Secure Data Provenance in Internet of Vehicles with Verifiable Credentials for Security and Privacy

Anuj Nepal, Robin Doss, Frank Jiang
Deakin Cyber Research and Innovation Centre (Deakin Cyber)
Deakin University, Geelong, Australia

***Abstract*—The emergence of the Internet of Vehicles (IoVs) has also exposed security challenges that require advanced strategies to maintain secure data provenance (SDP) and ensure data credibility and anomaly detection. This paper introduces an innovative framework tailored for the dynamic and distributed nature of IoVs that enables the secure tracing of data origins and ensures the reliability of data through plausibility checks. Our approach leverages the principles of decentralized SDP using Verifiable Credentials (VCs) and distributed ledger technology (DLT) to establish a traceable and tamper-evident data lineage, enhancing the integrity and authenticity of vehicular communications. To address the complexities of anomaly detection, we integrate checks that scrutinize data streams for abnormal patterns, enabling the timely identification and mitigation of potential security breaches. We also propose a robust mechanism to assess data plausibility, ensuring that only credible and verifiable data influence the decision-making processes in the IoVs ecosystem. Through detailed experimentation and analysis, our methodology demonstrates significant improvements in securing IoVs against common threats such as impersonation, data tampering, and privacy breaches. This fosters a trustworthy and resilient vehicular network environment.**

***Index Terms*—Verifiable Credentials, Secure Data Provenance, Data Plausibility, Location Verification, Source Authentication, Data Privacy, Internet of Vehicles, Data Integrity.**

I. Introduction

The Internet of Vehicles (IoVs) is swiftly becoming an integral component of the smart transportation ecosystem, enabling a network of connected vehicles that communicate with each other and with roadside units (RSUs) to facilitate a more efficient, safe, and intelligent transportation system. This integration is set to redefine vehicular dynamics, projected to connect an unprecedented number of vehicles. However, the rapid expansion and the inherent complexity of IoVs networks have surfaced pronounced challenges in communication, security, and privacy, as the dynamic and multi-hop nature of IoVs poses many vulnerabilities.

The integration of connected vehicles into crucial sectors has exposed significant limitations in traditional security frameworks, which were designed for more static and predictable network environments. These frameworks struggle with the scalability and security demands of the dynamic IoVs landscape, leading to potential risks in the security and privacy domain. Secure data provenance (SDP) has emerged as a promising mechanism which addresses various security and privacy aspects. In the IoVs, data provenance refers to the tracing and verification of data origins, movements, and transformations across the network. Ensuring SDP is vital for maintaining the trustworthiness of vehicular communications and supporting critical decisions in autonomous driving, traffic management, and vehicular safety systems. As SDP for IoVs is still in the developing stage and much research has not provided a complete SDP framework that addresses every aspect of it, it requires a robust framework to ensure the authenticity, integrity, and confidentiality of the vehicular data that traverse its vast network. Traditional security mechanisms designed primarily for more static and centralized networks are often found wanting in the face of the dynamic and distributed nature of IoVs. This discrepancy not only strains scalability but also exposes the network to various security vulnerabilities, undermining the trust and reliability essential for IoVs operations. Our study advances the IoVs domain [1] by leveraging Verifiable Credentials (VCs) [2] and distributed ledger technology (DLT) [3], robust RSU infrastructure, and advanced cryptographic measures to maintain decentralized SDP protocol for robust security, privacy, and trust in vehicular communications.

II. Motivation

In the landscape of IoVs, SDP focuses on various aspects of security and privacy aspects rather than the integrity of data only, facilitating a more agile and secure data exchange. This provenance-centric approach is advantageous for IoVs, where the origin and integrity of the data are more critical than direct vehicle-to-vehicle connections. This shift to a provenance-centric approach is advantageous for IoVs, where the origin and integrity of data are more critical than the direct vehicle-to-vehicle connections. However, while SDP enhances the system's security and efficiency, it also exposes the network to unique vulnerabilities such as replay, impersonation, data falsification, and data tampering attacks, exploiting the decentralized and multi-hop nature of IoVs, thus posing risks to the security and privacy and the overall network efficiency.

Previous research has primarily focused on isolated security threats and only a few aspects of SDP in IoVs, resulting in a fragmented and costly approach. The existing SDP techniques face several challenges: being reliant on expensive hardware, needing to execute complex computations tailored to specific devices, vulnerable to physical attacks and cloning, and lacking privacy preservation [4]- [20]. These issues underscore the urgent need for innovative solutions through the exploration of new perspectives. Our study addresses this limitation by proposing a unified SDP protocol for IoVs that not only

2833-292X/24/$31.00 ©2024 IEEE
DOI 10.1109/DSN-S60304.2024.00025

identifies but also mitigates various attacks. Motivated by the urgent need to enhance the security and trustworthiness of IoVs, our research aims to solidify the transition to a more secure vehicular environment, thereby improving the scalability and security of vehicle-to-everything connectivity cost-effectively and efficiently.

Our research explores several critical facets within the IoVs domain:

- **Decentralized data provenance protocol:** Established a protocol leveraging VCs and distributed ledger technology (DLT) for authenticating and ensuring the integrity of data sources in IoVs's dynamic multi-hop environments.
- **Comprehensive security and privacy solution:** Developed a framework that not only authenticates the source identity, location, and data integrity but also enhances the privacy of data and plausibility of the data across the network.
- **Robust attack mitigation strategies:** Implemented measures to safeguard against impersonation, replay, data falsification and data tampering attacks, reinforcing the overall trust and security in IoVs communication systems.
- **Advanced security analysis:** Conducted a thorough formal and informal analysis to validate the resilience of our protocol against a spectrum of potential cybersecurity threats.
- **Quantum-safe solution:** Working on a strategy to provide a quantum-safe solution to protect against future attacks with the help of quantum systems.

III. Proposed Framework and Methodology

This section outlines the high-level architectural framework of our SDP protocol for IoVs, aiming to bolster the integrity and trustworthiness of vehicular networks. Our proposed architecture uses VCs and DLT to improve connectivity and security within IoVs, address the unique challenges of the network and exploit its strengths. It accommodates a wide range of vehicular devices, each integrating with the decentralized network for secure and reliable data exchange. The framework encompasses comprehensive attack detection and mitigation strategies, ensuring robust defence mechanisms against various cyber threats. The architecture of SDP in IoVs is depicted in Figure 1.

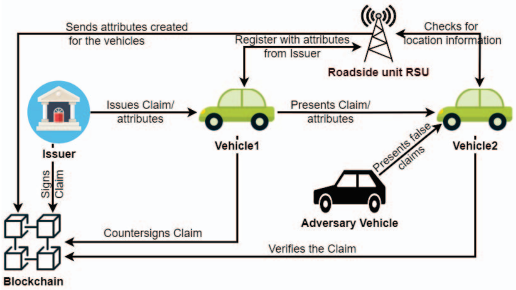

Fig. 1: SDP architecture in IoVs

The key components of our SDP framework for the IoVs include the decentralized protocol leveraging VCs and DLT for data authentication, and the infrastructure that supports dynamic multi-hop communications. Our framework processes data through these components, ensuring secure transmission and accurate origin verification. In addition, we integrate a data plausibility check module to detect and classify various attacks. For countermeasures, we have developed techniques such as cryptographic validation and adaptive security mechanisms tailored to IoV conditions, which effectively distinguish between authentic and malicious activities. Scyther [21] is used as a security verification tool to rigorously evaluate the SDP framework. It was thoroughly tested and confirmed that it adheres to the Scyther confidentiality and authentication criteria against several types of attacks. The effectiveness of our architecture was validated through simulations, showing a high accuracy of 96% in attack detection and robustness in securing IoVs communications, confirming our framework's capability to enhance the trustworthiness and reliability of the IoVs ecosystem.

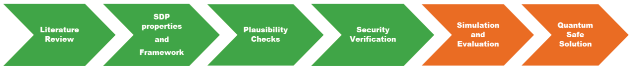

Fig. 2: Phases of Work for SDP in IoVs

In a nutshell, our work phases are depicted in Figure 2 which highlights completed phases (green arrows) and ongoing work (orange arrows). This framework enhances security across IoVs by utilizing VCs and a decentralized network approach, offering a scalable and efficient solution that elevates the standards of resilience and trust in vehicular communications.

IV. Conclusion

In conclusion, our research concentrates on bolstering the security, efficiency, and trustworthiness of the IoVs through the implementation of the SDP protocol. This protocol integrates VCs and DLT to authenticate and validate the identity of data sources, along with RSUs, and cryptographic functions, to address significant security issues such as impersonation, replay, data falsification, and data manipulation attacks. To combat these vulnerabilities, we have executed plausibility checks for anomaly detection and applied cryptographic strategies to ensure data integrity and privacy. The protocol's effectiveness and security, affirmed through the Scyther security verification tool, illustrates its proficiency in meeting the desired security objectives within multi-hop environments. Our ongoing efforts are directed towards experimental evaluations to determine protocol efficiency and the development of quantum-safe solutions to protect against prospective cyber threats, thus creating a secure, reliable, and scalable IoV ecosystem.

Acknowledgements

This research is funded by the Australian Government Automotive Engineering Graduate Program and iMOVE CRC and supported by the Cooperative Research Centres program, an Australian Government initiative.

References

[1] A. Nepal, R. Doss and F. Jiang, "Secure Data Provenance for Internet of Vehicles with Verifiable Credentials," 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2023, pp. 0210-0218, doi: 10.1109/UEMCON59035.2023.10315994.

[2] "Verifiable Credentials Data Model v2.0," Verifiable Credentials Data Model v2.0, Mar. 16, 2023. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/.

[3] X. Wang, P. Zeng, N. Patterson, F. Jiang and R. Doss, "An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology," in IEEE Access, vol. 7, pp. 45061-45072, 2019, doi: 10.1109/ACCESS.2019.2909004.

[4] M. N. Aman, K. C. Chua, and B. Sikdar, "Secure Data Provenance for the Internet of Things,", in Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi, United Arab Emirates, 2017, pp. 11–14.

[5] M. Elkhodr, B. Alsinglawi and M. Alshehri, "Data Provenance in the Internet of Things," 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Poland, 2018, pp. 727-731, doi: 10.1109/WAINA.2018.00175.

[6] U. Javaid, M. N. Aman, and B. Sikdar, "BlockPro: Blockchain Based Data Provenance and Integrity for Secure IoT Environments,', in Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems, Shenzhen, China, 2018, pp. 13–18.

[7] S. Ali, G. Wang, M. Z. A. Bhuiyan and H. Jiang, "Secure Data Provenance in Cloud-Centric Internet of Things via Blockchain Smart Contracts," 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 2018, pp. 991-998, doi: 10.1109/SmartWorld.2018.00175.

[8] M. S. Siddiqui, A. Rahman, and A. Nadeem, "Secure Data Provenance in IoT Network using Bloom Filters,", Procedia Computer Science, vol. 163, pp. 190–197, 2019.

[9] U. Javaid, M. N. Aman and B. Sikdar, "DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 2019, pp. 1-5, doi: 10.1109/VTC-Spring.2019.8746499.

[10] Z. Tang and S. L. Keoh, "An Efficient Scheme to Secure Data Provenance in Home Area Networks," 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 115-120, doi: 10.1109/5GWF49715.2020.9221402.

[11] U. Javaid, M. N. Aman and B. Sikdar, "A Scalable Protocol for Driving Trust Management in Internet of Vehicles With Blockchain," in IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11815-11829, Dec. 2020, doi: 10.1109/JIOT.2020.3002711.

[12] M. N. Aman, M. H. Basheer and B. Sikdar, "A Lightweight Protocol for Secure Data Provenance in the Internet of Things Using Wireless Fingerprints," in IEEE Systems Journal, vol. 15, no. 2, pp. 2948-2958, June 2021, doi: 10.1109/JSYST.2020.3000269.

[13] M. N. Aman, U. Javaid and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 1123-1139, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3010893.

[14] M. Kamal, G. Srivastava and M. Tariq, "Blockchain-Based Lightweight and Secured V2V Communication in the Internet of Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 3997-4004, July 2021, doi: 10.1109/TITS.2020.3002462.

[15] H. Hamadeh and A. Tyagi, "Privacy Preserving Data Provenance Model Based on PUF for Secure Internet of Things," 2019 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), Rourkela, India, 2019, pp. 189-194, doi: 10.1109/iSES47678.2019.00050.

[16] M. N. Aman, M. H. Basheer and B. Sikdar, "Data Provenance for IoT using Wireless Channel Characteristics and Physically Unclonable Functions," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8761945.

[17] M. Sigwart, M. Borkowski, M. Peise, S. Schulte, and S. Tai, "Blockchain-Based Data Provenance for the Internet of Things," in Proceedings of the 9th International Conference on the Internet of Things, Bilbao, Spain, 2019.

[18] M. N. Aman, M. H. Basheer and B. Sikdar, "Data Provenance for IoT With Light Weight Authentication and Privacy Preservation," in IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10441-10457, Dec. 2019, doi: 10.1109/JIOT.2019.2939286.

[19] M. N. Aman, M. H. Basheer and B. Sikdar, "Two-Factor Authentication for IoT With Location Information," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3335-3351, April 2019, doi: 10.1109/JIOT.2018.2882610.

[20] M. Kamal and S. Tariq, "Light-Weight Security and Data Provenance for Multi-Hop Internet of Things," in IEEE Access, vol. 6, pp. 34439-34448, 2018, doi: 10.1109/ACCESS.2018.2850821.

[21] C. J. F. Cremers, Scyther: semantics and verification of security protocols[M], Netherlands:Eindhoven University of Technology, 2006.