

# Abstract

The Internet of Vehicles (IoV) is a large-scale, highly dynamic network of heterogeneous communications. Maintaining a balance between authentication and privacy is crucial in such types of networks. Moreover, ensuring a high level of security through heterogeneous communication can result in significant computational overhead due to the numerous cryptographic operations required, which have higher execution times. Such trade-off between security and efficiency, are impractical in IoV networks, where the IoV devices have limited processing power and storage capacity. Furthermore, diverse communications generate substantial data that requires secure storage. Therefore, it is essential to minimize data storage and retrieval times to facilitate real-time communication in rapidly changing resource-constrained IoV network. These problems can be solved using lightweight security solutions that make sure users are authenticated without compromising their privacy. These solutions can also improve the trade-off between security and performance and make it easier to store and retrieve the large amounts of data that are created by different types of communication in the IoV network.

The research is conducted in two phases. The first phase proposes advanced security solutions for the aforementioned issues using Tamper-Proof Devices (TPD). The TPD, a type of Hardware Security Module (HSM), stores cryptographic keys along with secret parameters and performs cryptographic operations such as authentication, encryption, decryption, and so on within the device. Initially, a lightweight conditional-privacy preservation-based authentication mechanism is proposed, enhancing security through innovative key management mechanisms, such as Hard Key Update (HKU) and Soft Key Update (SKU). These mechanisms safeguard against key disclosure and ensure continuous protection even in the case of key compromise. The proposed solution significantly reduces computational and communication overhead using cryptographic techniques such as Message Authentication Codes (MACs), hash functions, and XOR operations. The research is further extended to mitigate the security-performance trade-off by implementing the idea of static and dynamic batch verification of multiple messages, leveraging lightweight cryptographic operations. The proposed method reduces computational overhead and ensures data integrity and confidentiality across the network. Additionally, it provides a solution for efficient and secure storage-retrieval of information while enhancing the responsiveness and efficiency of IoV services having dynamic and large-scale environment. The proposed approach reduces latency and prevents bottleneck issues in a centralized system by integrating edge computing with the Vehicular Cloud (V-Cloud).

Despite their robust design, TPDs can still be vulnerable to advanced physical attacks because of potential hardware flaws or inadequate protection against complex tampering techniques. Attackers can exploit these weaknesses to bypass security measures, potentially compromising the integrity of the device. This issue is resolved by introducing alternative approaches using Physical Unclonable Functions (PUF) devices. PUFs use hardware's inherent physical irregularities to generate cryptographic keys on demand, making them nearly impossible to clone and highly resistant to tampering, unlike TPDs, which require secure key storage. In the second phase, PUF devices are used as secure hardware modules to design a highly secure and lightweight authentication scheme using a Challenge-Response Pair (CRP) mechanism. Furthermore, the research provides an effective solution for enhancing security on resource-constrained devices, where efficient and secure data handling is crucial. The framework uses PUFs to generate dynamic nonce and keys to address nonce reuse issue, without imposing significant computational or energy demands. Additionally, implementing this framework on low-power hardware platforms demonstrates its suitability for systems that require high security with efficient power usage, making it an ideal choice for securing resource constrained IoV devices.

Comprehensive security analysis using BAN logic, Random Oracle Model (ROM), and the ProVerif tool validates the technical depth of the proposed solutions, making them highly effective in countering a wide variety of security threats prevalent in IoV scenarios. The proposed methods are also evaluated against existing techniques, demonstrating improvements in terms of computational overhead, communication overhead, energy consumption, latency, and scalability.