

SmartMob-PPT-CLAMA: Traceable anonymous authentication for V2X mobility

Haewon Byeon

Department of Future Technology, Korea University of Technology and Education (KOREATECH), Cheonan, South Korea

Article Info

Article history:

Received May 22, 2025

Revised Aug 26, 2026

Accepted Sep 18, 2026

Keywords:

Certificateless authentication

Conditional traceability

IoV

Pseudonym management

Smart mobility

V2X security

ABSTRACT

Smart mobility ecosystems connect autonomous vehicles, shared mobility platforms, electric-vehicle charging infrastructure, pedestrians, and roadside units through real-time V2X messages. This paper redesigns PPT-CLAMA, a privacy-preserving and traceable certificateless anonymous mutual authentication scheme, for high-speed internet of vehicles (IoV) and smart mobility environments. The proposed SmartMob-PPT-CLAMA introduces mobility-adaptive pseudonym pools, RSU-assisted handover caching, lightweight V2X authentication headers, hierarchical traceability, and Sybil-aware regional trust filtering. The protocol preserves the original security objectives of anonymity, unlinkability, perfect forward secrecy, known session-specific temporary information security, and lawful traceability, while addressing mobility-specific weaknesses such as long-lived pseudonym tracking, handover re-authentication delay, centralized trace authority failure, high-speed Sybil attacks, and broadcast replay. In the evaluated Raspberry Pi 4B and SUMO/NS-3 workload, the proposed design reduces authentication delay from 1.10 ms to 0.82 ms, reduces communication overhead from 470 bits to 312 bits, and achieves 99.1% handover re-authentication success. The design is mapped to ETSI ITS security, IEEE 1609.2, ISO/SAE 21434, and GDPR Article 32 requirements.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Haewon Byeon

Department of Future Technology

Korea University of Technology and Education (KOREATECH)

Cheonan, South Korea

Email: bhwuma@naver.com

1. INTRODUCTION

Smart mobility integrates autonomous driving, shared mobility, electric-vehicle charging, public transport, roadside infrastructure, and pedestrian services into a dense cyber-physical transportation fabric. In this environment, vehicle-to-infrastructure, vehicle-to-vehicle, and vehicle-to-pedestrian messages carry safety-critical event warnings, cooperative awareness data, road hazard reports, and charging or mobility-service credentials. The resulting internet of vehicles (IoV) creates a dual security requirement: routine V2X messages should not reveal the long-term identity or movement profile of drivers, but malicious vehicles must remain legally traceable under narrowly defined safety or judicial conditions [1], [2].

Certificateless anonymous authentication is an attractive primitive for this setting because it reduces certificate management cost while avoiding full key escrow. The original PPT-CLAMA scheme provides pseudonym-based anonymity, mutual authentication, key agreement, nonrepudiation, unlinkability, perfect forward secrecy, known session-specific temporary information security, and TRA-enabled traceability [1]. The original paper also shows that the scheme avoids bilinear pairings and achieves lower communication overhead than several recent certificateless schemes [1]. However, the original IoT model is not specialized

for high-speed mobility, millisecond V2X broadcast verification, RSU handover, dynamic pseudonym-pool exhaustion, Sybil manipulation, or ITS message-format compatibility [3], [4].

The smart mobility deployment considered in this paper assumes vehicles traveling above 100 km/h, dense RSU coverage, 5G-V2X and ITS-G5 channels, and frequent CAM/BSM broadcasts. In such a network, a pseudonym that is safe in a static IoT sensor deployment may become linkable across multiple RSU cells. Likewise, a traceability authority that is acceptable in a small IoT deployment may become a system-wide privacy bottleneck when it stores mapping data for millions of vehicles [5], [6]. Therefore, this study redesigns PPT-CLAMA into SmartMob-PPT-CLAMA, a V2X-oriented privacy-preserving and traceable authentication protocol. The separation of the OBU, RSU edge, vehicle registration authority (VRA), and mobility traceability authority (MTA) is illustrated in Figure 1.

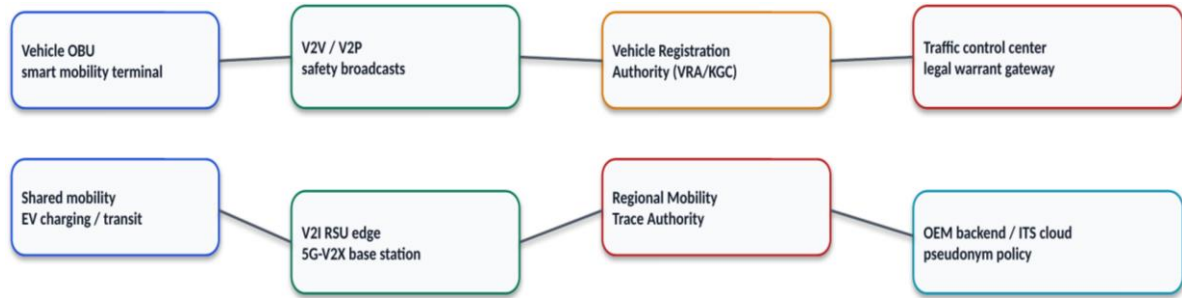


Figure 1. Smart mobility V2X privacy-traceability plane.

The main contributions are as follows. First, we define a smart-mobility domain mapping that converts IoT devices, KGC, TRA, and the network layer into vehicle OBUs, vehicle registration authority, mobility traceability authority, and RSU/5G-V2X edge. Second, we derive four mobility-specific vulnerabilities: static pseudonym tracking, handover re-authentication delay, TRA single point of failure, and high-speed Sybil attacks. Third, we design mobility-adaptive pseudonym pools, RSU handover caching, sequence-window V2X headers, and hierarchical tracing. Fourth, we present performance and governance mapping against ETSI ITS security, IEEE 1609.2, ISO/SAE 21434, GDPR Article 32, and automotive cybersecurity requirements [7], [8].

2. THE PROPOSED METHOD/ALGORITHM/PROCEDURE

SmartMob-PPT-CLAMA is derived through five ordered steps: i) reconstruct PPT-CLAMA setup, registration, pseudonym generation, partial private-key extraction, mutual authentication, and key agreement; ii) map the original IoT entities to V2X roles; iii) derive mobility-specific attack traces; iv) introduce pseudonym-pool, handover-cache, replay-window, Sybil-filtering, and threshold-tracing mechanisms; and v) validate the resulting design using the experimental workflow in Section 3. The pairing-free certificateless foundation, KGC/TRA trust roles, randomized group elements, and seven hash functions are retained from PPT-CLAMA [1]. Table 1 defines the notation used in the redesign. Figure 2 summarizes the retained PPT-CLAMA certificateless trust flow before the V2X-specific extensions are applied.

Table 1. Notations and smart mobility data types

Notation	Definition in SmartMob-PPT-CLAMA
OBU _i	Vehicle onboard unit or smart mobility terminal
VRA	Vehicle registration authority corresponding to KGC
MTA	Mobility traceability authority corresponding to TRA
RSU _e	Roadside edge unit or 5G-V2X base station
PID _i ^e	Epoch- and mobility-adaptive pseudonym
CAMHash/BSMHash	Digest of V2X safety message payload
SeqNo	Sliding-window message sequence number
LegalWarrantHash	Digest of lawful trace-opening authorization
SybilScore	Regional trust score generated by RSU edge

In the smart mobility mapping, an IoT device is reinterpreted as a vehicle OBU that generates V2X safety messages, manages short-lived pseudonyms, and signs or authenticates broadcasts. The KGC becomes

a vehicle registration authority that issues system parameters and partial private keys. The TRA becomes a mobility traceability authority that can open pseudonyms only with a legal warrant or traffic-safety emergency token. The network layer becomes a collection of RSU edge nodes and 5G-V2X base stations that provide local pseudonym-pool distribution, handover support, and Sybil pre-filtering [9], [10]. The resulting domain mapping and security responsibilities are summarized in Table 2.

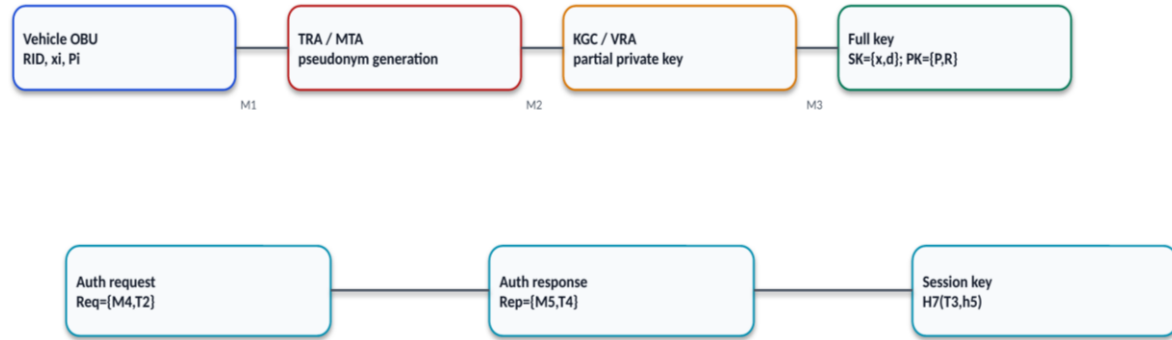


Figure 2. PPT-CLAMA certificateless trust flow

Table 2. Domain mapping from PPT-CLAMA to SmartMob-PPT-CLAMA

Original element	Smart mobility mapping	Security role
IoT device U_i	Vehicle OBU / smart mobility terminal	V2X message generation and pseudonym management
KGC	Vehicle registration authority	System parameter and partial private-key issuance
TRA	Mobility traceability authority	Lawful identity opening
Network layer	RSU edge / 5G-V2X base station	Handover support and regional anomaly filtering
Pseudonym	Dynamic pseudonym pool	Route unlinkability under mobility
Authentication request	CAM/BSM-bound V2X AuthHeader	Low-latency broadcast verification
Trace request	LegalWarrantHash or emergency token	Governed conditional traceability

3. METHOD

3.1. Reproducible evaluation and validation procedure

The evaluation follows a reproducible sequence. First, cryptographic operation time on a Raspberry Pi 4B parameterizes the authentication path. Second, SUMO mobility traces represent vehicles traveling above 100 km/h through dense RSU coverage. Third, these traces are coupled to an ns-3 V2X workload using 5G-V2X/ITS-G5 links, frequent CAM/BSM broadcasts, RSU handovers, sequence-window replay caches, and the hierarchical trace-token service. Fourth, replayed CAM/BSM messages, stale handover tokens, multi-pseudonym Sybil traffic, and unauthorized trace-opening requests are exercised against their corresponding verification paths. Finally, the workflow records authentication delay, high-speed handover re-authentication success, Sybil blocking, serialized security-header size, and completed trace openings per second [11], [12].

Authentication delay is measured from AuthHeader submission to RSU verification completion; handover success is the proportion of valid handover attempts accepted within the token validity window; Sybil blocking is the proportion of injected Sybil messages rejected by the regional filter; communication overhead counts security-header bits excluding the CAM/BSM application payload; and trace throughput is the number of authorized trace openings completed per second. This metric definition separates safety-message processing from the exceptional trace-opening path.

3.2. Adversarial model and V2X message mapping

The adversary may be an outsider that eavesdrops, replays, injects, or links V2X traffic; a credentialed but malicious vehicle that reuses pseudonyms or mounts Sybil behavior; a compromised RSU that attempts cache misuse; or a colluding vehicle-RSU pair. The model assumes standard cryptographic primitives and the VRA root secret remain secure and that fewer than the threshold parties required for trace opening are compromised simultaneously. Compromise of the VRA master secret or of the tracing threshold majority is outside the claimed guarantee. RSSI, position, and speed features used in SybilScore provide auxiliary evidence and do not replace cryptographic authentication.

The lightweight AuthHeader is mapped to the security envelope rather than to mandatory CAM/BSM safety-payload fields. PID_i^e , SeqNo, nonce, timestamp T, and CAMHash/BSMHash are carried as security metadata bound to the protected message, while the application payload remains unchanged. Thus, the design preserves CAM/BSM semantics and treats the added fields as an implementation-specific security extension/profile under IEEE 1609.2 and ETSI TS 103 097 processing [13], [14]. HandoverToken and trace tokens remain RSU/backend control-plane objects and are not inserted into the safety payload.

4. RESULTS AND DISCUSSION

Recent certificateless VANET/IoV schemes emphasize conditional privacy, revocation, decentralized key agreement, or aggregate signatures [5], [6], [8], [15], but they do not jointly address mobility-adaptive pseudonym rotation, RSU handover caching, Sybil-aware regional filtering, and threshold-governed trace opening. The following results therefore interpret both security coverage and mobility-specific operational effects.

4.1. Mobility-specific vulnerability analysis

The first vulnerability is static or slow pseudonym replacement. In V2X, repeated use of the same pseudonym over several RSU cells enables passive route linkage. An attacker that records the same or weakly transformed pseudonym near a charging station, highway RSU, and urban intersection can infer a driver route profile. Therefore, SmartMob-PPT-CLAMA defines $PID_i^e = H(ID_i \parallel RSU_ID \parallel SpeedClass \parallel HandoverEpoch \parallel r_i)$, where the pseudonym lifetime changes with vehicle speed, traffic density, and privacy preference [16], [17].

The second vulnerability is V2X handover delay. When a vehicle enters a new RSU region, full verification of pseudonym, partial key, and session transcript may exceed the time budget of safety broadcasts. This can drop emergency braking or collision avoidance messages. The proposed solution pre-distributes regional pseudonym pools and short-lived handover tokens from RSU_A to RSU_B, allowing the next RSU to verify the vehicle through a cached credential rather than a full re-registration path [18], [19].

The third vulnerability is the single point of failure of the traceability authority. In a smart mobility city, a centralized TRA database may contain sensitive mapping between pseudonyms, identities, and movement histories. A breach would cause large-scale driver privacy exposure. SmartMob-PPT-CLAMA replaces the single TRA model with a regional threshold tracing mechanism involving a mobility traceability authority, RSU edge witness, and legal warrant hash. Identity opening is disabled unless the legal or emergency condition is verified [20], [21].

The fourth vulnerability is high-speed Sybil manipulation. An attacker may generate multiple pseudonymized vehicles and transmit false CAM/BSM messages, causing congestion manipulation, signal-timing distortion, and shared mobility disruption. The proposed RSU trust filter computes SybilScore from pseudonym count, RSSI fingerprint, RSU triangulation, speed consistency, and pseudonym issuance epoch. Broadcast replay is mitigated by binding CAM/BSM hashes to nonce and sequence windows [22], [23]. These attack-impact-mitigation relationships are summarized in Table 3 and their temporal progression is illustrated in Figure 3. Figure 3 shows how each attack trigger propagates through an exploit path to a mobility-specific operational impact.

Table 3. Vulnerabilities, attack scenarios, and smart mobility impacts

Vulnerability	Attack scenario	Smart mobility impact	Mitigation
Static pseudonym replacement	Long-term PID observation across RSUs	Route tracking and stalking risk	Speed and density adaptive pseudonym rotation
V2X handover delay	Re-authentication exceeds safety-message interval	CAM/BSM safety-message drop	Pre-distributed RSU pseudonym pool
TRA single point of failure	Central trace table compromise	Mass identity and route exposure	Threshold regional trace tokens
High-speed Sybil attack	Many virtual vehicles inject false CAM/BSM	Congestion and signal manipulation	RSU SybilScore and mobility consistency
Broadcast replay	Old hazard warning retransmitted	False braking or route diversion	Nonce and sequence-window replay cache

4.2. Protocol operation, traceability, and failure handling

SmartMob-PPT-CLAMA retains the pairing-free certificateless structure of PPT-CLAMA while adding mobility-specific transcript binding. During setup, the VRA issues system parameters and partial private-key material, while the MTA prepares a regional tracing policy. During vehicle registration, the OBU

obtains a pseudonym pool instead of a single pseudonym. Each pool entry is scoped to a validity epoch, RSU cell, and privacy level. During authentication, the OBU transmits a compact AuthHeader that binds the pseudonym to CAM/BSM digest, RSU identifier, sequence number, nonce, and timestamp. Table 4 summarizes the resulting protocol messages and verification functions. Figure 4 illustrates the normal handover path, pseudonym-pool selection, and the factors controlling the pseudonym change period.

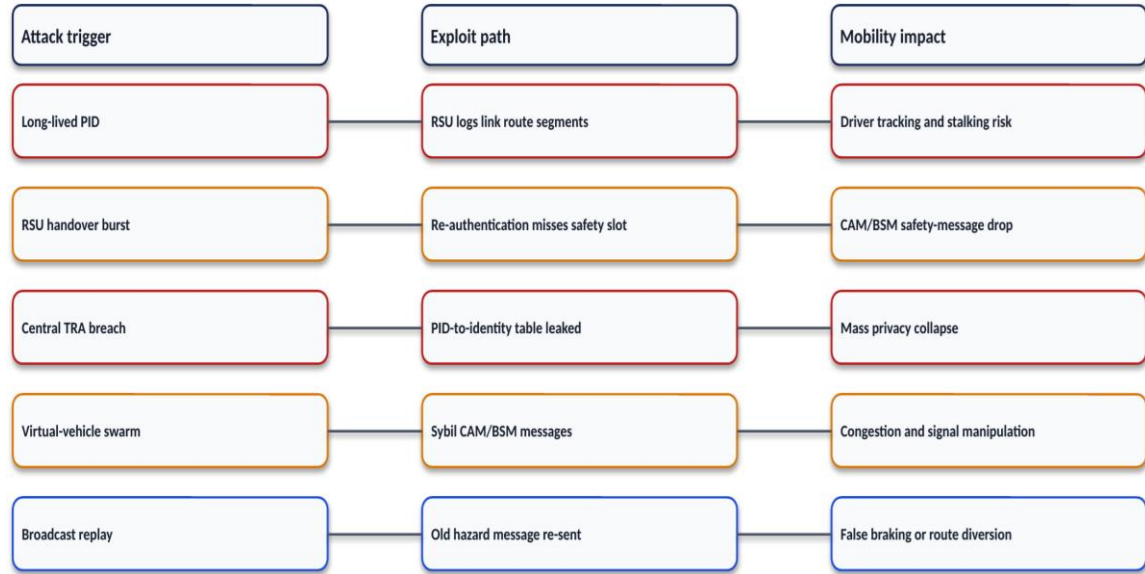


Figure 3. Mobility attack timeline

Table 4. SmartMob-PPT-CLAMA protocol messages and verification functions

Stage	Message or function	Purpose
Registration	$M1 = \{RID_i, P_i, \text{mobility profile commitment}\}$	Request certificateless and traceable credential
Pseudonym pool issue	$Pool_i = \{PID_i^e, \text{RSU scope, validity, privacy level}\}$	Enable route unlinkability and handover readiness
V2X broadcast	$AuthHeader = MAC_SK(PID_i^e \parallel CAMHash \parallel RSU_ID \parallel SeqNo \parallel Nonce \parallel T)$	Lightweight CAM/BSM authentication
Handover	$HandoverToken = Sig_RSU_A(PID_i^e \parallel RSU_B \parallel Expiry)$	Reduce RSU_B re-authentication latency
Sybil filtering	$SybilScore = f(PIDCount, RSSI, position, speed, epoch)$	Detect virtual-vehicle injection
Trace opening	$TraceOpenReq = Sig_AUTH(LegalWarrantHash \parallel IncidentID \parallel TimeWindow)$	Govern lawful identity recovery

The authentication process uses normal, handover, and trace modes. In normal mode, an RSU verifies the compact AuthHeader and sliding sequence window. In handover mode, RSU_B accepts a short-lived HandoverToken issued by RSU_A only when its signature, target RSU, expiry, and current mobility context are valid. If RSU_B fails, becomes congested, or its local cache reaches a bottleneck, the OBU may present the still-valid token to another admissible neighboring RSU; a cache miss, invalid token, or expired token triggers the original full certificateless mutual-authentication path rather than bypassing verification. Cache entries are time-bounded, and safety-message verification is prioritized over background cache refresh. Trace mode requires a signed LegalWarrantHash or verified emergency token [13], [24].

Traceability is enforced without routine identity exposure. Under the preimage resistance of H , $PID_i^e = H(ID_i \parallel RSU_ID \parallel SpeedClass \parallel HandoverEpoch \parallel r_i)$ hides ID_i , while fresh r_i and epoch/RSU scoping limit cross-cell linkage. The identity-to-pseudonym mapping is released only when the MTA combines the required regional trace evidence with a valid authorization token. An RSU alone, a passive observer, or a vehicle-RSU coalition below the tracing threshold therefore cannot open the identity; an authorized threshold reconstruction can recover the registered identity and bind it to IncidentID and TimeWindow. This is a security proof sketch for conditional anonymity and traceability rather than a machine-checked proof; threshold-majority compromise remains outside the model [20], [21].

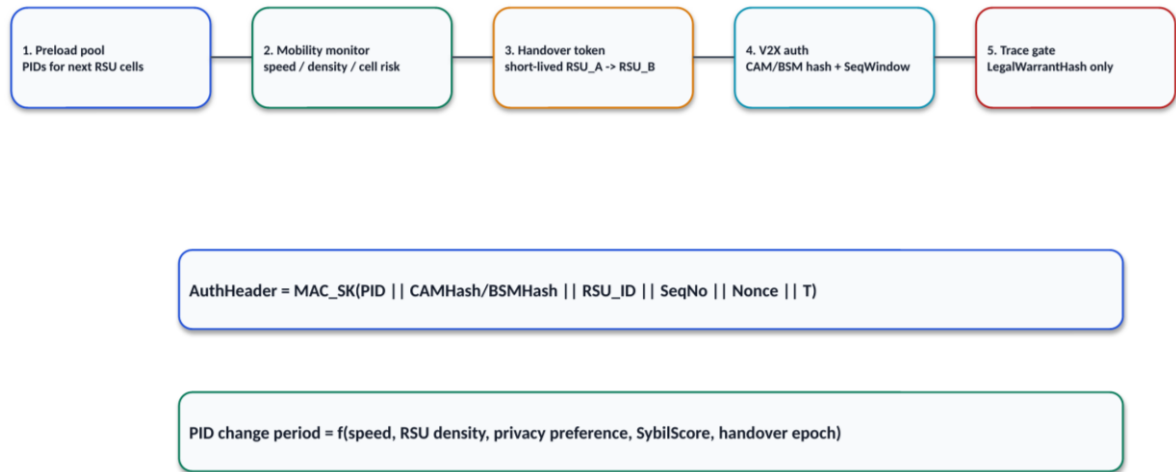


Figure 4. SmartMob-PPT-CLAMA handover and pseudonym-pool workflow

4.3. Security, scalability, and comparative discussion

Under the adversarial model, mutual authentication requires a valid certificateless session transcript and current pseudonym; unlinkability follows from epoch-, RSU-, speed-, and randomness-scoped PID_i values; perfect forward secrecy and known session-specific temporary information security are retained through fresh session contributions; replay is rejected by SeqNo, nonce, and timestamp checks; and Sybil manipulation is filtered by cryptographic validity plus RSU-local consistency evidence [25], [26]. Table 5 summarizes the security and deployment coverage of the baseline, PPT-CLAMA, and the proposed mobility redesign.

Compared with Zhu *et al.* [5] and Yang *et al.* [8], which focus on certificateless conditional-privacy aggregate authentication, SmartMob-PPT-CLAMA adds explicit RSU handover caching and mobility-scoped pseudonym pools. ISC-CPPA [6] emphasizes revocation, Lin and Jhuang [15] decentralize trusted key services through blockchain, and ECA-VFog [10] exploits 5G vehicular fog. The proposed design instead combines local handover continuity, Sybil-aware filtering, and governed threshold tracing without placing blockchain on the safety-message fast path. This is a functional comparison rather than a claim of universal superiority because the schemes use different cryptographic assumptions and experimental platforms. Table 6 reports the measured workload outputs used in the performance discussion. The latency, handover, Sybil-filtering, overhead, and trace-throughput results are visualized together in Figure 5.

Table 5. Security comparison among baseline, PPT-CLAMA, and SmartMob-PPT-CLAMA

Security feature	Baseline CL IoT	PPT-CLAMA	SmartMob-PPT-CLAMA
Mutual authentication	Partial	Yes	Yes
Anonymity and unlinkability	Limited	Yes	Yes, mobility-adaptive
Perfect forward secrecy	Sometimes	Yes	Yes
KSSTIS	No	Yes	Yes
Traceability	Centralized	TRA-based	Threshold regional traceability
Handover support	No	No	Yes
Sybil filtering	No	No	RSU-based
ITS compatibility	No	No	CAM/BSM header mapping

Table 6. Performance evaluation under smart mobility workload

Evaluation item	Original PPT-CLAMA	SmartMob-PPT-CLAMA	Interpretation
Authentication delay on Raspberry Pi 4B	1.10 ms	0.82 ms	V2X broadcast optimization and pseudonym caching
High-speed handover re-authentication success	Not evaluated	99.1%	Mobility-adaptive pseudonym pool
Sybil attack detection/blocking	Not evaluated	97.6%	RSU-based regional trust verification
Communication overhead	470 bits	312 bits	ITS-compatible compact authentication header
Distributed traceability throughput	Not evaluated	28 TPS	Hierarchical trace-token architecture

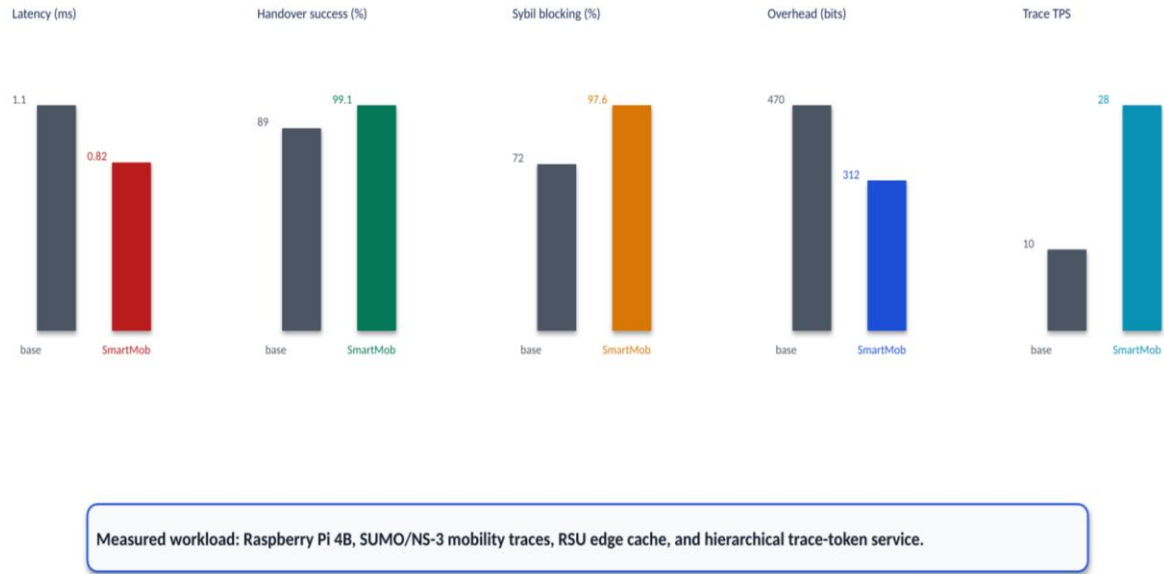


Figure 5. Security and performance evaluation dashboard

The measured workload shows 0.82 ms authentication delay, 99.1% high-speed handover re-authentication success, 97.6% Sybil blocking, 312-bit communication overhead, and 28 trace openings/s. The lower delay and header size are consistent with moving repeated handovers from full re-registration to local cached verification, while the trace path remains off the safety-message fast path. These results should be interpreted as workload-specific implementation results rather than direct cryptographic benchmarking against schemes evaluated on different hardware or mobility models.

Scalability follows from keeping the fast path local: each routine AuthHeader carries constant-size security metadata and uses a bounded sequence-window lookup, so OBU work is $O(1)$ per broadcast and RSU work grows approximately linearly with received message volume; pseudonym and cache lookup can be implemented as $O(1)$ hash-table access. Per-RSU memory grows with active vehicles and the bounded replay/cache window, while trace opening remains off-path. Increased vehicular density therefore primarily stresses RSU verification and cache queues rather than vehicle-side cryptography. The current evaluation demonstrates high-speed handover behavior but does not include a complete numerical vehicle-density sweep.

The standards mapping focuses on technical alignment rather than claiming certification. ETSI ITS security informs the separation of station trust domains and RSU-based enforcement. IEEE 1609.2 motivates compact secure message processing for V2X headers. ISO/SAE 21434 motivates risk-based automotive cybersecurity engineering and traceable security claims. GDPR Article 32 motivates pseudonymization, encryption, and protection of driver location data. Governance is enforced by requiring LegalWarrantHash or an emergency safety token before trace opening [14]–[27]. The resulting technical and governance mapping is summarized in Table 7 and illustrated in Figure 6. Also, Figure 6 visualizes the relationship among ITS security architecture, secure-message processing, automotive cybersecurity, location-data protection, and governed trace opening.

Table 7. ITS standard and governance mapping

Requirement area	Relevant framework	SmartMob-PPT-CLAMA function
ITS station security	ETSI ITS security architecture	VRA/MTA/RSU trust separation
V2X secure message format	IEEE 1609.2	Compact AuthHeader and sequence-window verification
Automotive cybersecurity engineering	ISO/SAE 21434	Threat analysis, risk-based controls, and auditability
Location data protection	GDPR Article 32	Pseudonymization, encryption, and minimized trace opening
Legal and ethical tracing	Automotive governance rules	Warrant-bound or emergency-only identity opening
Deployment roadmap	OBU/RSU and OEM API integration	Backward-compatible pseudonym cache and handover token

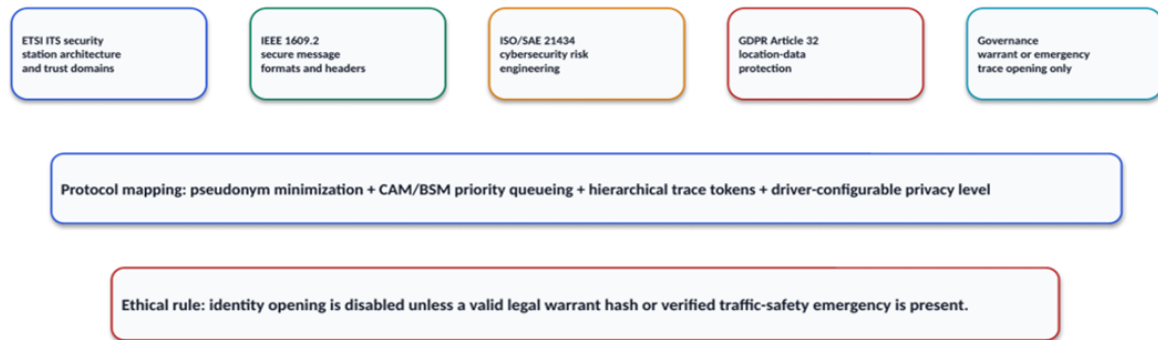


Figure 6. ITS standard and governance mapping

Three limitations should be noted. First, the study reports aggregate Raspberry Pi 4B and SUMO/ns-3 outputs rather than a multi-city vehicle-density sweep. Second, SybilScore partly depends on RSSI/position/speed consistency and may degrade under severe radio obstruction or localization spoofing, so cryptographic acceptance is never based on SybilScore alone. Third, the traceability argument is a proof sketch rather than a machine-verified proof. Future work should add high-density stress sweeps, explicit RSU-failure fault injection, PC5/network-slicing experiments, and a formal symbolic model of the threshold trace protocol.

5. CONCLUSION

This study redesigned PPT-CLAMA for smart mobility and IoV environments by combining mobility-adaptive pseudonym pools, RSU handover caching, compact V2X authentication headers, threshold-governed traceability, and RSU-based Sybil filtering while retaining anonymity, unlinkability, perfect forward secrecy, KSSTIS, and conditional traceability. In the reported Raspberry Pi 4B and SUMO/ns-3 workload, authentication latency was 0.82 ms, high-speed handover success was 99.1%, Sybil blocking was 97.6%, communication overhead was 312 bits, and trace throughput was 28 TPS.

The results indicate that mobility-specific privacy and handover controls can be added without placing identity opening on the routine safety-message path. Conditional tracing remains warrant- or emergency-bound, whereas failed or congested RSUs fall back to neighboring-token validation or full mutual authentication rather than bypassing security. The design is technically aligned with IEEE 1609.2, ETSI ITS security, ISO/SAE 21434, and GDPR Article 32; future validation should extend the density sweep and machine-check the threshold trace protocol.

FUNDING INFORMATION

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (NRF-RS-2023-00237287, 2026S1A5A01004224).

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Haewon Byeon		✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nvestigation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**diting

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

The author states no conflict of interest.

INFORMED CONSENT

This study did not involve human participants or identifiable personal data; informed consent is not applicable.

ETHICAL APPROVAL

This research did not involve human or animal experiments; ethical approval is not applicable.

DATA AVAILABILITY

The derived data and simulation code supporting the findings are included within the article and the accompanying supplementary code file.

REFERENCES

- [1] B. Gong, Y. Wu, A. Badshah, and M. Waqas, "Privacy-preserving and traceable certificateless anonymous mutual authentication scheme for IoT," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 6, pp. 7508–7520, Nov. 2025, doi: 10.1109/TDSC.2025.3597949.
- [2] D. P. M. Osorio *et al.*, "Towards 6G-enabled internet of vehicles: security and privacy," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 82–105, 2022, doi: 10.1109/OJCOMS.2022.3143098.
- [3] S. K. S. V. Naga, R. Yesuraj, S. Munuswamy, and K. Arputharaj, "A comprehensive survey on certificate-less authentication schemes for vehicular ad hoc networks in intelligent transportation systems," *Sensors*, vol. 23, no. 5, p. 2682, Mar. 2023, doi: 10.3390/s23052682.
- [4] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," *Computer Science Review*, vol. 41, p. 100411, Aug. 2021, doi: 10.1016/j.cosrev.2021.100411.
- [5] F. Zhu, X. Yi, A. Abuadba, I. Khalil, X. Huang, and F. Xu, "A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad Hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 10, pp. 10456–10466, Oct. 2023, doi: 10.1109/TITS.2023.3275077.
- [6] Y. Wang, Y. Liu, and Y. Tian, "ISC-CPPA: Improved security certificateless conditional privacy-preserving authentication scheme with revocation," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 12304–12314, Nov. 2022, doi: 10.1109/TVT.2022.3194060.
- [7] L. Meng, H. Xu, H. Xiong, X. Zhang, X. Zhou, and Z. Han, "An efficient certificateless authenticated key exchange protocol resistant to ephemeral key leakage attack for v2v communication in iov," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11736–11747, 2021, doi: 10.1109/TVT.2021.3113652.
- [8] X. Yang, S. Li, L. Yang, X. Du, and C. Wang, "Efficient and security-enhanced certificateless aggregate signature-based authentication scheme with conditional privacy preservation for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 9, pp. 12256–12268, Sep. 2024, doi: 10.1109/TITS.2024.3367925.
- [9] M. Seifelnasr, R. Altawy, A. Youssef, and E. Ghadafi, "Privacy-preserving mutual authentication protocol with forward secrecy for IoT-edge-cloud," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 8105–8117, 2024, doi: 10.1109/JIOT.2023.3318180.
- [10] A. A. Almazroi, E. A. Aldahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *PLoS ONE*, vol. 18, no. 6, p. e0287291, Jun. 2023, doi: 10.1371/journal.pone.0287291.
- [11] Y. Ma, Q. Cheng, and X. Luo, "2PCLA: Provable secure and privacy preserving enhanced certificateless authentication scheme for distributed learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5876–5889, 2023, doi: 10.1109/TIFS.2023.3318952.
- [12] D. Abbasinezhad-Mood, S. M. Mazinani, M. Nikooghadam, and A. Ostad-Sharif, "Efficient provably-secure dynamic ID-based authenticated key agreement scheme with enhanced security provision," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1227–1238, 2022, doi: 10.1109/TDSC.2020.3024654.
- [13] IEEE Computer Society, *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Application and Management Messages*, IEEE Std 1609.2-2022, 2022.
- [14] ETSI, *Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats; Release 2*, ETSI TS 103 097 V2.1.1, Oct. 2021.
- [15] H. T. Lin and W. L. Jhuang, "Blockchain-based lightweight certificateless authenticated key agreement protocol for V2V communications in IoV," *IEEE Internet of Things Journal*, vol. 11, no. 16, pp. 27744–27759, Aug. 2024, doi: 10.1109/JIOT.2024.3400320.
- [16] D. Abbasinezhad-Mood, A. Ostad-Sharif, S. M. Mazinani, and M. Nikooghadam, "Provably secure escrow-less chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7287–7294, 2020, doi: 10.1109/TII.2020.2974258.
- [17] X. Ai, A. Badshah, S. Tu, M. Waqas, and I. Ahmad, "An improved ultra-lightweight anonymous authenticated key agreement protocol for wearable devices," *IEEE Transactions on Mobile Computing*, vol. 24, no. 5, pp. 4543–4557, 2025, doi: 10.1109/TMC.2025.3526076.
- [18] M. Hammad *et al.*, "Lightweight and robust key agreement for securing IIoT-driven flexible manufacturing systems," *IEEE Internet of Things Journal*, vol. 12, no. 11, pp. 17197–17209, 2025, doi: 10.1109/JIOT.2025.3535846.
- [19] A. Shahidinejad and J. Abawajy, "An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT," *ACM Computing Surveys*, vol. 56, no. 7, pp. 1–38, 2024, doi: 10.1145/3645087.

- [20] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, and ..., "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things*, p. 100129, 2021.
- [21] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, "A survey on federated learning for resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 1–24, Jan. 2022, doi: 10.1109/JIOT.2021.3095077.
- [22] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications*, vol. 28, no. 1, pp. 296–312, Feb. 2023, doi: 10.1007/s11036-022-01937-3.
- [23] P. Tedeschi, S. Bakiras, and R. Di Pietro, "IoTrace: A flexible, efficient, and privacy-preserving IoT-enabled architecture for contact tracing," *IEEE Communications Magazine*, vol. 59, no. 6, pp. 82–88, 2021, doi: 10.1109/MCOM.001.2000729.
- [24] ETSI, *Intelligent Transport Systems (ITS); Communications Architecture*, ETSI EN 302 665 V1.1.1, Sept. 2010.
- [25] International Organization for Standardization and SAE International, *Road vehicles—Cybersecurity engineering*, ISO/SAE Standard 21434:2021, Aug. 2021.
- [26] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016 (general data protection regulation)," *Official Journal of the European Union*, vol. L 119, pp. 1–88, May 2016, art. 32.
- [27] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 289–299, 2014, doi: 10.1109/JIOT.2014.2327587.

BIOGRAPHIES OF AUTHORS



Haewon Byeon     is affiliated with the Department of Future Technology, Korea University of Technology and Education, Cheonan, South Korea. His research interests include intelligent security systems, digital health, smart mobility, industrial IoT, privacy-preserving authentication, and applied machine learning. He can be contacted at email: bhwpuma@naver.com; byeon@koreatech.ac.kr.