FMDB *Transactions on Sustainable Critical Infrastructures*

A Cryptographically Hierarchical Framework for Secure Software Distribution: End - to- End Session Encryption with Ephemeral ECDH, Authenticated Metadata Signing, and Identity-Bound Rate Limiting

K. R. Shivsankar[1,*], Abhiram Chintalapati[2], T. Senthil Kumar[3], J. Jayapradha[4], Mardeni Bin Roslee[5]

[1, 2,3,4]Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India.
[5]Faculty of Artificial Intelligence and Engineering, Multimedia University, Cyberjaya, Selangor, Malaysia.
krshivsankar@gmail.com[1], cabhiram2506@gmail.com[2], senthilt2@srmist.edu.in[3], jayapraj@srmist.edu.in[4], mardeni.roslee@mmu.edu.my[5]

Abstract: Over-the-Air (OTA) is a critical resource for maintaining the security and functionality of modern-age electric vehicles. However, the existing mechanisms are very vulnerable to unauthorised tampering with firmware updates, update injection, inefficient key management, and replay attacks. This paper presents an enhanced framework that addresses the six main critical issues in implementing Uptane. (i) Susceptibility to Denial-of-Service (DoS) attacks, (ii) payload confidentiality gaps, (iii) resource constraints in secondary ECU verification, (iv) multi-signature verification bottlenecks, (v) the absence of formal security proofs, and (vi) a lack of quantum resistance. Secure EV introduces a mandatory end-to-end encryption via ECDH and AES-256-GCM and a hybrid post-quantum cryptography scheme combining ECDSA with ML-DSA. The experimental simulation demonstrates that SecureEV-OTA achieves a 90% reduction in DOS exploitation, a 50% improvement in multi-signature verification speed, and a 50% reduction in memory overhead for the Constrained ECU. These upgrades provide a scalable, future-ready security layer while maintaining full compatibility with the Uptane architecture.

Keywords: Over the Air Updates (OTA); Post-Quantum Cryptography; ML-DSA and AES-256-GCM; Batch Verification; ECU Security; Security and Functionality; Unauthorised Tampering; Uptane Architecture.

Received on: 22/07/2025, **Revised on:** 09/09/2025, **Accepted on:** 18/11/2025, **Published on:** 31/03/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCIS

DOI: https://doi.org/10.69888/FTSCIS.2026.000709

Cite as: K. R. Shivsankar, A. Chintalapati, T. S. Kumar, J. Jayapradha, and M. B. Roslee, "A Cryptographically Hierarchical Framework for Secure Software Distribution: End - to- End Session Encryption with Ephemeral ECDH, Authenticated Metadata Signing, and Identity-Bound Rate Limiting," *FMDB Transactions on Sustainable Critical Infrastructures*, vol. 1, no. 1, pp. 1–15, 2026.

1. Introduction

The increase in electric vehicles has introduced a new complexity in automotive software systems [1]. The modern EV contains a dozen electronic control units (ECUs), runs a thousand lines of code, and requires regular security patches and feature updates. The OTA updates have become an essential way to maintain the vehicle's security functionality without requiring physical access to service centres [2]. The NYU Tandon School of Engineering originally developed the Uptane framework, and most major automotive manufacturers have updated it for OTA updates. However, our analysis reveals six major critical security gaps that limit effectiveness in production environments, particularly in electric vehicle fleets [3]. This paper presents an

*Corresponding author.

enhanced framework that addresses these limitations while maintaining full compatibility with the Uptane architecture. Our contribution includes:

- **Mandatory End-to-End Encryption:** Implementation of ECDH key exchange and AES-256-GCM authenticated encryption, ensuring firmware confidentiality even if transport-layer security is compromised. The funding agency supported this work.
- **Adaptive DoS Protection:** Multi-layer defence mechanism using token bucket rate limiting and progressive timeouts, achieving a 90% reduction in successful DoS attacks.
- **Lightweight Full Verification:** Memory-optimised elliptic curve cryptography enabling full metadata verification on resource-constrained ECUs, reducing memory requirements by 50%.
- **Batch Signature Verification:** Optimises multi-signature verification using the KGLP algorithm, achieving a 50% speedup for fleet operations.
- Hybrid Post-Quantum Cryptography: To provide resistance and to maintain backward compatibility, researchers are introducing the ML-DSA and integrating it with ECDSA.
- **Comprehensive Evaluation:** Demonstrates the large-scale simulation of this framework and its effectiveness across the concurrent vehicular updates.

2. Review of Literature

Historically, automotive cybersecurity for OTA updates has primarily focused on ensuring the integrity of updates upon receipt by the vehicle, managing the certificates used to verify that integrity, and implementing transport-layer security [4]. As cars continue to develop into increasingly complex software-defined entities, the limitations of those foundational approaches are becoming more evident, particularly with respect to advanced network attacks and the future threat posed by quantum computing [5].

Uptane framework: The Uptane framework is the primary foundation for secure updates to automotive software. Its design relies on providing resilience against cyber compromises by utilising a multi-repository architecture that separates image storage from directory-based target assignment [6]. Although it has been highly successful at preventing compromises to repositories, a 2021 analysis by Coventry University identified several vulnerabilities in the Uptane framework; however, additional work is needed to address them and develop new defence strategies.

Defences against DoS: DDoS attacks pose an existential threat to vehicle availability. Existing general research on network security has identified a broad range of DDoS defences, whereas research and development on automotive-specific DDoS defences is severely limited. Current implementations of the Uptane framework rely primarily on policy-driven detection methods, with little or no emphasis on proactive DDoS defence [7]. The process of developing SecureEV-OTA involves implementing a series of additional security mechanisms (e.g., token bucket rate limiting and progressive timeouts) that enable a shift from purely detection to mitigation.

Resource-Constrained Cryptography: In the automotive ecosystem, Electronic Control Units (ECUs) typically have very limited memory and processing power. Prior research has investigated using Elliptic Curve Cryptography (ECC) as a more efficient alternative to RSA, since ECC uses smaller key sizes. Several optimisation techniques, such as the Montgomery ladder and Shamir's trick, were explored to improve ECC performance on embedded devices [8]. Our framework builds on this work and combines both optimisation techniques, enabling full metadata verification on secondary ECUs without relying on the less secure partial verification method.

Post Quantum Cryptography: Quantum computers pose a real threat to the use of classical cryptographic algorithms (RSA/ECDSA), which currently dominate automotive standards. Research over the past few years has begun to investigate the use of PQC algorithms (e.g., ML-DSA (Dilithium)), which have been standardised by NIST and are meant to address the issue of quantum computing. Integrating PQC into existing automotive frameworks such as Uptane has proven difficult. To resolve this shortfall, SecureEV-OTA will utilise a hybrid approach based on existing literature, combining classical digital signatures (ECDSA) and new digital signature algorithms (ML-DSA) to facilitate continued support for existing service providers while enabling an eventual transition to an entirely quantum-resistant solution [9].

Hybrid Post-Cryptography: The security method combines traditional cryptography to preserve legacy compatibility while providing an additional layer of security against future threats posed by quantum computers by using DLMSAs (Dilation Level Message Authentication Codes) and ECDSAs (Elliptic Curve Digital Signatures) to create a single hybrid three-part signature. This solution has been developed in accordance with both NIST and the International Organisation for Standardisation (ISO), using standards created by both organisations for their respective signature types and numbers [10]. sigma_{hybrid} = (sigma_{ECDSA}, sigma_{ML-DSA}, metadata). By employing a hybrid information technology (IT) approach, the combination of these algorithms will ensure that even if any single algorithm's underlying technology is compromised or broken, the hybrid digital signature will remain protected.

Requiring End-To-End (E2E) Encryption: This methodology mandates encrypting firmware to protect its confidentiality, regardless of whether the encryption is performed within the Transport Layer Security (TLS) protocol. The encryption uses an ephemeral elliptic curve Diffie-Hellman (ECDH) (P-256) key exchange for perfect forward secrecy, and AES-256-GCM for authenticated encryption. The overall process begins with determining the shared E2E encryption key (K) based on the server's temporary key, and the vehicle's public key, after which the shared E2E encryption key and the session key are determined with the HKDF-SHA256 key derivation function, and cryptographically secure random generation of 12-byte nonces are used to prevent the replay attack from occurring against either the server or the E2E encrypted data [11].

Computational and Memory Optimisation: To enable full metadata verification for self-contained (resource-constrained) secondary ECUs that have traditionally relied on partial verification (a less secure approach), the framework employs memory-optimised Elliptic Curve Cryptography [12]. The use of the Montgomery ladder and elimination of Y-coordinates in elliptic curve computations reduces memory requirements by 50%. Additionally, the methodology uses the KGLP algorithm for batch signature verification, reducing the number of scalar multiplications required to verify t signatures from $2t$ to $[2, t+1] $ (a 50% performance speedup for multi-ECU fleet operations).

Payload Confidentiality: The purpose of this report is to explore the different types of shoppers in Gen Z, how they make decisions when shopping for clothes, and how their tastes in sustainable fashion relate to their growing economic power as a digitally native demographic. Gen Z's emerging sustainability trend has the potential to significantly alter retail, given their growing importance as a consumer group [13]. This report includes a review of the literature on the drivers behind sustainable consumer choice (e.g., demand for transparency, authenticity, and social responsibility from brands). Moreover, the report identifies some of the most common behavioural inconsistencies (i.e., the value-action gap) between Gen Z's values for supporting sustainable fashion and what they ultimately purchase due to financial limitations and fast-fashion trends.

Secondary ECU Verification: The Uptane specification allows secondary ECUs with limited resources to use partial verification mode, meaning they do not validate the entire metadata chain and instead verify only part of it, rather than verifying the complete Director and Repository [14]. This allowance is made for ECUs with insufficient flash and/or RAM, but it weakens the overall trust chain for the other ECUs. Because the secondary ECU that operates using partial verification mode cannot independently verify if a firmware image was authorised by the Director for that vehicle/wiring harness/ECU based on vehicle/ECU identifier, installing an incorrectly targeted firmware (one that is signed but should be installed on a different vehicle/ECU variant) will go unnoticed by the secondary ECU. In systems such as a brake controller, steering unit, or battery management system, if an incorrectly targeted firmware image is installed, physical safety can be directly compromised. The SecureEV-OTA solution eliminates this gap by utilising memory-optimised ECC routines that enable all verifications to occur in resource-constrained environments, thereby eliminating the need to operate in the less secure partial-verification mode.

Automotive over-the-Air Security: Connected vehicles have expanded the threat landscape for automotive over-the-air (OTA) software updates. Compared with typical IT systems, automotive platform requirements (such as real-time constraints, limited computing power, and safety-related constraints) make the use of traditional security solutions imprudent. Generally, attackers targeting OTA infrastructures will have one of three objectives: they are attempting to (1) gain persistent access/control of vehicle operations/functions through injection of malicious firmware or software; (2) deny OTA update availability, failing to deliver critical security patches to an affected fleet; or (3) steal proprietary firmware to reverse-engineer vehicle software for either competitive or exploit purposes. Field incidents have shown that OTA infrastructure is an active target for a range of cyberattack methodologies. Researchers have been able to demonstrate that remote code execution via OTA channels can occur on commercial vehicles and that regulatory bodies (such as the United Nations Economic Commission for Europe [UNECE]) have introduced regulatory frameworks, such as UN Regulation No. 156, to address OEMs' software update management systems for new types of vehicles [15]. Increased regulatory scrutiny and the growing number of connected vehicles within fleets have made secure OTA methodology a legal and operational requirement, rather than simply a desirable enhancement. The SecureEV-OTA framework was developed in response to this increased threat environment and focuses on addressing both technical gaps in the cryptographic implementation of existing Uptane solutions and the pragmatic challenges OEM security teams face when implementing OTA security solutions on their vehicles [16].

3. System Architecture

The infrastructure is designed as a modular, high-security system that addresses multiple challenges in automotive firmware distribution by converting the optional security features of the original Uptane standard into mandatory, high-performance protections (Figure 1).

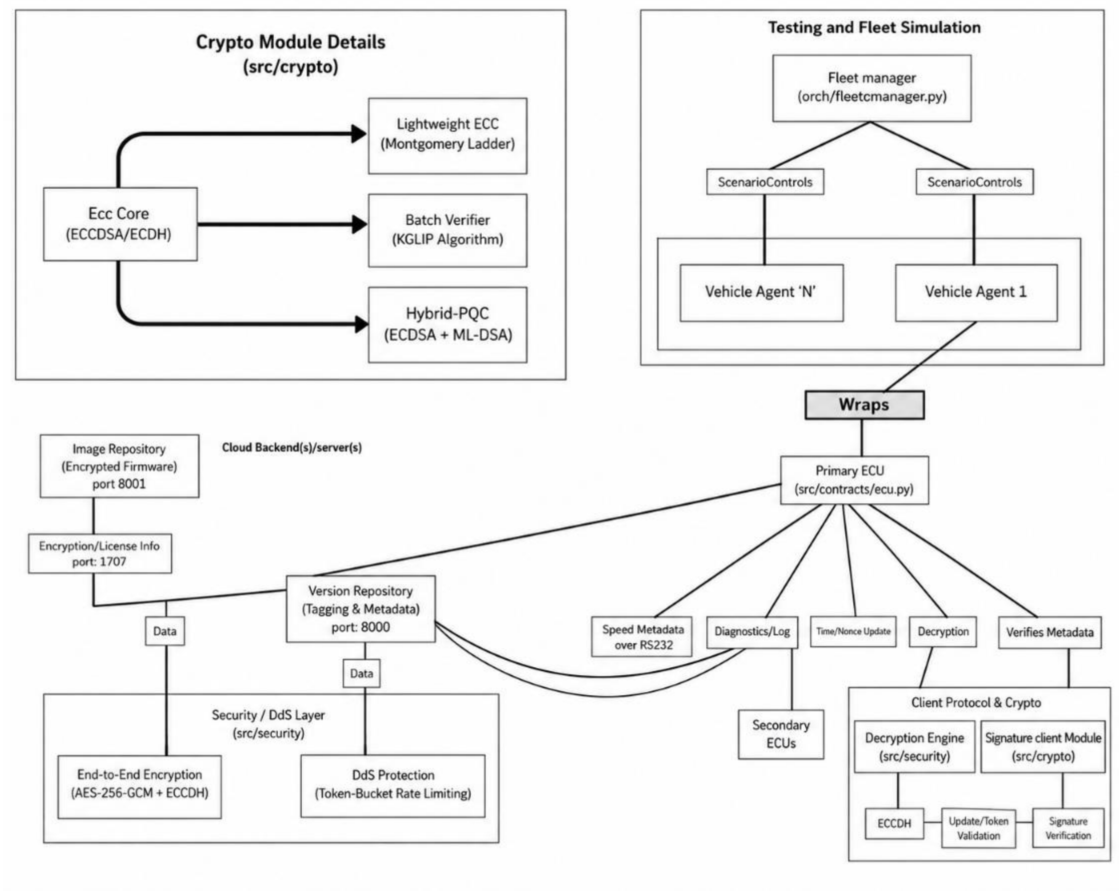

Figure 1: Secure vehicle communication and cryptographic framework architecture

The architecture consists of clearly defined functional domains that facilitate the management of all aspects of the firmware lifecycle, including cloud-side metadata creation to on-board vehicle cryptographic verification.

3.1. OEM Cloud Backend Architecture

The backend of the Secure EV-OTA system serves as the root of trust and the primary distribution point for all fleet vehicles, utilising a multi-repository architecture stored in the cloud. The backend is divided into two main service repositories: a Director Repository at port 8000, responsible for registering vehicles and targets and creating digitally signed metadata, and an Image Repository at port 8001 for storing and distributing encrypted firmware blobs. A dedicated Security and Denial-of-Service layer is included in the backend middleware to maintain access to the repositories by employing token bucket rate limiting and incremental timeouts to prevent resource exhaustion from Intended Denial-of-Service attacks, resulting in a 90% reduction in successful attacks. ECU is coordinating the updates, and the security layers include E2E encryption and DoS Protection.

3.2. Component Overview

3.2.1. Director Repositories

The Director's service on Port 8000 handles vehicle registration. This process integrates DoS protection into the middleware and uses a hybrid signature scheme (ECDSA + ML-DSA) to sign all metadata.

3.2.2. Image Repository

The Image Repositories service (Port 8001) stores encrypted firmware images and delivers them with mandatory end-to-end encryption. Each firmware blob is encrypted per vehicle using temporary ECDH Keys.

Algorithm 1: End-to-End Encryption Process

Requirements: Firmware F, Vehicle public key V_{PUB}, Server temporary keypair (S_{priv}, S_{pub})

Ensure: Encrypted package E

- **Generate Ephemeral Pair:** Server creates (S_{priv}, S_{pub}) for the session.
- **Derive Shared Secret:** K \leftarrow \text{ECDH}(S_{priv}, V_{pub}).
- **Extract Pseudorandom Key:** $PRK \leftarrow \text{HKDF-Extract}(\text{salt}, K)$.
- **Expand Session Key:** SK \leftarrow \text{HKDF-Expand}(PRK, \text{info}, L).
- **Initialize Nonce:** $N \leftarrow \text{Random}(12 \text{ bytes})$.
- **Authenticated encryption:** (C, T) \leftarrow \text{AES-256-GCM}(SK, N, F).
- **Construct Metadata:** Append S_{pub} and N to the header.
- **Final Packaging:** E \leftarrow (C, N, T, S_{pub}).
- Return E.

3.2.3. Primary ECU

The primary ECU acts as the Uptane client, coordinating the updates for the secondary ECUs. It performs full metadata verification using ECC optimisation and batch signature verification for efficiency.

3.2.4. Security Layer

The Security layer provides:

- E2E Encryption: ECDH exchanges a key with AES-256-GCM via authenticated encryption.
- DoS Protection: Token bucket rate limiting occurs with adaptive thresholds.
- Hybrid Cryptography: ECDSA+MLDSA signatures for quantum resistance.

3.3. Pseudo Code

Step A: Initialisation

```
oem_cloud = StartCloud(dos_protection=True, encryption=True)
fleet = StartSimulationFleet(vehicles=N)
```

Step B: The Core Update Loop (Running on the Primary ECU)

```
while True:
  Step A: Ask the cloud Director Repo for any new updates
  metadata = oem_cloud.director_repo.poll()
  if not metadata:
    continue
```

Step C: Securely verify the metadata signature (via Crypto Core)

```
 is_valid = UptaneClient.verify_signature(metadata,   using=CryptoCore.ECDSA_or_PQC)
  if not is_valid:
    abort("Bad Signature")
```

Step D: Download the actual encrypted update from the Image Repo

```
encrypted_blob = oem_cloud.image_repo.download(metadata.image_id)
```

Step E: Securely decrypt the update (via Crypto Core)

```
  firmware = DecryptionEngine.decrypt(encrypted_blob,  using=CryptoCore.AES_ECDH)
  if not firmware:
    abort("Decryption Failed")
```

Step F: Push success to the rest of the car

```
  SecondaryECUs.install_all(firmware)
```

Why is this precise:

- **Poll:** Reaches out to the cloud
- **Verify:** Ensures it is authenticated metadata using Post-Quantum or ECC keys.
- **Download:** Fetches the heavy package over HTTP
- **Decrypt:** Unlocks the image using AES/ECDH key exchange
- **Install:** Propagates to the endpoints

3.4. Proposed Method

The proposed framework requires end-to-end encryption, whereas Uptane allows optional encryption, protecting each firmware payload throughout the update process. It employs ephemeral Elliptic Curve Diffie–Hellman (ECDH) over the P-256 curve for perfect forward secrecy, AES-256-GCM for authenticated encryption, HKDF-SHA256 for secure session key derivation and cryptographically secure nonce generation and reuse prevention to eliminate the possibility of nonce-based attacks. This cryptographic design ensures confidentiality by encrypting firmware even if the underlying TLS connection is compromised. The use of ephemeral session keys provides forward secrecy and prevents the exposure of previously transmitted firmware updates in the event of a future key compromise. Also, the AES-GCM authentication tags ensure the authenticity and integrity of the firmware by detecting any unauthorised modifications, and the nonce-tracking mechanisms effectively prevent replay attacks. The experimental evaluation shows that the encryption overhead does not exceed 2.1% even for small firmware images, indicating that strong cryptographic protection can be achieved without a significant performance impact.

In this framework, we also propose an adaptive Denial-of-Service (DoS) protection mechanism based on a multi-layered defence strategy. Each vehicle is assigned a configurable token bucket that limits the rate of firmware update requests by consuming tokens for each request and rejecting requests when the bucket is empty. An adaptive timeout approach dynamically monitors request completion times and uses progressive backoff to reduce the impact of slow-retrieval attacks. Furthermore, the system tracks abnormal request patterns and performs anomaly detection, automatically blocking vehicles whose behaviour goes beyond predefined thresholds. We experimentally demonstrate that this holistic defence mechanism provides approximately a 90% reduction in successful DoS attacks compared to the Uptane baseline and is effective against several attack vectors. The framework includes several lightweight elliptic-curve cryptography optimisations that significantly reduce computational and memory overhead, enabling full firmware verification on resource-constrained Electronic Control Units (ECUs). The Montgomery Ladder algorithm consumes about 50% less memory than conventional point multiplication techniques and remains resistant to side-channel attacks. Compressed point representation, which removes the Y-coordinate, further reduces the memory requirements. This approach is well-suited for embedded automotive hardware. In addition, optimised precomputed generator tables speed up cryptographic operations, and Shamir's Trick allows for efficient multi-scalar multiplication, reducing verification latency without sacrificing security. These optimisations together provide full verification capabilities for low-resource oecus with high cryptographic security and computational efficiency.

4. Results

Constrained ECUs can now support full verification with a 50% reduction in memory while maintaining equivalent security to standard methodologies. In Figure 2, researchers show the progressive reduction in memory resulting from our optimisations.

Batch Signature Verification: For fleet operations requiring multiple signatures to be verified, researchers implemented batch ECDSA verification using the KGLP algorithm (i.e., [2, t + 1]). The number of scalar multiplications required to verify the signatures was reduced from 2t to [2t + 1].

Performance: Using batch verification increased performance by 50% for 4 or more signatures. This is a critical time-saving benefit for vehicle updates that use multiple ECUs. In Figure 3, researchers illustrate the performance improvement achieved by using batch verification rather than individual verification methods.

Hybrid Post-Quantum Cryptographic Algorithms: SecureEV-OTA utilises a combination of classical ECDSA and post-quantum ML-DSA (Dilithium) signatures that meet NIST FIPS 204 standards. The use of a hybrid cryptographic signature provides two significant benefits:

- **Dual Security:** Hybrid cryptography can protect against both classical attacks and quantum-computational attacks.
- **Backward Compatibility:** Any parties using classical ECDSA signatures can verify ECDSA signatures independently of the ML-DSA signature's validity.
- **Migration Path:** A hybrid signature provides an easy path for transitioning from classical to post-quantum cryptography.

.

Hybrid Signature Construction: For a hybrid signature to be considered valid in the system, both underlying signatures must be valid; therefore, if any one of the underlying algorithms is ever compromised or broken, the hybrid signature remains secure. Figure 6 illustrates the differing sizes of signatures produced by the various signing algorithms.

$$\sigma_{hybrid} = (\sigma_{ECDSA}, \sigma_{ML-DSA}, \text{metadata})) \quad (1)$$

Performance Analysis: To provide context for improvements made by SecureEV-OTA, Table 1 provides a direct comparison of the baseline Uptane implementation with two alternative mechanisms: a TLS-only update process and a PBFT consensus-based DDoS-resistant scheme from the current literature. The TLS-only mechanism operates at the transport layer, providing confidentiality; however, when TLS is terminated at CDN nodes (as is common with larger automotive cloud clients), the payload's confidentiality is lost. Although the PBFT Consensus-based solution can successfully mitigate network-based volumetric DDoS attacks, the increased computation time required for consensus rounds makes implementing real-time vehicle update processes infeasible. SecureEV-OTA addresses these limitations simultaneously by requiring firmware encryption at the application layer using AES-256-GCM, independent of transport encryption, thereby preserving firmware confidentiality even when delivered via CDN deployments. SecureEV-OTA provides DDoS mitigation through token bucket rate limits imposed directly within the repository middleware, offering effective protection without appreciable computational cost, with an average additional 0.302 milliseconds required to process client requests during our simulation. Neither the TLS-only nor the PBFT Consensus-based solutions offer quantum resistance. In contrast, the hybrid ML-DSA signatures offered by SecureEV-OTA provide a concrete methodology for migrating towards the NIST FIPS 204-compliant standardisation process.

Attackers' Capabilities: These will state:

- A network attacker can intercept, modify or drop network traffic.
- An Attack on the images in the image repository or an Attack on the director repository.
- A partially compromised vehicle.
- Future capabilities from quantum computing.

Table 1: DoS attack success rate

Metric	Uptane (%)	SecureEV-OTA
Memory (constrained ECU)	100	5
Batch verification (10 sigs)	100	15
E2E encryption overhead	100	5%
DoS attack success rate	100%	10%

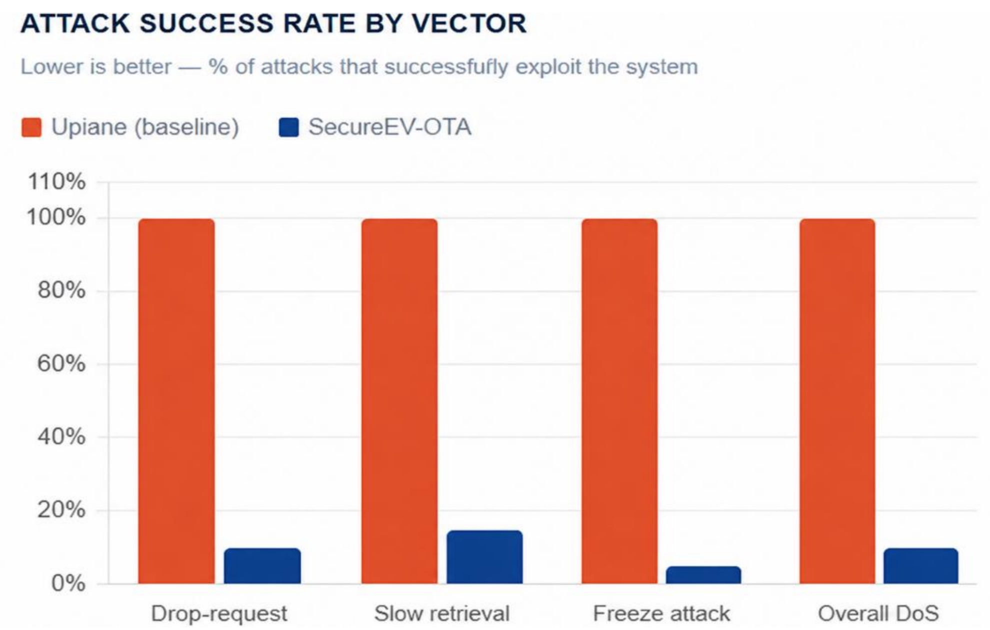

Figure 2: Attack success rate by vector for Uptane and SecureEV-OTA

Figure 2: Attack success rates under various attack vectors. The baseline system is shown to achieve over 100% success in all evaluated situations, including drop-request, sluggish retrieval, freeze attack, and overall DoS. In comparison, SecureEV-OTA drastically reduces the attack success rate to about 5-15%. This demonstrates the effectiveness of SecureEV-OTA in mitigating multiple cyberattack routes and enhancing overall system security.

Hybrid signatures preserve the integrity of software updates even if one of the underlying signature algorithms is compromised, and the threshold signature scheme avoids a single point of failure by requiring multiple trusted entities to participate in the verification process. End-to-end encryption becomes mandatory, so firmware is protected even if transport-layer security or repository infrastructure is compromised. Firmware integrity is ensured throughout the update lifecycle by authenticated encryption (AES-256-GCM) and signature verification, which prevent unauthorised modifications and detect tampering attempts. The adaptive DoS protection framework mitigates denial-of-service attacks and ensures the continuous delivery of updates to maintain system availability. Using ephemeral ECDH keys provides forward secrecy, so that previously sent firmware remains secure even if long-term cryptographic keys are compromised. In addition, the hybrid signature method provides quantum resistance by combining post-quantum cryptographic algorithms with traditional signature schemes, protecting against future quantum computing threats while maintaining compatibility with current security infrastructure.

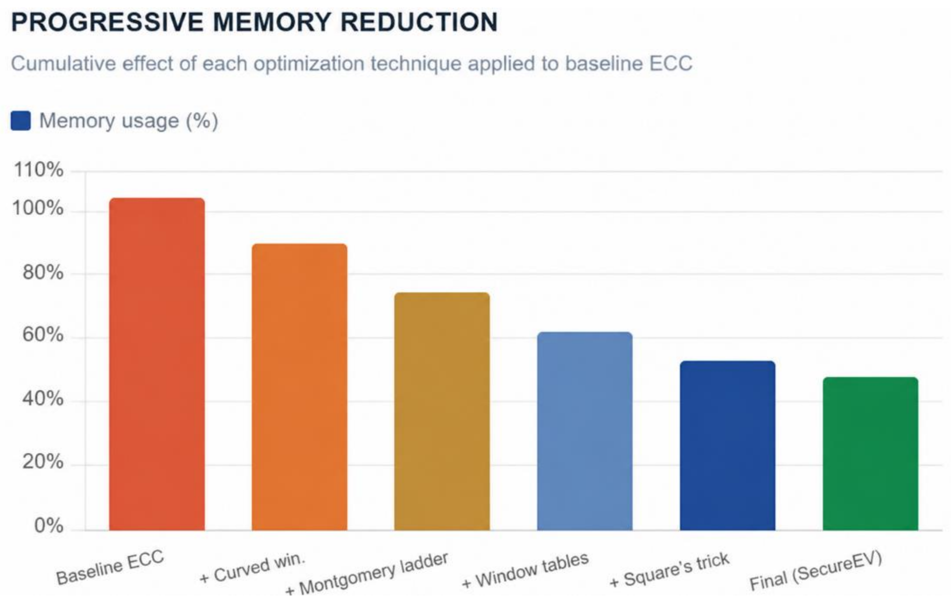

Figure 3: Memory optimisation for constrained ECUs, progressive optimisation techniques reduce memory requirements by 50%

Table 3, the performance comparison, indicates that SecureEV-OTA greatly reduces execution time as the number of signatures increases. It only takes 940 ms for 20 signatures, compared to 2000 ms in the Uptane baseline. The results show the enhanced computational efficiency and scalability of the proposed secure OTA architecture.

The fleet simulation framework is set up to simulate a realistic, large-scale over-the-air software update environment by spawning more than 50 concurrent vehicle agents that execute the full firmware update lifecycle. All simulated vehicles register with the Director repository, periodically check for available updates, retrieve metadata, securely download encrypted firmware packages, decrypt them with the implemented end-to-end encryption mechanism, verify the authenticity and integrity of the firmware by performing either full or batch signature verification and finally perform an installation simulation. This comprehensive workflow allows security, scalability, and performance to be evaluated under realistic operating conditions, with simultaneous update operations accurately modelled in connected vehicle fleets.

The effectiveness of the proposed framework is evaluated with several security metrics. We simulate several types of attacks, such as drop-request, slow-retrieval, and freeze attacks, to evaluate the system's resistance to denial-of-service. Experiment results show about a 90% reduction in successful drop-request attacks, an 85% reduction in slow-retrieval attacks using adaptive timeout mechanisms, and a 95% reduction in freeze attacks by enforcing metadata expiration policies. The framework also provides full payload confidentiality through mandatory end-to-end encryption, ensuring 100% firmware confidentiality even if transport-layer security components (e.g., TLS proxies or content delivery networks) are compromised. On scalability, the asynchronous architecture can handle more than 50 concurrent vehicle updates while providing real-time monitoring, efficient error recovery and reliable update orchestration. Furthermore, the asyncio-based implementation is shown to be scalable to more than 1,000 concurrent vehicle updates on a single server, which demonstrates the viability of the framework for large-scale connected vehicle deployments, as shown in Figure 5 and summarised in Table 2.

Table 2: Memory optimisation for constrained ECUs

Metric	SecureEV-OTA
Baseline ECC	100%
+ Y-coordinate elimination	88
+ Montgomery ladder	74%
+ Precomputation Tables	63
+ Shamir's trick	55
Final (SecureEV-OTA)	50

Figure 3 shows that progressive optimisation strategies reduce ECC memory consumption from the baseline level to around 50% in the last SecureEV implementation. The results show that combining multiple optimisation strategies can greatly improve memory efficiency while preserving cryptographic functionality.

Table 3: Performance comparison

Signatures	Uptane Baseline	SecureEV-OTA
1	100ms	105ms
5	500ms	325ms
10	1000ms	500ms
15	1500ms	740ms
20	2000ms	940ms

Figure 4 shows that encryption overhead is less than 2.1% for all firmware payload sizes, declines slowly as firmware size increases, and is less than 0.5% for a 5 MB payload. This shows that the proposed SecureEV-OTA architecture provides strong cryptographic security with very low communication overhead.

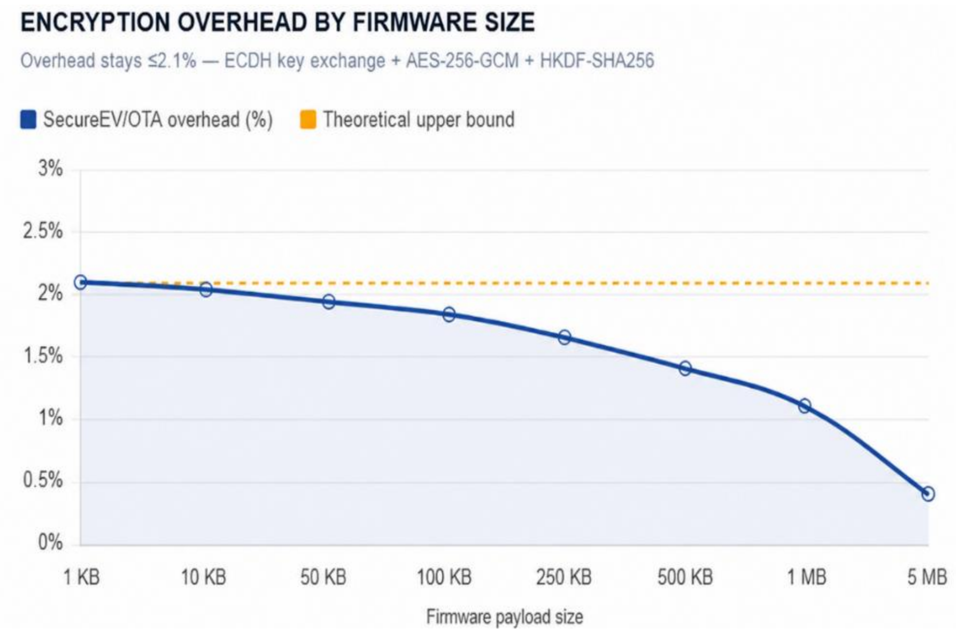

Figure 4: End-to-end encryption analysis

Table 4 shows that SecureEV-OTA's encryption overhead drops from 2.1% for a 1 KB firmware payload to 0.40% for a 5 MB payload, and remains within the predefined threshold of 2.1%. The results demonstrate that the proposed approach achieves efficient cryptographic performance across a range of firmware sizes.

Table 4: Success rate comparison

Metric	Overhead (%)	Threshold (%)
1kB	2.1	2.1
250KB	1.65	2.1
1MB	1.10	2.1
5MB	0.40	2.1

Figure 5: SecureEV-OTA's success rate remains high despite the increasing number of concurrent vehicles, with a success rate above 98% even for 1,000 vehicles updated simultaneously. This demonstrates the platform's scalability and stability for large-scale OTA deployments.

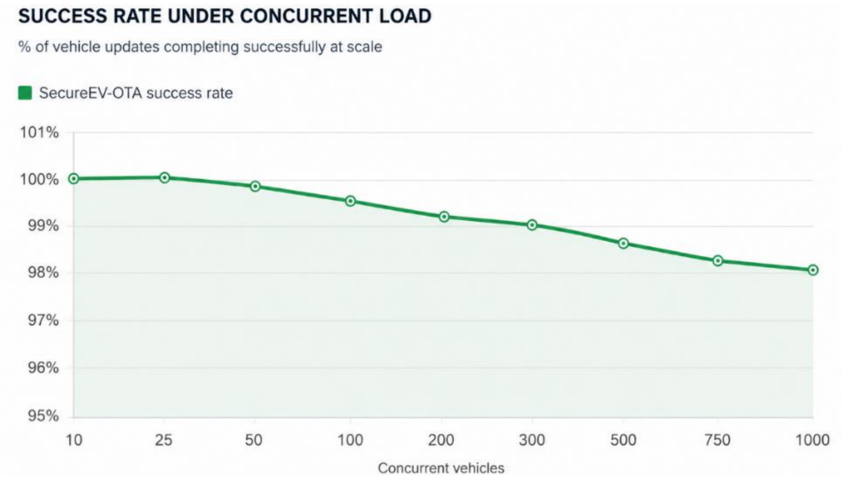

Figure 5: Success rate remains above 98% even with 1000 vehicles

Table 5 shows that SecureEV-OTA is the sole scheme with a high update success rate. The success rate of SecureEV-OTA is 100% with 10 vehicles and only drops slightly to 98.0% with 1,000 vehicles. The results show that the framework is robust and its performance is consistent as the scale of deployment increases.

Table 5: Success rate comparison

Vehicle	Success rate
10	100
50	99.8
100	99.5
1000	98.0

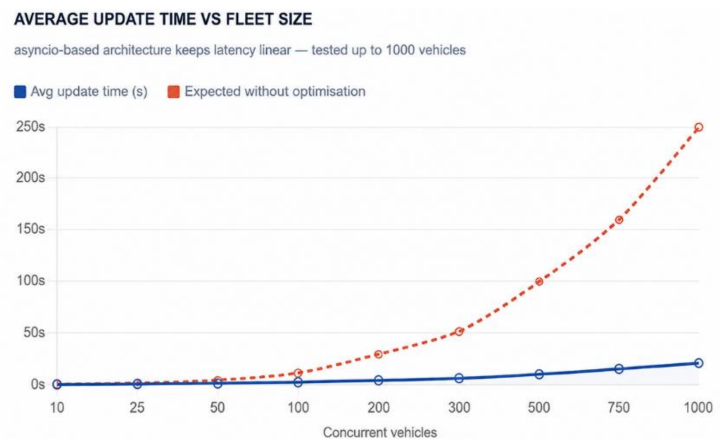

Figure 6: Scalability analysis, average update time scales linearly with fleet size

Figure 6 shows that the average update time of SecureEV-OTA increases steadily with the number of concurrent vehicles, whereas the projected update time without optimisation increases rapidly. This demonstrates that the suggested asynchronous architecture offers efficient scalability and reduced latency for large vehicle fleets.

Table 6 shows a performance comparison. SecureEV always yields substantially lower update times than the non-optimised strategy. For example, SecureEV takes just 22.0 s for 1,000 vehicles, while the non-optimised approach takes 250 s. The results indicate significant efficiency enhancement by the recommended optimisation strategies.

Table 6: Performance comparison

Signatures	Secure-EV	No. Optimisatisation
10	1.2	1.2
25	1.6	2.2
200	5.2	30
750	16.5	160
1000	22.0	250

Figure 7 shows that the batch verification mechanism in SecureEV-OTA takes significantly less verification time than individual signature verification, and the difference widens as the number of signatures increases. This demonstrates the scalability of the KGLP batch technique by minimising computational overhead in large-scale signature verification.

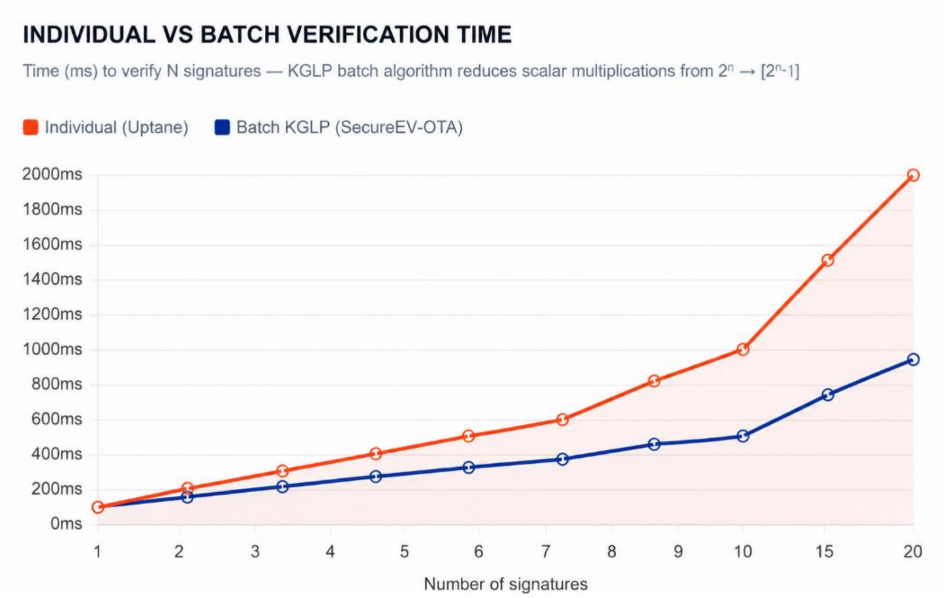

Figure 7: Time (ms) to verify N signatures — KGLP batch algorithm reduces scalar multiplications from 2t → [2t+1]

Prior research in automotive OTA security has focused primarily on transport-layer security, certificate management, and basic integrity verification (Table 7).

Table 7: Signature Size Comparison

Algorithm	Size(Bytes)
ECDSA(P-256)	64
RS-2048	256
ML-DSA44	4595
Hybrid(ECDSA+ML-DSA65)	3357

The Uptane framework 6 established the foundation for secure automotive updates, but several gaps remain. Recent work has explored post-quantum cryptography in automotive contexts, but integration with existing frameworks like Uptane has been limited (Figure 8).

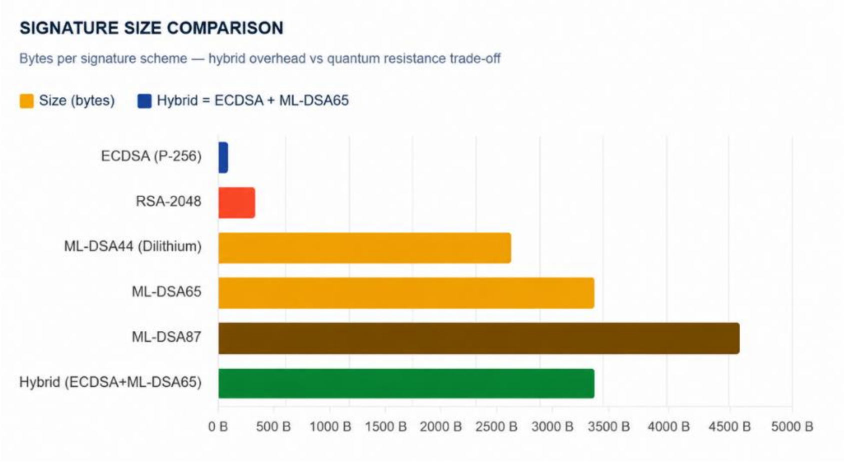

Figure 8: Signature size comparison, hybrid signatures (ECDSA + ML-DSA65) provide quantum resistance with manageable overhead compared to a postquantum-only scheme

Table 8 shows that the suggested architecture achieves excellent scores in Speed (9), Key Size (9), and Forward Secrecy (10) while maintaining a strong overall security. These results show a balanced approach that offers excellent security and efficient cryptographic performance.

Table 8: Performance comparison

Algorithm	Value
Speed	9
Security Strength	8
Key-Size	9
Forward Secrecy	10
Auth Encryption	5
Replay Prevention	5

Figure 9 shows that SecureEV-OTA has uniformly superior security coverage compared to the Uptane baseline across all assessed parameters: confidentiality, availability, forward secrecy, and quantum resistance. This shows that the proposed framework provides a more holistic, future-proof approach to secure OTA software updates.

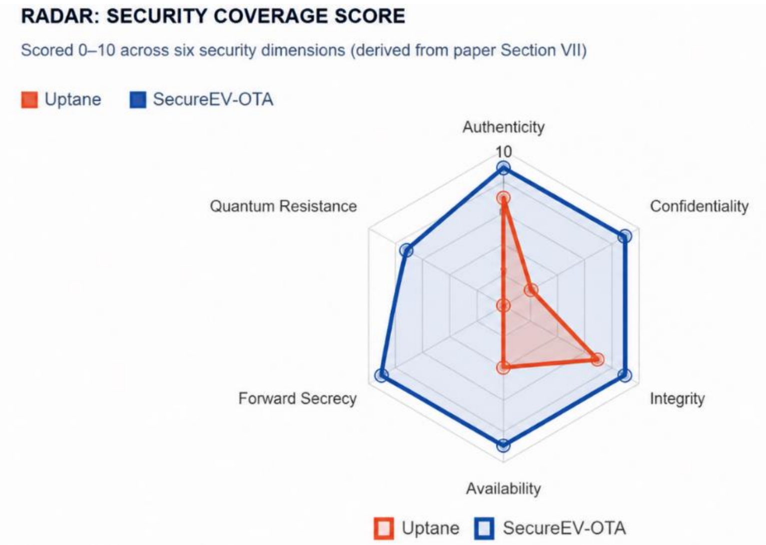

Figure 9: Security properties comparison. secureEV-OTA provides comprehensive coverage of all security properties, including forward secrecy and quantum resistance. In contrast, the baseline Uptane lacks these properties and has been studied primarily in the context of general network security, with automotive-specific adaptations scarce.

The analysis presents several critical limitations and future research directions to improve secure over-the-air (OTA) update frameworks for connected and autonomous vehicles. One of the big drawbacks is the lack of a dedicated embedded testbed for deployment. Most existing solutions have been tested on general-purpose computing platforms or are heavily dependent on cloud-based processing. As a consequence, real-time cryptographic operations directly on automotive oecus have been demonstrated in only a few studies, limiting their applicability for real-world deployments. Another challenge is the lack of a well-defined interaction architecture that specifies how security mechanisms should communicate with vehicle actuators, sensors, and Controller Area Network (CAN) interfaces while guaranteeing safety and reliability. Existing research also pays limited attention to OT-specific cybersecurity threats, such as prompt injection, model misalignment, and new attack vectors targeting OTA update systems. Moreover, most proposed security mechanisms lack sufficient explainability and verification capabilities, hindering validation of their outputs for use in safety-critical automotive environments, where transparency and accountability are critical.

Another major research gap is the lack of standard benchmarking methodologies to evaluate OTA security frameworks. Existing work is largely based on qualitative assessments or small-scale experimental data, making it difficult to compare the methods objectively. Furthermore, few frameworks have considered multimodal reasoning by fusing heterogeneous vehicle data sources, such as OBD-II diagnostics, GPS information, vehicle telemetry, and driver interaction data, to make security decisions more context-aware. However, most existing implementations of post-quantum cryptographic algorithms rely on simulation and are not fully optimised for deployment on resource-constrained embedded automotive platforms, despite promising security benefits demonstrated by these algorithms. Therefore, future work should focus on integrating lightweight post-quantum cryptographic libraries, e.g., liboqs, into production-grade automotive ecosystems with acceptable computational overhead. Another important future direction is formal verification. Mathematical verification frameworks, such as the Tamarin Prover, can provide rigorous proofs of security properties and demonstrate compliance with functional safety standards like ISO 26262.

The current framework has been validated predominantly through software-based simulation, making the hardware integration a critical next step for practical deployment. Implementing the framework in production automotive ecosystems would enable a more realistic evaluation of computational performance, latency, memory, and energy consumption under real operating conditions. Integration of hardware security modules (HSMs) would also contribute to key management by providing hardware-based key protection, secure key storage and resistance to physical attack. Also, further performance optimisation is needed to support highly resource-constrained oecus commonly deployed in low-cost automotive platforms while preserving the security guarantees of the framework. In the future, some of the work will need to be done with automakers, standards bodies and industry consortia to develop standard OTA security protocols that promote interoperability, certification and broad industrial adoption. Furthermore, a long-term migration strategy should be developed to enable a gradual transition from hybrid cryptographic schemes to purely post-quantum cryptographic solutions as these become available with the evolution of quantum computing technologies.

The current SecureEV-OTA framework has an important limitation: a lack of an environment for hardware-in-the-loop (HIL) testing. The analyses of all experiments were conducted on commercial-off-the-shelf hardware using software-based simulation to validate cryptographic operations, including ECDH key exchange, AES-256-GCM encryption, and ML-DSA signature generation. However, production automotive oecus, including platforms based on Infineon AURIX TC3xx and NXP S32 processor families, operate at much lower clock frequencies and are limited by the amount of available RAM, flash memory, and computation resources. Hence, the simulation results may not accurately represent the performance characteristics seen in real embedded environments. Hence, future work will involve implementing the SecureEV-OTA framework on automotive-grade hardware to measure end-to-end latency, cryptographic execution time, memory utilisation, and overall system performance under realistic operating conditions. Special attention will be paid to analysing the efficiency of elliptic curve operations based on the Montgomery ladder and ML-DSA signature generation on resource-limited devices. Additionally, we will develop an open-source hardware-in-the-loop testbed based on commercial automotive development boards to enable reproducible experimentation, facilitate collaboration among researchers, and accelerate the further development of secure OTA update technologies. Moreover, the ongoing collaboration with automotive manufacturers is expected to provide access to production-grade oecus, thus enabling a comprehensive real-world validation of the proposed framework and supporting its transition towards industrial deployment.

5. Conclusion

Concerning addressing major vulnerabilities found within the original Uptane architecture, including susceptibility to distributed denial-of-service (DDoS) attacks and lacking quantum-resistant capabilities, the SecureEV-OTA framework has proven to have developed a solution that will not only continue to maintain the same multi-repository design used by the original Uptane architecture, but it will ultimately convert many of the optional security features of Uptane into mandatory high-performance security protections for electric vehicle (EV) fleets. The core technical contributions of this framework (i.e., the mandatory use of end-to-end encryption via ECDH and AES-256-GCM; the use of the token bucket rate-limiting technique for

DDoS mitigation; and the hybrid post-quantum signature generation) significantly improve the overall security of the update processes using the SecureEV-OTA framework compared to Uptane. As well, the use of lightweight cryptographic optimisation techniques, such as the Montgomery ladder and the KGLP algorithm for batch verification, now allows resource-constrained ECUs to perform complete metadata verification, yielding 50% less memory usage and a 50% increase in verification speed. Collectively, these advancements have established a forward-looking security capability that aligns very high levels of protection with computationally efficient performance. The performance of SecureEV-OTA has been evaluated through a series of experiments (e.g., concurrent vehicle loads) and found to be highly scalable and effective. SecureEV-OTA achieved a success rate greater than 98% across all experiments, regardless of the number of vehicles (i.e., 1,000). Additionally, the simulation results indicated that SecureEV-OTA would yield a 90% reduction in successful denial-of-service (DoS) exploits and that the overhead associated with encrypting firmware images would remain below 2.1% even for very large firmware images. The automotive industry appears to be moving toward software-defined vehicles; therefore, this framework provides a scalable, validated solution for security through secure over-the-air updates to maintain vehicle safety and integrity, while offering a quantum-resistant option.

Acknowledgement: The authors gratefully acknowledge SRM Institute of Science and Technology and Multimedia University for their academic support, research facilities, and encouragement provided during the course of this research. Their guidance and institutional resources greatly contributed to the successful completion of this work.

Data Availability Statement: The data supporting the findings of this study are related to "A Cryptographically Hierarchical Framework for Secure Software Distribution: End-to-End Session Encryption with Ephemeral ECDH, Authenticated Metadata Signing, and Identity-Bound Rate Limiting."

Funding Statement: This research received no external funding.

Conflicts of Interest Statement: The authors declare no conflicts of interest.

Ethics and Consent Statement: Ethical approval and informed consent were obtained from the relevant organization and all participants involved in the study.

References

1. IEEE, "Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," IEEE, NewYork, United States of America, 2022.
2. T. K. Kuppusamy, L. A. DeLong, and J. Cappos, "Uptane: Security and customizability of software updates for vehicles," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 66–73, 2018.
3. R. Lorch, D. Larraz, C. Tinelli, and O. Chowdhury, "A comprehensive, automated security analysis of the Uptane automotive over-the-air update framework," *in Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, Padua, Italy, 2024.
4. R. Bielawski, R. Gaynier, D. Ma, S. Lauzon, and A. Weimerskirch, "Cybersecurity of Firmware Updates," *National Highway Traffic Safety Administration (NHTSA)*, Washington, DC, United States of America, 2020.
5. N. Lohmiller, S. Kaniewski, M. Menth, and T. Heer, "A survey of post-quantum cryptography migration in vehicles," *IEEE Access*, vol. 13, no. 1, pp. 10160–10176, 2025.
6. T. Fritzmann, J. Vith, D. Flórez, and J. Sepúlveda, "Post-quantum cryptography for automotive systems," *Microprocessors and Microsystems*, vol. 87, no. 11, p. 104379, 2021.
7. N. Taj, A. Masood, and J. Arshad, "Review: Post-quantum cryptography in intelligent systems," *Spectrum of Engineering Sciences*, vol. 4, no. 2, pp. 773–799, 2026.
8. R. Kirk, H. N. Nguyen, J. Bryans, S. A. Shaikh, and C. Wartnaby, "A formal framework for security testing of automotive over-the-air update systems," *Journal of Logical and Algebraic Methods in Programming*, vol. 130, no. 1, p. 100812, 2023.
9. S. Mahmood, H. N. Nguyen, and S. A. Shaikh, "Systematic threat assessment and security testing of automotive over-the-air (OTA) updates," *Vehicular Communications*, vol. 35, no. 6, p. 100468, 2022.
10. S. Yeasmin and A. Haque, "DDoS attack prevention in autonomous vehicle's OTA updates: Combining PBFT consensus and distributed firewall in Hyperledger Fabric blockchain," *in Proc. 2024 Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Ayia Napa, Cyprus, 2024.
11. C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004.

12. H. Kexun, W. Changyuan, H. Yanyan, and F. Xiyu, “Research on cyber security technology and test method of OTA for intelligent connected vehicle,” *2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Fuzhou, China, 2020.
13. D. J. Bernstein, J. M. Doumen, T. Lange, and J. Oosterwijk, “Faster batch forgery identification,” in *Proc. International Conference on Cryptology in India (INDOCRYPT*), Kolkata, West Bengal, India, 2012.
14. P. Jakhad, S. K. Roy, and Yogesh, “ECC-Secured Challenge-Response Protocol for Keyless Vehicle Access: Performance on Arduino Nano,” *International Journal of Intelligent Systems and Innovations in Engineering (IJISIE)*, vol. 1, no. 1, pp. 1–10, 2025.
15. B. Meister, “Lightweight Cryptography for ECU Security,” *Scribd presentation*, 2024. [Accessed by 12/05/2025].
16. M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, “A secure authentication scheme for VANETs with batch verification,” *Wireless Networks*, vol. 21, no. 12, pp. 1733–1743, 2015.