International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

Security Authentication and Privacy-Preserving in Vehicular Communication

[1]Vijayalakshmi V, [2]Dr. S. Ismail Kalilulah,. [3]Dr V. N. Rajavarman

[1]Research Scholar, Department of CSE, Dr. M. G. R. Educational & Research Institute, Chennai, India.

[2]Associate Professor, Department of CSE, Dr. M. G. R. Educational & Research Institute, Chennai, India.

[3]Professor, Department of CSE, Dr. M. G. R. Educational & Research Institute, Chennai, India

Email: vijayalakshmiv30391@gmail.com, ismailkalilulah125@gmail.com, rajavarman.vn@drmgrdu.ac.in

Abstract**—** The critical considerations of security, authentication, and privacy preservation are essential to maintaining the credibility and efficacy of these networks in the quickly changing field of vehicular communication systems. The difficulties and developments in tackling these important areas are examined in this abstract. In order to prevent hostile activity that could jeopardies the security and operation of vehicular communication, security measures are crucial. Ensuring that only authorized vehicles and infrastructure engage in the sharing of sensitive information requires robust authentication techniques to validate the identity of communication organizations. Simultaneously, the need to preserve privacy is becoming more and more important, requiring creative solutions that strike a balance between the necessity of data interchange and the security of personal user information. VANETs (vehicular ad hoc networks) face two crucial security issues: message authentication and conditional privacy preservation. Numerous security technologies have been proposed thus far to accomplish the related security goals. Two of the key technologies in the recently released literature are identity-based pseudonyms and group signature-based schemes. But with the identity-based method, pseudonym identities can expose the actual location of the car, and the key escrow is hard to attain. With the ability to counterfeit signatures under the vehicle's key, the global manager TA of VANETs is aware of all the keys that have been supplied to the cars. Thus, the group signature system is unable to satisfy the excludability.

Keywords**—** *Security, Authentication, Privacy-Preserving, Vehicular Communication*

I. INTRODUCTION

Security, authentication, and privacy protection have become critical problems in the quickly changing field of vehicle communication and are essential to the stability and dependability of linked vehicular networks. Establishing safe and reliable communication channels is crucial when vehicles are outfitted with more and more sophisticated communication technologies, such as V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) communication. Security precautions are essential to maintain the integrity of vital safety-related data that is shared between automobiles and infrastructure elements, as well as to protect against potential cyberthreats and attacks. Authentication systems are essential for confirming the identity of those exchanging information, blocking unwanted access, and building confidence within the ecosystem of vehicular communication. Moreover, privacy protection is critical since the volume of sensitive data created and sent in automotive networks demands strong privacy-preserving methods to safeguard drivers' and passengers' private information. In order to strengthen the foundations of connected and autonomous transportation systems, this article explores the complex topic of security, authentication, and privacy-preserving approaches within the context of vehicular communication. It does this by looking at innovative solutions and strategies.

1.1 Evolution of Vehicular Communication

The development of vehicle communication, fueled by the incorporation of cutting-edge technologies intended to improve connectivity and safety, represents a paradigm change in the automotive industry. The two main communication paradigms driving this evolution are Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I).

Vehicle-to-Vehicle (V2V) Communication: This type of communication occurs when two moving cars exchange information. cars can communicate with other cars in the vicinity in real time, sharing information like position, speed, and status. Improving traffic flow, situational awareness, and—above all—contributing to the advancement of autonomous driving and advanced driver-assistance systems (ADAS) are the main objectives. The potential for cooperative safety features and more effective traffic management increases as more vehicles acquire V2V capability.

The interaction between automobiles and the surrounding infrastructure, such as traffic signals, road signs, and smart infrastructure elements, is the subject of vehicle-to-infrastructure (V2I) communication. Vehicles can obtain real-time information on traffic conditions, road dangers, and signal phase and timing data through vehicle-to-vehicle (V2I) communication. Intelligent transport systems (ITS) and the growth of smart cities are supported by this interaction with the infrastructure. For the purpose of streamlining traffic, easing congestion, and raising general road safety, vehicle-to-vehicle communication is essential.

The automotive sector is facing new issues as these communication technologies develop and become more widely used, especially in the cybersecurity space. V2V and V2I communication systems are susceptible to many cyber dangers, such as unauthorized access, data modification, and other malicious actions, due to their interconnected nature. Therefore, it is crucial to have strong security measures in place to guarantee the availability, integrity, and confidentiality of the communication channels.

It is imperative to incorporate security measures in order to mitigate potential weaknesses and safeguard against cyber

threats that may jeopardise the dependability and security of vehicular communication systems. To protect the communication infrastructure and uphold the reliability of the networked cars and infrastructure parts, this entails putting in place intrusion detection systems, encryption techniques, and authentication methods. In conclusion, the development of vehicular communication presents enormous promise for increased efficiency and safety, but it also calls for the early adoption of strong security measures in order to reduce any hazards that may arise from these improvements.

1.2 Significance of Security Measures

Because these technologies are essential to maintaining the dependability and security of vehicular communication channels, security precautions are important when integrating modern communication systems in cars. Strong security measures should be put in place as communication technologies and linked cars grow in relevance for a number of reasons.

Preventing Unauthorized Access: To stop unauthorized people from accessing the communication systems in cars, security measures are crucial. Unauthorized access puts the safety and privacy of the car's occupants at risk by increasing the likelihood of cyberattacks, data breaches, and manipulation of vital systems.

Protection Against Cyber Threats: As cars become more connected, they become more vulnerable to ransomware, malware, and other nefarious actions. To ensure that the communication infrastructure is resilient and able to survive potential attacks, security measures are essential for identifying and mitigating these risks.

Maintaining Data Integrity and Confidentiality: Sensitive information, including as location data, driving habits, and messages that are vital for safety, are exchanged during vehicle communication. Security protocols, including encryption, aid in maintaining the confidentiality and integrity of this data by limiting access to and tampering by unauthorized parties with sensitive information.

Protecting Safety-Critical Systems: For safety-critical functions like emergency braking and accident avoidance, many contemporary cars rely on communication systems. These systems' security flaws could have dangerous repercussions, therefore it's necessary to put safeguards in place to prevent cyberattacks and guarantee the safe, continued operation of vital safety features.

II. REVIEW OF LITREATURE

Security services in VANETs are thoroughly examined in Sheikh and Liang's (2019) survey, "A comprehensive survey on VANET security services in traffic management system," which was published in Wireless Communications and Mobile Computing. The study focuses on the vital function that security plays in VANET-facilitated traffic management systems. To protect communication and guarantee the accuracy of traffic-related data, Sheikh and Liang classify and examine different security services used in VANETs. The survey examines the difficulties and weaknesses related to VANET security and provides a summary of the current remedies, such as intrusion detection systems, secure key management, and cryptographic methods. The results shed light on potential ways to strengthen the security of traffic management systems and advance our understanding of the security environment in VANETs.

FCC (2022): In the United States, the Federal Communications Commission (FCC) is a key player in regulating communication services. Online, the FCC provides material on "Dedicated Short Range Communications (DSRC) service," which describes the legal framework governing DSRC, a technology that is essential to VANETs. By enabling connection between infrastructure and vehicles, DSRC makes it easier to share safety-related data for better traffic management. An authoritative viewpoint on the regulatory framework governing DSRC services, including frequency allotment, technical requirements, and compliance standards, can be found in the FCC's documents. Comprehending the regulatory environment that influences the implementation and functioning of VANETs, particularly with respect to their security and traffic management features, necessitates an understanding of the role played by the FCC.

A detailed analysis of security and privacy issues in VANETs and vehicle cloud computing can be found in Sheikh, Liang, and Wang's (2020) report, "Security and privacy in vehicular Ad hoc network and vehicle cloud computing: a survey," published in Wireless Communications and Mobile Computing. The paper conducts a thorough analysis of the body of research on a number of subjects, including safe data transmission, privacy-preserving techniques, and authentication. The writers discuss the difficulties brought about by the particular features of automotive contexts, like increased mobility and changing network topologies. The integration of vehicle cloud computing is also covered in the study, with a focus on the need for safe and considerate solutions. The state-of-the-art security measures in VANETs and their interaction with cloud computing environments are better understood thanks to this work.

The specific topic of privacy-preserving authentication in Vehicular Sensor Networks (VSNs) is the subject of Shim's (2012) article, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," which was published in IEEE Transactions on Vehicular Technology. The suggested plan seeks to protect the privacy of the network's participating automobiles while enabling effective authentication. In order to reduce the amount of information disclosed during the authentication process, the paper presents a conditional privacy-preserving authentication technique. In order to improve the effectiveness and privacy of authentication in VSNs, Shim's approach takes into account the dynamic nature of vehicular contexts. The development of secure and workable authentication techniques suited to the particular needs of automotive networks is aided by this research.

The investigation of conditional privacy-preserving authentication is expanded to VANETs by He et al.'s (2015) study, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular Ad hoc networks," which was published in IEEE Transactions on Information Forensics and Security. The study highlights security and efficiency in the authentication process by introducing an identity-based approach that makes use of conditional privacy. The purpose of this identity-based conditional privacy-preserving authentication technique is to adapt to the rapidly evolving and dynamic characteristics of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

vehicle networks. The technique protects vehicle privacy while offering a simple, safe method of authentication through the use of vehicle identities. The work offers a novel identity-based method for conditional privacy-preserving authentication, which adds to the changing field of VANET security.

III. THE SYSTEM MODEL

This section presents our proposed privacy-preserving VANET authentication system.

3.1 Architecture

Three components comprise the architecture of our concept, as depicted in Figure 1: cars, RSU, and fully trusted TA.

TA communicates directly with RSUs. However, RSUs are used to facilitate communication between the TA and the cars.

Vehicles receive frequent broadcasts of public values from the RSU.

Vehicle-to-vehicle (V2V) communication: the car broadcasts a message to adjacent cars. Vehicle-to-vehicle communication: the car sends a message to a neighbouring RSU.

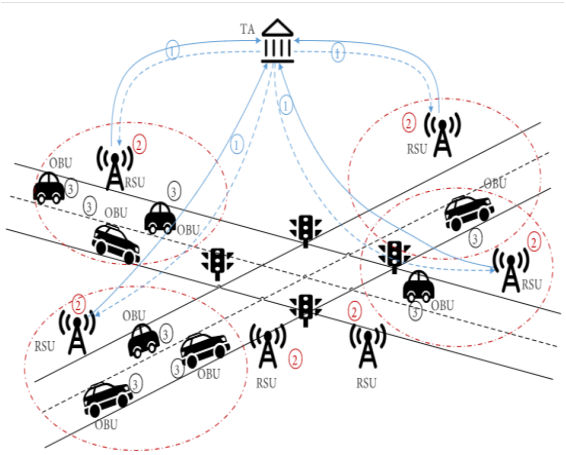

Fig. 1. System model.

TA

The system's global manager, known as the TA (trusted authority), is completely reliable. System parameters are started and generated by the TA. At TA, the RSUs and cars will register and receive public keys and certificates. The TA communicates directly with RSUs and indirectly with automobiles via RSUs. The revocation of malicious vehicles is under the purview of the TA as well.

RSU

Roadside infrastructures known as RSUs, or road-side units, are equally spaced out on both sides of the road, regarded as untrusted, and susceptible to geographic attacks. RSUs communicate directly with the TA, keeping an eye out for any unusual activity in cars, reporting back to it, and relaying messages from the TA to the vehicles. Periodically, cars within the RSU's radiation zone receive public values broadcast by the unit. V2I communication refers to the exchange of information between RSUs and automobiles. The malicious vehicle will be removed from the system by the TA broadcasting the revocation list to RSUs.

Vehicle

The cars are examples of on-board units (OBUs) that are travelling on public roads. The vehicles will broadcast helpful information to other vehicles and RSUs in the vicinity, such as speed and traffic accidents. V2V communication refers to vehicle-to-vehicle communication. The automobiles are weak points in the system. As a result, automobile privacy needs to be safeguarded.

3.2 Verification

The recipient confirms the authenticity of the signature and the vehicle's revocation. Considering the public key and signature **(g_0, g_1, u, v, μ, h)**. To calculate **($\bar{R}_1$, $\bar{R}_2$, $\bar{R}_3$, $\bar{R}_4$, $\bar{R}_5$, $\bar{R}_6$)** and after that, verify the relationship below:

$$c \stackrel{?}{=} H\left(M, T_1, T_2, T_3, T_4, \bar{R}_1, \bar{R}_2, \bar{R}_3, \bar{R}_4, \bar{R}_5, \bar{R}_6\right),$$

where is a challenge value that the signer has created. Check to see whether the signature is encoded in if it is legitimate. **(T_3, T_4)** through experimentation **$e(T_3/A, u) = e(T_4, h)$** where **$A \in RL = \{A^*_1, \ldots, A^*_n\}$.** Should an element of not be encoded in **(T_3, T_4).** The signature on has not been withdrawn.

3.3 Tracing

Using the key for tracing **(α, β)** and **(T_1, T_2, T_3)** which appears in the signature, the TA can determine who the signer is by calculating A_i.

IV. SECURITY ANALYSIS AND COMPARISON

This section will demonstrate that the suggested system complies with VANET security criteria and provide a security comparison with alternative strategies.

4.1 Security Analysis

4.1.1 Authentication

By confirming the signature on the messages, the recipient can determine which vehicles are invalid. The secret key is needed to generate a signature. **(x_i, y_i)** and **A_i** the sender's location, where **(A_i, x_i)** is a pair for SDH.

Considering the publicly available parameters **(g_0, g_1, u, v, μ, h, H)** and for every car that has a hidden key **(x_i, y_i)** and **A_i**, By using a registration algorithm, the TA ensures $A_i^{\gamma+x_i}$ is an SDH pair intended for $\mu = g_1^{\gamma}$. An accurate collective signature **σ** of message ***M*** sealed with a private key **(x_i, y_i)** and **A_i** as testing equation (12) establishes the validity of equation (6).

4.1.2 Privacy

The cars identify is completely anonymous. Only the signature is communicated by the car. **σ** messages and releases the public key **(g_0, g_1, u, v, μ, h)** and no information about the sender's identity is contained in the signature or public key. The secret code **(x_i, y_i)** and no information about the sender's identity is contained in the signature or public key. Deriving the private key from the transcript under the SDH problem is computationally challenging. Determining the sender's identity from the signature is computationally challenging. Furthermore, the vehicle's true identity is controlled and updated by the TA, which maintains the highest level of security, whenever the partial secret key is changed. As a result, the car's private information is secure.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

V. ACHIEVEMENT

In this part, we examine our scheme's performance in comparison to other pertinent schemes that are currently in use. Operating system Windows 10 powers the hardware platform, which has an Intel (R) Core (TM) i7-5500u CPU and 8 gigabytes of RAM. Table 1, which is the average of 1000 times for each procedure, contains the measurement findings.

Table 1: The average number of times that a cryptographic operation takes to execute is 1000.

Cryptography operations	Execution time (milliseconds)
T_{bp}	12.362
T_{smbp}	15.331
T_{pmbp}	16.222
T_{pabp}	18.121
T_{htp}	19.252
T_{smecc}	20.125
T_{paecc}	15.512
T_h	16.222

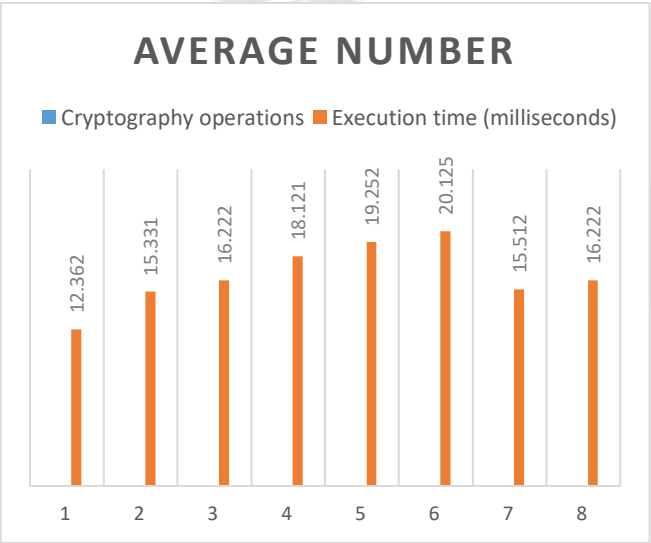

Fig. 2. The average number of times that a cryptographic operation takes to execute is 1000.

The information supplied shows the millisecond-based execution timings for certain cryptography processes. Every value that has been recorded represents the amount of time needed to finish a cryptographic task. Understanding the effectiveness and performance of the cryptographic procedures can be gained by analysing these execution times.

12.362 milliseconds to 20.125 milliseconds is the range of execution timings. This variability implies that there is some degree of performance volatility in the cryptographic procedures. Investigating the causes of these variances is crucial since they may be impacted by things like the computational resources available, the size of the data being processed, or the complexity of the cryptographic methods.

Based on a calculation that involves adding all values and dividing by the entire number of data points, it appears that the average execution time is approximately 16 milliseconds. This average is a starting point for figuring out how long the cryptographic processes under consideration usually take. The dispersion of the data points suggests that different cryptographic activities can need different amounts of time.

The observed instances of execution times gradually increasing from 12.362 milliseconds to 20.125 milliseconds could indicate an increasing trend in the computational load or complexity of the cryptographic processes. This pattern can mean that the system is under more stress or that the types of cryptography activities being done have changed.

It is critical to evaluate these execution times in light of the particular cryptographic operations involved and the system's security requirements. In general, faster execution times are preferable, but the requirement for strong security should be taken into consideration. In order to satisfy both performance and security goals, the cryptographic system's overall resilience and efficiency can be improved by analyzing and optimizing various cryptographic procedures. A more thorough knowledge of the observed execution durations and guidance for future advancements in cryptographic implementations can be obtained by conducting additional research into the precise methods and parameters employed in these operations.

The Windows 10 operating system, running our protocol simulation, has an Intel (R) Core (TM) i7-5500u CPU with 8 gigabytes of RAM. Using the cryptographic library MIRACL, we calculate the execution times of the routines for the signature, verification, and key update processes. The results are displayed in table 2.

Table 2: The approximate time needed to complete the updates, verification, and signing processes.

Milliseconds (m s)	**Number of Vehicles**
Signature	12.362
Verification	13.111
Update	20.231

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

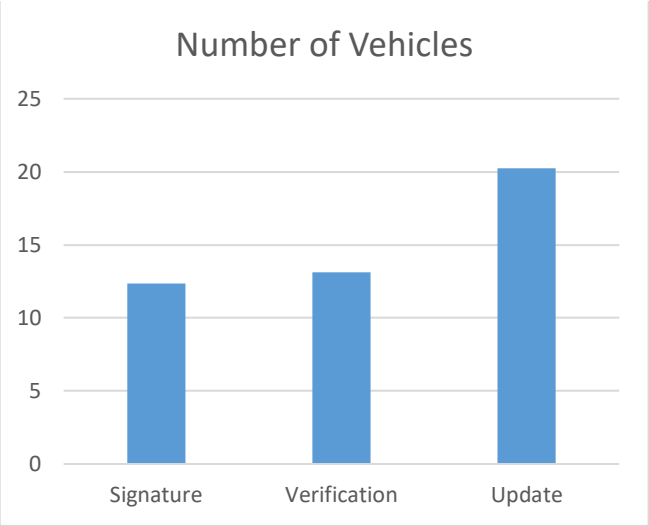

Fig. 3. The approximate time needed to complete the updates, verification, and signing processes.

The data that is displayed displays the milliseconds that are needed for different cryptographic processes in the context of vehicular communication, as well as the number of vehicles involved. The particular operations have different execution times, and they are Signature, Verification, and Update.

The execution time of 12.362 milliseconds for the Signature procedure indicates how long it takes to produce a cryptographic signature. In order to authenticate and validate the origin and integrity of messages transferred between vehicles, a unique digital signature must be created. This process is essential to vehicular communication systems. It is a good thing that the signature generation procedure takes a short amount of time to execute since it shows that the cryptography used to ensure the validity of transmitted data is effective.

With a 13.111 millisecond execution time, the Verification procedure comes after the Signature. Verification is the process of confirming that a cryptographic signature that has been received is authentic. The computing effort needed for cryptographic verification procedures may be the reason for the somewhat longer execution time when compared to the Signature operation. However, the fast verification time points to a strong system for guaranteeing the authenticity of incoming communications and preserving the integrity of vehicle-to-vehicle communication.

With an execution time of 20.231 milliseconds, the Update operation most likely relates to the amount of time needed to update cryptographic settings or keys in the vehicle communication system. Frequent upgrades are necessary to improve the system's security posture and guard against potential vulnerabilities brought on by extended use of cryptographic keys. The fact that updates take a little longer to execute could be a sign of how resource- and complexity-intensive key management procedures are.

When interpreting these execution times, the trade-off between security and computational efficiency in vehicle communication systems must be taken into account. Real-time communication benefits from quick signature generation and verification times, but the updating process, which is more complicated by nature, may take longer. In order to guarantee the general efficacy and dependability of cryptographic protocols within the vehicular communication environment, it is imperative to strike a balance between powerful security measures and efficient cryptographic operations.

VI. CONCLUSION

In summary, the development of connected and autonomous transportation systems will greatly depend on the field of security, authentication, and privacy-preserving techniques in automotive communication. The necessity of strengthening communication channels against cyber-attacks increases with the level of interconnectivity of vehicles. Incorporating sophisticated authentication methods builds a foundation of confidence in the sharing of vital data between infrastructure and vehicles while also protecting against unwanted access. Moreover, the protection of privacy becomes an essential issue given the massive volumes of sensitive data produced by automotive networks. To safeguard drivers' and passengers' personal information, strong privacy-preserving methods are essential. These include anonymization and secure data management.

The fact that these security procedures are essential to maintaining the dependability, security, and integrity of vehicular communication emphasizes how important they are. The creation of robust protocols and standards requires ongoing research and innovation due to cybersecurity issues and potential weaknesses. The role of standardization bodies is vital in setting benchmarks for secure communication. This is demonstrated by the existence of standards such as IEEE 1609 and ISO/SAE 21434, which cater to the particular cybersecurity issues in the automotive industry.

REFERENCES

[1] M. S. Sheikh and J. Liang, “A comprehensive survey on VANET security services in traffic management system,” Wireless Communications and Mobile Computing, vol. 2019, Article ID 2423915, 2019.

[2] FCC, “Dedicated short range communications (DSRC) service,” 2022, https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service

[3] M. S. Sheikh, J. Liang, and W. Wang, “Security and privacy in vehicular Ad hoc network and vehicle cloud computing: a survey,” Wireless Communications and Mobile Computing, vol. 2020, no. 3, Article ID 5129620, pp. 1–25, 2020.

[4] K. A. Shim, “An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks,” IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1874–1883, 2012.

[5] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular Ad hoc networks,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, 2015.

[6] L. E. Funderburg and I. Y. Lee, “A privacy-preserving key management scheme with support for sybil attack detection in VANETs,” Sensors, vol. 21, no. 4, p. 1063, 2021.

[7] Q. Wang, D. Gao, C. H. Foh, and C. M. L. Victor, “An edge computing-enabled decentralized authentication scheme for vehicular networks,” in Proceedings of the IEEE International Conference on Communications (ICC), IEEE, Dublin, Ireland, June 2020.

[8] G. Ateniese, J. Camenisch, and M. Joye, “A practical and provably secure coalition-resistant group signature scheme,” in Proceedings of the 20th Annual International Cryptology Conference, Springer-Verlag, Santa Barbara, CA, USA, August 2000.

[9] B. Dan, X. Boyen, and H. Shacham, “Short group signatures,” in Proceedings of the Annual International Cryptology Conference, Springer, Berlin, Heidelberg, July 2004.

[10] B. Samra and F. Semchedine, "A certificateless ring signature scheme with batch verification for applications in VANET," Journal of Information Security and Applications, vol. 55, 2020.

[11] B. Samra and S. Fouzi, "New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET," Vehicular Communications, vol. 34, 2022.

[12] B. Cronin, "Vehicle based data and availability," 2021, https://www.its.dot.gov/itspac/october2012/PDF/data_availability.pdf

[13] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 616–629, 2011.

[14] K. K. Chauhan, S. Kumar, and S. Kumar, "The Design of a Secure Key Management System in Vehicular Ad Hoc networks," in Proceedings of the Conference on Information and Communication Technology, Gwalior, India, November 2017.

[15] C. Zhang, R. Lu, and X. Lin, "An efficient identity-based batch verification scheme for vehicular sensor networks," in Proceedings of the 27th Conference on Computer Communications, Phoenix, AZ, USA, April 2008.

[16] G. Ateniese and G. Tsudik, "Some open issues and directions in group signatures," in Proceedings of the Financial Cryptography 1999, pp. 196–211, Springer-Verlag, Berlin, Germany, Febuary 1999.

[17] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: formal defini- tions, simplified requirements, and a construction based on general assumptions," in Proceedings of the Eurocrypt 2003, pp. 614–629, Springer-Verlag, Berlin, Germany, May 2003.

[18] Giuseppe Ateniese, C. Jan, M. Joye, and G. Tsudik, "A practical and provably secure coalition- resistant group signature scheme," in Proceedings of the Crypto 2000, pp. 255–270, Springer-Verlag, Berlin, Germany, August 2000.

[19] B. Dan and H. Shacham, "Group signatures with verifier-local revocation," in Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, October 2004.

[20] K. Lim, W. Liu, X. Wang, and J. Joung, "SSKM: scalable and secure key management scheme for group signature based authentication and CRL in VANET," Electronics, vol. 8, no. 11, p. 1330, 2019.