IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

# Secure Many-To-Many Authentication and Key Agreement Scheme for Vehicular Networks

**Mr. Nagaraja G[1], Nama Manasa[2], Poorvika Nagesh B N[3], Preethi G R[4], Priyanka A[5]**
Associate Professor, Department of Information Science and Engineering[1]
Student, Department of Information Science and Engineering[2,3,4,5]
S J C Institute of Technology, Chikkaballapur, Karnataka, India

**Abstract:** *Increase in demand for web and communication technology, vehicles will analyze and choose their all-time knowledge collected by varied cloud service suppliers (CSPs) in a conveyance network. However, in an exceedingly conveyance network atmosphere, period knowledge area units transmitted through wireless channels might result in security and privacy problems. To avoid access for third parties, vehicle authentication, and key agreement mechanism have been considered collectively the promising security measures in conveyance network environments. Besides, most of the solutions concentrate on authentication between one vehicle and one CSP. In such methods, the implementation of economical authentication for several vehicles and CSPs at the same time is typically difficult. Further, they're conjointly subjected to performance limitations because of the overhead incurred. to unravel these problems, we have a tendency to propose a many-to-many authentication and key agreement theme for secure authentication between multiple vehicles and CSPs. The projected theme will forestall unauthorized access and supply SK- security (strong key). To improve the service, the CSP solely has to broadcast associate degree anonymous messages sporadically rather than having to get a singular anonymous message for every vehicle. Similarly, once a vehicle needs to request the services of m CSPs, it solely has to send one request message rather than n. Therefore, the proposed theme not solely implements many-to-many communication however conjointly considerably reduces the computation and communication overhead.*

**Keywords:** Base station, Registration authority, Cloud service provider, Diffie-hellman key exchange

## I. INTRODUCTION

HE rapid growth in the number of vehicles and diverse user demand for services has led to an exponential growth in the data generated by vehicles. Therefore, cloud computing with the ability to collect, process, and share real-time data is widely used in vehicular networks. To reduce data transmission delays and prevent single points of failure, efforts have been made to decentralize cloud services and instead work with multiple cloud service providers (CSPs). This has led to the emergence of multi cloud environments in vehicular networks. The lower layer consists of vehicles and base stations (BSs). The upper layer contains a registration authority (RA) and CSPs with different service functions. The entities can communicate with each other through wireless communication, such as IEEE 802.11p, 4G, and 5G. Although CSPs are expected to play an important role in vehicular network environments, there are some challenges in terms of data exchange with the vehicles. One of the challenges is the security and privacy issues that are introduced due to the use of wireless communication in vehicular network. For instance, sensitive and important transmission messages may be subjected to unauthorized access. Alternatively, if an adversary modifies, imitates, or replays the transmitted message, it may result in fatal harm to the data owner. The vehicular networks are accountable for accidents, which not only require user privacy protection but also the ability to trace the identities of the offender by authoritative institutions. Therefore, to avoid illegal access to data and prevent malicious attackers, conditional privacy protection authentication and key agreement mechanisms are considered effective security measures.

## II. PROBLEM IDENTIFICATION

In the multi-party cloud authentication causes vulnerable to an ephemeral secret leakage attack and proposed an enhanced scheme to withstand this attack. As the vehicle anonymity and hash function are public, the real identity of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

the CSP is revealed to the authenticated vehicle. Thus, the scheme cannot withstand an ephemeral secret leakage attack. The existing schemes cannot prevent impersonation and man-in-the-middle attacks. In a vehicular network environment, real-time data are transmitted via wireless channels, which can lead to security and privacy issues. To avoid illegal access by adversaries, vehicle authentication and key agreement mechanism has been considered as one of the promising security measures in vehicular network environments. Besides, most of the solutions focus on authentication between one vehicle and one CSP. In such strategies, the implementation of efficient authentication for multiple vehicles and CSPs simultaneously is usually challenging. Further, they are also subjected to performance limitations due to the overhead incurred.

## III. METHODOLOGY

**We are using SHA-1 Algorithm to Generate Key**

**Steps Involved to Generate the Key**

**Step 1:** The first step is to initialize five random strings of hex characters that will serve as part of the hash function:

H0 = 67DE2A01
H1 = BB03E28C
H2 = 011EF1DC
H3 = 9293E9E2
H4 = CDEF23A9

**Step 2:** The message is then padded by appending 1, followed by enough 0's until the message is 448 bits. The length of the message represented by 64 bits is then added to the end, producing a message that is 512 bits long.

**Step 3:** The padded input obtained above M, is then divided into 512-bit chunks, and each chunk is further divided into sixteen 32-bit words, $W_0 \ldots W_{15}$.

**Step 4:** For each chunk, begin the 80 iterations i, necessary for hashing and execute the following steps on each chunk.

$$W(i)=S1(W(i-3)\oplus W(i-8)\oplus W(i-14)\oplus W(i-16))$$

**Step 5:** Now store the hash values defined in step 1 in the following variables:

A = H0
B = H1
C = H2
D = H3
E = H4

**Step 6:** Store the result of the chunk's hash to the overall hash value of all chunks, as shown below and proceed to execute the next chunk.

H0 = H0 + A
H1 = H1 + B
H2 = H2 + C
H3 = H3 + D
H4 = H4 + E

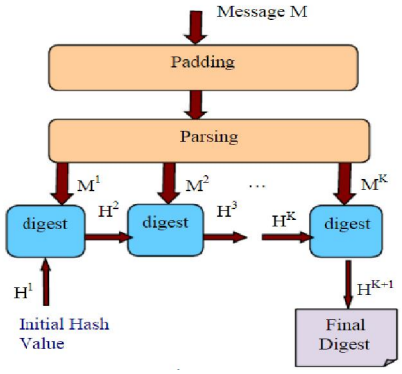


**Figure 1 :** SHA-1 algorithm steps

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

## IV. IMPLEMENTATION

We are developing this with the following modules.

### 4.1 Modules

1. Vehicle
2. Base Station
3. CSP
4. RA

### A. Vehicle

Each vehicle is equipped with an on-board unit (OBU) and a trusted platform module (TPM). The OBU is used for wireless communication with other vehicles or a BS, whereas the TPM is used to store security materials and handle cryptographic operations.

**Pseudo code**

- Step 1: Create node.
- Step 2: for each node assign the key.
- Step 3: connect to nearest base station.

### B. BS

A BS is a wireless communication device deployed on the side of the road and is considered to be untrustworthy. It does not participate in any storage and computation and serves only as an intermediate transmission medium. The BS has a super-fast transmission speed to support seamless coverage for vehicle communication.

**Pseudo code:**

- Step 1: Base Station.
- Step 2: Connect to CSP.
- Step 3: Generate and assign Key.
- Step 4: Forward data from vehicle to cloud service provider.

### C. CSP

A CSP is an honest but curious entity that connects to the Internet and provides various network access services for vehicles.. To improve traffic safety and convenience, the CSP periodically broadcasts safety- and entertainment-related services to nearby vehicles.

**Pseudo code:**

- Step 1: Create CSP.
- Step 2: Connect to Base station.
- Step 3: Encrypt the data.
- Step 4: Exchange key using Diffie-hellman key exchange.
- Step 5: store data.

### D. RA

The role of an RA, which is a highly secure entity that is fully trusted and uncompromisable, is generally undertaken by an intelligent transport system department of the government. During system registration, the RA cooperates with each vehicle and CSP and generates unique long-term private keys for them. The RA is notably the only entity that can track the true identity of any vehicle.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

**Pseudo code:**

- Step 1: Create RA.
- Step 2: Connect to Network.
- Step 3: Exchange keys.
- Step 4: Verify the nodes using keys.
- Step 5: Authenticate node.

## V. CONCLUSION

This paper proposed a many-to-many authentication and key agreement scheme to achieve secure authentication between multiple vehicles and multiple CSPs for vehicular networks. In this scheme, the broadcast mechanism (at the CSP side) and hybrid encryption algorithm (such as elliptic curve, hash, and AES) are used to realize efficient many-to-many authentication. Moreover, the proposed scheme provides better SK security compared with those of existing schemes, even if the session ephemeral secret is unexpectedly leaked. Utilizing the widely-used ROR model and formal security analysis, the proposed scheme is proven to be resistant to several attacks. Finally, through performance evaluation, we conclude that the proposed scheme has lower computation and communication overhead, and provides higher security than those of existing schemes.

## REFERENCES

**[1].** Y. Yu et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767–778, Apr. 2017.

**[2].** L. Zhang, "OTIBAAGKA: A new security tool for cryptographic mixzone establishment in vehicular ad hoc networks," IEEE Trans. Inf. Forensics Security, vol. 12, no. 12, pp. 2998–3010, Dec. 2017.

**[3].** Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated authentication and key agreement framework for vehicular cloud computing," IEEE Netw., vol. 32, no. 3, pp. 28–35, May 2018.

**[4].** J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs—An efficient and privacy-preserving cooperative downloading scheme," IEEE J. Sel. Areas Commun., vol. 38, no. 6, pp. 1191–1204, Jun. 2020.

**[5].** R. Yu et al., "Cooperative resource management in cloud-enabled vehicular networks," IEEE Trans. Ind. Electron., vol. 62, no. 12, pp. 7938–7951, Dec. 2015.

**[6].** S. Azodolmolky, P. Wieder, and R. Yahyapour, "Cloud computing networking: Challenges and opportunities for innovations," IEEE Commun. Mag., vol. 51, no. 7, pp. 54–62, Jul. 2013.

**[7].** J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," IEEE Trans. Inf. Forensics Security, vol. 15, pp. 1654–1667, 2020.

**[8].** J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," IEEE Trans. Dependable Secure Comput., early access, Mar. 11, 2019, doi: 10.1109/TDSC.2019.2904274.

**[9].** V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," IEEE Trans. Inf. Forensics Security, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

**[10].** J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "An extensible and effective anonymous batch authentication scheme for smart vehicular networks," IEEE Internet Things J., vol. 7, no. 4, pp. 3462–3473, Apr. 2020.

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

**[12].** Z. Ning et al., "A cooperative quality-aware service access system for social Internet of Vehicles," IEEE Internet Things J., vol. 5, no. 4, pp. 2506–2517, Aug. 2018.

**[13].** Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

**[14].** M. Ma, D. He, H. Wang, N. Kumar, and K.-K.-R. Choo, "An efficient and provably secure authenticated

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 6, June 2022
Impact Factor: 6.252

key agreement protocol for fog-based vehicular ad-hoc networks," IEEE Internet Things J., vol. 6, no. 5, pp. 8065–8075, Oct. 2019.

**[15].** A. I. Croce, G. Musolino, C. Rindone, and A. Vitetta, "Sustainable mobility and energy resources: A quantitative assessment of transport services with electrical vehicles," Renew. Sustain. Energy Rev., vol. 113, Oct. 2019, Art. no. 109236.