquire a P-certificate from a regional PCA. Regional PCA validates P-certificate acquisition request and issues P-certificate to the subject after successful validation.

P-certificate validity is determined not only by time but also by valid and associated regional PCA information. Each time a vehicle enters a new region, it needs to update its P-certificate from the regional PCA. The lifecycle of a car ends when a car is revoked in case of misconduct.

Calandriello *et al.* [98] integrates GS with P-certificate and uses the concept of "Web of trust", where each subject self-certifies its P-certificate. In [98], each vehicle self-signs its P-certificate on-the-fly using GSK, which can be verified using GPK. A recipient uses GPK to validate that the P-certificate is generated and certified by legitimate node of the VPKI. After P-certificate validation, the signed message verification is carried out as in any baseline VPKI. They also proposed some optimization for baseline and hybrid VPKI schemes. However, [98] cannot thwart Sybil-attacks on system resources.

Wang and Yao [99] proposed an anonymous authentication protocol by integrating VPKI with identity-based encryption to mitigate the latency caused by CRL checking during VPKI authentication. In [99], LTCA issues an LT-certificate to each RSU and vehicle, and RSU CRL (RCRL) and Vehicle CRL (VCRL) are distributed to revoke RSUs and vehicles, respectively. Each RSU generates a master-key for vehicles entering its communication range after successful identity validation. Then the master-key signed P-certificate is used by the vehicle to sign messages while being anonymous as well as support both single and batch verifications.

Wasef *et al.* [100] complemented VPKI by proposing enhancements to authentication and revocation mechanisms to support location privacy and distributed revocation. They built a group and leveraged the Message Authentication Acceleration Code (MAAC) to eliminate CRL and boost revocation checking. They also mitigated DoS attacks by appending Hash-based Message Authentication Code (HMAC) to messages calculated using GS. However, their scheme can only ensure privacy within a group [55].

Dong *et al.* [101] integrated certificateless PKC with light-CA to ensure security with minimum computational overhead. They used onion routing with on-path encryption to hide devices' real-identities from attackers. The scheme [101] reduced PK management complexity and encryption cost compared to conventional VPKI proposals and encryption schemes. This approach induced higher computational costs during routing because forwarding nodes need to encrypt messages to thwart tracing messages by intruders.

Rajput *et al.* [102] merged GS with P-certificate to eliminate CRL distribution and searching delay. An LTCA enrolls each vehicle by issuing an LT-certificate after successful identity verification, which is then used in acquiring P-certificate. Whenever a vehicle enters a new geographic area, it requests a region-specific GS credential through P-certificate. Rajput *et al.* [102], however, used computationally expensive GS for V2V and V2I secure communication.

RHyTHM [103] addresses the privacy issues of vehicles running out of VPKI-based P-certificates and have no way to refill their P-certificates pool. The authors leveraged GS to generate on-the-fly P-certificates with neighboring vehicles' helping to join the P-certificate generation process. Vehicles can also switch between self-certified and PCA-certified P-certificates to enhance the level of communication privacy. However, RHyTHM [103] does not specify how to create a group and revoke malicious devices.

3) Registry-Based Schemes: Registry-based schemes use the initial Diffie and Hellman [115] concept of PKs registry to simplify the PK management in VC and eliminate the performance issues of CRL.

Shen *et al.* [104] proposed the PKR scheme based on the concept of a PKs registry to maintain PKs in a centralized directory. Reference [104] attempted to reduce deployment cost and management efforts. LTCA shares a signed read-only copy of the PKs directory with each RSU. The PK registry contains mappings between vehicles' PK and real-identities testified and verified by LTCA. The PK verification and its revocation status checking are eliminated through the distribution of the PKs directory. However, each vehicle needs to validate each fresh PK with RSU before communicating with the subject of the PK. Secondly, [104] is unable to thwart DoS attack since a corrupted vehicle can overwhelm RSU by sending many PK verification requests [105]. Thirdly, PKR does not consider the privacy of vehicles.

SA-KMP [105] integrated the PKR [104] and 3D matrix-key distribution [116] schemes for secure and efficient VC. PKR mitigates the exchange of certificates through a read-only centralized PK registry maintained by RSUs, while the 3D matric key method establishes a cost-effective symmetric key to reduce reliance on asymmetric operations. RSUs play an important role in SA-KMP, and they are assumed to be trustworthy. In SA-KMP [105], vehicles need to authenticate PKs before connecting, and the RSUs know which vehicle is connecting to which service or vehicle. Thus violating devices' connection privacy. In addition, SA-KMP left the privacy of devices as an open research problem.

4) Distributed Ledger-Based VPKI: Ledger-based VPKI design leverages a publicly verifiable ledger technology to make CAs' operations and behaviors transparent and open to public scrutiny. Any interested party can validate, check, and monitor the distributed ledger to identify and detect any miss-issued credentials. These proposals prevent CAs from abusing the clients stealthily, and any of their misbehavior will not remain undetected.

BARS [106] presented a blockchain-based model to manage vehicular certificates, revocation, trustworthiness evaluation, and IVC messages. They used three different ledgers: CerBC (blockchain for certificates), RevBC (blockchain for revoked PKs), and MesBC (blockchain for messages) to carry out the credential provision and update, revocation, and messaging operations. BARS comprise initialization, certificate update, PK revocation, and authentication phases. In system initialization, each vehicle is issued an LT-certificate. A credential is updated in the second phase if it expires or the key is leaked. The revocation phase includes canceling corrupted vehicles' registration by recording the vehicles' PKs on the RevBC. The authentication process is carried out on blockchains, where a vehicle needs to perform two checks on blockchains for each received certificate besides validating its expiry. Each vehicle checks that the received certificate is recorded on the CerBC

and the certificate's PK is not yet recorded on the RevBC. They also introduce a vehicle trust evaluation mechanism to examine the trust degree of safety messages. However, Law Enforcement Authority (LEA) can link a vehicle's identity to its PKs.

BPPA [107] designed a blockchain-based privacy-preserving authentication protocol to make CAs' operations transparent. A vehicle lifecycle starts with the initialization phase, where a vehicle computes its PK/SK and sends a certificate acquisition request. The P-certificate acquisition request is sent to LEA, which after vehicle validation, forwards to PCA. After issuance, the PCA records the P-certificate on the blockchain with real-identity to PK mapping being encrypted by LEA. The vehicle can send and receive BSM, where each certificate is authenticated in a distributed fashion and with updated information received from RSUs. A vehicle is rescinded if found guilty of performing misconduct or abusing system resources. As in BARS [106], BPPA [107] also assumes that LEA is trusted; however, a corrupted LEA can trivially link PKs to the real-identities of vehicles.

Lasla *et al.* [108] overlaid the blockchain platform on top of VPKI. Each device in [108] first passes through registration, where each device gets an LT-certificate from a concerned LTCA. Vehicles are admitted on the blockchain network after successfully passing registration. Admitted vehicles on the blockchain can send and verify signed BSMs, where PK of vehicles are searched on blockchain during verification operation. Finally, vehicles' admissions on the blockchain network are canceled if they misbehave or their private-key is leaked. Unfortunately, maintaining a local history of all valid devices by each vehicle and timely updates are significant issues of this scheme since it may cost storage in GBs.

Malik *et al.* [109] have presented the use of private blockchain to enhance CA issues and improve authentication efficiency in VC. During registration with LTCA, each vehicle acquires a pseudo-identity, which is used to join the communication group of RSU in range after being successfully validated in the blockchain. Malicious vehicles are prevented from communication by setting revocation flags to true in the blockchain network. In [109], LTCA generates public/private key-pairs; hence LTCA knows the private-keys of all vehicles, which is one of the main concerns of this work [109].

IOTA-VPKI [110] instantiated SECMACE [82] on distributed ledger technology to mitigate the adopted CA model's problems of VPKI schemes, such as the lack of transparency in CAs' operations. They leveraged IOTA [117] distributed ledger technology, which is known as the IOTA Tangle ledger, to carry out VPKI operations. Each LTCA and PCA own an IOTA wallet as well as an encrypted channel to ensure private acquisitions of LT-certificate, P-certificate, and privacy during their update operations. Each vehicle has a symmetric SK shared with the home LTCA for private channel usage. Each authority records the signature of hashes of issued credentials (ticket and P-certificate) on the blockchain and shares the address of signature with the device to whom the credential is issued. The signature on the IOTA ledger is accessed and verified to authenticate BSMs signed with the credential during communication. IOTA-VPKI [110] employs distributed ledger to make CAs' operations transparent and open to public scrutiny; however, the framework does not fully achieve it as only signatures are saved on distributed ledger instead of credentials.

BCPPA [111] combined Ethereum's blockchain platform and key-derivation algorithm to design an effective credential management system. BCPPA consists of three phases: initialization, message signing, and verification. In the initialization phase, LTCA distributes PKs/certificates to vehicles to enable them to participate in secure VC. After the initialization phase, vehicles sign BSMs and verify BSMs received from other participants. However, BCPPA does not guarantee strong privacy and security against corrupted LTCA as a single LTCA can link a vehicle's real-identity to signed BSMs and register malicious devices.

George *et al.* [112] proposed a blockchain-based PKs management framework, where LTCA assigns and records vehicles' pseudo-identities and PKs on a permissioned blockchain after successful identity verification of vehicles. Each vehicle has a partial local copy of pseudo-identity to PK mappings, which is searched whenever a vehicle receives a signed BSM from another device. If the PK of the signing device is found in the partial copy of mappings, then the signed BSM is accepted; otherwise, the vehicle sends a query to RSU to validate the PK. The work in [112] has the same private-key leakage issue to LTCA as in Malik *et al.* [109].

ACMS [18] is another recent proposal built on a transparency log server (ledger technology) to bring credential transparency to VC. ACMS comprises LT-certificate and P-certificate provision, their registration at transparency log, secure communication, P-certificate resolution and revocation, and monitoring of the transparency log server for malicious credential issuance. Multi LTCAs signed LT-certificate is issued during the enrollment phase to discourage a single LTCA from enrolling illegal devices. ACMS maintains the same privacy by design as in [16] through the P-certificate provision and butterfly-key expansion method. Both LT-certificate and P-certificates are recorded on the transparency log server to ensure transparency and detection of maliciously issued credentials. Security of ACMS is verified formally through security games as well as the automated security verification tool Tamarin [118]. Although, ACMS enhances defense against LTCA through multi LTCAs signed LT-certificate. Yet, like the other VPKI proposals mentioned above, a single corrupted PCA and a log server can successfully abuse the system by maliciously issuing and registering fake P-certificates. Table III summarizes VPKI proposals.

B. Credential Revocation

Several revocation methods are proposed to prevent corrupted devices from abusing VC in VANETs. We classify revocation mechanisms into five different types based on the data structure and distribution mechanism used by them, namely, CRL-based, OCSP-based [119], [120], tree-based (e.g., binary hash tree, Halfman tree), distributed ledger-based (e.g., blockchain and ledger technology), and code-based (e.g., activation/deactivation codes) certificate revocation proposals.

TABLE III
SUMMARY OF REVIEWED VPKI PROPOSALS

Proposals	IEEE Standard Compliance	ETSI Standard Compliance	Evaluation Metric	Evaluation Method	Strengths	Weaknesses
Baseline VPKI Schemes						
SRAAC [73]	✗	✗	Not available	Not available	Distributes trust among servers and makes certification provision process blind.	RSUs are assumed fully trusted and secure.
Sha et al. [75]	✗	✗	Anonymity reduction factor, response time	Prototype/testbed	User-controlled anonymity.	RSUs are assumed secure as in SRAAC [73].
Papadimitratos et al. [76]	✗	✗	Entropy, privacy	Not available	Provides a comprehensive and practical security and privacy solution.	P-certificate issuer knows the real-identity of nodes.
Schaub et al. [77]	✗	✗	Not available	Not available	Makes P-certificates resolution blind by inserting resolution information in them.	Massive message exchange during P-certificates acquisition process.
Bissmeyer et al. [66]	✗	✓	Not available	Not available	First generic VPKI with detailed roles and specifications.	Does not provide CRL distribution mechanism.
Shen et al. [78]	✗	✗	Latency, No. of authentication	Simulation	It provides strong mutual V2I authentication	It ignores V2V authentication.
Copra [67]	✗	✓	Latency	Not available	Introduces validation of revocation reason before providing revocation data.	It ignores V2V authentication.
VeSPA [80]	✗	✗	Latency	Prototype/testbed	Guarantees AAA VC's requirements	LTCA can reveal real-identity of a vehicle.
ETSI ITS [68]	✗	✓	Not available	Not available	Defines roles, security, and privacy requirements for VC in Europe	Does not specify any P-certificate revocation.
Alexiou et al. [83]	✓	✓	Latency	Prototype/testbed	Offers multi-domains and multi-servers architecture.	The set of P-certificates can be linked by issuing PCA
SEROSA [84]	✓	✓	Latency	Prototype/testbed	It provides a comprehensive suite of identity and service management with existing SPs.	It has the privacy concern where SP can trivially link P-certificates issued in response to a single request.
Khodaei et al. [85]	✓	✗	Latency, revocation update probability, processing delay	Prototype/testbed	Increases anonymity and simple P-certificate issuance.	PCA can link set of P-certificates issued to vehicles.
Cincilla et al. [89]	✗	✓	Latency, throughput	Prototype/testbed	Introduces weak consistency model.	Replication anomalies by operators.
PUCA [90]	✗	✗	Latency, communication overhead	Simulation	Offers strong degree of privacy against corrupted trusted servers.	Assumes trusted, honest, and correctly functioning vehicles.
Haidar et al. [29]	✗	✓	Packet size, latency	Prototype/testbed	Optimizes VPKI issuance process.	Conducts experiments under dense scenarios.
SECMACE [82]	✓	✗	Latency, revocation update probability	Prototype/testbed	Provides inter-domain communication with privacy support.	Vehicle's P-certificates set is linkable by PCA as in [85].
SCMS [16]	✓	✗	Not available	Not available	Enables acquiring an anonymous set of P-certificates with a single seed expansion and offers privacy preserving revocation.	Vulnerable to Sybil-attack.
Haidar et al. [95]	✗	✓	Latency, no. of P-certificates reloaded, speed	Prototype/testbed	Finds relationship between speed and P-certificate change.	Conducts experiments under dense scenarios as in Haidar et al. [29].
Gaiduk et al. [96]	✗	✓	Authentication, latency, memory consumption	Prototype/testbed	Eliminates the need for having separate LTCA and PCA.	Makes revocation process opaque and PCA can issue P-certificates to OBUs with lower reputation scores.
Hybrid VPKI Schemes						
TACK [97]	✗	✗	Key update, bandwidth	Simulation	Eliminates CRL.	Revoked vehicle cannot be prevented from using system resource with unexpired certificate.
Calandriello et al. [98]	✗	✗	Communication/computational overhead, reliability, safety, efficiency	Simulation	Optimizes authentication.	Vulnerable to Sybil-attack.
Wang et al. [99]	✗	✗	Delay, verification cost, packet loss ratio	Simulation	On the fly P-certificate issuance.	Increased dependency on RSUs and RSUs can link signed messages.
Wasef et al. [100]	✗	✗	Delay, Message Loss Ratio (MLR)	Simulation	Efficient revocation checking.	Privacy within the group only.
Dong et al. [101]	✗	✗	Encryption cost	Not available	Efficient and simple PK management.	Encryption during routing induces high cost.
Rajput et al. [102]	✗	✗	Delay, Packet Delivery Ratio (PDR), packet loss	Simulation	Eliminates CRL searching delay.	Uses computationally expensive GS for V2V and V2I communication.
RHyTHM [103]	✗	✗	Latency, computational overhead	Prototype/testbed	Addresses the privacy issues of vehicles running out of P-certificates.	Does not support malicious vehicle revocation.
Registry-based VPKI Schemes						
PKR [104]	✗	✗	Latency, transmission overhead	Simulation	Eliminates CRL.	Does not offer privacy.
SA-KMP [105]	✗	✗	Latency, transmission overhead, scalability	Simulation	Eliminates DoS attack applicable to PKR.	Does not ensure privacy as its predecessor.
Ledger-based VPKI Schemes						
BARS [106]	✗	✗	Reputation, delay, storage	Simulation	Enables transparent trust evaluation of vehicles.	High storage cost by recording credentials, revocation, and messages on blockchain.
BPPA [107]	✗	✗	Transaction rate and latency, delay	Prototype/testbed	Monitors CAs operation.	High storage on blockchain and high transmission cost.
Lasa et al. [108]	✗	✗	Latency	Simulation	Introduces a lightweight authentication mechanism.	Does not consider the privacy requirements of C-ITS devices.
Malik et al. [109]	✗	✗	Latency, throughput, PDR	Simulation	RSUs-based revocation of vehicles.	LTCA knows private-keys of all vehicles.
IOTA-VPKI [110]	✗	✗	Not available	Not available	Enables detection of malicious credentials.	Set of P-certificates are linkable by issuing PCA.
BCPPA [111]	✗	✗	Delay, packet loss	Simulation	Introduces a key derivation mechanism to avoid P-certificates preloading.	LTCA can link signed messages to corresponding vehicles.
George et al. [112]	✗	✗	Delay, communication overhead	Simulation	It introduces a lightweight authentication mechanism.	LTCA knows private-keys of all vehicles.
ACMS [18]	✗	✗	Latency, MLR, scalability, storage, transmission overhead	Simulation	Defends against corrupted LTCA.	Vulnerable to Sybil-attack.

1) CRL-Based Revocation: CRL [71] is a blacklist of digital identifiers of revoked certificates, signed by RA and periodically distributed to clients to prevent misuse of already canceled certificates. CRL's size and searching latency linearly increase with an increase in the number of entries, which is the main bottleneck of CRL and raises concerns about its suitability in safety-related VC applications.

Raya *et al.* [121] used probabilistic Bloom Filter (BF) [122] with CRL to mitigate CRL searching latency by compressing CRL using BF. Haas *et al.* [123] used the concept of

evicting a set of P-certificates of a vehicle with a single entry. Moreover, they adopted similar concepts of Delta-CRL [124] and BF [122] to overcome CRL distribution cost and size. Hass *et al.* [125] extended their previous work [123] by introducing backward privacy during revocation. SCMS [16] design also proposes improvements to reduce the number of entries and size of CRL by recording a single seed value, which can be used to cancel a set of P-certificates while preserving privacy.

Nowatkowski *et al.* [126] proposed the inclusion of "valid after" entry to P-certificates to reduce the size and latency of CRL. Di Crescenzo and Zhang [127] designed a solution with one-to-one mapping among revoked vehicles and a set of pseudonyms instead of one-to-many mapping. This work [127] reduces size and latency through local CRL pseudonym tags management along with the expiry time of P-certificates. Rabieh *et al.* [128] employed Chameleon hashing [79] to generate special trapdoor information for a certified set of P-certificates. This trapdoor footprint is inserted into CRL while revoking a set of P-certificates, which reduces the CRL transmission cost and shortens the CRL's searching time.

Papadimitratos *et al.* [129] addressed the CRL distribution in VC by dividing the VC into regions. Each RA is responsible for managing and distributing CRLs to RSUs, which are further distributed to vehicles. The limitation of this work [129] is that there is no RSU-to-RSU communication and reduced RSU-to-RA communications. Laberteaux *et al.* [130] complemented V2I CRL distribution by introducing CRL exchange among devices during V2V communications. Wasef and Shen [131] proposed integrating key distribution centers with VPKI to carry out timely and efficient revocation of vehicles without reliance on RA and RSUs.

Nowatkowski and Owen [132] and Michael and Henry [133] employed Raptor coding [134] during CRL generation to enhance and improve CRL's distribution process of work [130]. Rigazzi *et al.* [135] used BF to revoke P-certificates and simulated Compressed CRL (C^2RL) in urban and rural scenarios. Tuladhar and Lim [136] used dual BF and regional CRL distribution mechanisms to minimize false positive rate, CRL size, and dissemination cost. Global CRL is divided into smaller regional CRL to reduce distribution cost and CRL size. Asghar *et al.* [137] used the voting process to revoke corrupted OBUs and reduce CRL size and searching delay through Shamir's secret-sharing mechanism. The voting-based scheme ensures security, privacy, and better performance.

2) Online Certificate Status Protocol (OCSP)-Based Revocation: OCSP [119], [120] offers online validation of credentials where specialized servers forward attested validity response messages to queries by clients. Papapanagiotou *et al.* [138] adapted OCSP [119], [120] to mobile ad hoc networks by distributing OCSP servers. Papapanagiotou *et al.* [139] further adapted to VANETs and evaluated the performance of their modified scheme in the VC scenario. Serna-Olvera *et al.* [140] proposed an authentication scheme for VANETs real-time application using OCSP and demonstrated its feasibility in real-time safety applications.

3) Tree-Based Revocation: Besides the standard CRL, some proposals adopted binary hash tree (e.g., Merkl Hash Tree (MHT) [141]) to overcome the performance problems of CRL. For example, Gañán *et al.* [142] designed an Efficient and Privacy-Aware revocation mechanism (EPA) to mitigate CRL performance issues and ensure privacy while validating the revocation status of devices. EPA is based on MHT and anonymous relaying protocol for efficiency and privacy-preservation. RA instantiates each new version of CRL as an MHT and forwards the CRL along with the signed root hash of MHT to RSUs, where each RSU regenerates the MHT by applying the hash function. The leaves of MHT contain hash values of revoked certificates in ascending order, and each device sends a credential along with the proof of validity from RSUs during communication. Martín-Fernández *et al.* [143] leveraged the Huffman k-ary tree to handle vehicular credentials' revocation. However, work in [143] does not specify how to conceal real-identities during revocation.

Alrawais *et al.* [144] instantiated CRL on MHT to maintain the integrity of revocation data while using fog nodes to enable the efficient distribution of revocation information. Martín-Fernández [145] leveraged a dynamic hash tree to manage revocation in VC, where leaves nodes contain revoked credentials information. Their scheme is applicable to revocation in both VPKI and identity-based key management schemes, where revocation authority distributes revocation information to RSUs after each update. Vehicles carry out credentials validation by querying the revocation status of credentials from RSU within the communication range, which induces an extra delay to authentication.

4) Activation Code-Based Revocation: Activation code-based schemes rely on the concept to issue at first a large amount of P-certificate for an extended period (e.g., a few years [146]) to devices. However, they activate them later if the devices are still working correctly. Issue First Activate Later (IFAL) [146] used this idea to incorporate a revocation mechanism to European VPKI [68], which is yet to finalize a revocation method for P-certificates. IFAL provides privacy resilience against a corrupted TA as well as eliminates bidirectional communication for P-certificate provision. REWIRE [91] revocation scheme employed trusted computing to eliminate the need for P-certificates resolution by RA and prevent RA from learning real-identities. Whitefield *et al.* [147] proposed an OTOKEN extension to REWIRE and conducted a security analysis of REWIRE and OTOKEN using Tamarin [118]. They also complement REWIRE revocation by enabling eviction of devices even if they have changed P-certificate.

BCAM [148] relied on the activation code mechanism to eliminate the need for bidirectional communication in SCMS [16], [50]. BCAM builds on the design and provision method of SCMS for enrollment certificate provision; yet, P-certificates are preloaded for an extended lifecycle and maintained in the form of a binary hash tree. A Certificate Access Manager (CAM) server interacts with a proxy server as well as enables subjects to access public/private key-pairs by providing them activation codes. They used a soft revocation list and CRL to revoke devices' LT-certificates and abandon them from participating in secure communication.

Simplicio *et al.* [149] identified birthday attacks against BCAM [148] and mitigated the attack by enhancing the binary hash tree. Reference [149] also improved the privacy resilience against colluding corrupted authorities. Reference [150] identified two types of birthday attacks against [16] linkage values, which are getting serious with the passage of time and an increase in the number of revocations. Reference [150] presented an alternative revocation process design to thwart SCMS's security degradation and allow temporary suspension of vehicles. Later, [151] extended [150] and eliminated the need for linkage values and linkage servers. Thus, [151] simplifies the architecture and cuts down SCMS's deployment cost. Simplicio *et al.* [152] compared [149] with ETSI VPKI [68] and CRL design of SCMS [16], [50] in terms of efficiency and privacy-preservation and showed advantages over them.

5) Distributed Ledger-Based Revocation: Recently, blockchain and distributed ledger technology emerged as a promising technology to detect maliciously issued certificates by CAs. Besides, several proposals also attempted to revoke credentials on blockchain technology, which ensures timely dissemination of information. For example, recent works [153], [154] based their revocation mechanisms on the ledger technology to evict devices. Lie *et al.* [153] instantiated CRL on blockchain and introduced another layer to carry out devices' revocation. Lei *et al.* [153] carried out devices' revocation at two levels—infrastructure and vehicular. At the infrastructure level, nodes are revoked through CRL, which is broadcast in a peer-to-peer manner in the blockchain platform. Revocation is carried out at the vehicular level by deleting a corrupted vehicle from the communication group through updating GS PK. Moreover, they also carry out P-certificates shuffling on the blockchain, which exposes shuffling strategy to attackers to launch privacy attacks.

Tesei *et al.* [154] managed credentials revocation on IOTA [117] distributed ledger. They complemented their previous VPKI model [110] and integrated another distributed ledger to resolve the revocation left unresolved in their previous VPKI framework. Whenever a device receives signed messages from other participants, then the device checks the revocation status of credentials on the Tangle [117] ledger. This additional operation of revocation checking introduces an extra delay. Cho and Perera [155] instantiated activation codes mechanism on blockchain to prevent corrupted devices from activating their P-certificates and reducing CRL size. Reference [155] managed activation codes distribution and P-certificate change through shuffling combined with a mixed zone. Table IV summarizes the revocation proposals.

V. Observations and Discussions

In this section, leading VPKI schemes are first examined systematically using the metrics defined in Section III-F and observations are made. Next, we present key lessons learned from our comprehensive survey on VPKI proposals. Table V, Table VI, Table VII, and Table VIII compare them using the trust, security, privacy, availability, and performance metrics. We also investigate leading revocation proposals using metrics defined in Section III-G, which is given in Table IX. After examining and observing the different VPKI schemes and revocation solutions, many open and emerging problems are raised, which are expanded in the next section.

Table V and Table VI examine VPKI solutions based on trust and security metrics. Table V and Table VI help to systematically investigate, compare, and find the pros and cons of each solution in terms of trust and security.

Limited trust model: VPKI proposals inherit the Single-Point-of-Failure (SPoF) issues from PKIX design, where a corrupted CA can maliciously authorize illegitimate devices to join the system and abuse system resources. Many of the reviewed schemes have attempted to increase the resilience to privacy violations by decoupling a CA into LTCA and PCA. Some proposals, such as SCMS and ACMS, provide greater immunity against privacy attacks by introducing a proxy server to prevent linking the set of P-certificates assigned to a device. ACMS has increased the level of security against corrupted LTCA by introducing multi-signature certificates and logging credentials on a distributed ledger. However, colluding PCA and distributed ledger can still register fake and malicious credentials to abuse the system and its resources.

Trust flexibility: The current CA model adopted in VPKI does not offer this feature since any LTCA and PCA can issue a valid certificate for any device. Hence, VPKI proposals do not allow devices to define their list of trusted LTCAs and PCAs to better guard themselves against them. Outside the VPKI realm, several PKI proposals such as AKI [156], ARPKI [157], ATCM [158], and CA Authentication (CAA) [159] allow clients to assert a list of trusted CAs who are valid and authorized to issue and certify their digital identities.

Malicious credential detection: From Table VI, it is clear that baseline, hybrid, and registry-based VPKI proposals have no built-in mechanism to detect malicious credentials, even though researchers recommended it. However, the mentioned works assume that existing misbehavior detection algorithms can be utilized to detect maliciously issued credentials, which may not prove effective against malicious-issuance. On the other hand, some proposals such as ACMS and IOTA-VPKI have publicly verifiable and detectable credentials ledgers, enabling interested parties to detect fraudulent credentials and attacks through fake PKs. However, BARS and PBBA do not fully provide this feature as mappings between credentials and related identities are recorded in encrypted form on the ledgers, violating the primary purpose of transparency.

Malicious credential prevention: All VPKI proposals except ACMS cannot thwart attacks when a TA issues fraudulent certificates. Most systems inherit the SPoF problems by design from PKIX, where malicious certificates had been used in attacks against clients. Fortunately, ACMS has introduced multi-signature LT-certificates that discourage illegal enrollment of devices and deter illegal registration on transparency log maintainers by exposing LTCA and PCA operations to public scrutiny.

Formal security analysis: Since VPKI is a complex system with complicated corner cases, only formal security verification can detect the loopholes in the design and implementation

TABLE IV
SUMMARY OF REVIEWED CERTIFICATE REVOCATION PROPOSALS

Proposals	Data Structure	Distribution strategy	Evaluation Metrics	Evaluation Method	Strengths	Weaknesses
CRL-based Schemes						
Raya et al. [121]	CRL with BF	V2I	Vehicles density, speed, authentication	Simulation	Data integrity and regional authentication.	Privacy is not preserved during revocation.
Haas et al. [123]	CRL with BF	V2I and V2V	Insertion and searching latency	Simulation	Revokes a set of P-certificates with a single entry and keeping privacy.	No backward privacy of evicted devices.
Hass et al. [125]	CRL with BF	V2I and V2V	Insertion and searching time, CRL distribution rate	Simulation	It provides backward privacy of evicted vehicles.	No mechanism of RSU-to-RSU CRL distribution.
Nowatkowski et el. [126]	CRL	Not available	Revocation rate, CRL size	Simulation	Reduces CRL by introducing special entry.	Does not provide impact of the special entry on the security of VC.
Crescenzo et al. [127]	CRL and Hash tag list	Not available	latency	Simulation	Boosts revocation searching time through binary search and hash tag list.	Does not preserve backward privacy.
Rabieh et al. [128]	CRL	V2I and V2V	Communication and computational overhead, latency	simulation	Reduces CRL size through recording a single entry per set of P-certificates.	Does not consider backward privacy of revoked devices.
Papadimitratos et al. [129]	CRL	V2I	CRL receiving success rate, CRL size, bandwidth, delay	Simulation	Simple, fast and efficient CRL distribution.	Dense vehicles in a region may cause broadcast flooding which can increase CRL distribution delay.
Laberteaux et al. [130]	CRL	V2I and V2V	Latency, Revocation update probability	Simulation	Large scale simulation with real-movement traces and better results over RSUs only distribution.	Every OBU broadcast CRL pieces which may cause channel contention.
Wasef et al. [131]	CRL	V2I and V2V	Delay, Revocation update probability	Simulation	CA and RSU independent and decentralized revocation by OBUs through voting.	An evicted OBU can join the VC by changing a credential as a legitimate user.
Nowatkowski et al. [132]	CRL	V2I and V2V	Bandwidth, OBUs density	Simulation	Reduces flooding and collision of broadcasting CRL.	Hidden nodes and OBUs with large amount of CRL pieces may cause collision and flooding.
Michael et al. [133]	CRL	V2I and V2V	PDR, normalized packet overhead	Simulation	Performance evaluation using realistic vehicle traces.	No privacy of revocation process.
Rigazzi et al. [135]	CRL with BF	V2I	Compression gain, CRL size	Simulation	Does not keep track of revoked devices traveling between regions [137].	Reduces CRL size through optimized BF with a configurable false positive rate.
Tuladhar et al. [136]	CRL with BF	V2I	CRL size, domain size	Analytical analysis	Reduces false positive rate through dual BF.	Assumes proactive synchronization of regional and global CRLs.
Asghar et al. [137]	CRL	V2I and V2V	CRL size	Analytical Analysis	Reduces false positive with dual BF.	Synchronization is required between global CRL and local copy.
OCSP-based Schemes						
Papapanagiotou et al. [139]	Not available	V2I	Delay, overhead per validation request, bandwidth	Simulation	Provides fresh revocation information.	Extra connection and privacy concerns as in traditional OCSP [119], [120].
Serna et al. [140]	Not available	V2I	PDR, delay	Simulation	Enables evaluation of CA trust and security.	Same additional connection and privacy concerns as in traditional OCSP [119], [120].
Tree-based Schemes						
Ganan et al. [142]	MHT	V2I and V2V	MLR, bandwidth, delay, anonymity	Simulation	Eliminates CRL through decentralized repositories.	Induces extra storage overhead.
Martin et al. [143]	Huffman k-ary tree	Not available	Not available	Not available	Optimizes revocation checking through query frequencies and running time of vehicles.	Trusted authority knows actual running time of each vehicle.
Alrawais et al. [144]	MHT	V2I	Verification cost	Quantitative Analysis	Reduces verification cost by maintaining a regional MHT.	Does not provide detailed privacy and security analysis.
Martin et al. [145]	Dynamic hash tree	V2I	Revocation information size, authentication queries	Simulation	Optimizes search and insertion operations in the tree.	RSUs can learn vehicles' validation history as they query RSUs for each revocation status validation.
Code-based Schemes						
IFAL [146]	Activation code	V2I	Bandwidth	Prototype/testbed	Formal security and privacy analysis.	PCA can link P-certificates to the corresponding device.
REWIRE [91]	Deactivation code	V2I	Not available	Not available	Eliminates the need to know the real-identity of devices during revocation.	Can not revoke a device if it changes its P-certificate.
OTOKEN [147]	Deactivation code	V2I	Not available	Not available	Performs automated formal analysis of REWIRE and OTOKEN.	Relies on a strong assumption that devices trusted computing are reliable and cannot get corrupted.
BCAM [148]	Activation code and Binary hash tree	V2I	Bandwidth	Numerical Analysis	Eliminates bi-directional communication for P-certificate provision.	Preloads vehicles with P-certificates for an extended period (e.g., 30 years), which may reduce system agility.
Simplicio et al. [149]	Activation code and binary hash tree	V2I	Bandwidth, computational cost	Numerical analysis	Mitigates birthday attacks on [149].	Preloading P-certificates for an extended period.
Simplicio et al. [151]	Activation code and binary Hash tree	V2I	Computational cost, bandwidth cost, deployment cost	Simulation	Enhances security and simplify SCMS' architecture.	Induces an extra computational cost at PCA.
Ledger-based Schemes						
Lie et al. [153]	Ledger	V2I	Bandwidth cost, delay, number of transaction	Simulation	Timely revocation and dissemination of revocation information.	Leverages computationally expensive GS for revocation at vehicular level.
Tesei et al. [154]	Ledger	V2I	Delay	Simulation	Eliminates the need for complex CRL distribution protocol.	Additional connection to check revocation status.
Cho and Perera [155]	Ledger	V2I	Not available	Not available	Instantiate activation code mechanism on blockchain in IoV scenario.	Induces high storage cost at devices.

of VPKI. As shown in Table VI, only SA-KMP and ACMS are formally verified, and the security of both protocols is proved against different attacks.

DoS attack mitigation/Truststore and keystore protection: All VPKI proposals offer resistance against DoS attacks except PKR. As mentioned in Section IV-A3, in PKR, a

TABLE V
COMPARISON OF VPKI PROPOSALS BASED ON TRUST METRIC

Proposals	Limited Trust Model	Trust Flexibility	Credential Issuance Transparency	Revocation Transparency	Trust Delegation Transparency
Baseline VPKI Schemes					
SRAAC [73]	✗	✗	✗	✗	✗
Sha et al. [75]	✗	✗	✗	✗	✗
Papadimitratos et al. [76]	✗	✗	✗	✗	✗
Schaub et al. [77]	✗	✗	✗	✗	✗
Bissmeyer et al. [66]	✗	✗	✗	✗	✗
Shen et al. [78]	✗	✗	✗	✗	✗
VeSPA [80]	✗	✗	✗	✗	✗
ETSI ITS [68]	✗	✗	✗	✗	✗
Alexiou et al. [83]	✗	✗	✗	✗	✗
SEROSA [84]	✗	✗	✗	✗	✗
Khodaei et al. [85]	✗	✗	✗	✗	✗
Cincilla et al. [89]	✗	✗	✗	✗	✗
PUCA [90]	✗	✗	✗	✗	✗
Haidar et al. [29]	✗	✗	✗	✗	✗
SECMACE [82]	✗	✗	✗	✗	✗
SCMS [16]	✗	✗	✗	✗	✗
Haidar et al. [95]	✗	✗	✗	✗	✗
Gaiduk et al. [96]	✗	✗	✗	✗	✗
Hybrid VPKI Schemes					
TACK [97]	✗	✗	✗	✗	✗
Calandriello et al. [98]	✗	✗	✗	✗	✗
Wang et al. [99]	✗	✗	✗	✗	✗
Wasef et al. [100]	✗	✗	✗	✗	✗
Dong et al. [101]	✗	✗	✗	✗	✗
Registry-based VPKI					
PKR [104]	✗	✗	✗	✗	✗
SA-KMP [105]	✗	✗	✗	✗	✗
Ledger-based VPKI					
BARS [106]	✓	✗	✓	✓	✗
BPPA [107]	✓	✗	✓	✓	✗
IOTA-VPKI [110]	✓	✗	✓	✗	✗
ACMS [18]	✓	✗	✓	✓	✗

corrupted device can send multiple PKs validation requests to overwhelm an RSU and temporarily block the RSU from serving other devices. On the other hand, none of the existing VPKI proposals protect their client's truststore, which exposes them to a malicious CA's PK/certificate installation in the devices' truststore. Existing VPKI schemes left such issues on manufacturers'/vendors' side, making it possible for vendors/manufacturers to maliciously insert a root CA certificate to compromise the system's security/privacy. Regrettably, manufacturers/vendors in practice have inserted malicious CAs certificates, and researchers have replaced truststores of devices with fake and corrupted truststores by taking down devices [158], [160], [161]. In addition, Table V and Table VI show that baseline and hybrid VPKI proposals do not meet many of the objectives of an advanced and sophisticated PKI system. The main reason is that baseline and hybrid VPKI architectures adopt several major building blocks (e.g., CA trust model, weaker attacker, keystore management, and truststore management) from PKIX architecture, which has inherit flaws [18]. Various studies [156], [158], [162] have been conducted to fix the shortcomings of PKIX and perform formal security of PKIX protocols. Unfortunately, fewer efforts have investigated how to mitigate these same issues in VPKI architectures.

Table VII and Table VIII examine VPKI solutions based on privacy, availability, and performance metrics. Table VII and Table VIII help to analyze and find the advantages and disadvantages of each solution in terms of mentioned metrics.

Device/Connection privacy: As can be observed from Table VII, baseline, hybrid, and distributed ledger-based VPKI schemes neither learn the real-identity of vehicles nor know devices' connection history. However, registry-based proposals expose vehicles to privacy-related cyber-attacks by maintaining a read-only centralized copy at each RSU, enabling RSUs to track inter-vehicle connections.

P-certificates set linkage: SCMS and its subsequent enhancement proposals offer strong anonymity where insider and outsider attackers cannot reveal the identity as well as cannot link the set of pseudonyms issued in response to a single acquisition request. All other proposals are not ensuring unlinkability to the set of P-certificates issued in response to a single acquisition request.

Offline PK verification: In baseline and hybrid VPKI schemes, devices only need to verify the expiry and validity

TABLE VI
COMPARISON OF VPKI PROPOSALS BASED ON SECURITY METRIC

Proposals	Malicious Credential Detection	Malicious Credential Prevention	Formal Security Analysis	DoS Attack Mitigation	Truststore Protection	Keystore Protection
Baseline VPKI Schemes						
SRAAC [73]	✗	✗	✗	✓	✗	✗
Sha et al. [75]	✗	✗	✗	✓	✗	✗
Papadimitratos et al. [76]	✗	✗	✗	✓	✗	✗
Schaub et al. [77]	✗	✗	✗	✓	✗	✗
Bissmeyer et al. [66]	✗	✗	✗	✓	✗	✗
Shen et al. [78]	✗	✗	✗	✓	✗	✗
VeSPA [80]	✗	✗	✗	✓	✗	✗
ETSI ITS [68]	✗	✗	✗	✓	✗	✗
Alexiou et al. [83]	✗	✗	✗	✓	✗	✗
SEROSA [84]	✗	✗	✗	✓	✗	✗
Khodaei et al. [85]	✗	✗	✗	✓	✗	✗
Cincilla et al. [89]	✗	✗	✗	✓	✗	✗
PUCA [90]	✗	✗	✗	✓	✗	✗
Haidar et al. [29]	✗	✗	✗	✓	✗	✗
SECMACE [82]	✗	✗	✗	✓	✗	✗
SCMS [16]	✗	✗	✗	✓	✗	✗
Haidar et al. [95]	✗	✗	✗	✓	✗	✗
Gaiduk et al. [96]	✗	✗	✗	✓	✗	✗
Hybrid VPKI Schemes						
TACK [97]	✗	✗	✗	✓	✗	✗
Calandriello et al. [98]	✗	✗	✗	✓	✗	✗
Wang et al. [99]	✗	✗	✗	✓	✗	✗
Wasef et al. [100]	✗	✗	✗	✓	✗	✗
Dong et al. [101]	✗	✗	✗	✓	✗	✗
Registry-based VPKI Schemes						
PKR [104]	✗	✗	✗	✗	✗	✗
SA-KMP [105]	✗	✗	✓	✓	✗	✗
Ledger-based VPKI Schemes						
BARS [106]	✓	✗	✗	✓	✗	✗
BPPA [107]	✓	✗	✗	✓	✗	✗
IOTA-VPKI [110]	✓	✗	✗	✓	✗	✗
ACMS [18]	✓	✓	✓	✓	✗	✗

of a received certificate. Both schemes satisfy this feature. Registry-based strategies do not fulfill this requirement since each vehicle must contact RSU when receiving a new PK. In distributed ledger-based VPKI proposals, BARS, BPPA, and IOTA-VPKI do not propose any method how to carry out offline verification of devices' PKs. They also do not provide light-client verification of PK when the devices are offline. In contrast, ACMS supports this feature because the proof of LT-certificate and P-certificate validity are offered to communicating parties during communication.

Timely key update: Baseline and distributed ledger-based VPKIs support this feature as PK is usable after being attested by the concerned CA. However, in the case of hybrid VPKI, revocation from the assigned group and rejoining a fresh one after identity verification is not clear and may cause a delay. Similarly, registry-based schemes are likely to cause delay and may not support this feature because PKs become usable after PKs' updated information is disseminated by the LTCA and observed by RSUs.

Scalability: C-ITS VPKI needs to handle a larger amount of credentials than PKIX (e.g., SCMS needs to manage 278 billion credentials annually while PKIX needs to handle around 2 million certificates) [64]. Hence, scalability becomes a challenging factor for C-ITS VPKI. It can be observed from Table VIII that VPKI proposals can hardly scale to C-ITS in case of future expansion except for the ETSI ITS proposal. The primary reason behind the baseline schemes and hybrid schemes is their complex design, while the reason behind registry-based schemes is the centralized read-only registry [18], [64]. The main reason behind blockchain-based proposals [106], [107], [110] is the scalability issues of the underlying blockchain technology, such as the low transaction throughput [163], [164]. In addition, storing a huge amount of credentials on a blockchain platform can rapidly grow ledger size [163].

P-certificate revocation check elimination/Certificate chain validation: Except for the European VPKI scheme and hybrid schemes, all proposals validate the revocation status of a P-certificate. However, a revoked vehicle can use P-certificate till its expiry in both European VPKI and hybrid frameworks. Similarly, certificate chain validation is performed by every scheme, which induces extra latency to the authentication process. It is clear from the discussion that baseline VPKI proposals can ensure the basic security and privacy of VC. However, they lack the mechanisms to issue P-certificates to vehicles running out of P-certificates with no connectivity to PCA and detect malicious credential issuance. Patching hybrid proposals with baseline proposals can address the P-certificate provision problem of vehicles with no connectivity [103] to PCA, while integrating distributed ledgers can ensure timely fake credential issuance detection [18].

TABLE VII
COMPARISON OF VPKI PROPOSALS BASED ON PRIVACY AND AVAILABILITY METRICS

Proposals	Device Privacy	P-certificates' Set Linkage	Connection Privacy	Offline Verification	LT-certificate/P-certificate Revocation
Baseline VPKI Schemes					
SRAAC [73]	✓	✗	✓	✓	CRL/CRL
Sha et al. [75]	✓	✗	✓	✓	CRL/CRL
Papadimitratos et al. [76]	✓	✗	✓	✓	CRL/CRL
Schaub et al. [77]	✓	✗	✓	✓	CRL/CRL
Bissmeyer et al. [66]	✓	✗	✓	✓	CRL/CRL
Shen et al. [78]	✓	✗	✓	✓	CRL/CRL
VeSPA [80]	✓	✗	✓	✓	CRL/CRL
ETSI ITS [68]	✓	✗	✓	✓	CRL/ Not yet decided
Alexiou et al. [83]	✓	✗	✓	✓	CRL/CRL
SEROSA [84]	✓	✗	✓	✓	CRL/CRL
Khodaei et al. [85]	✓	✗	✓	✓	CRL/CRL
Cincilla et al. [89]	✓	✗	✓	✓	CRL/CRL
PUCA [90]	✓	✗	✓	✓	CRL/CRL
Haidar et al. [29]	✓	✗	✓	✓	CRL/CRL
SECMACE [82]	✓	✗	✓	✓	CRL/CRL
SCMS [16]	✓	✓	✓	✓	CRL/CRL
Haidar et al. [95]	✓	✗	✓	✓	CRL/CRL
Gaiduk et al. [96]	✓	✗	✓	✓	CRL/CRL
Hybrid VPKI Schemes					
TACK [97]	✓	✓	✓	✓	GS Revocation List (RL)/ Does not support revocation.
Calandriello et al. [98]	✓	✓	✓	✓	RL/ Does not support revocation.
Wang et al. [99]	✓	✓	✓	✓	RL/ Does not support revocation.
Wasef et al. [100]	✓	✓	✓	✓	RL/ Does not support revocation.
Dong et al. [101]	✓	✓	✓	✓	RL/ Does not support revocation.
Registry-based VPKI Schemes					
PKR [104]	✗	✗	✗	✗	Registry/Does not support P-certificates.
SA-KMP [105]	✗	✗	✗	✗	Registry/Does not support P-certificates.
Ledger-based VPKI Schemes					
BARS [106]	✓	✗	✗	✗	Ledger/Ledger
BPPA [107]	✓	✗	✗	✗	Ledger/Ledger
IOTA-VPKI [110]	✓	✗	✗	✗	Does not support revocation/ Does not support revocation.
ACMS [18]	✓	✓	✓	✓	CRL/Ledger

At last, we discuss the revocation proposals in a less verbose manner. Table IX provides an overview of the performance and privacy features of each revocation proposal. Table IX shows that all schemes except OCSP-based as well as Chao/Perier do not support the real-time validation property. However, OCSP-based methods do not ensure privacy and require an extra connection for each validation, while Chao/Peirer proposal needs to keep fresh revocation data in devices memory. Similarly, all schemes except REWIRE and OTOKEN need mappings of real-identities to pseudo-identities during revocation of devices.

A. Lessons Learned

Revocation of devices has been thoroughly investigated in the area of VC, and significant improvements have been identified [16], [146], [147], [151]. CRL with several improvements dominates in the trial and standardization in US standard VPKI, while the European standard still has no consensus method of revoking P-certificates. New revocation schemes have been proposed to complement both architectures in terms of revocation. However, there is still a lack of original research to evaluate the security (e.g., blocking of revocation information by attackers to get revoked P-certificates accepted by devices), privacy (e.g., disclosing real-identity from revocation data), and effectiveness (e.g., ensuring timely revocation information dissemination) of CRL and the new proposals when integrated with a standard VPKI architecture. Nor is there an automated security tool or established evaluation model (either analytical or simulation-based) that can be used to verify the security of revocation proposals and evaluate their performance on a set of precise requirements for real-time VC. Furthermore, none of the existing proposals investigated the case of a CA (i.e., LTCA, PCA) certificate revocation and how to avoid the collateral damage (e.g., revoking PCA certificate invalidates all devices P-certificates signed by the PCA) caused by revocation of a CA certificate. Designing a mechanism to gracefully revoke a CA is of utmost importance as such circumstances will arise with the large-scale adoption and implementation of VPKI frameworks.

Notable contributions are made in the area of anonymous VPKI-based authentication, and some protocols have achieved interesting results regarding privacy [16], [18], [82]. However, VPKI-based authentication performance issues and the problems in achieving the goal of 1000 authentications per second recommended by SeVeCOM [19] have received less research attention. To fulfill the goal, a thorough investigation of challenges in VPKI-based authentication would be vital. New and enhanced VPKI-based authentication methods are required to efficiently authenticate a massive amount of safety messages, so as to fulfill the authentication requirements of VC. The new enhanced authentication methods must consider either batch verification of P-certificates or cooperative method of P-certificates verification through sharing of P-certificates verification results among devices.

TABLE VIII
COMPARISON OF VPKI PROPOSALS BASED ON PERFORMANCE METRIC

Proposals	Timely Key Update	Certificate Chain Validation	Scalability	P-certificate Revocation Check Elimination
Baseline VPKI Schemes				
SRAAC [73]	✓	✓	Low	✗
Sha et al. [75]	✓	✓	Low	✗
Papadimitratos et al. [76]	✓	✓	Low	✗
Schaub et al. [77]	✓	✓	Low	✗
Bissmeyer et al. [66]	✓	✓	Low	✗
Shen et al. [78]	✓	✓	Low	✗
VeSPA [80]	✓	✓	Low	✗
ETSI ITS [68]	✓	✓	High	✓
Alexiou et al. [83]	✓	✓	Low	✗
SEROSA [84]	✓	✓	Low	✗
Khodaei et al. [85]	✓	✓	Low	✗
Cincilla et al. [89]	✓	✓	Low	✗
PUCA [90]	✓	✓	Low	✗
Haidar et al. [29]	✓	✓	Low	✗
SECMACE [82]	✓	✓	Low	✗
SCMS [16]	✓	✓	Medium	✗
Haidar et al. [95]	✓	✓	Low	✗
Gaiduk et al. [96]	✓	✓	Low	✗
Hybrid VPKI Schemes				
TACK [97]	✗	✓	Medium	✓
Calandriello et al. [98]	✗	✓	Medium	✓
Wang et al. [99]	✗	✓	Low	✓
Wasef et al. [100]	✗	✓	Low	✓
Dong et al. [101]	✗	✓	Low	✓
Registry-based VPKI Schemes				
PKR [104]	✗	✗	Medium	Does not support P-certificates.
SA-KMP [105]	✗	✗	Medium	Does not support P-certificates.
Ledger-based VPKI Schemes				
BARS [106]	✓	✓	Low	✗
BPPA [107]	✓	✓	Low	✗
IOTA-VPKI [110]	✓	✓	Low	✓
ACMS [18]	✓	✓	Medium	✗

Despite efforts to evaluate the performance of VPKI proposals through the use of various performance metrics, the lack of unified performance evaluation metrics and the absence of an evaluation tool for VPKI architecture remain shortcomings. Most proposals focus on evaluating a specific aspect of VPKI architecture (e.g., P-certificate generation rate, revocation efficiency, latency) using either a general purpose simulation tool (e.g., Analytical simulation, ns2[1]) or through unstandardized local prototype/testbed. Most proposals are unable to conduct dedicated and standardized testbed/tool-based evaluation and full scale VPKI scheme evaluation by integrating all protocols and components. An automated performance evaluation framework with extendable evaluation metrics would be a significate milestone towards a unified evaluation of VPKI proposals. Similarly, few proposals have used automated security verification tools to verify the security of their VPKI schemes. Hence, an automated protocol verification tool able to prove both the security and privacy of VPKI proposals would be vital.

Security and privacy are prime priorities in VC as safety applications directly rely on them. Security and privacy breaches have two-fold consequences in VC. On one hand, attackers can take control of vehicles by compromising them in C-ITS or driverless scenarios, which can lead to serious damages to VC or human life. On the other hand, attackers can steal sensitive information of drivers (e.g., location, travel route, identity information) from system servers. Some proposals have ensured strong privacy during credential issuance and revocation, where a single authority is unable to disclose real-identities of vehicles. On the other side, fewer efforts are devoted to fixing security loopholes of VPKI architectures. For example, countermeasures against CAs (i.e., LTCA, PCA) compromises are overlooked. Potential countermeasures against them are required because the use of cryptographic algorithms provides no benefits without correct and proper working of CAs. Hence, extensive research is needed to fix security loopholes inherited from predecessors (e.g., insecure truststore management) and new security loopholes (e.g., vulnerabilities of linkage values of SCMS) caused by architectural changes of VPKI before proper deployment. Some of the security issues with most of VPKI proposals are based on naïve assumptions of potential threats, insecure truststore management, and centralized CRL management. In practice, attackers and research have consistently shown that existing security

[1]The Network Simulator-ns-2: https://www.isi.edu/nsnam/ns/

TABLE IX
COMPARISON OF REVOCATION PROPOSALS ON THE BASIS OF METRICS DEFINED IN SECTION III-G

Proposals	Scalability	Communication Overhead	Memory Overhead	Validation Support	Extra Connection	Real-time Validation	Validation Privacy	Mapping
CRL-based Schemes								
Raya et al. [121]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Haas et al. [123]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Hass et al. [125]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Nowatkowski et el. [126]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Crescenzo et el. [127]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Rabieh et el. [128]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Papadimitratos et al. [129]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Laberteaux et al. [130]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Wasef et al. [131]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Nowatkowski et al. [132]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Michael et al. [133]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
Asghar et al. [137]	Low	0	MBs	Online/Offline	✗	✗	✓	✓
OCSP-based Schemes								
Papapanagiotou et al. [139]	Medium	KB	0	Online	✓	✓	✗	✓
Serna et al. [140]	Medium	KB	0	Online	✓	✓	✗	✓
Tree-based Schemes								
Ganan et al. [142]	Medium	KB	Bytes	Online/Offline	✗	✗	✓	✓
Martin et al. [143]	Medium	KB	MBs	Online/Offline	✗	✗	✓	✓
Alrawais et al. [144]	Medium	KB	Bytes	Online/Offline	✗	✗	✓	✓
Code-based Schemes								
IFAL [146]	High	0	0	Offline	✗	✗	✓	✓
REWIRE [91]	High	0	0	Offline	✗	✗	✓	✗
OTOKEN [147]	High	0	0	Offline	✗	✗	✓	✗
BCAM [148]	Medium	0	0	Offline	✗	✗	✓	✓
Simplicio [149]	Medium	0	0	Offline	✗	✗	✓	✓
Simplicio [151]	Medium	0	0	Offline	✗	✗	✓	✓
Ledger-based Schemes								
Lie et al. [153]	Low	KB	KB	Online	✗	✗	✗	✓
Tesei et al. [154]	Medium	KB	KBs	Online	✗	✗	✗	✓
Cho and Perera [155]	Low	0	GBs	Offline	✗	✓	✓	✓

protocols are inadequate and at risk. In fact, in the current CA trust model adopted by VPKI architecture, compromising any CA is enough to breach the security of the system [156].

There are still several challenges for deploying cost-effective and secure VPKI, each of which requires further investigation, exploration, and examination. Both standard architectures assume uniform communication with CAs for credential provision and revocation. The challenge in deploying VPKI in countries with large geographic areas and irregularly interspersed urban centers would be to tackle the potential disruption of network connectivity between CAs and devices. Hence, it would be vital to investigate efficient placement strategies of CAs to avoid connectivity issues with devices, reduce deployment cost, and ensure credential provision and revocation services.

VI. RESEARCH GAP AND FUTURE PERSPECTIVE

VPKI deployment is still in the infancy stage and different corner cases need to be explored before real-world deployment based on the trust, security, privacy, performance and availability metrics. Many challenges in VPKI remain, beyond those inherited directly from PKIX design. In this article, we emphasized some of these VPKI architecture issues, and suggest the following strategies to enhance overall VPKI security and performance in the future.

1) Keystore/Truststore protection: Vehicles and IoT devices are exposed physically to attackers in case of C-ITS deployment in the near future. It is likely that intruders can either gain control of a vehicle either by physically owning it or by extracting SK material from old OBU units. A hardware security module is proposed by [165], however, the application software code can be compromised to manipulate the SK saved on trusted hardware for sending arbitrary signed messages and is not cost-effective [15], [166]. Furthermore, truststore is a central point of failure as attackers can insert malicious CAs by gaining control over the application software or hardware of a vehicle. The malicious CA can be used to breach the security of devices. Such kinds of attacks are witnessed in the Internet PKIX protocol and against IoT devices. Running all devices on trusted hardware will cause a substantial increase in deployment and maintenance cost. Thus, ensuring protection

of keystore and truststore should be investigated on a priority basis.

2) Discouraging malicious credential issuance and mississuance: Malicious credential issuance is a major problem of already deployed PKIX, where 1 million fraudulent credentials are issued for top websites [18]. Prevention of fake credential issuance in VPKI needs special investigation as the issuance rate is several orders higher than PKIX [64], which makes detecting them a more challenging task. Besides, each PCA needs to issue a large amount of P-certificates. Therefore, CAs (i.e., LTCA, PCA) in VPKI have higher chances of mississuance, which is also a major problem of CAs in PKIX [167]. It is recommended to design new mechanisms to prevent malicious issuance as well as mississuance caused by software, hardware, and human errors.

3) Privacy-preserving transparency: Recently, transparency emerged as an advanced security feature to make CAs accountable to the public through monitoring of their operations and scrutiny. Transparency has increased the security of communication systems through monitoring. For example, Facebook detected fake but valid certificates being issued for its domains to launch cyber-attacks against its domain before being deployed to production systems [168]. This type of detection was not possible before deployment of Google Certificate Transparency [162] and subsequent proposals [156], [157], [169], [170]. Hence, achieving privacy transparency in VPKI architecture can boost the overall security of VC.

4) Elimination of certificate chaining: As mentioned in Section III-F, certificate chain verification includes at least two signature verification operations to authenticate CAM/BSM. This induces extra latency to the authentication process and makes it difficult to achieve VC authentication requirements. Redesigning authentication protocol to bypass certificate chain validation without compromising security will be a major step towards meeting VC authentication requirements.

5) Elimination of SPoF: LTCA and PCA are SPoF, and they can be attacked by powerful adversaries. Various famous CAs (e.g., Lets Encrypt) had been taken down by hackers and researchers in practice [169]. LTCA and PCA are no exception and are vulnerable to similar attacks. LTCA and PCA can breach the security of the system and can cause avoidable fatal crashes. Hence, SPoF mitigation is highly necessary for safety-related applications, where failures can endanger human lives [18].

6) Mapping attacks from PKIX to VPKI: In addition to CAs failures, bugs in the cryptographic library (e.g., Open SSL) also experienced cyber-attacks in various applications [171]. Hence, such attacks mapping from already deployed applications to VC scenario and proposing countermeasures are still open areas of research in VPKI frameworks.

7) Real-time revocation status validation: Efficient real-time revocation status validation remains an open research topic in VPKI architecture. This feature is a high priority as safety-applications are reliant on VPKI for secure and private communication. OCSP is not a suitable solution for VC workload; OCSP falls short in PKIX and is abandoned by major applications and browsers in the Internet PKIX. Hence, designing real-time revocation validation is of utmost importance for real-time and secure VC.

VII. Conclusion

C-ITS is expected to be widely deployed because of its anticipated benefits for transportation efficiency and safety. VPKI is recommended to ensure the security and privacy of C-ITS as it is deployed both in the US and Europe. However, designing a secure VPKI is more complex than any PKI, as complicated corner cases ensure privacy must be handled. In this work, we give the detail of PKI background, evolution, basic concepts, generic VPKI architecture, and the two dominant VPKI standards adopted in the US and Europe. We focused on classifying VPKI proposals and proposals complementing the VPKI revocation process. The article compares VPKI proposals systematically to investigate the research gap despite the existing VPKI and revocation proposals. We also highlighted that the classical CA model adopted by VPKI is no longer adequate for safety-related applications. Finally, we presented lessons learned and highlighted certain security loopholes and performance issues of VPKI schemes, which may improve resilience against cyber-attacks and may meet real-time performance requirements of VC if addressed in the future.

References

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

[2] S. Sharma and B. Kaushik, "A survey on Internet of Vehicles: Applications, security issues & solutions," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100182. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209619302293

[3] C. Mathilde. "Number of passenger cars and commercial vehicles in use worldwide from 2006 to 2015 in (1000 units)." Mar. 2021. [Online]. Available: https://www.statista.com/statistics/281134/number-of-vehicles-in-use-worldwide/ (Accessed: Oct. 29, 2020).

[4] J. Voelcker. "It's official: We now have one billion vehicles on the planet." Aug. 2011. [Online]. Available: https://www.greencarreports.com/news/1065070_its-official-we-now-have-one-billion-vehicles-on-the-planet

[5] C. Harrison *et al.*, "Foundations for smarter cities," *IBM J. Res. Develop.*, vol. 54, no. 4, pp. 1–16, Jul./Aug. 2010.

[6] BT Telecom. "BT cityverve portal." [Online]. Available: https://portal.bt-hypercat.com (Accessed: Oct. 28, 2020).

[7] A. Memedi and F. Dressler, "Vehicular visible light communications: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 161–181, 1st Quart., 2021.

[8] X. Wang *et al.*, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1314–1345, 2nd Quart., 2019.

[9] E. Uhlemann, "The U.S. and Europe advances V2V deployment [connected vehicles]," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 18–22, Jun. 2017.

[10] E. Uhlemann, "The battle of technologies or the battle of business models? [Connected vehicles]," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 14–18, Mar. 2018.

[11] M. Saini, A. Alelaiwi, and A. E. Saddik, "How close are we to realizing a pragmatic VANET solution? A meta-survey," *ACM Comput. Surveys*, vol. 48, no. 2, pp. 1–40, Nov. 2015. [Online]. Available: https://doi.org/10.1145/2817552

[12] Z. Sun *et al.*, "Applications of game theory in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2660–2710, 4th Quart., 2021.

[13] M. A. Rahim, J. Liu, Z. Zhang, L. Zhu, X. Li, and S. Khan, "Who is driving? Event-driven driver identification and impostor detection through support vector machine," *IEEE Sensors J.*, vol. 20, no. 12, pp. 6552–6559, Jun. 2020.

[14] M. A. Rahim *et al.*, "Zero-to-stable driver identification: A non-intrusive and scalable driver identification scheme," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 163–171, Jan. 2020.

[15] D. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," *IEEE Intell. Transp. Syst. Mag.*, vol. 13, no. 1, pp. 181–196, Apr. 2021.

[16] B. Brecht *et al.*, "A security credential management system for V2X communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3850–3871, Dec. 2018.

[17] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

[18] S. Khan *et al.*, "Accountable credential management system for vehicular communication," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100279. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209620300504

[19] T. Leinmüller *et al.*, "Sevecom-secure vehicle communication," in *Proc. IST Mobile Wireless Summit*, Sep. 2006, pp. 1–22.

[20] *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Application and Management Massages*, IEEE Standard 1609.2-2016, Jun. 2016, Accessed: Nov. 25, 2020.

[21] Preserve Consortium. "Preparing secure vehicle-to-x communication systems—PRESERVE." [Online]. Available: http://www.preserve-project.eu (Accessed: Oct. 25, 2020).

[22] "Car-to-car communication consortium (C2C-CC)." [Online]. Available: http://www.car-2-car.org(Accessed: Dec. 20, 2020).

[23] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 3015–3045, 4th Quart., 2017.

[24] A. Boualouache, S. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2018.

[25] M. Zhao, J. Walker, and C.-C. Wang, "Security challenges for the intelligent transportation system," in *Proc. 1st Int. Conf. Security Internet Things (SecurIT)*, Aug. 2012, pp. 107–115. [Online]. Available: https://doi.org/10.1145/2490428.2490444

[26] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209614000187

[27] T. Zhang and L. Delgrossi, *Public Key Infrastructure for Vehicle Networks*. New York, NY, USA: Wiley, 2012, pp. 209–236.

[28] D. Kent, B. H. Cheng, and J. Siegel, "Assuring vehicle update integrity using asymmetric public key infrastructure (PKI) and public key cryptography (PKC)," *SAE Int. J. Transp. Cybersecurity Privacy*, vol. 2, pp. 141–158, Aug. 2020.

[29] F. Haidar, A. Kaiser, and B. Lonc, "On the performance evaluation of vehicular PKI protocol for V2X communications security," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–5.

[30] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[31] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, "A survey of inter-vehicle communication protocols and their applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 3–20, 2nd Quart., 2009.

[32] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[33] M. Riley, K. Akkaya, and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks," *Security Commun. Netw.*, vol. 4, no. 10, pp. 1137–1152, Jul. 2011. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.239

[34] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012.

[35] E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward," in *Proc. 20th Int. Conf. Autom. Comput.*, Sep. 2014, pp. 176–181.

[36] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *J. Netw. Comput. Appl.*, vol. 40, pp. 325–344, Apr. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804513001793

[37] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366414000863

[38] M. Gerla, C. Wu, G. Pau, and X. Zhu, "Content distribution in VANETs," *Veh. Commun.*, vol. 1, no. 1, pp. 3–12, Jan. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209613000028

[39] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[40] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, Dec. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110016815001246

[41] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[42] H. Lu and J. Li, "Privacy-preserving authentication schemes for vehicular ad hoc networks: A survey," *Wireless Commun. Mobile Comput.*, vol. 16, no. 6, pp. 643–655, Apr. 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.2558

[43] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, Jul. 2016. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-its.2015.0072

[44] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Veh. Commun.*, vol. 10, pp. 13–28, Oct. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209617300803

[45] T. Khan *et al.*, "Certificate revocation in vehicular ad hoc networks techniques and protocols: A survey," *Sci. China Inf. Sci.*, vol. 60, no. 10, Oct. 2017, Art. no. 100301.

[46] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870517300562

[47] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209616300018

[48] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209616301231

[49] T. Weil, "VPKI hits the highway: Secure communication for the connected vehicle program," *IT Prof.*, vol. 19, no. 1, pp. 59–63, Feb. 2017.

[50] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," in *Proc. IEEE Veh. Netw. Conf.*, Dec. 2013, pp. 1–8.

[51] P. Asuquo *et al.*, "Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4778–4802, 3rd Quart., 2018.

[52] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1858–1877, 3rd Quart., 2018.

[53] R. W. Van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 779–811, 1st Quart., 2019.

[54] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Apr. 2019.

[55] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (VANETs)," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100247. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209620300188

[56] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2725–2764, 4th Quart., 2020.

[57] Q. Wang, D. Gao, and D. Chen, "Certificate revocation schemes in vehicular networks: A survey," *IEEE Access*, vol. 8, pp. 26223–26234, 2020.

[58] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Comput. Security*, vol. 89, Feb. 2020, Art. no. 101664. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818312872

[59] H. Leibowitz, A. Herzberg, and E. Syta, "Provable security for PKI schemes," in *Proc. IACR Cryptol. ePrint Arch.*, 2019, p. 807.

[60] R. L. Rivest and B. W. Lampson, "SDSI—A simple distributed security infrastructure," in *Proc. USENIX Assoc.*, Jul. 1996, pp. 1–9.

[61] J. R. Vacca, *Computer and Information Security Handbook*. London, U.K.: Newnes, 2012.

[62] C. Ellison, "SPKI requirements," IETF, Fremont, CA, USA, Sep. 1999.

[63] P. R. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press, 1995.

[64] E. Foo, C. Djamaludin, and A. Rakotonirainy, "Security issues for future intelligent transport systems," in *Proc. Aust. Road Safety Conf. (ARSC)*, Dec. 2015, pp. 1–10. [Online]. Available: https://eprints.qut.edu.au/90175/

[65] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," *Eur. Wireless*, to be published.

[66] N. Bissmeyer, H. Stübing, E. Schoch, S. Götz, J. P. Stotz, and B. Lonc, "A generic public key infrastructure for securing car-to-x communication," in *Proc. 18th ITS World Congr.*, vol. 14, Oct. 2011, p. 12.

[67] N. Bissmeyer, J. Petit, and K. M. Bayarou, "Copra: Conditional pseudonym resolution algorithm in VANETs," in *Proc. 10th Annu. Conf. Wireless On-Demand Netw. Syst. Services (WONS)*, Mar. 2013, pp. 9–16.

[68] *Intelligent Transport Systems (ITS) Security, ITS Communication Security Architecture Security Management*, ETSI Standard 102 940, 2016. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/ts_102941v010301p.pdf

[69] "U.S. Department of Transportation. Safety pilot model deployment." [Online]. Available: https://safetypilot.umtri.umich.edu(Accessed: Dec. 25, 2020).

[70] "U.S. Department of Transportation National Highway Traffic Safety Administration. U.S. dot federal motor vehicle safety standards; v2v comunications." [Online]. Available: https://www.federalregister.gov/documents/2017/01/12/201631059/federal-motor-vehicle-safety-standards-v2v-communications (Accessed: Dec. 29, 2020).

[71] D. Cooper *et al.*, "Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile," IETF, RFC 5280, May 2008.

[72] X. Zheng, L. Pan, H. Chen, and P. Wang, "Investigating security vulnerabilities in modern vehicle systems," in *Proc. Int. Conf. Appl. Techn. Inf. Security*, Sep. 2016, pp. 29–40.

[73] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (SRAAC)," in *Proc. 4th Conf. Embedded Security Cars (ESCAR)*, 2006, pp. 1–9.

[74] M. Jakobsson and M. Yung, "Distributed 'magic ink' signatures," in *Proc. Adv. Cryptol. EUROCRYPT*, May 1997, pp. 450–464.

[75] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *Proc. 1st Int. Conf. Commun. Netw. China*, Oct. 2006, pp. 1–8.

[76] P. Papadimitratos *et al.*, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[77] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in VANETs," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2010, pp. 1–6.

[78] A. Shen, S. Guo, D. Zeng, and M. Guizani, "A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2012, pp. 2543–2548.

[79] H. Krawczyk and T. Rabin, "Chameleon hashing and signatures," in *Proc. IACR Cryptol. ePrint Arch.*, 1998, p. 10.

[80] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, "VeSPA: Vehicular security and privacy-preserving architecture," in *Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Security Privacy (HotWiSec)*, Apr. 2013, pp. 19–24. [Online]. Available: https://doi.org/10.1145/2463183.2463189

[81] B. C. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 33–38, Sep. 1994.

[82] M. Khodaei, H. Jin, and P. Papadimitratos, "SECMACE: Scalable and robust identity and credential management infrastructure in vehicular communication systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 5, pp. 1430–1444, May 2018.

[83] N. Alexiou, S. Gisdakis, M. Laganà, and P. Papadimitratos, "Towards a secure and privacy-preserving multi-service vehicular architecture," in *Proc. IEEE 14th Int. Symp World Wireless Mobile Multimedia Netw. (WoWMoM)*, Jun. 2013, pp. 1–6.

[84] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, "SEROSA: service oriented security architecture for vehicular communications," in *Proc. IEEE Veh. Netw. Conf.*, Dec. 2013, pp. 111–118.

[85] M. Khodaei, H. Jin, and P. Papadimitratos, "Towards deploying a scalable robust vehicular identity and credential management infrastructure," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2014, pp. 33–40.

[86] M. Khodaei and P. Papadimitratos, "The key to intelligent transportation: Identity and credential management in vehicular communication systems," *IEEE Veh. Technol. Mag.*, vol. 10, no. 4, pp. 63–69, Dec. 2015.

[87] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET)," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2014, pp. 25–32.

[88] M. Ullmann, C. Wieschebrink, and D. Kügler, "Public key infrastructure and crypto agility concept for intelligent transportation systems," in *Proc. 4th Int. Conf. Adv. Veh. Syst. Technol. Appl.*, Oct. 2015, pp. 14–19.

[89] P. Cincilla, O. Hicham, and B. Charles, "Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–8.

[90] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks," *Ad Hoc Netw.*, vol. 37, pp. 122–132, Feb. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870515002280

[91] D. Förster, H. Löhr, J. Zibuschka, and F. Kargl, "REWIRE—Revocation without resolution: A privacy-friendly revocation mechanism for vehicular ad-hoc networks," in *Trust Trustworthy Computing*, M. Conti, M. Schunter, and I. Askoxylakis, Eds. Cham, Switzerland: Springer Int., Aug. 2015, pp. 193–208.

[92] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols," in *Proc. Int. Conf. Security Commun. Netw.*, Sep. 2002, pp. 268–289.

[93] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, Oct. 1985.

[94] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, "How to win the clonewars: Efficient periodic *n*-times anonymous authentication," in *Proc. 13th ACM Conf. Comput. Commun. Security (CCS)*, Oct. 2006, pp. 201–210. [Online]. Available: https://doi.org/10.1145/1180405.1180431

[95] F. Haidar, A. Kaiser, B. Lonc, and P. Urien, "C-ITS PKI protocol: Performance evaluation in a real environment," in *Proc. 15th Annu. Conf. Wireless On-Demand Netw. Syst. Services (WONS)*, Jan. 2019, pp. 52–55.

[96] P. Gaiduk, K. R. Ranjan, T. Basmer, and F. Tschorsch, "Privacy-preserving public key infrastructure for vehicular networks," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, Nov. 2020, pp. 154–163.

[97] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking together efficient authentication, revocation, and privacy in VANETs," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sensor Mesh Ad Hoc Commun. Netw.*, Jun. 2009, pp. 1–9.

[98] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "On the performance of secure vehicular communication systems," *IEEE Trans. Depend. Secure Comput.*, vol. 8, no. 6, pp. 898–912, Nov./Dec. 2011.

[99] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366417309520

[100] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 22–28, Oct. 2010.

[101] X. Dong, L. Wei, H. Zhu, Z. Cao, and L. Wang, "EP^{2}DF: An efficient privacy-preserving data-forwarding scheme for service-oriented vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 580–591, Feb. 2011.

[102] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access*, vol. 5, pp. 12014–12030, 2017.

[103] M. Khodaei, A. Messing, and P. Papadimitratos, "RHyTHM: A randomized hybrid scheme to hide in the mobile crowd," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 155–158.

[104] P.-Y. Shen, V. Liu, M. Tang, and B. Caelli, "An efficient public key management system: An application in vehicular ad hoc networks," in *Proc. 15th Pac.–Asia Conf. Inf. Syst. (PACIS)*, 2011, pp. 1–15.

[105] H. Tan, M. Ma, H. Labiod, A. Boudguiga, J. Zhang, and P. H. J. Chong, "A secure and authenticated key management protocol (SA-KMP) for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9570–9584, Dec. 2016.

[106] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[107] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019.

[108] N. Lasla, M. Younis, W. Znaidi, and D. B. Arbia, "Efficient distributed admission and revocation using blockchain for cooperative ITS," in *Proc. 9th IFIP Int. Conf. New Technol. Mobility Security (NTMS)*, Feb. 2018, pp. 1–5.

[109] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust Security Privacy Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 674–679.

[110] A. Tesei, L. Di Mauro, M. Falcitelli, S. Noto, and P. Pagano, "IOTA-VPKI: A DLT-based and resource efficient vehicular public key infrastructure," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–6.

[111] C. Lin, D. He, X. Huang, N. Kumar, and K. R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 7408–7420, Dec. 2021.

[112] S. A. George, A. Jaekel, and I. Saini, "Secure identity management framework for vehicular ad-hoc network using blockchain," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.

[113] D. Chaum and E. van Heyst, "Group signatures," in *Proc. Adv. Cryptology EUROCRYPT*, Apr. 1991, pp. 257–265.

[114] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Proc. Adv. Cryptol. (CRYPTO)*, Aug. 1997, pp. 410–424.

[115] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[116] M. A. Hamid, M. S. Islam, and C. S. Hong, "Developing security solutions for wireless mesh enterprise networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2008, pp. 2549–2554.

[117] S. Popov, "The tangle," White paper, 2018.

[118] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The TAMARIN prover for the symbolic analysis of security protocols," in *Proc. 25th Int. Conf. Comput.-Aided Verification (CAV)*, vol. 8044, Jul. 2013, pp. 696–701.

[119] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet public key infrastructure online certificate status protocol-OCSP," IETF, RFC 2560, Jun. 1999.

[120] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet public key infrastructure online certificate status protocol-OCSP," IETF, RFC 6960, Jun. 2013.

[121] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[122] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, no. 7, pp. 422–426, 1970. [Online]. Available: https://doi.org/10.1145/362686.362692

[123] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in *Proc. 6th ACM Int. Workshop Veh. Internetw. (VANET)*, Sep. 2009, pp. 89–98. [Online]. Available: https://doi.org/10.1145/1614269.1614285

[124] D. A. Cooper, "A more efficient use of delta-CRLs," in *Proc. IEEE Symp. Security Privacy. S P*, May 2000, pp. 190–202.

[125] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Efficient certificate revocation list Organization and distribution," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 595–604, Mar. 2011.

[126] M. Nowatkowski, C. McManus, J. Wolfgang, and H. Owen, "Cooperative certificate revocation list distribution methods in VANETs," in *Ad Hoc Networking*, J. Zheng, S. Mao, S. F. Midkiff, and H. Zhu, Eds. Berlin, Germany: Springer, Sep. 2010, pp. 652–665.

[127] G. Di Crescenzo and T. Zhang, "Efficient CRL search in vehicular network PKIS," in *Proc. 6th ACM Workshop Digit. Identity Manag. (DIM)*, Oct. 2010, pp. 17–26. [Online]. Available: https://doi.org/10.1145/1866855.1866862

[128] K. Rabieh, M. Pan, Z. Han, and V. Ford, "SRPV: A scalable revocation scheme for pseudonyms-based vehicular ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[129] P. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proc. VANET*, Sep. 2008, pp. 86–87. [Online]. Available: https://doi.org/10.1145/1410043.1410062

[130] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for VANET," in *Proc. 5th ACM Int. Workshop Veh. Inter-Netw. (VANET)*, Sep. 2008, pp. 88–89. [Online]. Available: https://doi.org/10.1145/1410043.1410063

[131] A. Wasef and X. Shen, "EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5214–5224, May 2009.

[132] M. E. Nowatkowski and H. L. Owen, "Certificate revocation list distribution in VANETs using most pieces broadcast," in *Proc. IEEE SoutheastCon (SoutheastCon)*, Mar. 2010, pp. 238–241.

[133] E. N. Michael and L. O. Henry, "Scalable certificate revocation list distribution in vehicular ad hoc networks," in *Proc. IEEE Globecom Workshops*, Dec. 2010, pp. 54–58.

[134] A. Shokrollahi, "Raptor codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2551–2567, Jun. 2006.

[135] G. Rigazzi, A. Tassi, R. J. Piechocki, T. Tryfonas, and A. Nix, "Optimized certificate revocation list distribution for secure V2X communications," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–7.

[136] K. M. Tuladhar and K. Lim, "Efficient and scalable certificate revocation list distribution in hierarchical VANETs," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, May 2018, pp. 620–625.

[137] M. Asghar, L. Pan, and R. Doss, "An efficient voting based decentralized revocation protocol for vehicular ad hoc networks," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 422–432, Nov. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352864819300161

[138] K. Papapanagiotou, G. Marias, P. Georgiadis, and S. Gritzalis, "Performance evaluation of a distributed OCSP protocol over MANETs," in *Proc. 3rd IEEE Consum. Commun. Netw. Conf. (CCNC)*, vol. 1, Jan. 2006, pp. 1–5.

[139] K. Papapanagiotou, G. F. Marias, and P. Georgiadis, "A certificate validation protocol for VANETs," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–9.

[140] J. Serna-Olvera, V. Casola, M. Rak, J. Luna, M. Medina, and N. Mazzocca, "Performance analysis of an OCSP-based authentication protocol for VANETs," *Int. J. Adapt. Resilient Auton. Syst.*, vol. 3, no. 1, pp. 19–45, Jan. 2012. [Online]. Available: https://doi.org/10.4018/jaras.2012010102

[141] R. C. Merkle, "A certified digital signature," in *Proc. Conf. Theory Appl. Cryptol.*, Aug. 1989, pp. 218–238.

[142] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, "EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks," *Pervasive Mobile Comput.*, vol. 21, pp. 75–91, Aug. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574119214000194

[143] F. Martín-Fernández, P. Caballero-Gil, and C. Caballero-Gil, "Managing certificate revocation in VANETs using hash trees and query frequencies," in *Proc. Comput.-Aided Syst. Theory (EUROCAST)*, Dec. 2015, pp. 57–63.

[144] A. Alrawais, A. Alhothaily, B. Mei, T. Song, and X. Cheng, "An efficient revocation scheme for vehicular ad-hoc networks," *Procedia Comput. Sci.*, vol. 129, pp. 312–318, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S187705091830317X

[145] F. Martín-Fernández, P. Caballero-Gil, and C. Caballero-Gil, "Revocation management in vehicular ad-hoc networks," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 1210–1217.

[146] E. Verheul, C. Hicks, and F. D. Garcia, "IFAL: Issue first activate later certificates for V2X," in *Proc. IEEE Eur. Symp. Security Privacy (EuroS & P)*, Jun. 2019, pp. 279–293.

[147] J. Whitefield *et al.*, "Formal analysis of V2X revocation protocols," in *Security Trust Management*, G. Livraga and C. Mitchell, Eds. Cham, Switzerland: Springer Int., Sep. 2017, pp. 147–163.
[148] V. Kumar, J. Petit, and W. Whyte, "Binary hash tree based certificate access management for connected vehicles," in *Proc. 10th ACM Conf. Security Privacy Wireless Mobile Netw.*. Jul. 2017, pp. 145–155. [Online]. Available: https://doi.org/10.1145/3098243.3098257
[149] M. A. Simplicio, E. L. Cominetti, H. Kupwade Patil, J. E. Ricardini, and M. V. M. Silva, "ACPC: Efficient revocation of pseudonym certificates using activation codes," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101708. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870518304761
[150] M. A. S. Junior, E. L. Cominetti, H. K. Patil, J. Ricardini, L. Ferraz, and M. V. Silva, "Privacy-preserving method for temporarily linking/revoking pseudonym certificates in VANETs," in *Proc. 17th IEEE Int. Conf. Trust Security Privacy Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1322–1329.
[151] M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini, L. T. D. Ferraz, and M. V. M. Silva, "Privacy-preserving certificate linkage/revocation in VANETs without linkage authorities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3326–3336, Jun. 2021.
[152] M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini, and M. V. M. Silva, "Revocation in vehicular public key infrastructures: Balancing privacy and efficiency," *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100309. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209620300802
[153] A. Lei *et al.*, "A blockchain based certificate revocation scheme for vehicular communication systems," *Future Gener. Comput. Syst.*, vol. 110, pp. 892–903, Sep. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X1831522X
[154] A. Tesei, D. Lattuca, P. Pagano, M. Luise, J. Ferreira, and P. C. Bartolomeu, "A transparent distributed ledger-based certificate revocation scheme for VANETs," 2020, *arXiv:2010.13555*.
[155] E. M. Cho and M. N. S. Perera, "Efficient certificate management in blockchain based Internet of Vehicles," in *Proc. 20th IEEE/ACM Int. Symp. Clust. Cloud Internet Comput. (CCGRID)*, May 2020, pp. 794–797.
[156] T. H.-J. Kim, L.-S. Huang, A. Perrig, C. Jackson, and V. Gligor, "Accountable key infrastructure (AKI): A proposal for a public-key validation infrastructure," in *Proc. 22nd Int. Conf. World Wide Web (WWW)*, May 2013, pp. 679–690. [Online]. Available: https://doi.org/10.1145/2488388.2488448
[157] D. Basin, C. Cremers, T. H.-J. Kim, A. Perrig, R. Sasse, and P. Szalachowski, "ARPKI: Attack resilient public-key infrastructure," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Nov. 2014, pp. 382–393. [Online]. Available: https://doi.org/10.1145/2660267.2660298
[158] S. Khan, Z. Zhang, L. Zhu, M. Li, Q. G. K. Safi, and X. Chen, "Accountable and transparent TLS certificate management: An alternate public-key infrastructure with verifiable trusted parties," *Security Commun. Netw.*, vol. 2018, Jul. 2018, Art. no. 8527010. [Online]. Available: https://doi.org/10.1155/2018/8527010
[159] P. Hallam-Baker, R. Stradling, and B. Laurie, "DNS certification authority authorization (CAA) resource record," Internet Eng. Task Force, Fremont, CA, USA, Jan. 2013.
[160] S. Shasha, M. Mahmoud, M. Mannan, and A. Youssef, "Playing with danger: A taxonomy and evaluation of threats to smart toys," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2986–3002, Apr. 2019.
[161] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures," Mar. 2019, *arXiv:1903.01541*.
[162] B. Laurie, "Certificate transparency," *Commun. ACM*, vol. 57, no. 10, pp. 40–46, 2014. [Online]. Available: https://doi.org/10.1145/2659897
[163] P. C. Bartolomeu and J. Ferreira, "Blockchain enabled vehicular communications: Fad or future?" in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–5.
[164] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, Aug. 2020.
[165] M. Wolf and T. Gendrullis, "Design, implementation, and evaluation of a vehicular hardware security module," in *Proc. Inf. Security Cryptol. (ICISC)*, Nov./Dec. 2012, pp. 302–318.
[166] B. Poudel and A. Munir, "Design and evaluation of a reconfigurable ECU architecture for secure and dependable automotive CPS," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 1, pp. 235–252, Jan./Feb. 2021.
[167] D. Kumar *et al.*, "Tracking certificate Misissuance in the wild," in *Proc. IEEE Symp. Security Privacy (SP)*, May 2018, pp. 785–798.
[168] B. Dowling, F. Günther, U. Herath, and D. Stebila, "Secure logging schemes and certificate transparency," in *Proc. Eur. Symp. Res. Comput. Security*, Sep. 2016, pp. 140–158.
[169] S. Khan, L. Zhu, Z. Zhang, M. A. Rahim, K. Khan, and M. Li, "Attack-resilient TLS certificate transparency," *IEEE Access*, vol. 8, pp. 98958–98973, 2020.
[170] S. Khan, Z. Zhang, L. Zhu, M. A. Rahim, S. Ahmad, and R. Chen, "SCM: Secure and accountable TLS certificate management," *Int. J. Commun. Syst.*, vol. 33, no. 15, Jul. 2020, Art. no. e4503. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4503
[171] I. Ghafoor, I. Jattala, S. Durrani, and C. Muhammad Tahir, "Analysis of OpenSSL Heartbleed vulnerability for embedded systems," in *Proc. 17th IEEE Int. Multi-Topic Conf.*, Dec. 2014, pp. 314–319.

Salabat Khan received the Ph.D. degree in computer science and technology from the Beijing Institute of Technology, Beijing, China. He is currently working as a Postdoctoral Fellow with the College of Computer Science and Software Engineering, Shenzhen University, China. His current research interest includes security and privacy, VPKI, PKIX, cryptographic algorithms, blockchain, and distributed ledger technologies.

Fei Luo received the B.Sc. degree from the Jiangxi University of Science and Technology, the M.Sc. degree in surveying and mapping from Wuhan University, and the Ph.D. degree from the Queen Mary University of London, London, U.K., in 2020. He is currently working as a Postdoctoral Fellow with Shenzhen University. His research interests include geographic information systems, human activity detection, and machine learning.

Zijian Zhang received the Ph.D. degree from the Beijing Institute of Technology, where he is an Associate Professor with the School of Cyberspace Science and Technology. His research interests include authentication and key agreement, behavior recognition, and privacy preserving.

Mussadiq Abdul Rahim received the Ph.D. degree in computer science and technology from the Beijing Institute of Technology, Beijing, China. He is an Assistant Professor with the Computer Science Department, NUTECH, Islamabad, Pakistan. His recent research interests include vehicular networks, applied machine learning for human-machine behavior studies, and deep learning-based solution to real-world problems.

Mubashir Ahmad received the B.S. degree (Hons.) in computer science from Hazara University Mansehra, Pakistan, the M.S. degree in computer science from IQRA University Islamabad, Pakistan, in 2012, and the Ph.D. degree from the Beijing Institute of Technology China in 2019. He is currently an Assistant Professor with the Computer Science Department, University of Lahore, Pakistan, His research interests include deep learning, pattern recognition, and medical imaging. He was a recipient of the Chinese Government Scholarship for his Ph.D. studies and got excellent research paper award in IGTA-Springer in 2017 at Beijing, China. He serves as a reviewer for the IEEE ACCESS and other Journals.

Kaishun Wu received the Ph.D. degree in computer science and engineering from HKUST in 2011, where he worked as a Research Assistant Professor. In 2013, he joined Shenzhen University as a Distinguished Professor. He has coauthored two books and published over 100 high quality research papers in international leading journals and primer conferences, like IEEE Transactions on Mobile Computing, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, ACM MobiCom, and IEEE INFOCOM. He is the inventor of six U.S. and over 100 Chinese pending patents. He received the 2012 Hong Kong Young Scientist Award, the 2014 Hong Kong ICT Awards: Best Innovation, and the 2014 IEEE ComSoc Asia–Pacific Outstanding Young Researcher Award.