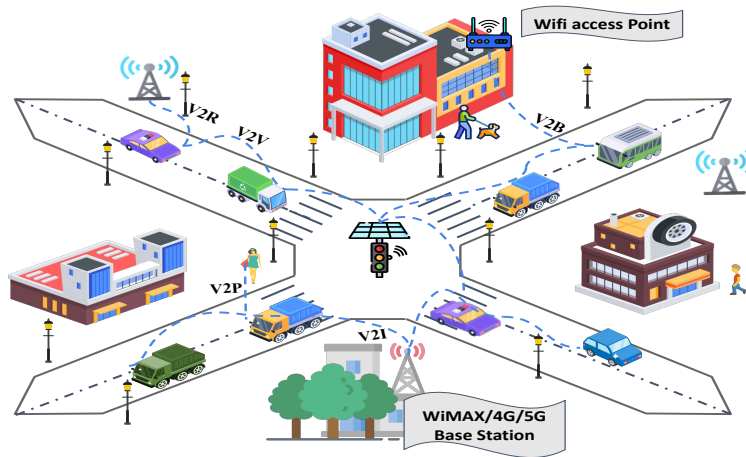


# Introduction

Internet of Vehicles (IoV) represents a significant advancement in modern transportation systems. It plays a crucial role in addressing urban traffic congestion, enhancing road safety, and promoting environmental sustainability through real-time data exchange. However, the integration of diverse communication technologies and the sensitive nature of the data exchanged introduce numerous security challenges that must be addressed to maintain the integrity and reliability of IoV systems. Security in IoV networks is essential due to the potential risks associated with data breaches and cyber-attacks. Key security requirements, including data integrity, confidentiality, access control, availability, and privacy preservation, are crucial for maintaining trust and ensuring the reliable operation of Intelligent Transportation Systems (ITS). This thesis focuses on developing advanced security solutions for large-scale and highly dynamic IoV networks. By examining these security challenges and proposing innovative solutions, this thesis aims to enhance the efficiency, safety, and environmental sustainability of urban mobility systems. This chapter offers a detailed discussion of IoV and its significant impact on modern transportation systems. It examines the essential security requirements for IoV networks, highlighting the necessity of robust measures to protect sensitive data and ensure public safety. Furthermore, this chapter outlines the motivation behind this research, detailing the need for advanced security solutions in IoV. It defines the specific objectives of the study and summarizes the key contributions made by this thesis in the field of IoV security. To provide a solid foundation for the research, the chapter covers the preliminaries necessary for understanding the subsequent discussions. Finally, the chapter presents an overview of the thesis structure, guiding the reader through the various sections and chapters that comprise this work. This structured approach ensures a clear understanding of how the research is organized and how each part contributes to the overall objective of enhancing security in IoV networks.

## 1.1 BACKGROUND

IoV signifies an advancement in vehicular communications, building on the foundational technologies established by Vehicular Ad-hoc Network (VANET) and the broader Internet of Things (IoT)[1]. VANET initially emerged to facilitate communication between vehicles and roadside infrastructure, focusing on enhancing road safety, improving traffic efficiency, and providing infotainment services[2]. These networks enabled direct Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications through Dedicated Short-Range Communications (DSRC) technologies operating in the 5.9 GHz frequency band[3]. In parallel, the development of IoT led to the interconnection of devices and systems across various domains,

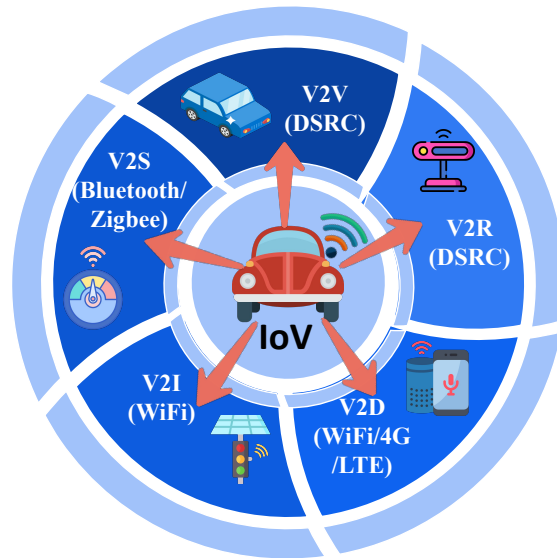


**Figure 1.1:** A smart city scenario implementing the Internet of Vehicle (IoV) network

including smart homes, industrial automation, and healthcare[4]. Integrating VANETs and IoT has resulted in the development of IoV, creating a comprehensive system where vehicles, infrastructure, and pedestrians are interconnected through a heterogeneous network environment[1], as described in the Figure 1.1.

IoV leverages a broad spectrum of communication technologies to facilitate seamless connectivity and data exchange among diverse entities. The primary communication types in IoV, described in Figure 1.2, include Vehicle-to-Pedestrian (V2P), and Vehicle-to-Everything (V2X) along with the basic V2V and V2I communications[5]. To meet these diverse connectivities, IoV employs multiple communication technologies, each operating in specific frequency bands. DSRC operates in the 5.9 GHz band, providing low-latency, high-reliability V2V and V2I communications essential for safety-critical applications such as collision avoidance and traffic signal coordination[6]. Cellular networks, including LTE and 5G, utilize frequency bands such as 700 MHz, 2.3 GHz, and 3.5 GHz, offering extensive coverage and high data rates for V2X communications[7]. Wi-Fi (IEEE 802.11p), also operating in the 5.9 GHz band, is tailored for vehicular environments, providing robust V2V and V2I communications. Bluetooth and Zigbee, operating in the 2.4 GHz band, are used for short-range V2P communications, enabling interactions between vehicles and pedestrians' mobile devices[8]. Additionally, Bluetooth Low Energy (BLE) and Ultra-Wideband (UWB) play significant roles in IoV. BLE, recognized for its low power usage and short-range communication, is essential for energy-efficient and reliable data exchange scenarios[9]. UWB, with its ability to offer high-precision localization and robust performance in dense environments, is useful for applications requiring accurate positioning, such as parking assistance and proximity-based services[10].

However, integrating these diverse communication technologies in IoV introduces significant security challenges[11]. Interception and eavesdropping pose threats of unauthorized entities accessing communications, potentially leading to the leakage of sensitive information such as vehicle location and driver behavior[12]. Data tampering is another risk, where attackers manipulate data transmitted between vehicles and infrastructure, causing the dissemination of false information that can lead to accidents or traffic congestion[13]. IoV systems are also vulnerable to Denial-of-Service (DoS) attacks, where excessive traffic overwhelms the network, rendering critical services unavailable[14]. Spoofing and Sybil attacks involve malicious entities creating fake identities or masquerading as legitimate vehicles or infrastructure, disrupting the network's trust model and leading to potential safety hazards[15]. Furthermore, vehicles connected to the internet are susceptible to malware and ransomware attacks, compromising vehicle control systems and



**Heterogeneous Communications:**

V2V - Vehicle-to-vehicle, V2R - Vehicle-to-RSCN, V2S - Vehicle-to-sensor, V2I - Vehicle-to-infrastructure, V2D - Vehicle-to-device

**Figure 1.2:** Heterogeneous communications in IoV network

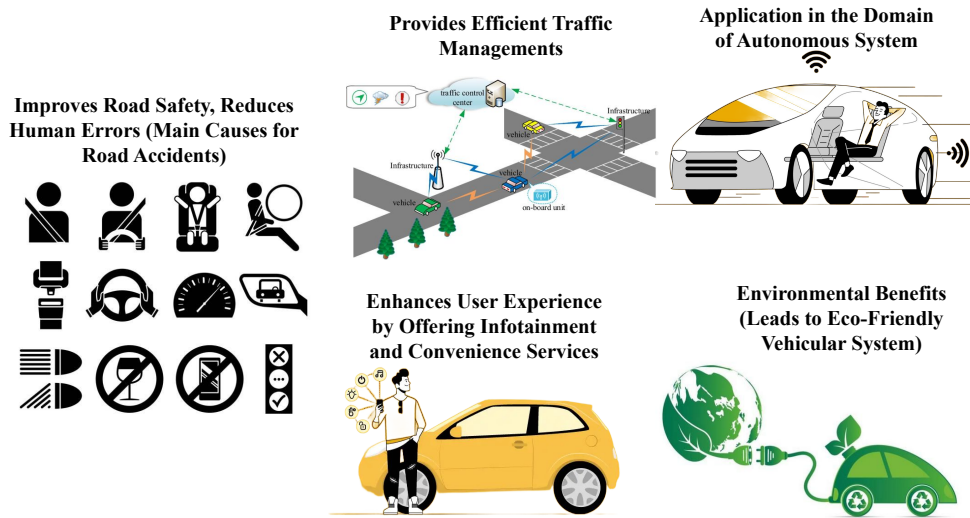
user data[16]. Understanding the specific frequency bands and technological vulnerabilities is crucial for developing robust security measures and ensuring the safety and reliability of IoV systems. As these technologies continue to evolve, addressing their security implications are essential to fully realize the potential of IoV in enhancing transportation efficiency and safety[17].

### 1.1.1 Need of Internet of Vehicles

The need for IoV arises from the increasing challenges of urbanization, including traffic congestion, road safety, and environmental sustainability[18]. Central to the evolution of IoV is the significant enhancement of road safety. Traditional vehicular systems predominantly rely on the capabilities of individual drivers and isolated vehicular safety mechanisms, which often prove inadequate in preventing accidents and ensuring optimal road usage[19]. IoV facilitates the sharing of real-time data regarding vehicle speed, location, and driving intentions, which is crucial for collision avoidance systems capable of proactive measures such as automatic braking or steering adjustments[20]. Technologies like DSRC, Wireless Access in Vehicular Environments (WAVE), operating in the 5.9 GHz band, provide the low latency and high reliability essential for these safety applications, ensuring timely and precise information dissemination[21].

Moreover, IoV significantly contributes to improving traffic efficiency and management. By enabling communication between vehicles and traffic management centers, IoV aids in reducing congestion and optimizing traffic flow through Advanced Driver Assistance Systems (ADAS)[22]. Advanced algorithms analyze data from various IoV components to predict traffic patterns and implement strategies to alleviate bottlenecks[23]. For instance, adaptive traffic light systems can adjust their timings based on real-time traffic loads, reducing idle times and enhancing overall traffic throughput. The extensive coverage and high data rates of cellular networks, particularly 5G, support the massive data exchange necessary for efficient traffic

management. Environmental benefits are also a substantial advantage of IoV[24]. By optimizing driving



**Figure 1.3:** Basic advantages of IoV including road safety, traffic management, environmental sustainability, infotainment services, and autonomous system

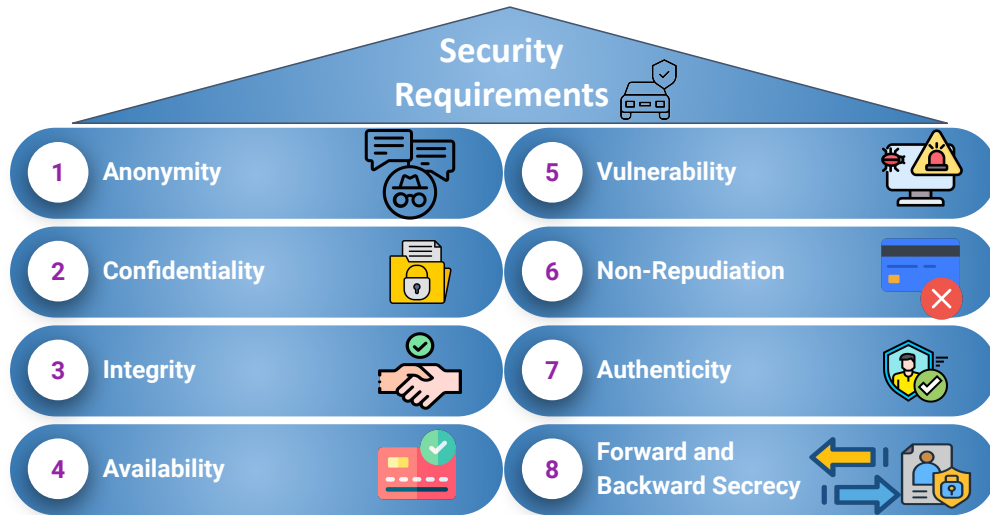
behaviors and minimizing idle times, IoV reduces fuel consumption and emissions. ITS can provide eco-friendly routing suggestions based on real-time traffic conditions and vehicle performance metrics, thereby lowering the carbon footprint and fuel costs. Technologies such as BLE, with high precision localization capabilities, enable applications like parking assistance, reducing the time spent searching for parking spots and further minimizing unnecessary fuel consumption and emissions[25].

Furthermore, IoV enhances the user experience by offering a range of infotainment and convenience services, as described in the Figure 1.3. Vehicle-to-Cloud (V2C) communication connects vehicles to cloud services, enabling features such as real-time navigation updates, remote diagnostics, and over-the-air software updates[26]. Wi-Fi, tailored for vehicular environments, supports robust V2V and V2I communications, ensuring vehicles remain connected to access various online services. Bluetooth and Zigbee technologies facilitate short-range communication with mobile devices, enabling seamless interactions between vehicles and passengers’ smartphones. Collectively, these technologies provide a more connected and convenient driving experience, integrating the vehicle into the broader digital environment[27]. One of the most transformative applications of IoV lies in the domain of autonomous driving. Autonomous vehicles rely on an array of sensors and communication technologies to navigate safely and efficiently. IoV provides the necessary infrastructure for these vehicles to communicate with each other and with traffic management systems, ensuring coordinated and informed decision-making[20]. The high data rates and low latency of 5G networks are particularly critical for autonomous driving applications, enabling real-time data exchange and processing. The integration of these technologies ensures autonomous vehicles can operate safely and efficiently, facilitating the widespread adoption of autonomous driving[28].

### 1.1.2 Security Requirements in Internet of Vehicles

The interconnected nature of IoV involves continuous communication between vehicles, traffic management systems, and other IoT devices, creating numerous potential entry points for cyber threats[15]. Unautho-

rized access, data breaches, and malicious attacks can lead to terrible consequences, such as traffic signal manipulation, unauthorized vehicle control, and leakage of sensitive personal data[11]. Furthermore, to ensure accurate and reliable information flow, it is essential to protect the real-time data exchange such as location, speed, and vehicular conditions[29]. Compromised data integrity or confidentiality can result in incorrect navigation instructions, traffic congestion, and even catastrophic accidents. Additionally, the highly dynamic and large-scale nature of IoV networks necessitates robust security measures to maintain system availability and resilience against attacks like DoS[30]. As a result, ensuring robust security in IoV is critical to protecting users' privacy, maintaining public safety, and ensuring the reliable operation of ITS[31]. Followings are the basic security requirements (refer Figure 1.4) that should be considered while designing the communication protocol for secure IoV network:

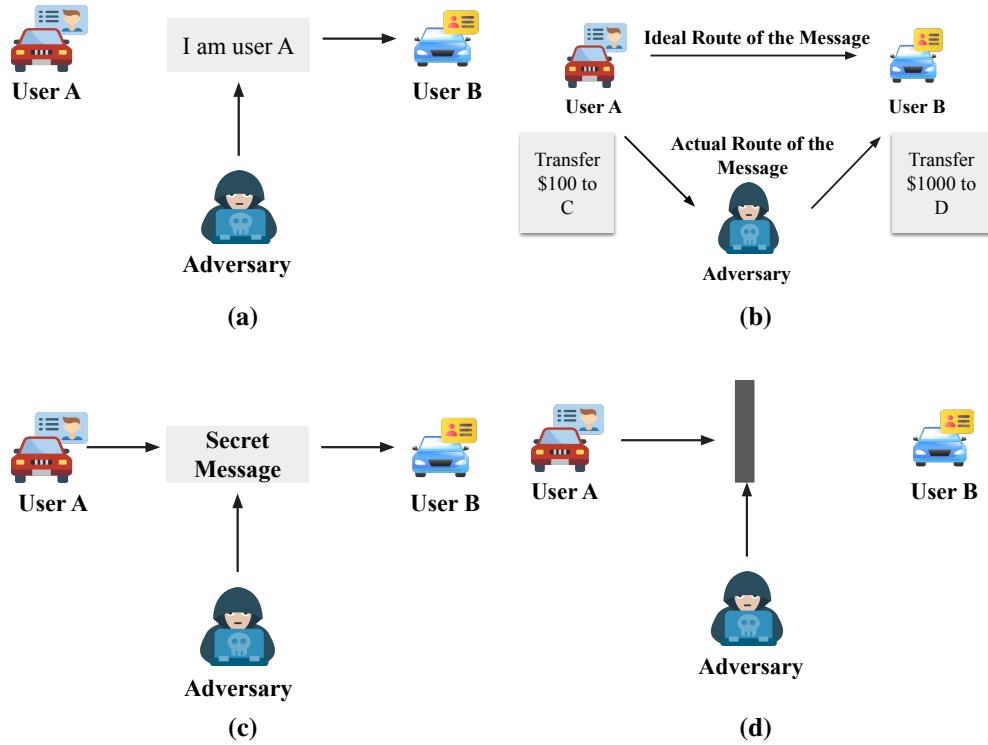


**Figure 1.4:** Security requirements for IoV communications

**Data integrity and authenticity:** IoV relies on the continuous exchange of data between vehicles, infrastructure, and other entities, necessitating the accuracy and integrity of this data[32]. The absence of data integrity and authenticity, as illustrated in Figure 1.5a and 1.5b, can lead to significant problems. For instance, altered or spoofed data can cause vehicles to make incorrect decisions, such as sudden braking due to fake traffic jam alerts, potentially resulting in collisions[33]. Additionally, malicious nodes could introduce false messages into the network, causing widespread chaos and distrust among users. Inaccurate traffic information can lead to inefficient route planning, increased congestion, and higher emissions, undermining the overall effectiveness of IoV systems[34]. In emergencies, tampered data could delay first responders, potentially endangering lives. Therefore, the lack of data integrity and authenticity compromises the safety, efficiency, and user trust in IoV technologies[31].

**Confidentiality:** In an IoV network, vehicles exchange substantial amounts of sensitive information, such as location data, driving patterns, and user-specific details. Protecting these information from unauthorized access and interception is critical for ensuring user data confidentiality[35]. A lack of confidentiality (refer Figure 1.5c) poses significant risks. For example, if sensitive data such as vehicle locations and driving patterns are exposed, malicious nodes could track individuals' movements, potentially leading to physical threats. Unauthorized access to personal information could result in identity theft, financial fraud, and other forms of misuse[33]. Moreover, exposure of such data could undermine user trust in IoV networks,

discouraging the adoption of these technologies. On a larger scale, the breach of confidentiality could compromise the security of the transportation network as a whole, as intercepted operational data could be exploited to disrupt traffic flow or coordinate attacks on critical infrastructure[36]. Therefore, ensuring data confidentiality is vital for protecting user information, maintaining safety, and encouraging trust in IoV networks.



**Figure 1.5:** Primary security requirements in IoV: (a) Absence of authentication, (b) Absence of message integrity, (c) Absence of confidentiality, (d) Absence of network availability

**Access control:** The IoV network must restrict data access and modification to authorized entities only. The lack of robust access control mechanisms can lead to severe consequences. Without proper access control, malicious nodes could manipulate traffic signals, disrupt vehicle communications, or inject false data into the network, compromising road safety[15]. Unauthorized modifications to system settings or data could lead to operational failures, such as incorrect traffic management decisions, resulting in increased congestion and accidents. In critical situations, such as emergencies, the inability to ensure that only authorized user can control and access the system could delay response times and worsen the situation[20]. Therefore, the absence of access control compromises the security, reliability, and efficiency of IoV networks, posing significant risks to both individual users and the broader transportation infrastructure.

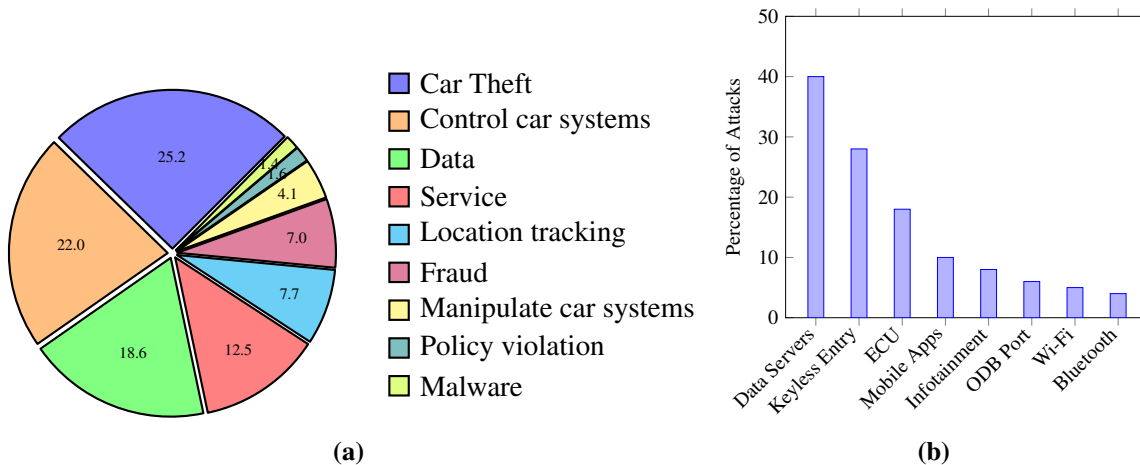
**Availability and resilience:** IoV network must ensure continuous operation even during attacks or failures, as the lack of availability can severely impact their effectiveness and reliability[37]. DoS attacks, which flood the network with excessive traffic, can disrupt communication and cause network failures, leading to significant operational issues. The unavailability of the network (refer Figure 1.5d) stops critical real-time data exchange between vehicles and infrastructure, resulting in traffic congestion, increased accident risks, and delayed emergency responses[11]. This unavailability also prevents timely updates on traffic

conditions, route optimization, and coordination of autonomous driving functions, thereby compromising overall traffic management and safety[38]. In critical situations such as emergency response or disaster management, unavailability can delay rescue operations and worsen the event’s impact. Therefore, ensuring the availability of IoV networks is essential for maintaining continuous and reliable service, ensuring safety, efficiency, and sustaining user trust[29].

**Privacy preservation:** Privacy preservation in IoV focuses on protecting personal data while enabling seamless communication between vehicles and infrastructure. Key principles include anonymization, which conceals individual identities during transmission[15]. Robust access control mechanisms restrict data access to authorized entities only, and techniques like differential privacy add controlled noise to datasets to prevent individual identification[39]. Implementing these measures helps maintain user trust and compliance with privacy regulations, protecting sensitive information against unauthorized access and misuse in the rapidly evolving IoV network. The lack of privacy preservation can have significant negative impacts[40]. Without proper preservation, personal data such as identity, location, driving habits, and vehicle usage can be exposed to malicious entities, leading to unauthorized surveillance, and tracking[30].

## 1.2 RESEARCH MOTIVATION

The rapid rise of connected vehicles has significantly increased cybersecurity risks, necessitating advanced security solutions for IoV network. The 2020 Automotive Cybersecurity Report[41] reveals key motivations for the security solutions, proposed in this thesis. There has been a dramatic 605% increase in cybersecurity incidents since 2016, with 82% of 2019’s incidents involving remote attacks, highlighting the urgent need for robust security measures[42]. The potential damage from cyber-attacks is immense, with 330 million connected vehicles and projections for only connected vehicle sales by 2020, posing risks that could disrupt entire cities and endanger lives. Cybercriminal activities, responsible for 57% of incidents in 2019, aim to disrupt businesses, steal property, and demand ransom[12].



**Figure 1.6:** Vulnerabilities and Attack Trends in Automotive Cybersecurity and IoV: (a) Cybersecurity issues in automotive industry, (b) Percentage of attacks by category in IoV

The pie chart in Figure 1.6a highlights that car theft and break-ins (25.2%), control car systems (22.0%), and data/privacy breaches (18.6%) are the top cybersecurity concerns. Car thefts necessitate enhanced physical security and robust digital authentication. Attacks on car control systems pose severe safety risks, requiring secure coding, regular updates, and intrusion detection. Data breaches emphasize the need for advanced encryption and strict access controls[41]. Further, the bar chart in Figure 1.6b emphasizes that data servers and keyless entry systems are the most frequently targeted. Data servers account for 40% of attacks, highlighting their critical role in storing sensitive information and their attractiveness to attackers. Keyless entry systems follow, comprising 25% of attacks, due to the rise in relay attacks that exploit these systems[43]. Based on the analytical data and the research gaps identified in the literature survey, this thesis proposes the following key points to motivate the development of advanced security solutions for IoV networks:

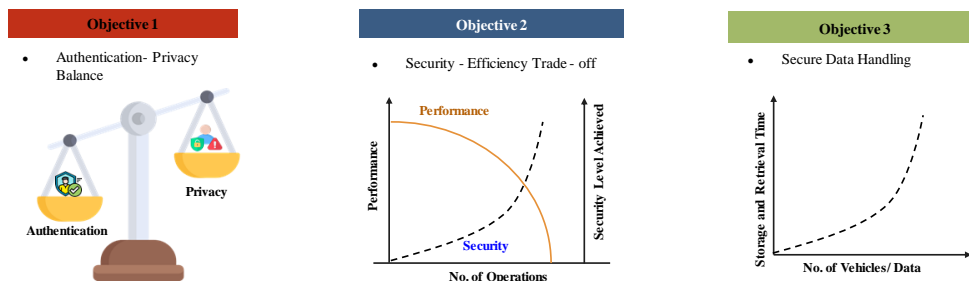
1. As the number of connected vehicles increases, the IoV network must securely handle a massive amount of data and maintain secure communication without bottlenecks[44]. However, current IoV architectures often struggle with scalability, leading to increased latency, reduced performance, and higher vulnerability to security attacks. Therefore, a robust IoV communication architecture is essential to efficiently accommodate a growing number of vehicles while ensuring security and privacy[45].
2. Further, by analyzing the report[41], it is concluded that ensuring security and privacy in IoV networks is important, but achieving a balance between robust authentication mechanisms and preserving user privacy presents significant challenges. Many authentication protocols[46, 47, 48, 49, 50] compromise user privacy by necessitating the disclosure of extensive personal information, potentially leading to privacy violations. Conversely, insufficient authentication measures might expose the network to unauthorized access, facilitating data breaches and unauthorized control of vehicles[51]. This imbalance undermines user trust, as individuals may perceive that their personal information is either inadequately protected or that the network is insufficiently secure to prevent malicious activities. Therefore, innovative approaches are needed to balance authentication and privacy effectively, ensuring secure yet privacy-preserving communication for users[42].
3. Furthermore, implementing robust security measures often comes at the cost of efficiency. High security can lead to increased computational overhead and longer processing times, which is not desirable in real-time IoV applications[52]. For instance, advanced encryption methods can cause latency and consume significant computing power, slowing down processing and communication speeds. Security mechanisms such as frequent key exchanges and mutual authentication protocols, necessary to prevent unauthorized access and ensure data integrity, can increase communication overhead, reducing overall network efficiency[12]. Even minor delays in the dynamic IoV environment, where vehicles are constantly moving and interacting, can have adverse effects, leading to outdated information for decision-making and compromising the safety and reliability of IoV applications. Therefore, minimizing the trade-off between security and efficiency is crucial to maintain the real-time functionality and overall dependability of IoV networks[32].
4. In addition to security and efficiency, IoV networks generate and process vast amounts of data, necessitating secure and efficient data handling and storage solutions. This data includes critical information such as vehicle locations, traffic conditions, sensor readings, and driver and passenger personal data[53]. Protecting this data from breaches is crucial, as unauthorized access or data leaks can lead to significant privacy violations, financial losses, and safety risks. Simultaneously, ensuring quick retrieval and minimal storage time is essential to support the real-time decision-making processes

required for applications like autonomous driving, traffic management, and emergency response[45]. Managing this data securely while maintaining high efficiency involves addressing issues such as data integrity and availability. Scalable storage solutions are necessary to accommodate the growing volume of data generated by an increasing number of connected vehicles and infrastructure components, ensuring quick and reliable data access[54].

- Proposing theoretical solutions alone is insufficient; practical scenarios must validate these solutions to evaluate their effectiveness and performance. Theoretical models and simulations can provide valuable insights, but they often cannot capture the full complexity and unpredictability of real-world environments[55]. Therefore, deploying the proposed scheme on the designed IoV architecture is essential. Testing the solution in an operational IoV network under real-world conditions, which include varying traffic patterns, environmental factors, and potential security threats, is crucial[56]. Conducting comprehensive security and performance evaluations in this real-world environment helps understand how the solution performs under practical constraints and interacts with other system components[57].

### 1.3 RESEARCH OBJECTIVES

The evolution of IoV networks requires innovative security mechanisms and communication architectures that can handle the increasing number of connected vehicles without compromising performance[1]. This thesis aims to develop secure IoV communication architectures with advanced security solutions that address key challenges related to authentication, privacy, and data management. There is also a need of decentralized and distributed computing resources to alleviate the load on central servers and decrease data transmission times[5]. Within these comprehensive goals, this thesis addresses security and efficiency challenges, categorized into three main objectives:



**Figure 1.7:** Primary research objectives that aim to balance authentication-privacy, to achieve high level of security having less overhead, and to securely handle the vast amount of IoV data

#### 1. To achieve an optimal balance between authentication and privacy

It is essential to consider the impact of robust authentication mechanisms alongside the importance of privacy preservation. Strong authentication mechanisms are crucial for enhancing security by preventing unauthorized access and ensuring that data exchanged within the IoV network originates from trusted sources[58]. This not only maintains data integrity but also ensures accountability through traceability and non-repudiation, allowing for actions to be traced back to their sources. It ensures that participated entities

cannot deny their activities. Simultaneously, privacy preservation involves protecting user identities, which reduces the risk of exposing sensitive information[59]. This protection enhances user trust, as users are more likely to engage with IoV services when they are confident their privacy is protected. Additionally, privacy preservation ensures compliance with stringent legal and regulatory requirements, such as the General Data Protection Regulation (GDPR)[60], which mandate the protection of personal data. Therefore, to achieve an optimal balance between authentication and privacy in the IoV, it is crucial to implement robust authentication mechanisms that ensure security and accountability while incorporating adaptive and context-aware privacy preservation techniques. By achieving this delicate balance, the IoV network can deliver secure, reliable, and user-friendly services while protecting user privacy[61].

## ***2. To reduce the trade-off between security and efficiency***

This objective aims to balance two critical aspects of IoV network: robust security algorithms and optimal system performance. In the context of IoV, security encompasses protecting against data integrity attacks, DoS attacks, privacy breaches, and vehicle hijacking or physical attacks[34]. Efficiency, on the other hand, involves reducing computation/ communication overheads, storage cost, energy consumption, minimizing latency, and optimizing bandwidth utilization. The primary goal is to implement security protocols that do not significantly impact the system's responsiveness and resource usage, thereby ensuring that the IoV network can operate safely without compromising the real-time performance and functionality required for applications such as traffic management, autonomous driving, and emergency response[12]. Reducing this trade-off is essential for the practical deployment and user acceptance of IoV technologies, where both security and efficiency are essential for overall system reliability and effectiveness.

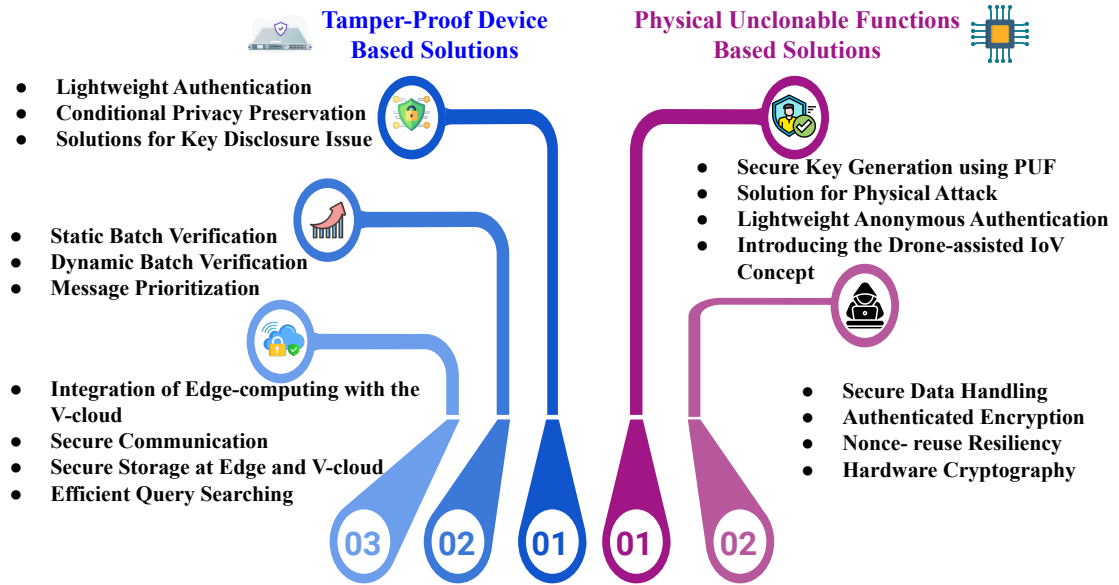
## ***3. To ensure secure data handling while minimizing data retrieval and storage time***

This objective aims to develop efficient data management strategies that protect sensitive information from breaches while ensuring quick and reliable data access, minimizing the time and resources required for data storage and retrieval[45]. In the context of IoV, the volume of data generated is vast, involving V2V and V2I communications, sensor data, user information, and real-time traffic updates. Managing this data effectively is crucial for the seamless operation, supporting applications such as autonomous driving, smart traffic management, and emergency response systems[62]. To achieve this, the goal is to implement scalable storage solutions capable of handling the increasing volume of data generated by IoV networks. Further, developing methods for secure, fast data retrieval is another critical component of this objective. This involves utilizing advanced techniques to expedite data queries, ensuring that relevant information is readily available for real-time decision-making processes[63]. Additionally, secure access controls are essential to protect the stored sensitive data from unauthorized access and breaches, ensuring that only authorized entities can access and manipulate the data. The overall goal is to create a robust data management framework that not only securely store sensitive information but also supports the reliable and quick access to necessary data for the optimal functioning of IoV network, thereby enhancing the overall safety, efficiency, and user experience in intelligent transportation environments[64].

Apart from these objectives, to validate the effectiveness of the proposed IoV communication architecture and associated security solutions, the research aims to implement the designed communication architecture and security mechanisms in real-world or simulated IoV environments[14]. The effectiveness, reliability, and practicality of the proposed solutions should be evaluated by conducting thorough security and performance evaluations[17]. This evaluation process demonstrates that the architecture meets the desired security and performance standards, ensuring its applicability and robustness in real-world IoV scenarios.

## 1.4 SUMMARY OF CONTRIBUTIONS

In the context of large-scale and highly dynamic IoV networks, ensuring robust security while maintaining performance and privacy is very essential[65]. This thesis addresses critical challenges in authentication, privacy, security efficiency, and data handling by proposing advanced security solutions leveraging two types of concepts: Tamper-Proof Device (TPD)[66] and Physical Unclonable Function (PUF)[67]. By integrating these concepts, the thesis aims to develop lightweight, efficient, and highly secure communication schemes suitable for the unique demands of IoV networks. The following are the detailed contributions that address the aforementioned challenges and achieve the stated objectives:



**Figure 1.8:** Contributions: Advance security solutions for large-scale and highly dynamic IoV

### 1.4.1 Tamper-Proof Device Based Solutions

TPDs are specialized hardware modules designed to provide secure storage and processing of cryptographic keys and sensitive data. These devices are integrated into the On-Board Unit (OBU)[68] of vehicles, ensuring that critical operations like authentication, encryption, and decryption occur within a secure environment, resistant to physical and logical attacks. The research leverages TPDs to enhance the security framework of IoV networks through the following contributions:

**Advanced security solutions that maintains the balance between efficient authentication and user’s privacy preservation:**

- Developed a lightweight conditional-privacy preservation-based authentication mechanism[42] that leverages pseudonymity to create pseudo-identities for communication purposes. This mechanism ensures privacy preservation by allowing users to interact within the network using these pseudo-identities, thus protecting their real identities[69]. Additionally, the research incorporates a traceabil-

ity feature, enabling legal authorities to uncover the real identity of users in case of any malicious activities. This dual functionality ensures both user privacy and accountability, balancing the need for secure communication with the ability to enforce legal oversight when necessary[52].

- The research provides secure key management techniques like Hard Key Updates (HKU) and Soft Key Updates (SKU). These updates are crucial in preventing key compromise and maintaining continuous protection. HKU and SKU ensure that even if keys are compromised, the system can securely update them without user intervention.
- Implemented cryptographic techniques such as Message Authentication Code (MAC)[70], hash functions[71], and Exclusive OR (XOR) operations within TPDs to minimize computational and communication overhead. This approach ensures that robust authentication can be achieved with minimal performance impact, thereby preserving user privacy using pseudonymity technique.

***Security solutions for verification that mitigates the trade-off between security and efficiency:***

- Proposed static and dynamic batch verification[55] methods that leverage lightweight cryptographic operations (i.e., one-way hash functions[71], XOR operations, etc.) within TPDs. These methods significantly reduce computational overhead while ensuring data integrity and confidentiality, enabling efficient and secure real-time operation in IoV networks.
- Integrated edge computing with the Vehicular Cloud (V-cloud)[72] to offload computational tasks from the central network to edge nodes reducing latency and preventing bottleneck issues. This integration enhances the responsiveness and efficiency of IoV services, particularly in dynamic and large-scale networks, by distributing computational and storage tasks across multiple nodes.
- Demonstrated the effectiveness of TPD-based solutions through extensive simulations and performance analysis, showing significant improvements in computational overhead, communication overhead, energy consumption, and latency. These results validate the feasibility of implementing robust security measures without significantly impacting system performance.

***Lightweight solution for secure data storage and quick data retrieval that minimizes data storage and access time:***

- Developed efficient data management strategies[45] using scalable storage and retrieval solutions using Searchable Symmetric Encryption (SSE)[73] that handle the increasing volume of data generated by IoV networks. These strategies ensure quick and secure access to data while minimizing the time and resources required for data storage and retrieval, crucial for real-time decision-making processes in IoV networks.
- Implemented secure storage-retrieval mechanisms by integrating edge computing. This approach reduces latency and prevents bottleneck issues by ensuring that data storage and retrieval operations are distributed and performed securely at the network edge, rather than relying solely on centralized systems[44, 74, 75, 76, 62, 77].
- Employed advanced cryptographic techniques and comprehensive security analysis tools like Burrows-Abadi-Needham (BAN) logic[78], Random Oracle Model (ROM)[79], and Protocol Verification Tool

(ProVerif) to validate the robustness of the proposed TPD-based solutions against various security threats. These validations ensure that data handling processes are secure, efficient, and resilient to potential attacks.

## 1.4.2 Physical Unclonable Function Based Solutions

PUF leverages the inherent physical variations in semiconductor manufacturing processes to generate unique, unclonable cryptographic keys[80]. PUFs are highly resistant to cloning and tampering, making them ideal for enhancing security in IoV networks[67]. The detailed descriptions about PUF devices are provided in the subsection 1.5.1. This thesis has been extended that utilizes PUFs to enhance the security while providing lightweight, efficient authentication and data handling mechanisms through the following contributions:

### *Enhanced security solutions to provide a balance between authentication and user's privacy:*

- Utilized PUF devices to generate cryptographic keys on-demand, leveraging the unique physical characteristics of each device. This approach ensures that keys are never stored, reducing the risk of key exposure and enhancing privacy.
- Developed a Challenge-Response Pair (CRP)[81] mechanism using PUFs for highly secure and lightweight authentication. This mechanism ensures that authentication processes do not compromise user privacy. As the keys are generated dynamically and are not stored, thus it mitigates the risk of key compromise and reduces the storage cost also.

### *Nonce-reuse resilient solution for secure data handling in resource-constraint IoV network:*

- Proposed an PUF-based encryption algorithm to secure the sensor data at the hardware-level by combining the concept of PUF and Authenticated Encryption with Associated Data (AEAD)[82]. It uses Advanced Encryption Standard (AES)-Counter Mode (CTR)[83] and MAC function[70] where nonce and encryption/ authentication keys are generated using PUF device. By utilizing PUF to generate dynamic nonces and keys, critical security issues like nonce reuse are addressed without imposing significant computational or energy demands.
- This research further uses the concept of hardware cryptography instead of software cryptography to achieve better performance in terms of energy consumption and memory usage for resource-constraint IoV devices. The practical implementation of the proposed algorithm on micro-controllers[84], integrated with a gyroscope sensor module[85]. It offers a comprehensive evaluation of the performance and security attributes of the algorithm. The results indicate notable reduction in encryption time, RAM usage, current consumption, energy efficiency, and enhancement in overall security. These improvements substantiate the practical efficacy of the approach in real-world applications.

These contributions, grounded in the integration of TPD and PUF-based solutions, collectively address the critical security challenges in the IoV network. They enhance security, efficiency, and data management while maintaining an optimal balance between authentication and privacy. The advanced frameworks and methodologies proposed in this thesis mark a significant advancement in the robustness and responsiveness of IoV security mechanisms.

## 1.5 PRELIMINARIES

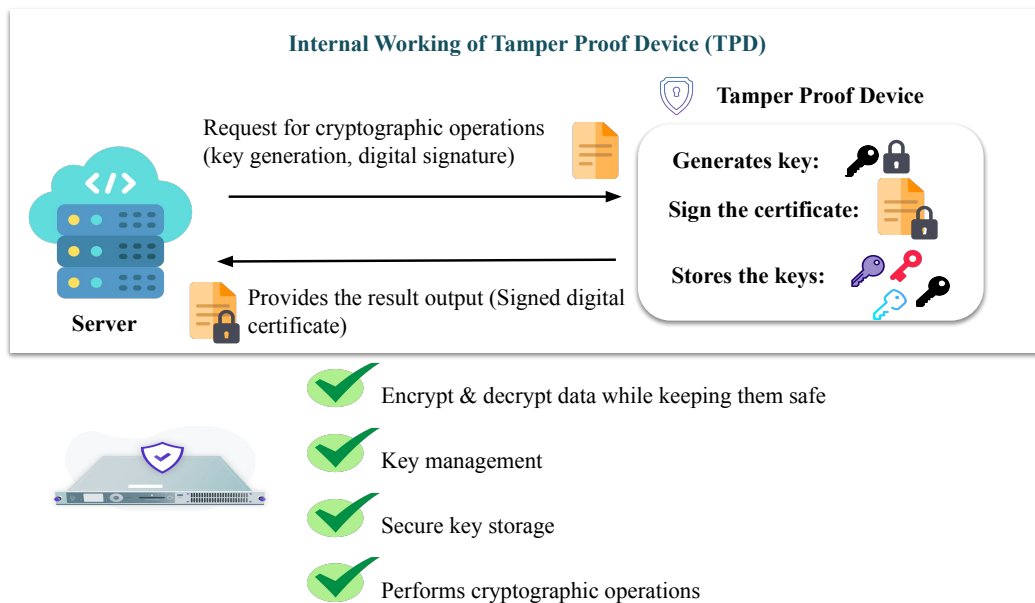
In the field of cryptographic research, a comprehensive understanding of foundational concepts is important. This section provides a detailed overview of secure hardware modules (i.e., TPD and PUF), simulation tools and security models that are used to discuss the proposed solutions and provide a base to validate the proposed algorithms in terms of security and efficiency. Hardware Security Module (HSM)[86] play a crucial role in cryptographic key management by providing a secure environment for key generation, storage, and management. These modules ensure that cryptographic keys are protected from unauthorized access and physical tampering, thus maintaining the integrity of secure operations. As our world becomes increasingly connected, particularly in the context of IoV, the security of vehicular communications becomes very important aspect. TPD[87] are essential in this domain, safeguarding the integrity and privacy of vehicular data, including performance metrics and driver behavior. Moreover, this thesis explores the innovative approach of PUF[67]. PUFs are highly resistant to cloning and tampering, providing a robust solution for secure on-demand key generation without the need for permanent key storage, thereby reducing the risk of key leakage. To validate and refine cryptographic protocols and network behaviors, simulation tools are indispensable. Network Simulator 2 (NS-2)[88] and ProVerif[89] are highlighted for their capabilities in this area. NS-2 is a versatile tool for simulating various network scenarios, making it invaluable for vehicular network research. ProVerif, on the other hand, offers a rigorous framework for verifying the security properties of cryptographic protocols, ensuring their robustness against potential attacks. Additionally, the ROM[79] and BAN logic[90] are employed to validate cryptographic assumptions and protocol's correctness, respectively. By presenting these foundational concepts and tools, this chapter establishes the groundwork for the methodologies detailed in this thesis.

### 1.5.1 Hardware Security Modules

Hardware Security Module is a specialized physical computing device essential for digital security, providing a secure framework for handling cryptographic operations. HSMs generate, store, and manage cryptographic keys, which are fundamental to modern encryption methods[86]. These devices are crucial in industries where key protection is important, including financial services, data centers, government, military, and healthcare. HSMs manage the entire lifecycle of cryptographic keys, including key generation, storage, and secure archival and destruction[91]. Using high-entropy sources and quantum phenomena, HSMs generate keys through True Random Number Generators (TRNGs)[92] or Quantum Random Number Generators (QRNGs)[93], ensuring the unpredictability and strength essential for secure encryption and decryption. Cryptographic keys are stored in an encrypted form within the HSM, typically using internal master keys, adding a layer of security to prevent unauthorized access. HSMs also provide mechanisms for secure key destruction, ensuring that keys cannot be recovered or misused once they are no longer needed or have been compromised, thus maintaining the integrity and security of cryptographic operations[94]. HSMs adhere to stringent regulatory standards and certifications, such as Federal Information Processing Standards (FIPS)[95] 140-2/3, which certifies that cryptographic modules meet specific security requirements suitable for sensitive government and military applications, and Common Criteria (International Organization for Standardization (ISO)[96]/ International Electrotechnical Commission (IEC) 15408[97]), an international standard ensuring rigorous security standards for IT security products. Additionally, Payment Card Industry (PCI HSM) standards secure payment systems and protect cardholder data, ensuring HSMs are suitable for financial transactions and payment processing environments[86]. In this thesis, the following two types of

HSM (TPD and PUF) are used to provide the security solutions for large scale and highly dynamic IoV networks:

**Tamper-proof device:** In the IoV, vehicles continuously interact with various networks and other vehicles, making them prime targets for cyber threats. Within an OBU in vehicles, TPDs protect data integrity and authenticity in these exchanges, preventing spoofing and tampering[87]. This ensures that only legitimate data is transmitted and received, maintaining the reliability of vehicular communications and protecting sensitive information like location and personal driver data[98]. Typically embedded within OBUs, TPDs enable secure communication with roadside units, other vehicles, and traffic management systems. OBUs manage tasks such as toll collection, vehicle diagnostics, and safety warnings. In electronic toll collection systems, TPDs secure communication between the OBU and toll gateways, preventing transaction tampering and protecting user data privacy[99]. In V2X communications, TPDs authenticate and encrypt messages be-



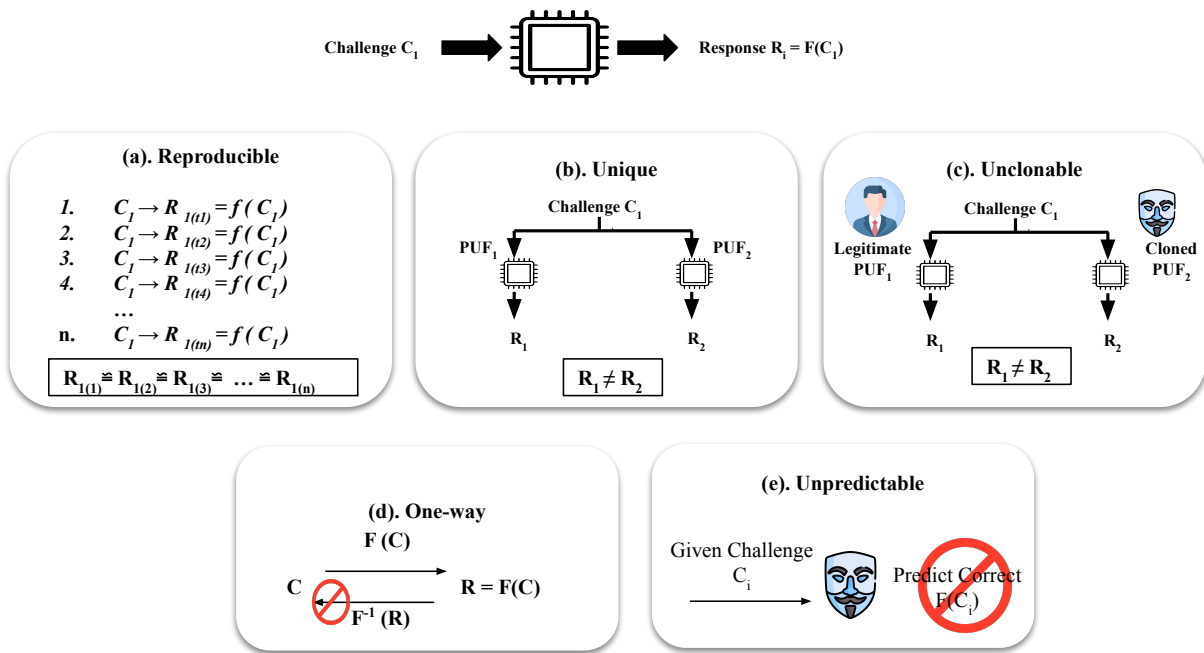
**Figure 1.9:** Internal working and the basic functioning of Tamper-Proof Device (TPD)

tween vehicles and infrastructure, crucial for applications like cooperative collision warning systems where data integrity is important for safety. In fleet management, OBUs with TPDs securely transmit vehicle location and status, aiding logistics management while protecting sensitive information[100]. Integrating TPDs within OBUs requires careful hardware and software considerations to ensure seamless functionality without disrupting vehicle operations. Hardware compatibility involves aligning the TPD's design with the OBU's existing systems to avoid negative impacts. On the software side, security functions must be intricately integrated into the vehicle's software architecture to maintain performance and reliability while enhancing security measures[101]. Figure 1.9 illustrates the internal workings of a TPD in the context of secure cryptographic operations. It describes an example of the interaction between a server and the TPD. The server requests cryptographic operations such as key generation and digital signature creation. The TPD processes these requests by performing essential cryptographic tasks[102]. It generates cryptographic keys, securely stores them, and signs digital certificates. Additionally, the TPD ensures the encryption and decryption of data, maintaining their safety. The results, such as signed digital certificates, are then provided

back to the server. This process ensures that all cryptographic operations are securely managed within the TPD, preserving data integrity and security[103].

Despite significant security benefits, integrating TPDs increases initial costs and complexity in automotive designs, impacting manufacturing, maintenance, and troubleshooting. Complex cryptographic operations of TPDs can add load to vehicle processing units, potentially affecting performance. Effective cryptographic key management is essential, involving secure generation, storage, rotation, and retirement of keys. Additionally, TPDs must be protected against physical attacks, necessitating advanced security measures[104].

**Physical unclonable functions:** PUFs utilize the inherent physical irregularities in semiconductor manufacturing to create unique, unclonable identities for each device[67]. This makes them exceptionally resistant to cloning and tampering, which is crucial for ensuring the authenticity and security of IoV communications. PUFs simplify key management by generating cryptographic keys on-demand, thereby reducing the risks associated with key storage and potential key leakage[80]. These features not only improve security but



**Figure 1.10:** Unique characteristics of Physical Unclonable Functions (PUF)

also reduce the overhead and complexity typically associated with managing TPDs, making PUFs a more scalable and robust solution in the rapidly evolving IoV environment[105]. PUFs operate on the principle of challenge-response mechanisms, where the unique physical characteristics of hardware components, arising from minor variations and imperfections during the manufacturing process, determine the response to a given challenge[106]. For instance, in an Static Random Access Memory (SRAM) PUF, the power-up state of memory cells is unpredictable and unique to each chip. When a PUF receives a challenge, it processes this input through its hardware, generating a unique output or response influenced by the device’s specific physical properties[107]. Because these properties result from random manufacturing processes, even identical devices cannot produce the same response to a given challenge.

Figure 1.10 illustrates several key characteristics[67] of PUF that contribute to their robustness and security in cryptographic applications and IoV communications. First, it demonstrates reproducibility, showing

that for a given challenge  $C_1$ , the same PUF consistently produces the same response  $R_1$  over multiple instances, indicating stable output over time. Second, it highlights uniqueness where different PUFs ( $PUF_1$  and  $PUF_2$ ) generate distinct responses ( $R_1$  and  $R_2$ ) to the same challenge due to inherent physical variations, ensuring each PUF's response is unique. Third, it emphasizes unclonability, as attempts to clone a PUF result in different responses, demonstrating that even cloned PUFs cannot replicate the original's output. Fourth, it illustrates the one-way functionality of PUFs, where the response  $R$  is derived from a challenge  $C$  through a one-way function  $F(C)$ , making it infeasible to reverse the process and deduce  $C$  from  $R$ . Finally, it showcases unpredictability, indicating that predicting the correct response  $F(C_i)$  to a given challenge without the PUF is extremely difficult, ensuring the responses are not easily guessed. These characteristics—reproducibility, uniqueness, unclonability, one-way functionality, and unpredictability[80]—are essential for enhancing the security and reliability of PUFs in various applications.

Compared to traditional cryptographic hardware, PUFs can be more cost-effective, leveraging existing variations in hardware without requiring additional components. PUFs enhance IoV communication security by generating cryptographic keys that are never stored in memory, making them difficult to extract[104]. Vehicles equipped with PUFs can establish secure communication channels between IoV components, using PUF-generated keys for encryption and decryption to ensure data confidentiality and integrity[108].

## 1.5.2 Simulation Tools

Simulation tools are necessary for validating and refining cryptographic protocols and network behaviors. This section introduces two prominent tools: NS-2 and ProVerif.

**Network simulator-2:** In this research, NS-2 was utilized to develop a simulation environment for evaluating security solutions in IoV. NS-2 is a discrete event simulator widely used in network research due to its flexibility and detailed simulation capabilities[88]. The simulation environment was designed to model a typical urban vehicular network, focusing on realistic vehicle mobility and communication scenarios. The simulation environment included a predefined urban area populated with numerous vehicles. The internal structure of NS-2, comprising Tcl scripts and C++ code, facilitated the customization and extension of standard simulation components. Tcl scripts were used to define the simulation scenario, configure nodes, set mobility patterns, and initiate traffic generation. The C++ core provided the performance and flexibility needed for implementing complex security protocols and communication models. Each vehicle was represented as a node in NS-2, using the Node class. The Node class is fundamental in NS-2, responsible for creating network nodes with specific characteristics such as position, speed, and communication capabilities. These nodes were configured to move according to the Random Waypoint Model, a standard mobility model in vehicular network simulations. Communication between vehicles was facilitated by the IEEE 802.11p protocol, implemented using the Agent and Application classes. The Agent class in NS-2 handles the protocol stack of each node, enabling the simulation of various communication protocols. In this simulation, the Agent/User Datagram Protocol (UDP) and Agent/Null agents were employed to manage the transmission and reception of data packets, simulating the exchange of safety messages in IoV. The Application class was used to generate traffic patterns representative of real-world vehicular communications. This class allowed for the creation of Constant Bit Rate (CBR) traffic sources, simulating the periodic transmission of safety-critical information between vehicles. The Application/Traffic/CBR class provided the necessary functionality to model these traffic patterns accurately. Security mechanisms were a critical aspect of the simulation. A lightweight cryptographic protocol based on Elliptic Curve Cryptography (ECC)[109] was integrated to ensure secure authentication of messages. The implementation of this proto-

col required modifications to the Agent class to include encryption and decryption processes. Additionally, an anomaly-based Intrusion Detection System (IDS)[110] was incorporated, utilizing the Application class to monitor and analyze network traffic for detecting potential security threats.

**ProVerif tool:** ProVerif, designed by Bruno Blanchet[89], is a powerful tool used for verifying the security properties of cryptographic protocols within the symbolic model. This tool is capable of handling both infinite and finite processes, modeling cryptographic operations as black boxes to simplify the analysis. In the symbolic model, cryptographic primitives are idealized, meaning adversaries can only interact with them via prescribed interfaces[100]. This abstraction simplifies the security analysis by reducing it to reasoning about algebraic properties defined by the primitives. Messages are treated as abstract entities rather than bit

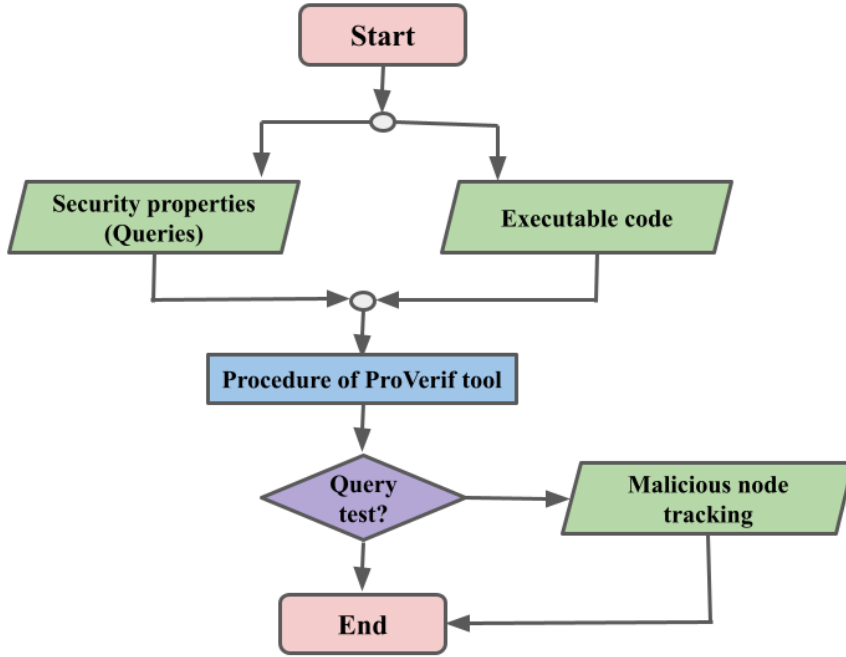


Figure 1.11: ProVerif tool flowchart

strings, which allows the analysis to focus on the structure and relationships between messages instead of their binary representations. ProVerif can verify a broad spectrum of security properties. One of the primary properties is secrecy, ensuring that a secret is not inferable by unauthorized entities. Formally, secrecy can be defined such that for any secret  $x$  and any knowledge set  $K$  that does not include the key  $k$ , the secret  $x$  should not be derivable from  $K$ :  $\forall x, k \notin K \implies \text{Secret}(x) \notin K$ . This equation asserts that if the key  $k$  is not part of the knowledge set  $K$ , then the secret  $x$  cannot be inferred from  $K$ , thereby preserving the secrecy of  $x$ . Another crucial property is authentication, which ensures that a claimed identity is valid by correlating specific actions or messages to individual entities. This verification helps in validating the authenticity of messages and the entities involved in the communication. Cryptographic primitives in ProVerif are specified using equational theories, which define how different operations interact. For example, the equation:  $\text{dec}(\text{enc}(x, k), k) = x$  states that decrypting an encrypted message  $x$  with key  $k$  retrieves the original message. This equation captures the fundamental property of encryption and decryption operations: if a message  $x$  is encrypted with a key  $k$ , then decrypting this encrypted message with the same key  $k$  will yield the original message  $x$ . This property is crucial for the correctness of many cryptographic protocols. Processes in ProVerif are described using a variant of process calculus, specifically a pi calculus variant.

The processes can be composed in parallel, communicate over channels, and operate conditionally based on received messages. ProVerif transforms these processes into Horn clauses, which are a form of logical representation. It then uses resolution techniques to decide whether queries about security properties can be satisfied. For instance, the query `query attacker(secret)` checks whether the `secret` can be derived by the attacker. If ProVerif determines that the `secret` cannot be derived by the attacker, it confirms that the secrecy property is maintained. Figure 1.11 outlines the procedure of ProVerif tool. It starts by defining security properties and preparing executable code, both of which are inputs for the tool. These inputs converge into the ProVerif procedure, leading to a query test. If the test detects issues, it proceeds to track malicious nodes and analyze vulnerabilities. The process concludes after successful verification or handling of detected issues. ProVerif’s ability to handle a wide range of security properties and its automated analysis capabilities make it an invaluable tool in the field of cryptographic protocol verification. Its use of the symbolic model and process calculus allows for a detailed and rigorous analysis of protocol security, ensuring robust protection against potential adversaries.

### 1.5.3 Models for Security Analysis

In the field of cryptography, robust models for security analysis are essential for ensuring the reliability and integrity of cryptographic protocols. These models provide a structured framework to evaluate the security properties and identify potential vulnerabilities within various cryptographic schemes. Two prominent models used in security analysis are the ROM[79] and BAN Logic[90]. The ROM offers an idealized abstraction for analyzing hash functions, enabling researchers to establish strong security guarantees under the assumption of perfect randomness. On the other hand, BAN Logic provides a formal method for reasoning about the beliefs of principals in authentication protocols, helping to verify the correctness and robustness of these protocols. This section provides the detailed concepts and applications of both models, illustrating their significance in the domain of cryptographic security.

**BAN logics:** BAN logic[90], named after its creators BAN, is a formal method used for analyzing and verifying authentication protocols. BAN logic provides a framework to reason about the beliefs of principals (such as users and servers) in a network regarding the authenticity and freshness of messages they exchange. This logic helps in identifying potential vulnerabilities and ensuring the security properties of the protocols. BAN logic uses a set of notations and rules (refer the Table 1.1) to express and reason about the beliefs of

**Table 1.1:** Burrow-Abadi-Needham (BAN) logic rules

Rule	Formal Representation	Meaning
<b>Message Meaning Rule</b>	$\frac{P \models Q \leftrightarrow P:K \quad P \models \text{Sees } \{X\}_K}{P \models Q \models X}$	If $P$ believes $K$ is a good key for communication with $Q$ and sees the message $X$ encrypted with $K$ , then $P$ believes $Q$ once said $X$ .
<b>Nonce Verification Rule</b>	$\frac{P \models \text{Fresh}(X) \quad P \models Q \models X}{P \models Q \models X}$	If $P$ believes $X$ is fresh and believes that $Q$ once said $X$ , then $P$ believes $Q$ believes $X$ .
<b>Jurisdiction Rule</b>	$\frac{P \models Q \models \text{Controls } X \quad P \models Q \models X}{P \models X}$	If $P$ believes that $Q$ controls $X$ and believes that $Q$ believes $X$ , then $P$ believes $X$ .
<b>Seeing Rule</b>	$\frac{P \models \text{Sees } X}{P \models P \models \text{Sees } X}$	If $P$ sees $X$ , then $P$ believes that $P$ sees $X$ .

principals. The key components of BAN logic include principals, messages, belief notations, and operators. Principals ( $P, Q, S$ ) are the entities participating in the communication, such as Alice (A), Bob (B), and a server (S). Messages ( $X, Y, K$ ) are the statements or data exchanged between these principals, which can

include cryptographic keys and nonces. These principals and messages form the basis of communication in the network, where principals exchange messages to achieve authentication and establish secure channels. Belief notations in BAN logic are used to express the beliefs of principals regarding the messages they exchange. These notations include:

$P \equiv X$  indicating that principal  $P$  believes  $X$

$P \mid \text{Said } X$  meaning principal  $P$  believes  $X$  was sent by another principal

$P \mid \text{Sees } X$  meaning principal  $P$  sees  $X$  (i.e., received message  $X$ )

$P \mid \text{Controls } X$  means that principal  $P$  has jurisdiction over  $X$  (i.e.,  $P$  can be trusted on the truth of  $X$ ).

Operators in BAN logic are used to manipulate and analyze the messages. These include:

$\{X\}_K$  denoting message  $X$  encrypted with key  $K$

$P \mid \text{Fresh}(X)$  indicating that  $X$  is fresh (i.e., has not been sent before)

$P \mid \text{Nonce}(X)$  meaning  $X$  is a nonce (a random number used only once).

To analyze a protocol using BAN logic, the analysis starts with a set of initial assumptions about the principals' beliefs and the messages they exchange. These assumptions include beliefs about shared keys and the freshness of nonces. For instance, Alice ( $A$ ) believes that the key  $K_{AB}$  is shared with Bob ( $B$ ) and is used for secure communication, denoted as:  $A \equiv A \leftrightarrow B : K_{AB}$ . Similarly, Bob believes the same about the key  $K_{AB}$ :  $B \equiv A \leftrightarrow B : K_{AB}$ . Furthermore, Alice believes that nonce  $N_A$  is fresh:  $A \mid \equiv \text{Fresh}(N_A)$  and Bob believes that nonce  $N_B$  is fresh:  $B \mid \equiv \text{Fresh}(N_B)$ .

BAN logic provides a set of assumptions and inference rules to derive new beliefs from existing ones. These rules help in systematically analyzing the authentication protocols. By applying the inference rules, the correctness and security properties of protocols can be verified, ensuring that they meet the desired authentication and freshness requirements.

**Random oracle model:** ROM[79] is a theoretical framework extensively used in cryptography to provide rigorous security proofs for cryptographic protocols and algorithms. Within this model, a hash function[71] is conceptualized as a "random oracle" that produces truly random output for each unique input, irrespective of any inherent patterns or structures in the input data. This idealized approach allows researchers to analyze and validate the security of cryptographic constructions under the assumption that the hash function behaves in an ideal manner. Although real-world hash functions are deterministic and cannot achieve the properties of a true random oracle, the ROM serves as a useful abstraction for theoretical analysis.

- **Properties of a random oracle:** A random oracle is an idealized black-box function  $H$  that maps any input  $x$  to a uniformly random output  $y$ . Formally, the random oracle  $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$  satisfies the following properties:
  - **Deterministic:** For any given input  $x$ , the output  $H(x)$  is fixed. Once  $H(x)$  is defined for a particular  $x$ , it remains the same for all future queries with the same  $x$ .
  - **Randomness:** The output  $H(x)$  is uniformly distributed over the output space  $\{0, 1\}^n$ , meaning each possible output is equally likely, ensuring no biases.

- **Independence:** The outputs for distinct inputs are independent of each other, implying no correlation between the hash values of different inputs.
- **Steps in security proofs in the ROM:** Security proofs in the ROM typically involve the following steps:
  - **Modeling the hash function:** The hash function used in the cryptographic scheme is modeled as a random oracle  $H$ . This abstraction allows for the analysis of the scheme under the idealized assumption of a perfectly random hash function.
  - **Reduction:** The security of the cryptographic scheme is reduced to the security of the random oracle. This involves showing that any attack on the scheme can be translated into an attack on the random oracle, thereby establishing a direct relationship between the two.
  - **Simulation:** The security proof includes a simulator that answers oracle queries in a way that is indistinguishable from a true random oracle. This step ensures that the behavior of the simulated oracle matches the expected behavior of a random oracle.
  - **Proof of security:** By demonstrating that breaking the cryptographic scheme implies breaking the random oracle, the security of the scheme is established under the ROM. This proof provides a strong theoretical foundation for the security of the cryptographic construction.

## 1.6 THESIS STRUCTURE

The thesis is structured to offer a comprehensive analysis of the security challenges within IoV networks. It proposes advanced security solutions using TPD and PUFs. Each chapter of this thesis is dedicated to addressing specific aspects of these challenges, providing a detailed exploration of the proposed solutions.

**Chapter 1: Introduction:** This chapter provides an overview of IoV networks, describing its evolution from conceptual frameworks to practical implementations. It outlines the architectural components of IoV, including the different types of communications such as V2V, V2I, V2P, V2X, etc. The chapter also discusses the need for robust security measures in IoV networks to protect against various types of cyber threats and to achieve basic security requirements including data integrity, confidentiality, and availability. Additionally, the chapter introduces preliminaries that form the base to discuss the proposed security solutions. These preliminaries include secure hardware modules such as TPD and PUF, simulation tools and validation models to prove the security aspects of the proposed solutions.

**Chapter 2: Related Work:** This chapter reviews the existing literature on security solutions for IoV networks, categorized into two main sections: TPD-based security solutions and PUF-based security solutions. For TPD-based solutions, it examines various authentication schemes, batch verification methods, and secure data handling techniques. The review highlights the limitations of current methods, such as high computational overhead and vulnerability to certain attacks. For PUF-based solutions, the chapter discusses authentication protocols and secure data handling mechanisms that utilize the unique properties of PUFs to enhance security. This chapter sets the stage for the proposed solutions by identifying gaps and challenges in the existing research.

**Chapter 3: Lightweight Authentication and Verification using Tamper-Proof Devices:** This chapter introduces a Novel MAC-based Authentication Scheme (NoMAS) for IoV that leverages TPDs. It details the design and implementation of NoMAS, including its key management techniques (hard key and soft key updates) and the use of cryptographic operations to ensure secure and efficient authentication. Additionally, it discusses static and dynamic batch verification schemes that are proposed to mitigate the security-efficiency trade-off. The chapter also presents the security and performance analysis of the proposed schemes, demonstrating its effectiveness in reducing computational and communication overhead while maintaining robust security.

**Chapter 4: Secure Data Handling using Tamper-Proof Devices:** This chapter focuses on secure data handling mechanisms using TPDs. It introduces the SecEdge framework, which combines secure communication, local and global secure storage, and secure query searching to protect data in IoV networks. The chapter elaborates on the design of SecEdge, including the encryption and decryption processes, key management, and the use of edge computing to reduce latency and prevent bottleneck issues. Performance analysis is provided to demonstrate the scalability and efficiency of SecEdge in handling large volumes of data generated by IoV networks.

**Chapter 5: Lightweight Authentication using Physical Unclonable Functions:** In this chapter, the focus shifts to PUF-based security solutions. It presents a PUF and Edge-computing based Secure Protocol for IoV (PESPI), which utilizes the unique properties of PUFs to generate cryptographic keys on-demand for secure and lightweight authentication. The chapter describes the CRP mechanism used for the secure authentication process. Further, the chapter details the extended research that propose a drone-based IoV infrastructure to provide a backup in case of Roadside Connecting Nodes (RSCN) failure. Performance analysis is conducted to compare the proposed schemes with other state-of-the-art schemes, highlighting its advantages in terms of computational efficiency, energy consumption, and security robustness.

**Chapter 6: Secure Data Handling using Physical Unclonable Functions:** This chapter explores PUF-based mechanisms for secure data handling in IoV networks. It introduces a modified AEAD algorithm that leverages PUF functions to generate dynamic nonce and keys, addressing critical security issues such as nonce reuse and key management. The chapter details the design and implementation of the PUF-based cryptographic hardware accelerator and provides performance analysis to validate its effectiveness in securing data transfer processes. The chapter also discusses the experimental setup and results, demonstrating the suitability of PUF-based solutions for resource-constrained IoV devices.

**Chapter 7: Conclusion and Future Direction:** The final chapter summarizes the key contributions of the thesis, highlighting the advanced communication architecture and methodologies developed to enhance the security, efficiency, and data management in IoV networks. It reflects on the research objectives and how they have been addressed through the proposed TPD and PUF-based solutions. The chapter also discusses the limitations of the research and suggests potential directions for future work, emphasizing the importance of continuous advancements in IoV security to keep pace with the evolving technological environment.