Integrating Blockchain Technology with PKI for Secure and Interoperable Communication in 5G and Beyond Vehicular Networks

Abdurahman Fetulhak, Abdelwahab Boualouache, Sidi Mohammed Senouci, Ines El-Korbi, Bouziane Brik, Anlay Fante

Integrating Blockchain Technology with PKI for Secure and Interoperable Communication in 5G and Beyond Vehicular Networks

Fetulhak Abdurahman Shewajo*‡, Abdelwahab Boualouache†, Sidi Mohammed Senouci*, *Senior Member, IEEE,* Ines El-Korbi*, Bouziane Brik§, *Senior Member, IEEE,* Kinde Anlay Fante‡

*DRIVE Lab, University of Burgundy, Nevers, France. e-mail: Firstname.Lastname@u-bourgogne.fr

†FSTM, University of Luxembourg, Luxembourg. e-mail: firstname.lastname@uni.lu

‡Faculty of Electrical and Computer Engineering, Jimma Institute of Technology, Jimma University, Jimma, Ethiopia. e-mail: firstname.middlename@ju.edu.et

§Computer Science Department, College of Computing and Informatics, Sharjah University, Sharjah, UAE, e-mail: (bbrik@sharjah.ac.ae)

***Abstract*—Security and privacy are crucial in V2X networks due to sensitive user information. Public Key Infrastructure (PKI) is widely used in C-ITS to ensure security and privacy. However, the practical implementation of PKI faces challenges in achieving seamless communication across diverse ITS projects worldwide. The absence of interoperability between PKI systems and unresolved issues in existing PKI standards hinder global adoption. Despite available security standardizations using centralized PKI technology for V2X, a universally adopted PKI-based security architecture is necessary. Furthermore, the progress made in 5G V2X technology has demonstrated significant potential for revolutionizing V2X communication in the future. Enhancing the level of trust through integration of the 5G Core Network (5GC) into the PKI security mechanism can lead to more secure and efficient V2X communication. To address these challenges, we propose a blockchain-based architecture that integrates the 5GC network with the PKI infrastructure, aiming to enhance privacy and security in 5G V2X communication. Our solution is designed to be distributed and interoperable, aligned with existing ETSI ITS PKI standard. By utilizing Hyperledger Fabric (HLF) platform, a permissioned blockchain framework, we present the architecture and conduct a comprehensive security analysis to ensure compliance with security and privacy requirements of V2X communications.**

***Index Terms*—5G and Beyond Vehicular Networks; Security and Privacy; Interoperability; Blockchain**

I. Introduction

The vehicular network, also known as vehicle-to-everything (V2X), plays a vital role in Cooperative Intelligent Transportation Systems (C-ITS), enabling communication between vehicles (V2V), vehicle-to-roadside infrastructure (V2I), Vehicle-to-Pedestrians (V2P), and vehicle-to-Network (V2N). With rapid advancements, C-ITS is set to improve traffic efficiency, reduce accidents, and curb air pollution [1].

Currently, no clear radio technology is selected or well-suited for V2X communications [4]. Two main candidates are considered: DSRC, based on IEEE 802.11p/802.11bd, supporting V2V, V2P, and V2I communications [5–7]; and 5G V2X from 3GPP, offering wide coverage, low latency, and high network capacity, making it a strong contender [8]. 5G V2X uses direct V2V, V2P, and V2I communications over PC5 interface, and V2N communication over the LTE/NR Uu interface [8, 9]. V2X communication faces significant threats, such as DDoS, man-in-the-middle, and Sybil attacks, posing risks to security and privacy [2]. Proposed defenses mechanisms encompass symmetric cryptography, identity-based signatures, certificateless cryptography, and ring/group signatures. Nevertheless, challenges persist, including key sniffing, non-repudiation concerns, communication overhead, escrow issues, and computational intensity.

3GPP has specified that security for broadcast and group cast communication via the PC5 interface can rely on application layer security protocols developed by other Standards Developing Organizations (SDOs) such as IEEE or ETSI ITS [12]. However, there's no mandatory solution to integrate these PKI systems into the 3GPP framework. Additionally, the LTE/NR Uu interface also lacks adequate security measures, relying on existing 5GS security (5G-AKA) [1]. This leads to privacy and non-repudiation issues for V2X applications involving location data and the inability to detect malicious ITS entities without further security measures.

On the other hand, conventional PKI systems in C-ITS have limitations like single-point failures, lack of transparency, and insufficient interoperability between PKIs across ITS domains (i.e., ITS systems deployed in different regions or countries). The absence of distributed trust lists and enrollment information hinders mobility and authentication of ITS stations (ITS-Ss), leading to challenges in seamless V2X message authentication across ITS domains. In this context, blockchain technology plays a crucial role. Blockchain is a decentralized and transparent digital ledger that records transactions across multiple nodes, ensuring decentralized and distributed sharing and storage of information.

In this paper, we aim on addressing the security challenges surrounding 5G V2X communication and to overcome the limitations of conventional centralized PKI standards. Our approach involves integrating a PKI system that aligns with the existing PKI standards of other SDOs, like ETSI ITS PKI,

specifically tailored for 5G V2X communication. Notably, we advocate the integration of the 5G core network as a pivotal element in our proposed architecture to enhance management of ITS-S authorization in collaboration with the PKI system. By leveraging this integration, we aim to safeguard the 5GC network resources against misuse by unauthorized or revoked ITS-Ss. In the current work presented in this paper, we contribute to the improvement of 5G V2X security in the following ways.

- Propose a blockchain-based architecture to integrate PKI with the 5GC network, providing enhanced and cooperative application-layer security for 5G and Beyond V2X communication over PC5 and Uu interfaces.
- The proposed architecture enhances the current ETSI ITS PKI by enabling distributed sharing of V2X data among diverse ITS domains, promoting global interoperability. It ensures adaptability, decentralization, and scalability for seamless communication as ITS-Ss traverse different ITS domains.
- Perform a security analysis of the proposed architecture, ensuring adherence to V2X communication security and privacy requirements. We also identify challenges and opportunities in C-ITS for potential research directions.

II. Related Work

PKI is crucial for trust and privacy in V2X communication. As future smart cities embrace connected vehicles, managing decentralized V2X data and interoperable PKI systems presents challenges. Blockchain offers a potential solution, enhancing ITS systems' decentralization, trust, transparency, and security. However, standardized blockchain-based PKIs are still in development. Integrating blockchain with already established PKI standards is currently a more viable option. There are limited works on blockchain-based decentralized PKI architectures that ensure interoperability and compatibility with existing standardized PKIs for C-ITS.

In [13], a decentralized vehicular PKI system links a vehicle's pseudonymous identity to its real identity on the blockchain. However, it lacks consideration for managing PKI information across domains and interoperability. In [14], a decentralized blockchain-based PKI integrates certificate management and revocation for IEEE SCMS-based PKI but lacks clear definitions for revocation and misbehavior handling. The approach in [15] uses a consortium blockchain for multi-domain vehicular networks but is vulnerable to attacks due to pre-loaded long-term pseudonym certificates and lacks compatibility with existing PKI standards.

Existing decentralized PKI architectures, except for [14], lack compatibility with existing PKI standards and do not address PKI integration with the 5GC network architecture. Our proposed architecture ensures detailed integration and backward compatibility of conventional ETSI ITS PKI through blockchain, incorporating 5GC network and PKI entities for distributed management of 5G V2X-related data. Table I summarizes the comparison of related works and our proposed architecture.

III. Architecture Overview

In the proposed architecture there are four components: 1) Blockchain Network; 2) 5GC Network; 3) the PKI and 4) ITS-Ss. Fig. 1 shows an overview of the proposed architecture. The Blockchain network enables collaborative integration and distributed V2X data management, ensuring interoperability across diverse ITS domains. The PKI is responsible for managing certificates of ITS-Ss. The 5GC network is responsible to configure V2X services for ITS-Ss over PC5 or Uu interfaces. ITS-Ss (vehicles, vulnerable road users (VRUs), roadside units (RSUs), and V2X application server (VAS)) obtain certificates from PKI authorities for secure communication.

*1) **The Blockchain Network**:* The proposed blockchain-based architecture utilizes the permissioned blockchain framework Hyperledger Fabric (HLF) with nodes comprising 5GC network peers and PKI authorities, including Root Certificate Authority (RCA), Enrollment Certificate Authority (ECA), Pseudonym Certificate Authority (PCA), and Distribution Center (DC). To efficiently handle V2X-related information across diverse ITS domains, the architecture leverages HLF's "channels." Three channel types are supported, with the first one ("Channel for ITS Domain A/B") dedicated to storing ITS-S's V2X-related data , encompassing V2X service profiles, enrollment, authorization and revocation information. This channel involves peer nodes from the 5GC network (managing ITS-S V2X service profile), ECA (handling enrollment-related information), and PCA (managing authorization or pseudonym certificate details for ITS-S on the blockchain).

The second channel, known as the "intermediary channel" connects ECA peer nodes from diverse ITS domains via the HLF network. It allows the ECA peer nodes, which are also connected to the first channel, to interact with each other and invoke smart contracts to securely transfer V2X related information of an ITS-S when an ITS-S roams from its home ITS domain into a new ITS domains. There is a third channel called "Global channel" for storage and management of trust list information such as Certificate Revocation List (CRL) and Certificate Trust List (CTL) across all ITS domains. The peer nodes of this channel comprise RCAs of all ITS domains for uploading trust list information and DCs for retrieving from the blockchain and distributing it to all ITS domain entities.

*2) **5GC Network**:* Once an ITS-S subscribes to 5G V2X service, its V2X profile, including supported service types, geographic restrictions, and service status, is uploaded to the blockchain. PKI authorities can then issue certificates based on the profile to ensure only authorized ITS-Ss by the 5GC network can request PKI credentials for using V2X service. If V2X service subscription for an ITS-S is revoked, a new transaction with a revoked status code is uploaded on the blockchain.

*3) **Enrollment of ITS-S**:* An ITS-S can request an Enrollment Certificate (EC) from any ECA within an ITS domain, which verifies the V2X profile through a smart contract. Based on the ITS-S's profile and the initial EC request, the ECA approves or rejects the request. If approved, the ECA issues an EC response to the ITS-S and uploads enrollment information onto the blockchain. This information includes the EC, EC's validity period, and the canonical identifier.

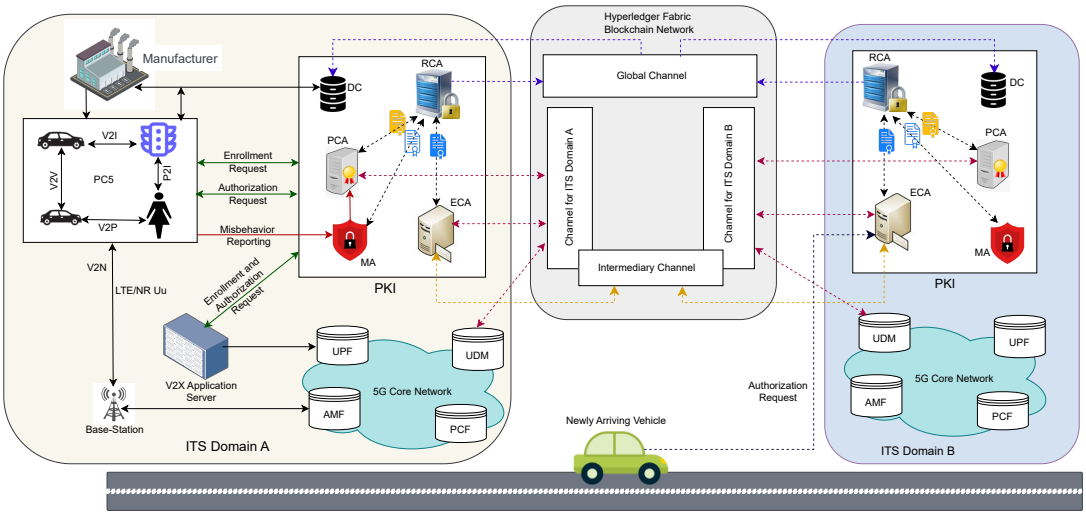

Fig. 1: General overview of the proposed architecture

TABLE I: Comparison of Related Works with the Proposed Architecture.

Scheme	Privacy	Distributed	Interoperable	Independent Domains	Compatibility	Smart Contract
[13]	Yes	Yes	No	No	No	No
[14]	Yes	Yes	Yes	No	Yes	No
[15]	Partial	Yes	Yes	Partial	No	Yes
Our proposal	Yes	Yes	Yes	Yes	Yes	Yes

*4) **Authorization of ITS-S**:* An enrolled ITS-S can request a pseudonym certificate (PC) from any PCA within an ITS domain. The PCA validates the request using a smart contract, ensuring the ITS-S's enrollment status, active V2X service, and revocation status. Based on the validation, the PCA grants or rejects the PC request. The PCA updates PC details on the blockchain using a cryptographic accumulator after providing PC to the ITS-S.

*5) **Misbehaviour Reporting and Certificate Revocation**:* When an ITS-S is flagged for misbehavior, neighboring ITS-Ss report its PC to the Misbehavior Authority (MA). After validation, MA forwards the PC to PCA, which triggers a revocation smart contract. The smart contract traces the PC on the blockchain, and the offending ITS-S's enrollment record is deleted from the ledger.

*6) **Publishing CRL and CTL Information**:* In the ETSI ITS PKI system, the RCA publishes trust list information (CRL and CTL), which is regularly updated to include new trusted ECA and PCA certificates, remove expired ones, and reflect changes in DC access points. In our proposed architecture, RCAs from diverse ITS domains upload CRL and CTL information on the global channel within their domains, enabling each domain to know trusted or revoked certificate authorities.

*7) **Distribution of CRL and CTL Information**:* The proposed architecture represents the DC as one blockchain node. Smart contract functions periodically read the ledger for up-to-date trust information. ITS-Ss can connect with the DC to retrieve up-to-date trust list information.

*8) **Interoperability Across ITS Domains**:* Upon entering a new ITS domain, an ITS-S initiates an authorization process by presenting its unique EC. An ECA peer node at the border validates the EC through a smart contract. If approved, the ECA enrolls the ITS-S in the new domain, granting access to request PCs from PCAs for service access.

IV. Security Analysis

In this section, we analyze the security aspects pertaining to the proposed architecture to prevalent security attacks.

*1) **Resistance to distributed denial of service - DDoS attack**:* The proposed architecture can resist DDoS and single-point failure threats. If a peer node fails, the shared Blockchain ledger allows other nodes to sustain the ITS system, preventing catastrophic failure. This ensures operational continuity even amid compromises or failures in certificate authorities or 5GC network nodes. Nodes can recover data from peers upon restoration, ensuring data integrity and system availability.

*2) **Identity Privacy Preservation**:* In the proposed architecture, safeguarding the identity privacy of ITS-Ss, especially vehicles and VRUs, is a critical consideration. To ensure this protection, the identity information of an ITS-S is stored as private data on the blockchain, accessible exclusively to authorized entities: the 5GC network, the ECA, and the ITS-S itself. In case of disputes, only smart contracts accessible to ECA nodes have the ability to reveal the real identity record from the ledger.

*3) **Traceability and Revocability**:* The proposed identity preservation approach is conditional and requires collaboration between the PCA and ECA. Smart contracts are utilized to trace the PC back to its real identity on the blockchain.

*4) **Unlinkability**:* To bolster privacy and thwart unauthorized access to PC information stored on the blockchain, a

cryptographic accumulator is utilized. This mechanism ensures that the PCs assigned to a particular ITS-S are not directly stored in plaintext, minimizing their visibility to trusted yet inquisitive nodes within the blockchain. This approach effectively reduces the risk of external adversaries linking the PCs to messages that have been signed using those certificates.

*5) **Resistance against tampering attacks**:* Storing ITS-S's V2X data on blockchain prevents tampering and ensures transparency and accountability. Modifications are traceable, holding entities accountable. Blockchain security prevents unauthorized changes by requiring consensus among network nodes.

V. Challenges, Opportunities and Potential Solutions

In this section, some prospective approaches for tackling the evolving challenges in C-ITS systems and conventional PKI standards are discussed as follows.

First, the existing PKI standards have security design ambiguities for managing non-vehicle ITS entities like RSUs and VRUs. It is essential to reevaluate how non-vehicle ITS components are handled within the current PKI standards and explore innovative methods of integration, utilizing blockchain-based PKI, to cater to their distinct behaviors. Addressing the growing role of smartphones in future C-ITS for pedestrians, there's a pressing need for energy-efficient architectures for processing V2X data.

Second, there are cutting-edge solutions like 5G network slicing (NS), Network Function Virtualization (NFV), Software-Defined Networking (SDN), and Multi-access Edge Computing (MEC) that hold promise for resolving future ITS system challenges. Nevertheless, effectively integrating these technologies necessitates additional investigation, such as addressing security concerns in MEC-enabled 5G V2X communication, optimizing resource allocation, ensuring network slicing security, handling Service Level Agreements (SLAs) among diverse slices, ensuring interoperability, securing handover processes, and mitigating vulnerabilities associated with edge and quantum computing.

Third, artificial intelligence (AI) offers a major security boost for C-ITS, but addressing AI vulnerabilities is crucial. Future research should focus on developing secure, privacy-focused AI algorithms for V2X. Techniques like secure multi-party computation, federated learning, and homomorphic encryption must be integrated for privacy compliance. Exploring ethical considerations like algorithmic bias and fairness is essential for responsible AI deployment in C-ITS.

Fourth, it is crucial for research to concentrate on developing streamlined blockchain platforms, optimizing consensus algorithms, considering the QoS requirements within blockchain-based MEC environments for C-ITS, mitigating vulnerabilities associated with blockchain and smart contracts, and establishing practical testing and validation systems.

VI. Conclusion

This paper proposes a blockchain-based architecture to integrate 5G Core Network and ETSI ITS PKI. It enables distributed V2X data management, promotes interoperability across regions, and addresses limitations in current PKI standards. The 5GC network serves as the primary service provider for 5G V2X communication, controlling data management and cooperative authorization of ITS stations. Our architecture aligns with existing PKI standards and utilizes Hyperledger Fabric for decentralized PKI. Ongoing work includes investigating performance and security analysis of the proposed architecture.

Acknowledgment

This work was supported by the 5G-INSIGHT bilateral project, (ID: 14891397) / (ANR-20-CE25-0015-16), funded by the Luxembourg National Research Fund (FNR), and by the French National Research Agency (ANR).

References

[1] Takahito Yoshizawa, Dave Singelée, Jan Tobias Mühlberg, Stéphane Delbruel, Amir Taherkordi, Danny Hughes, Bart Preneel, "A Survey of Security and Privacy Issues in V2X Communication Systems," ACM Comput. Surv. 55(9): 185:1-185:36 (2023).

[2] European Road Safety Observatory Annual statistical report on road safety in the EU 2020. https://road-safety.transport.ec.europa.eu/system/files/2021-07/asr2020.pdf. Accessed on March 2023.

[3] J. P. Monteuuis et al., "Securing PKI Requests for C-ITS Systems," 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 2017, pp. 1-8, doi: 10.1109/ICCCN.2017.8038492.

[4] Badis Hammi, Jean-Philippe Monteuuis, Jonathan Petit, "PKIs in C-ITS: Security functions, architectures and projects: A survey," Vehicular Communications, Volume 38, 2022, 100531, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2022.100531.

[5] JB. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," Proceedings of the IEEE, vol. 99, no. 7, pp. 1162-1182, 2011.

[6] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities," in IEEE Std 1609.2.1-2022 (Revision of IEEE Std 1609.2.1-2020) , vol., no., pp.1-261, 30 June 2022, doi: 10.1109/IEEESTD.2022.9810154.

[7] Wireless LAN Medium Access Control (MAC) Phys. Layer(PHY) Specications Amendment 6: Wireless Access Vehicular Environments, IEEE Standard 802.11p-2010, 2010.

[8] ETSI TS 123 287: V16.3.0 (2020-07). 5G; Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services (3GPP TS 23.287 version 16.3.0 Release 16).

[9] ETSI EN 302 665: V1.1.1 (2010-09). Intelligent Transport Systems (ITS); Communications Architecture.

[10] ETSI TS 102 941 V1.4.1 (2021-01). Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.

[11] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release from preparatory phase of C-ITS Delegated Regulation, 13rd March 2019. Available online at https://cpoc.jrc.ec.europa.eu/Documentation.html

[12] ETSI TS 133 536 V16.0.0 (2020). LTE; 5G; Security aspects of 3GPP support for advanced V2X services (Release 16).

[13] I. Agudo, M. Montenegro-Gómez and J. Lopez, "A Blockchain Approach for Decentralized V2X (D-V2X)," IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 4001-4010, May 2021, doi: 10.1109/TVT.2020.3046640.

[14] E. Kristianto, V. -L. Nguyen and P. -C. Lin, "Decentralized Public-Key Infrastructure With Blockchain in V2X Communications: Promising or Only Euphoria?," in IEEE Security & Privacy, vol. 20, no. 4, pp. 40-50, July-Aug. 2022, doi: 10.1109/MSEC.2022.3141727.

[15] D. Chulerttiyawong and A. Jamalipour, "A Blockchain Assisted Vehicular Pseudonym Issuance and Management System for Conditional Privacy Enhancement," in IEEE Access, vol. 9, pp. 127305-127319, 2021, doi: 10.1109/ACCESS.2021.3112013.