Survey on Security Credential Management System and Secure V2X by ChatGPT

ChatGPT

Robot Sam Chang
robot.sam.chang@gmail.com

***Abstract*—Due to the importance of security for Vehicular Ad-hoc NETwork (VANET), Security Credential Management System (SCMS) and Secure Vehicle-to-Everything (V2X) communication are surveyed in this study for SCMS researchers. This study designs sequential prompts that are presented in Section II to supervise ChatGPT for generating the reviews of SCMS and secure V2X. The hot research topics of security and privacy in V2X communications, authentication and access control in V2X networks, key management in V2X networks, and security and privacy in SCMS have been summarized and discussed. Finally, the limitations of SCMS and secure V2X are also surveyed for indicating the future work.**

***Index Terms*—Security credential management system, SCMS, secure V2X, ChatGPT**

I. Introduction

The objectives of a Security Credential Management System (SCMS) and Secure Vehicle-to-Everything (V2X) communication are to provide secure and trusted communication between vehicles and infrastructure components, to manage the distribution of security credentials, and to ensure the authenticity and integrity of the information exchanged between devices.

Provide secure and trusted communication between vehicles and infrastructure components: The first objective of SCMS and Secure V2X communication is to provide secure and trusted communication between vehicles and infrastructure components in a connected vehicle environment. This is achieved by implementing strong authentication and encryption mechanisms, and by ensuring that only authenticated and authorized devices are granted access to the communication network [1], [2].

Manage the distribution of security credentials: Another objective of SCMS and Secure V2X communication is to manage the distribution of security credentials, including the issuance, renewal, and revocation of security credentials. This is necessary to ensure that the security credentials are up-to-date and valid, and that any compromised or unauthorized credentials are promptly revoked [3], [4].

Ensure the authenticity and integrity of the information exchanged between devices: The final objective of SCMS and Secure V2X communication is to ensure the authenticity and integrity of the information exchanged between devices. This is accomplished through the use of security measures, such as digital signatures and encryption, which ensure that information is not tampered with or altered during transmission [5], [6].

In summary, the objectives of SCMS and Secure V2X communication are to provide secure and trusted communication between vehicles and infrastructure components, manage the distribution of security credentials, and ensure the authenticity and integrity of the information exchanged between devices. These objectives are crucial for the secure and efficient functioning of connected vehicle environments.

SCMS and secure V2X are important issues to build secure communications in Vehicular Ad-hoc NETwork (VANET), so this study reviews and summarizes the hot research topics of SCMS and secure V2X to obtain a guildline for SCMS and secure V2X beginners. For surveying the relevant studies, Robot Sam Chang supervises ChatGPT (i.e. an intelligent content generator) [7] to write the major contents of this manuscript through sequential prompts. The contributions of this study are summarized as follows.

- For generating the major contents of this manuscript, Robot Sam Chang proposes and creates original sequential prompts to write the surveys of SCMS and secure V2X through ChatGPT.
- For correcting the generation contents from ChatGTP, Robot Sam Chang rewrites the generation contents and removes the incorrect contents.
- For highlighting the contributions from Robot Sam Chang, the abstract, Section II and Section IX of this manuscript are written by Robot Sam Chang.

Nine sections are described in this manuscript. The proposed sequential prompts are shown in Section II for generating the surveys of SCMS and secure V2X by ChatGPT. The overview of SCMS and secure V2X including four research directions is presented in Section III, and the detailed hot topics of each research direction are summarized in Sections IV, V, VI, and VII. Moreover, Section VIII discusses the limitations SCMS and secure V2X for future work. Finally, the conclusions of this study are illustrated in Section IX.

II. Method

This study uses sequential prompts to generate the contents of each section through ChatGPT. The used prompts for each section are listed as follows.

- Section I is generated based on the prompt ”Please summarize the objectives of security credential management system and secure V2X, and please present each objective in detail with citations; furthermore give some references from refereed journals to support these objectives”.

- Section III is generated based on the prompt "Please summarize top four research topics of security credential management system and secure V2X; furthermore, please give some references from refereed journals to support these topics".
- Section IV is generated based on the prompt "Please summarize top four research topics of security and privacy in V2X communications; furthermore, please give some references from refereed journals to support these topics".
- Section V is generated based on the prompt "Please summarize top four research topics of authentication and access control in V2X networks; furthermore, please give some references from refereed journals to support these topics".
- Section VI is generated based on the prompt "Please summarize top four research topics of key management in V2X networks; furthermore, please give some references from refereed journals to support these topics".
- Section VII is generated based on the prompt "Please summarize top four research topics of security and privacy in security credential management system; furthermore, please give some references from refereed journals to support these topics".
- Section VIII is generated based on the prompt "Please summarize the limitations of security credential management system and secure V2X, and please present each limitation in detail; furthermore give some references from refereed journals to support the presentation" (shown in Fig. 1).

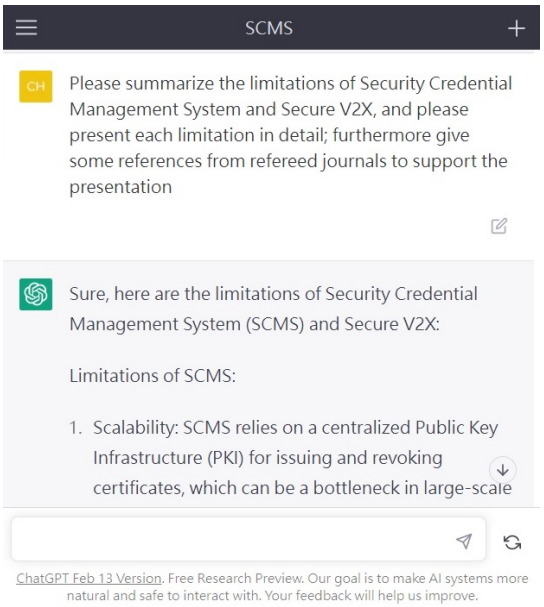

Fig. 1. The prompt for generating the contents of Section III [7].

III. The Overview of SCMS and Secure V2X

The top four research topics of SCMS and Secure V2X (shown in Fig. 2) are illustrated in the following subsections.

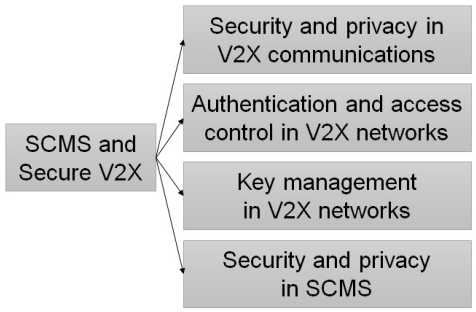

Fig. 2. The research topics of SCMS and Secure V2X

A. Security and privacy in V2X communications

The security and privacy of V2X communications is a critical issue that has received significant attention in recent years. Researchers have proposed various approaches to enhance the security and privacy of V2X communications, such as lightweight encryption algorithms, anonymous authentication schemes, and secure key management protocols [8], [9].

B. Authentication and access control in V2X networks

Authentication and access control are critical for securing V2X networks. Researchers have proposed various authentication and access control schemes, such as identity-based authentication, attribute-based access control, and trust-based access control [2], [10].

C. Key management in V2X networks

Key management is crucial for securing V2X networks. Researchers have proposed various key management schemes, such as certificate-based key management, group key management, and hybrid key management [11], [12].

D. Security and privacy in SCMS

SCMS is a critical component of V2X security infrastructure. Researchers have proposed various approaches to enhance the security and privacy of SCMS, such as lightweight certificate revocation schemes, secure communication protocols, and intrusion detection systems [13], [14].

IV. The Hot Topics of Security and Privacy in V2X Communications

This section presents the summary of four research topics on security and privacy in V2X communications (shown in Fig. 3) along with some references from refereed publications.

A. Lightweight and secure authentication schemes

Efficient authentication schemes are required in V2X communications to ensure security and privacy. Researchers have proposed various lightweight and secure authentication schemes for V2X communications, such as certificateless authentication and privacy-preserving authentication schemes [15], [16].

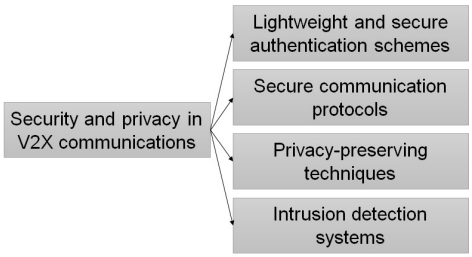

Fig. 3. The research topics of security and privacy in V2X communications

B. Secure communication protocols

Various secure communication protocols have been proposed for V2X communications, such as group key agreement protocols, privacy-preserving protocols, and secure message dissemination protocols [17], [18].

C. Privacy-preserving techniques

Privacy-preserving techniques are essential to protect the privacy of V2X users, such as location privacy and identity privacy. Researchers have proposed various privacy-preserving techniques, such as pseudonymous certificates, location obfuscation, and anonymous message authentication [13], [19].

D. Intrusion detection systems

Intrusion detection systems are used to detect and prevent various security attacks in V2X networks. Researchers have proposed various intrusion detection systems, such as behavior-based intrusion detection systems, machine learning-based intrusion detection systems, and anomaly-based intrusion detection systems [20], [21].

V. The Hot Topics of Authentication and Access Control in V2X Networks

This section presents the four research topics related to authentication and access control in V2X networks (shown in Fig. 4) along with some references from refereed publications.

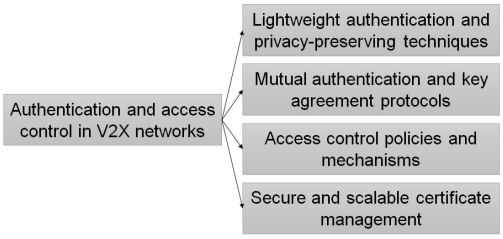

Fig. 4. The research topics of authentication and access control in V2X networks

A. Lightweight authentication and privacy-preserving techniques

With the increasing number of V2X devices and the need for secure communication, lightweight authentication techniques that can provide privacy and security are becoming more important. Some of the techniques include Identity-Based Encryption (IBE), Attribute-Based Encryption (ABE), and Anonymous Authentication (AA) [22].

B. Mutual authentication and key agreement protocols

Mutual authentication is an essential requirement for secure communication in V2X networks. Key agreement protocols like Elliptic Curve Diffie-Hellman (ECDH) and Password-Authenticated Key Exchange (PAKE) can provide secure mutual authentication [23].

C. Access control policies and mechanisms

Access control policies and mechanisms can prevent unauthorized access and ensure the confidentiality and integrity of V2X communication. Techniques like Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) can be used to define and enforce access control policies [24].

D. Secure and scalable certificate management

Certificate management is crucial for secure communication in V2X networks. Traditional Public Key Infrastructure (PKI) based approaches may not be scalable and efficient for V2X networks. Techniques like Certificateless Public Key Cryptography (CL-PKC) and Distributed PKI (DPKI) can be used to provide scalable and secure certificate management [25].

VI. The Hot Topics of Key Management in V2X Networks

This section presents the four research topics related to key management in V2X networks (shown in Fig. 5) along with some references from refereed publications.

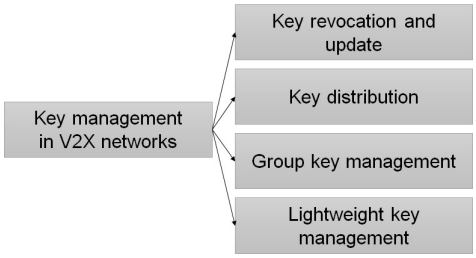

Fig. 5. The research topics of key management in V2X networks

A. Key revocation and update

Since V2X networks may involve a large number of devices and vehicles, key revocation and update become essential to ensure the security of the system. Researchers have proposed various methods to achieve efficient key revocation and update, such as using hash chains and symmetric key encryption algorithms [26].

B. Key distribution

Key distribution is a critical issue in V2X networks, as it determines the ability of the system to authenticate and securely communicate with other vehicles and devices. Various methods have been proposed for key distribution, including centralized and decentralized approaches [27].

C. Group key management

Group key management involves managing the keys of a group of vehicles or devices in V2X networks. This is particularly important in safety-critical applications, such as collision warning systems, where groups of vehicles need to securely exchange information in real-time. Researchers have proposed different group key management schemes to improve the security and efficiency of V2X networks [28].

D. Lightweight key management

As V2X networks often involve resource-constrained devices, such as sensors and small-scale devices, lightweight key management schemes are required. These schemes aim to reduce the computational overhead and energy consumption of key management operations while maintaining the required level of security. Researchers have proposed various lightweight key management schemes, such as elliptic curve cryptography-based schemes and lightweight certificate management schemes [29].

VII. The Hot Topics of Security and Privacy in SCMS

This section presents the four research topics related to security and privacy in SCMS (shown in Fig. 6) along with some references from refereed publications.

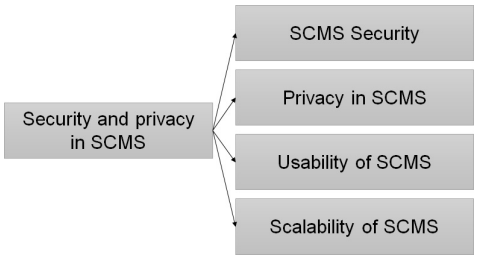

Fig. 6. The research topics of security and privacy in SCMS

A. SCMS Security

One of the primary concerns with SCMS is its security. Researchers have explored various security issues and proposed solutions to make SCMS more secure. Some of the issues include certificate revocation, certificate management, and certificate authentication. For example, a paper by Wu et al. proposed a certificate management framework for SCMS that is resilient to different types of attacks [30].

B. Privacy in SCMS

Another important aspect of SCMS is privacy. Researchers have explored ways to enhance the privacy of vehicles and their users in SCMS. One approach is to use pseudonyms that are periodically changed to avoid tracking. A paper by Blomer et al. proposed a privacy-enhanced SCMS that uses group signatures to protect the privacy of vehicles and their users [31].

C. Usability of SCMS

The usability of SCMS is also a critical research area. SCMS needs to be easy to use and deploy for both vehicle manufacturers and end-users. Researchers have explored different ways to simplify SCMS, including using lightweight cryptographic algorithms and automating the certificate management process. For example, a paper by Wang et al. proposed a lightweight certificate management scheme that reduces the computational overhead of SCMS [32].

D. Scalability of SCMS

As the number of connected vehicles increases, the scalability of SCMS becomes a concern. Researchers have proposed solutions to address this issue, including distributed certificate management systems and efficient key management schemes. For example, a paper by Zhang et al. proposed a distributed certificate management scheme for SCMS that improves the scalability and efficiency of the system [33].

VIII. The limitations of SCMS and Secure V2X

A. The limitations of SCMS

Scalability: SCMS relies on a centralized Public Key Infrastructure (PKI) for issuing and revoking certificates, which can be a bottleneck in large-scale deployments. The centralized architecture of SCMS makes it difficult to manage a large number of connected vehicles [34], [35].

Single point of failure: The centralized architecture of SCMS also makes it vulnerable to single-point-of-failure attacks. If the central PKI is compromised, the entire system can be rendered useless [34], [35].

Complexity: SCMS is a complex system that requires significant expertise to implement and operate. The complexity of SCMS can result in deployment and maintenance challenges [34], [35].

Privacy: SCMS does not provide adequate privacy protection for users. Although pseudonyms are used to protect user identities, the system can still be vulnerable to tracking attacks [34], [35].

B. The limitations of Secure V2X

Availability: Secure V2X relies on a reliable and uninterrupted network connection for the exchange of messages. In the absence of network connectivity, Secure V2X cannot function properly [36]- [38].

False positives: Secure V2X uses a trust-based model to validate received messages. However, this can result in false positives, where valid messages are incorrectly rejected due to a lack of trust [36]- [38].

Privacy: Secure V2X does not provide adequate privacy protection for users. Although pseudonyms are used to protect user identities, the system can still be vulnerable to tracking attacks [36]- [38].

Scalability: As the number of connected vehicles increases, the scalability of Secure V2X becomes a concern. The system needs to be able to handle a large number of connected vehicles while maintaining a high level of security [36]- [38].

IX. Conclusions and Future Work

This study proposes sequential prompts including the research directions of SCMS and the hot topics of each direction to summarize the surveys of relevant studies by ChatGPT. In accordance with the sequential prompts, the hot topics of security and privacy in V2X communications, authentication and access control in V2X networks, key management in V2X networks, and security and privacy in SCMS have been discussed, and the research issues of each topic have been indicated. In the future, more detailed sequential prompts could be designed to write deeper reviews.

Acknowledgment

The study was major written by ChatGPT. Thank OpenAI Inc. for the ChatGPT platform (i.e. https://chat.openai.com/).

References

[1] M. Hasan, S. Mohan, T. Shimizu, H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," IEEE Transactions on Intelligent Vehicles, vol. 5, no. 4, pp. 693–713, 2020.

[2] Z. Benyamina, K. Benahmed, F. Bounaama, "ANEL: A Novel Efficient and Lightweight Authentication Scheme for Vehicular Ad Hoc Networks," Computer Networks, vol. 164, p. 106899, 2019.

[3] T. Yoshizawa et al., "A Survey of Security and Privacy Issues in V2X Communication Systems," ACM Computing Surveys, vol. 55, no. 9, p. 185, 2023.

[4] B. Brecht et al., "A Security Credential Management System for V2X Communications," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 12, pp. 3850–3871, 2018.

[5] Y. Qian, F. Ye, H.-H. Chen, "Security in V2X Communications," Security in Wireless Communication Networks, pp.311-331, 2022.

[6] C. Xu, X. Huang, M. Ma, H. Bao, "A Secure and Efficient Message Authentication Scheme for Vehicular Networks based on LTE-V," KSII Transactions on Internet and Information Systems, vol. 12, no. 6., pp. 2841–2860, 2018.

[7] ChatGPT, Feb 13 Version. OpenAI Inc., 2023. url: https://chat.openai.com/

[8] T. Nandy et al., "An Enhanced Lightweight and Secured Authentication Protocol for Vehicular Ad-hoc Network," Computer Communications, vol. 177, pp. 57–76, 2021.

[9] X. Zhang, W. Wang, L. Mu, C. Huang, H. Fu, C. Xu , "Efficient Privacy-Preserving Anonymous Authentication Protocol for Vehicular Ad-Hoc Networks," Wireless Personal Comm., vol. 120, pp. 3171—3187, 2021.

[10] B. Akwirry, N. Bessis, H. Malik, and S. McHale, "A Multi-Tier Trust-Based Security Mechanism for Vehicular Ad-Hoc Network Communications," Sensors, vol. 22, no. 21, p. 8285, 2022.

[11] H. Tan, M. Ma, H. Labiod, A. Boudguiga, J. Zhang, P. H. J. Chong, "A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks," IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 9570–9584, 2016.

[12] R. Ramamoorthy, M. Thangavelu, "Group Based Dual Mode Key Management Scheme for Secure Communication in Vehicular Ad Hoc Networks," Wireless Personal Comm., vol. 120, pp. 949–973, 2021.

[13] Y. Yao et al., "LPC: A Lightweight Pseudonym Changing Scheme with Robust Forward and Backward Secrecy for V2X," Ad Hoc Networks, vol. 123, p. 102695, 2021.

[14] J. J. Haas, Y.-C. Hu, K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking, pp. 89—98, 2009. doi: 10.1145/1614269.1614285.

[15] S. Taha, M. Alhassany, X. Shen, "Lightweight Handover Authentication Scheme for 5G-Based V2X Communications," Proceedings of 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8648020.

[16] H. J. Nath, H. Choudhury, "A Privacy-preserving Mutual Authentication Scheme for Group Communication in VANET," Computer Communications, vol. 192, pp. 357–372, 2022.

[17] B. Ma et al., "An Authentication and Secure Communication Scheme for In-Vehicle Networks Based on SOME/IP," Sensors, vol. 22, no. 2, p. 647, 2022

[18] S. A. A. Hakeem, H. Kim, "Multi-Zone Authentication and Privacy-Preserving Protocol (MAPP) Based on the Bilinear Pairing Cryptography for 5G-V2X," Sensors, vol. 21, no. 2, p. 665, 2021.

[19] J. Wantoro, M. Mambo, "Efficient and Privacy-Preserving Certificate Activation for V2X Pseudonym Certificate Revocation," Journal of Sensor and Actuator Networks, vol. 11, no. 3, p. 51, 2022.

[20] S. Rajapaksha et al., "AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey," ACM Computing Surveys, vol. 55, no. 11, p. 237, 2023.

[21] J. Liang, J. Chen, Y. Zhu, R. Yu, "A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position," Applied Soft Computing, vol. 75, pp. 712–727, 2019.

[22] I. Ali, M. Faisal, S. Abbas, "A Survey on Lightweight Authentication Schemes in Vertical Handoff," International Journal of Cooperative Information Systems, vol. 26, no. 1, pp. 1630001, 2017.

[23] F. Hao, P. C. van Oorschot, "SoK: Password-Authenticated Key Exchange – Theory, Practice, Standardization and Real-World Lessons," Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, pp. 697—711, 2022. doi: 10.1145/3488932.3523256.

[24] H. Tan, W. Zheng, Y. Guan, R. Lu, "A Privacy-Preserving Attribute-Based Authenticated Key Management Scheme for Accountable Vehicular Communications," IEEE Transactions on Vehicular Technology, 2022, doi: 10.1109/TVT.2022.3220410.

[25] A. Wasef, Y. Jiang and X. Shen, "ECMV: Efficient Certificate Management Scheme for Vehicular Networks," Proceedings of 2008 IEEE Global Telecommunications Conference, New Orleans, LA, USA, 2008, doi: 10.1109/GLOCOM.2008.ECP.129.

[26] A. Alrawais, A. Alhothaily, B. Mei, T. Song, X. Cheng, "An Efficient Revocation Scheme for Vehicular Ad-Hoc Networks," Procedia Computer Science, vol. 129, pp. 312–318, 2018. doi: 10.1016/j.procs.2018.03.081.

[27] C. Li, S. Ji, X. Zhang, H. Wang, D. Li, H. Liu, "An Effective and Secure Key Management Protocol for Message Delivery in Autonomous Vehicular Clouds," Sensors, vol. 18, no. 9, p. 2896, Aug. 2018.

[28] S. Gillani, F. Shahzad, A. Qayyum, R. Mehmood, "A Survey on Security in Vehicular Ad Hoc Networks," Lecture Notes in Computer Science, vol. 7865, pp. 59—74, 2013. doi: 10.1007/978-3-642-37974-1_5.

[29] R. Melki, H. N. Noura, A. Chehab, "Lightweight and Secure D2D Authentication & Key Management Based on PLS," Proceedings of 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 2019, doi: 10.1109/VTCFall.2019.8891531.

[30] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, R. Goudy, "A Security Credential Management System for V2X Communications," arXiv, arXiv:1802.05323, 2018. doi: 0.48550/arXiv.1802.05323.

[31] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, "A security credential management system for V2V communications," Proceedings of 2013 IEEE Vehicular Networking Conference, Boston, MA, USA, 2013, pp. 1-8, doi: 10.1109/VNC.2013.6737583.

[32] W. Hathal, H. Cruickshank, Z. Sun, C. Maple, "Certificateless and Lightweight Authentication Scheme for Vehicular Communication Networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 16110-16125, 2020.

[33] A. Wasef, Y. Jiang, X. Shen, "DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks," IEEE Transactions on Vehicular Technology, vol. 59, no. 2, pp. 533-549, 2010.

[34] G. Karagiannis et al., "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," IEEE Comm. Surveys & Tutorials, vol. 13, no. 4, pp. 584-616, 2011.

[35] S. M. Pournaghi, B. Zahednejad, M. Bayat, Y. Farjami, "NECPPA: A Novel and Efficient Conditional Privacy-preserving Authentication Scheme for VANET," Computer Networks, vol. 134, pp. 78–92, 2018.

[36] B. Pourghebleh, N. J. Navimipour, "Towards Efficient Data Collection Mechanisms in the Vehicular Ad Hoc Networks" International Journal of Communication Systems, vol. 32, no. 5, p. e3893, 2019.

[37] C. Zhang, X. Lin, R. Lu, P. -H. Ho, X. Shen, "An Efficient Message Authentication Scheme for Vehicular Communications," IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3357–3368, 2008.

[38] Y. Cao, S. Xu, X. Che, Y. He, S. Jiang, "A Forward-secure and Efficient Authentication Protocol through Lattice-based Group Signature in VANETs Scenarios," Computer Networks, vol. 214, p. 109149, 2022.