Ministry of Higher Education and Scientific Research

وزارة التعليم العالي والبحث العلمي

Badji Mokhtar Annaba University
Université Badji Mokhtar – Annaba
Faculty of Technology
Computer Science Department

جامعة باجي ختار – عنابـــــــة
كلية تكنولوجيا
قســـــــم الإعلام الآلي

Thesis

Presented for obtaining the Doctorate degree in LMD

Doctorate

Field: Computer science

Speciality: Embedded Computing and Mobility

By:
SAHBI Roumissa

Theme:

The security of Internet of vehicles for smart cities.

Thesis defended in 2025 in front of the committee:

N°	Name and First Name	Grade	Establishment	Quality
1	TOLBA Cherif	Prof	University of Badji Mokhtar – Annaba	President
2	GHANEMI Salim	Prof	University of Badji Mokhtar – Annaba	Supervisor
3	FERRAG Mohamed Amine	MCA	University of 8 May 1945 – Guelma	Co Supervisor
4	LABOUDI Zakaria	MCA	University of Larbi Ben M'hidi – Oum El Bouaghi	Examiner
5	KOUAHLA Zineddine	Prof	University of 8 May 1945 – Guelma	Examiner
6	KHETATBA Mourad	MCA	University of Badji Mokhtar – Annaba	Examiner

Acknowledgments

First and foremost, praises and thanks to **ALLAH** the Almighty.

I would like to express my sincere and my deep gratitude to my thesis supervisor **Ghanemi Salim** for his help, guidance, and advice throughout the accomplishment of this thesis.

I would like to think **Ferrag Mohamed Amine** for his help and guidance.

I would like to thank the **committee members** for the great honor they have gave me by accepting to examine this thesis.

Dedication

I dedicated this thesis:

*To my whole **family** especially my grandmother, my parents, my sisters, and my brother.*

*To my supervisor **Ghanemi Salim***

*To my co supervisor **Ferrag Mohamed Amine***

*To all **people** who helped me to do this work.*

Thank you so much for your help, your love, and your support.

Roumissa

Abstract

In recent years, the number of connected devices has increased rapidly forming the internet of Things (IoT). IoT created a revolution in several domains like healthcare, agriculture, education, and transportation system. Transportation system is developed to an intelligent vehicular system in which the vehicle becomes a smart object. Smart vehicles can communicate, cooperate, and interact with the whole world. Such cooperation between the vehicle and other objects create challenges in terms of availability, scalability, and security. Security is an important aspect in vehicular system; a security failure can cause disasters in human life lose. In this thesis, we propose secure authentication and confidentiality schemes. Our proposed schemes based on Cloud Computing, Software Defined Network, and elliptic curve cryptography.

Keywords: Internet of Vehicles, Security, Authentication, Confidentiality, attacks, and Cryptography.

Résumé

Au cours des dernières années, le nombre d'appareils connectés a augmenté rapidement formant l'Internet des objets (IoT). L'IoT crée une révolution dans plusieurs domaines comme la santé, l'agriculture, l'éducation, et le système de transport. Le système de transport est développé en un système de véhicule intelligent dans lequel le véhicule devient un objet intelligent. Les véhicules intelligents peuvent communiquer, coopérer et interagir avec le monde entier. La coopération entre le véhicule et d'autres objets crée des défis en termes de disponibilité, d'évolutivité et de sécurité. La sécurité est un aspect important du système automobile ; une défaillance de la sécurité peut causer des catastrophes dans la vie humaine. Pour cela, nous proposons dans cette thèse des schémas d'authentification et de confidentialité sécurisés. Nos schémas proposés sont basés sur les technologies l'informatique en nuage, Réseau définie par logiciel et la cryptographie à courbe elliptique.

Mots Clés : Internet des véhicules, Sécurité, Authentification, Confidentialité, attaques, Cryptographie.

الملخص

في السنوات الأخيرة، يتزايد عدد الأجهزة المتصلة بشكل سريع مما يشكل إنترنت الأشياء .(IoT) أحدثت إنترنت الأشياء ثورة في العديد من المجالات مثل الرعاية الصحية والزراعة والتعليم ونظام النقل .تم تطوير نظام النقل إلى نظام ذكي للمركبات حيث تصبح السيارة شيئًا ذكيًا . يمكن للمركبات الذكية التواصل والتعاون والتفاعل مع العالم بأسره .يخلق هذا التعاون تحديات كبيرة من حيث التوافر وقابلية التوسع والأمن .يعد الأمان جانبًا مهمًا في نظام المركبات؛ الفشل الأمني يمكن أن يسبب كوارث في حياة الإنسان. لهذا الصدد، نقترح في هذه المذكرة خطط المصادقة الآمنة والسرية. مخططاتنا المقترحة تعتمد على الحوسبة السحابية، والشبكة المعرفة بالبرمجيات، وتشفير المنحنى الإهليجي.

الكلمات المفتاحية: إنترنت المركبات، الأمن، المصادقة، الخصوصية، الهجمات، التشفير.

Table of contents

List of Figures

List of tables

List of abbreviations

IoT	Internet of Things.
IoV	Internet of Vehicles.
AVISPA	Automated Validation of Internet Security Protocols and Applications.
ECC	Elliptic Curve Cryptography.
HLPSL	High Level Protocol Specification Language.
SC	Smart City
SDN	Software Defined Network
CDC	Cloud Data Center
SCC	Security Cloud Center
NC	Network center
BAN	Burrows-Abadi-Needham
ID	Identity
PhyW	Physical world
GPS	Global Positioning system
WSN	Wireless Sensor Network
RFID	Radio frequency Identification
MA	Mutual authentication
SH	Smart hospital
SA	Smart ambulance
SF	Smart factory
RSU	Road Side Unit
OBU	On Board Unit
TPD	Tamper-proof device

General Introduction

General Introduction

Context

Day by day, the number of connected objects grows exponentially forming the notion of "Internet of things". IoT refers to the concept of connecting any object to the Internet and to other connected objects. It plays a transformative role in the development of smart cities by creating new domains including Internet of grids, Internet of homes, Internet of education, Internet of healthcare, Internet of factory, and Internet of vehicles. Internet of grids integrates smart energy grids with renewable energy sources and advanced monitoring systems, ensuring efficient power distribution, reducing energy waste, and supporting sustainability initiatives. Internet of homes automates and connects household devices and systems, allowing for remote control and monitoring of lighting, security, heating, and appliances, which enhances convenience, energy efficiency and overall quality of life for residents. Internet of education transforms education by facilitating virtual classrooms, interactive learnings tools, and real time communication between students and educators. Internet of healthcare revolutionizes medical services by connecting objects, wearable health monitors, and healthcare systems. This connectivity ensures timely medical interventions, reduces hospital overcrowding, and enhances overall patient care through data driven insights. Internet of factory integrates industrial operations with IoT technologies to smart factories that enhance efficiency, productivity, and sustainability. Vehicular networks have involved into the Internet of vehicles by integrating advanced communication technologies. Traditional vehicular networks focused on two types of communication Vehicle to vehicle communication and vehicle to infrastructure communication, this communication provides only basic services such as limited traffic information, collision warnings, and emergency alerts. However, IoV extends beyond basic communication by creating an interconnected network where vehicle can communicate and interact with various IoT objects. IoV enhances transportation by optimizing mobility, reducing congestion, offering predictive maintenance, and improving road safety.

Smart city interconnects a large number of objects, enabling a seamless communication, data exchange, and automation across diverse sectors including agriculture, healthcare, manufacturing, and transportation.

Problem statement

The interconnection of smart objects within smart cities is pivotal for the advancement of urban living, but it introduces significant challenges and requires a high level of security especially in vehicular network, a security failure can cause disasters.

Ensuring authentication and confidentiality leads to significant challenges in IoV system due to the real time communication, the massive quantity of IoV data exchanged the distributed, heterogeneous, and highly dynamic IoV nature. The highly dynamic and mobility environment of IoV, where smart vehicles move rapidly across different geographical locations. Entering and leaving communication ranges, which leads to fluctuating network connectivity and varying signal quality. The dynamic nature makes it difficult to establish and maintain secure authentication and confidentiality mechanisms. Moreover, IoV networks consist of heterogeneous objects including smart vehicles, smart sensors, smart trucks, smart bicycles, and smart road units, all with different characteristics like storing and computing capabilities making it challenging to have a global authentication and confidentiality schemes. Distributed IoV network; the lack of a central authority to control and manage the authentication and confidentiality process increases the risk of authorized access, making it easier for malicious objects to exploit the IoV system. The real time communication in IoV system creates important challenge for both authentication and confidentiality. The high movement of smart IoV entities requires rapid authentication and rapid data encryption and decryption. If the authentication and confidentiality process takes a long time, it can disrupt the flow of data, leading to delays that can affect safety system including collision avoidance or emerging braking. Balancing the need for immediate response times with secure communication is difficult. The massive quantity of data exchanged between IoV entities presents significant challenges for authentication and confidentiality. As smart vehicles, continuously and increasingly generate and disseminate large volume of data, the complexity of ensuring that only authorized entities can decrypt data increases exponentially. Ensuring authentication and confidentiality in this context demand advanced encryption and decryption techniques to protect data.

Connecting a large number of objects with different nature and characteristics causes numerous challenges and raises many questions including:

- How can these heterogeneous objects communicate with each other?
- How can these objects authenticate each other?

- What are authentication mechanisms suitable for IoV devices?
- What are the encryption techniques suitable for ensuring confidentiality of data transmitted between IoV devices?

Objectives and contribution

To answer these questions, we propose a network model, an authentication and confidentiality schemes for vehicular network based on Cloud Computing, Software Defined Network and Elliptic Curve Cryptography. Software Defined Network (SDN) represents a transformative approach to network management and architecture. As IoV environments are dynamic and heterogeneous, SDN simplifies the orchestration of complex IoV infrastructures, providing an efficient traffic routing, resource allocation, and prioritization based on real-time conditions such as traffic patterns and vehicle locations. Cloud Computing (CC) provides an extensible storage and powerful data processing capabilities. CC improves vehicle performance and user experience by enabling remote access and seamless updates. Elliptic Curve Cryptography (ECC) is a very suitable method for vehicular network. It offers a short key generation and provides a fast encryption and decryption of vehicular message. Comparing to Lui et al scheme [59], Chien et al scheme [63], and Alshudukhi scheme [64], we found that our preposition has a lower computation.

We summarize the objectives of our thesis in the following points:

- Defining our proposed IoV architecture that integrates essential components to optimize V2X communication, data transmission, and security.
- Designing efficient authentication and confidentiality schemes using Elliptic curve cryptography.
- Evaluating the performance of the proposed schemes.

Thesis structure

Our thesis is divided into two parts state of arts and contribution. The first part is represented in two chapters Internet of vehicles essentials and Security aspects in IoV. In the second part, we explain our proposals followed by evaluation and results. Finally, we conclude by highlighting the main contributions of this thesis

Our thesis is composed of the following chapters:

- **Chapter One**: Internet of vehicles Essentials, we describe the most important concepts about smart cities and IoV. Terms, definitions, characteristics, applications, benefits, and challenges of IoV will be presented in this chapter.
- **Chapter Two:** Security Aspects in IoV, we introduce the main security features; we define the most serious attacks and its different countermeasures that are proposed by researchers in recent years.
- **Chapter Three:** Security Proposal Schemes, we present our proposal authentication and confidentiality schemes.
- **Chapter Four**: Evaluation and Results, our formal and informal security analysis will be developed in this chapter.
- **General conclusion**: we present the importance of ensuring security in vehicular networks, summarizing the main contributions of this work and illustrating that our approach is highly effective compared to other existing works.

Part I

Chapter One: Internet of vehicles in smart city

Chapter Two: Security of Internet of vehicles in smart city

Chapter One: Internet of vehicles in Smart City

1. Introduction

The concept of IoT was introduced in 1999 by Kevin Ashton in Procter & Gamble Company. IoT refers to distributed network that connects billions of devices over the world. This connection creates new domains such as smart grids, smart agriculture, smart health, smart factory, smart education, and smart transportation. According to Statista, the number of connected devices will be more than 29 billion devices by 2030 [1]. The main goal of IoT is to provide services for any object at any time and everywhere.

In this chapter, we describe the smart city network. We focus on the IoV domain and its different concepts including IoV characteristics, applications, objectives, and challenges.

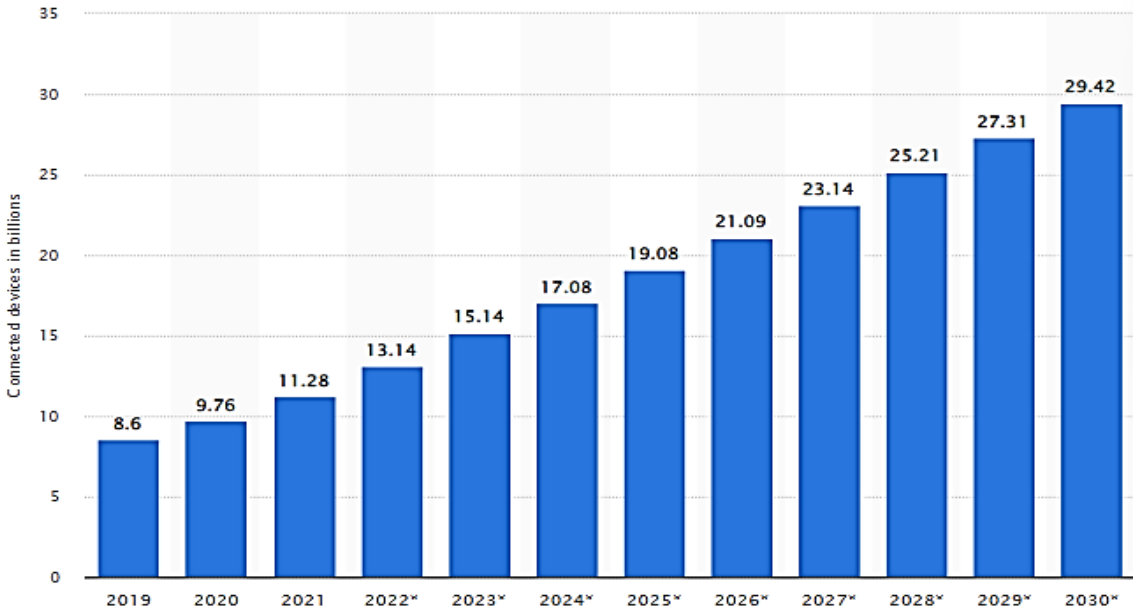

Figure 1. 1 Number of Internet of Things connected devices from 2019 to 2030 [1].

2. Smart Cities

2.1. Definition of smart cities

The term of smart city was first presented in 1990[2]. SC is a modern area that utilizes advanced IoT technologies to offer better life for citizens. It provides an effective utilization of resources and gives smart services in diverse domains (health, electricity, transportation, education…) at any time and from everywhere.

The term "Smart City" has several definitions. Many researchers [3] [4] [5] define SC as a geographical area equipped with smart objects and uses developed communication technologies in order to have an urban environment that is more connected and more efficient.

Many countries work hard to implement information technology communication (ITC) in their cities. ITC is used by smart cities to improve inhabitants' quality life, provide higher quality transportation services, reduce costs, promote economy, offer better connectivity, create a clean and healthy environment, and to provide an easy and fast access to resources and services. The following table illustrates the list of smart cities in the world in 2023.

Table 1. 1 List of intelligent cities in the world.

Region	**Cities**
Europe	Amsterdam (Netherlands) - Copenhangen (Denmark) - Barcelona (Spain). Amsterdam (Netherlands) - Stockholm (Sweden) - Helsinki (Finland). Vienna (Austria) - Zurich (Switzeland) - Lyon (France). Oslo (Norway) - Glasgow (UK) - Tallinn (Estonia) - Lisbon (Portugal).
Africa	Cape Town, Johannesburg (South Africa) - Lagos (Nigeria) - Kigali (Rwanda). Accra (Ghana) - Nairobi (Kenya) - Addis Ababa (Ethiopia) - Dakar (Senegal). Dar es Salaam (Tanzania).
Asia	Singapore (Singapore) - Tokyo (Japan) - Seoul (South Korea) - Dubai (UAE). Beijing, Shanghai, Hong Kong (China) - Tokyo (Japan), Taipei (Taiwan). New Delhi, Mumbai (India) - Doha (Qatar) - Kuala Lumpur (Malaysia). K Bangkok (Tailand) – Ho Chi Minh City (Vitnam) - Jakarta (indonisia).
North America	New York, San Francisco, Chigago, Los Angeles, Seattle, Boston, Austin, Columbus , San Diego, Washington, Attanta, Portland (USA). - Toronto, Montreal, Vancouver (Cannada).
Oceania	Sydey, Melboume, Brisbane, Perth, Adelaide, Gold Coast, Canberra (Australia). Auckland, Wellington, Christchurch (New Zeland).
Middle America	Panama City (Panama) - San Jose (Costa Rica).
South America	Bogota (Colombia) - Santiago (Chile) - Lima (Peru) - Buenos Aires (Argentina). Sao Paulo, Rio De Janiro (Brazi) - Meddelin (Colombia) - Quito (Ecuador). Montevideo (Uruguay) - Lima (Peru).

2.2. Subsystems of Smart City

SC subsystems work together to facilitate citizen's life, including smart government, smart manufacturing, smart citizens, smart transportation, smart grid, smart energy, smart home, smart agriculture, smart farming, smart health, and smart buildings.

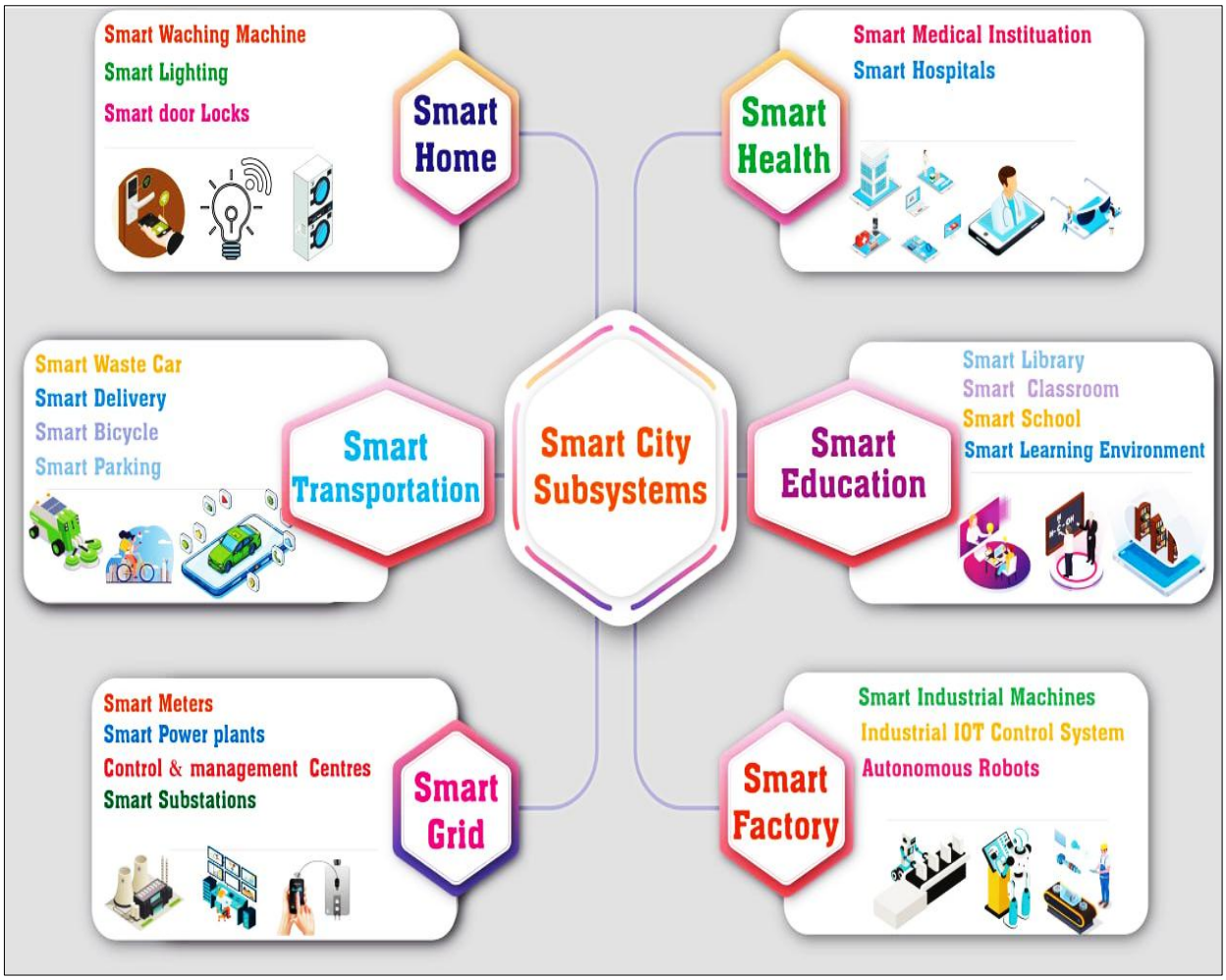

Figure 1. 2 Smart City Subsystems.

. In this section, we present the most important SC subsystem; smart home, smart health, smart education, smart factory, smart transportation, and smart grid.

2.2.1. Smart home

Smart home is an intelligent house equipped with several networked sensors, smart devices, and smart systems like smart appliance (refrigerators, washing machines…), smart thermostats, smart irrigation, smart lighting, smart locks… The main objective of smart home is to provide a greater comfort, convenience, safety, and security for homeowners [6] [7].

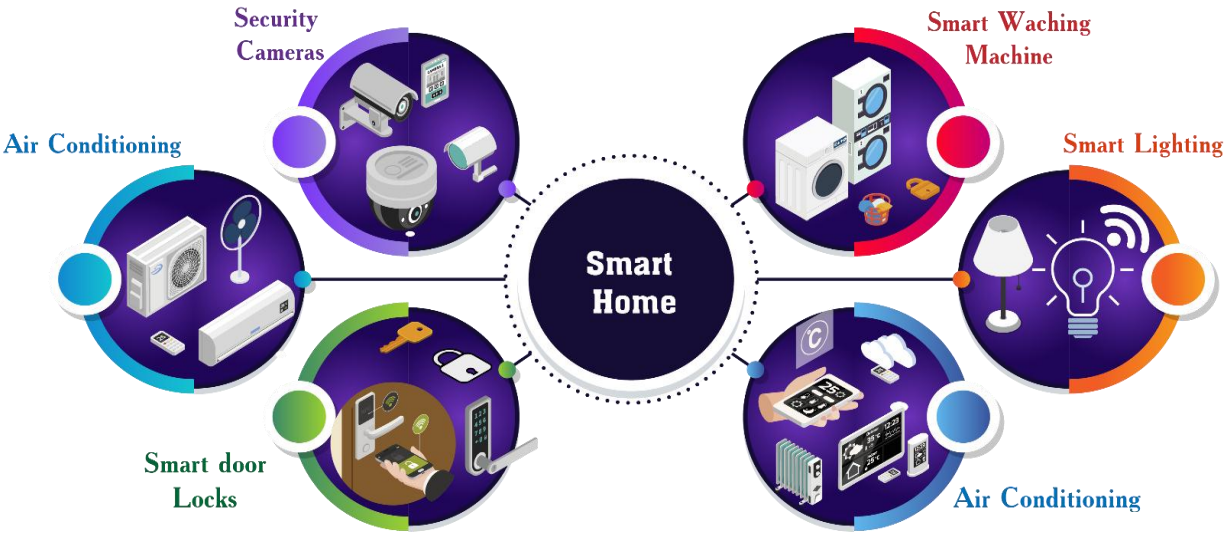

Figure 1. 3 Smart Home.

Researchers develop many applications for smart homes like Amazon Alexa, Google Home, and Samsung Smart Things [161] [170] [171][172]. Amazon Alexa developed by Amazon that interacts with users through voice commands. It helps users to control and manage smart home devices. It serves a wide range of tasks such as playing music, setting reminders, offering weather updates, and adjusting lights.

2.2.2. Smart health

One of the objectives of SC is to improve people's health using smart devices and new technologies. People can get health information such as blood pressure, heartbeat, and blood sugar from smart sensors attached to their body or to their clothes.

Smart health technology like electronic health records, wearable devices, artificial intelligence, and machine learning are used to collect, manage medical information, offer diagnostics, and treatment. It offers a dynamic access to services for smart health participants including smart hospitals, patients, doctors, and medical institutions [8] [9].

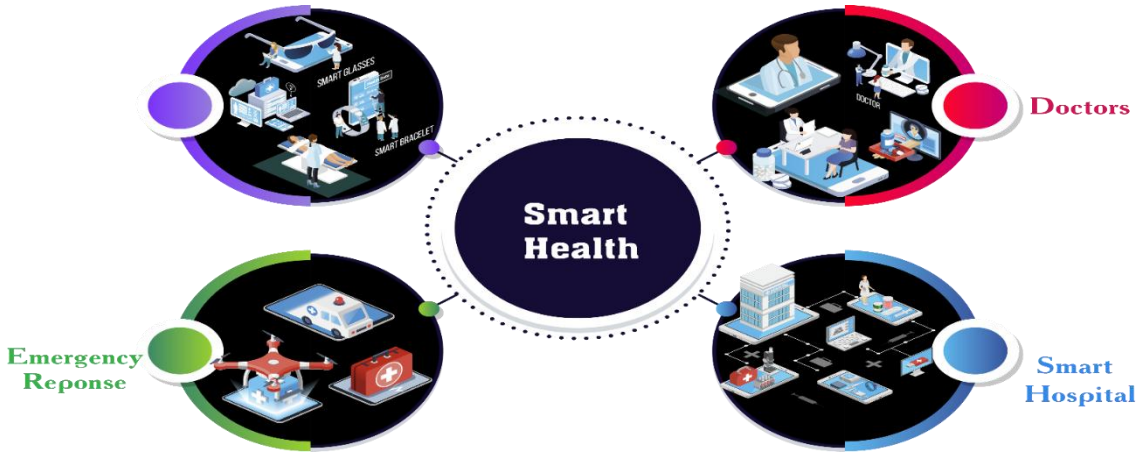

Figure 1. 4 Smart Health.

The Internet of Things (IoT) have completely transformed the healthcare sector by introducing smart health applications that leverage interconnected devices to monitor, analyze, and improve various aspects of health and well-being. Apple health is one of the popular framework of smart health, developed by Apple to help people tracking and controlling their health [162].

2.2.3. Smart education

Technology has an important impact on the education system. It enhances the quality of education, offers a rapid and easy access to educational resources, and encourages the communication and the collaboration between students, teachers, and educational institutions regardless of their physical location.

During the pandemic of Covid 19, smart education technologies played an important role in enabling schools, universities, and educational institutions to continue working [164][166][167]. Smart Education offers an efficient and an effective learning experience. It can take several forms like virtual classrooms [163] [165] [166], interactive boards [167][168], and online courses [169].

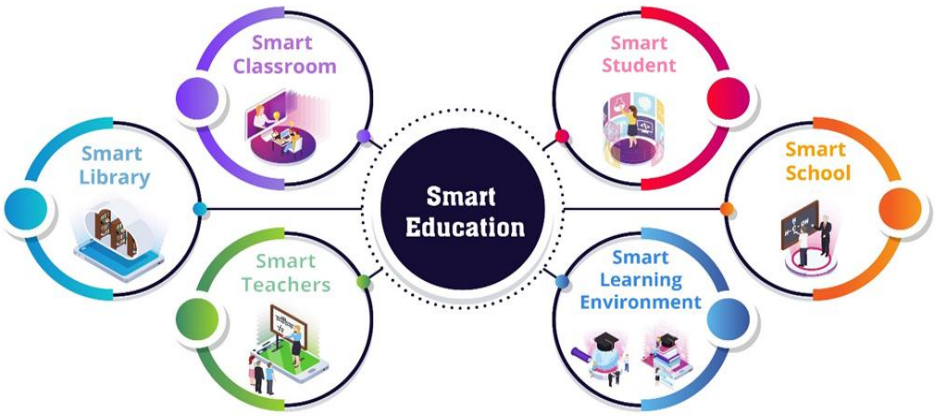

Figure 1. 5 Smart Education.

Many researches use various tools, platforms, and methodologies to build an efficient framework that make education more adaptive and more efficient. Zhi-Ting Zhu et al in [14] offered a conceptual framework that has three principal elements in smart education, smart environments, smart pedagogy, and smart learner. In [15], Richa Bajaja and Vidushi Sharmab propose a smart education framework that illustrate how students can interact with virtual teachers on a cloud environment.

2.2.4. Smart factory

One of the objective of SC is to have an intelligent and a connected manufacturing environment. SF is an intelligent industry that uses advanced technologies to enhance productivity, increase product quality, and to have a fast reconfiguration of products according to market needs.

SF is self-organized system that consists of diverse components such as physical and virtual machines, actuators, sensors, and industrial robots. These components work together to offering high quality products. It links virtual and physical organizations for having a real time simulation and maintenance, also for reducing cost, waste, and defects.

Integrating smart factory in smart city can offer platforms for collaboration between factories, regional universities, and research institutions.

Figure 1. 6 Smart Factory.

Researchers benefit from modern technology tools including artificial intelligence, robotics, and data analytics to build an efficient factory system. Industry 4 is the fourth industrial revolution, aims to build intelligent factories where the production process is fully automated

and adaptable to dynamic needs of market [16]. Smart factories can interact with each other for exchanging information, predicting maintenance needs, and making intelligent decisions with no human intervention [17].

2.2.5. Smart transportation

The traditional transportation system is a simple connected system used for managing traffic congestion. It focuses on offering basic transportation services. On the other hand, smart transportation (ST) aims to build connected, efficient, sustainable, safe and user-friendly transportation system.

Advanced technology (artificial intelligence, data analytics, and cloud computing…) and modern management strategies play crucial rule in the development of transportation system by allowing different transportation components, such buses, vehicles, bicycles, traffic lights, and sensors, to connect and share data through the internet.

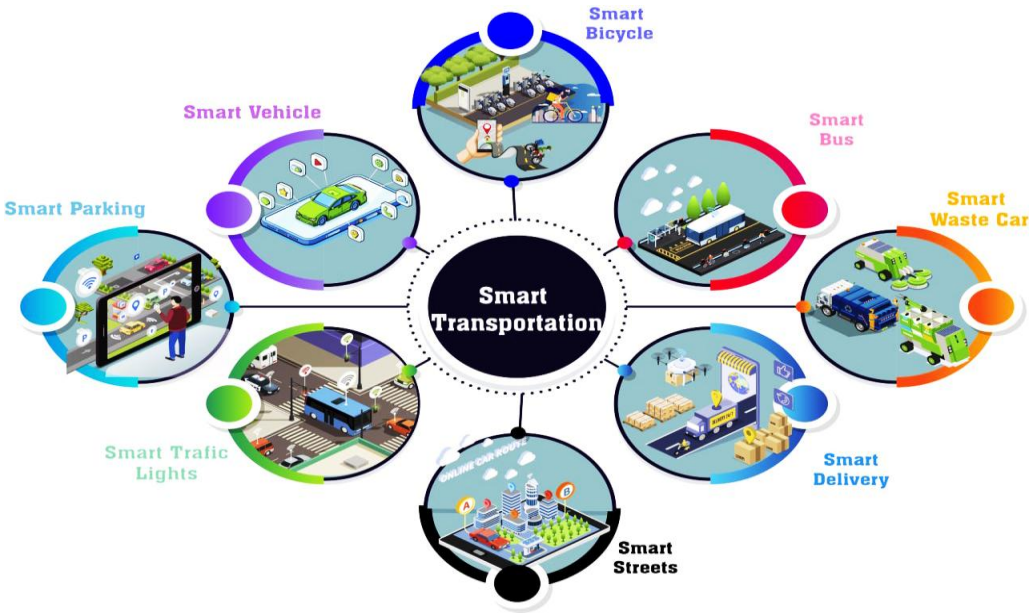

Figure 1. 7 Smart transportation.

2.2.6. Smart grid

Smart grid is an intelligent modernized electrical grid that integrates various digital technologies into the traditional power grid infrastructure for having a more intelligent and dynamic energy system.

Smart grids provide several benefits for smart cities. It enhances the use of renewable energy sources, reduces energy waste, increases energy efficiency, provides a better distribution of energy, and creates a more flexible and responsive energy infrastructures [10][11][12].

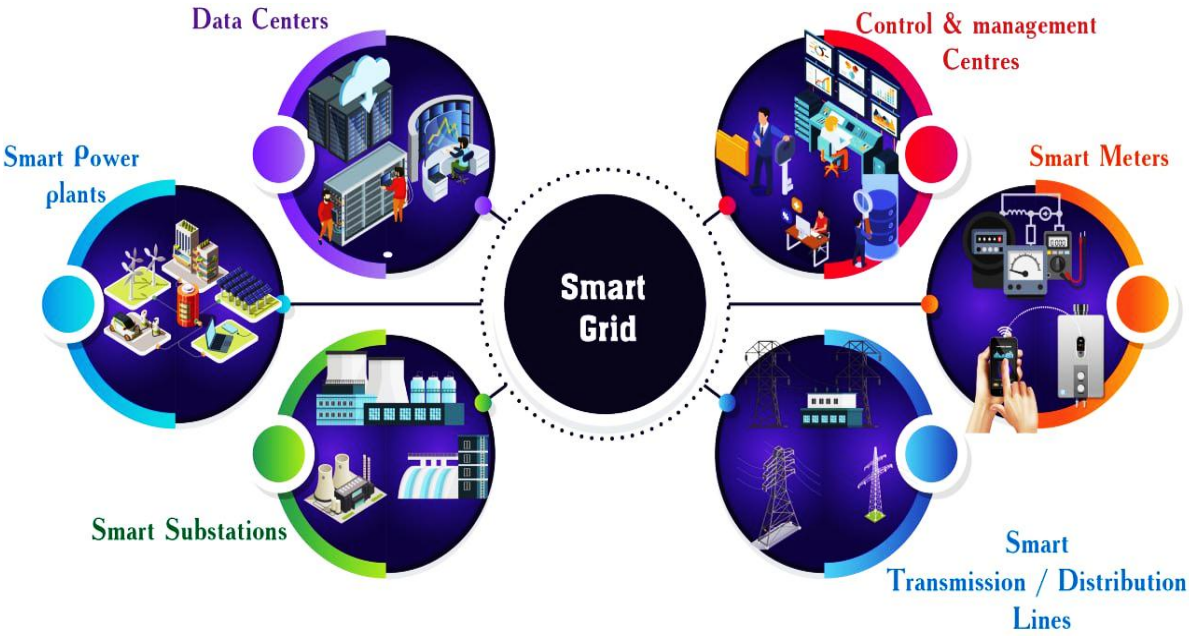

Figure 1. 8 Smart Grid.

Singapore has been making significant efforts to implement smart grids by integrating renewable sources and deploying smart meters that allow consumers to monitor their electricity.

2.3. Components of Smart City

As shown in figure 2.9, SC consists of four elements; data, objects, intelligence, and people

- ✓ **People** refers to all persons located in the smart city; not just a person who lives in this city but also a person who studies, works, and visits the city. Smart people is an active, connected, and informed person that uses smart IoT technologies to have access to smart city services in different domains including healthcare, education, public transportation….. SP participates in communication between smart city objects' to enhance the quality life of all members in the city.
- ✓ The term **intelligence** refers to the city that provides the necessary infrastructure and technology to offer an effective and an efficient service for their citizens in real time. It also refers to the ability of an object to make the best decisions using data collected from a wide range of sources.
- ✓ **Objects** are interconnected devices that use IoT technologies to communicate and interact with each other. An object can gather, analyse, and process data.
- ✓ In Smart City, object uses **data** for making decisions. This data is collected from cameras, sensors, and other objects about various SC aspects like air quality, and traffic patterns.

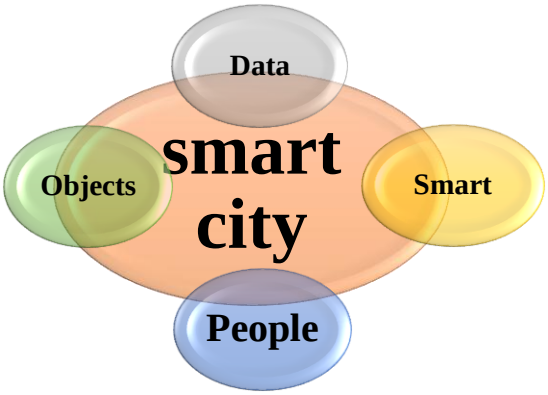

Figure 1. 9 The core components of smart city

2.4. Challenges of smart cities

There are many challenges of SC; we present in this section some of them, such as data and network management, energy consumption, connectivity, processing and storing capabilities, heterogeneity, and security challenges.

- **Management:** In SC, objects collect large amount of data from different sources. This leads to the need of an effective data management for collecting, analyzing, storing and delivering data.
- **Energy consumption:** As the number of services demanded by objects increases, the problem of energy consumption continue to rise. Objects need energy to operate, they consume a significant amount of energy for gathering, computing, maintaining, and saving data.
- **Connectivity:** Network connectivity has an important impact on the performance of SC system. It is affected by many factors like building structure, geographical location, and infrastructure. These factors can create dead zone or zone with weak connection.
- **Processing and storing capabilities:** Objects need a high computation, communication, and storage capabilities for analysing and processing data.
- **Heterogeneity,** SC integrates diverse network technologies, protocols, and devices.
- **Security:** One of the major challenges of SC is to protect data, network devices, and citizens' privacy from malicious objects (unauthorized access).
- **Technology:** The rapid advancement of technology offers at the same time opportunities and challenges for the development of smart city.

3. Internet of vehicles

3.1. Definition of IoV

IoV is the evolution of Vehicular Ad Hoc Networks (VANET) where vehicles are smart entities in IoT. VANET is a special class of Mobile Ad-hoc Network (MANET), a simple network that consider vehicle as a simple node with limited storage and computing capabilities. VANET does not support the collaboration with heterogeneous network. IoV extends this scope by the integration of vehicle, networks, Internet, and various technologies enabling vehicle to communicate not only with neighboring vehicles but also with different objects in the world. The following table illustrates the differences between VANET and IoV.

Table 1. 2 VANET VS IoV [178].

Characteristics	**VANET**	**IoV**
Vehicle	Simple node.	Smart object.
Processing and storage capabilities	Limited capabilities.	High capabilities.
Connectivity	- Connected/Disconnected. - Depending on network availability	- Always connected. - Any time and everywhere.
Network	Limited, homogeneous, flat, and simple network.	Huge, complex, hierarchical, and heterogeneous network.
Decisions	Based on simple logical system.	Based on artificial intelligence system.
Data resources	Limited data resources.	Unlimited data resources
Communication types	V2V and V2R communications.	V2X communications.
Scalability	Non scalable	Scalable
Applications	- Emergency vehicle warnings - Collision Avoidance - Intersection management	- Entertainment and infotainment applications - Remote diagnostics - Over the air updates - Navigation

IoV is an open, intelligent, dynamic, and complex system that provides advanced IoT technologies to offering seamless connectivity between vehicles and other objects. This connectivity allows vehicles to be a part of IoT network and to be able for acting and reacting with the world.

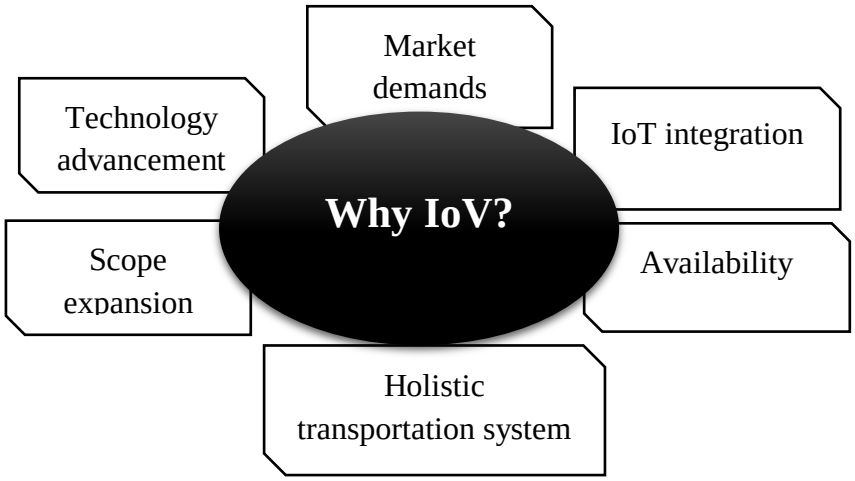

Figure 1. 10 Why IoV?

3.2. Smart vehicle

Vehicle evolves from traditional transportation mode to an intelligent object. It is equipped with a variety of sensors, navigation tools, energy management system, computing and storage units, artificial intelligence and machine learning modules, autonomous driving system, and control systems. These components work together to create an intelligent and a synergistic driving experience. Some components of smart vehicle are described below.

- Sensors; vehicles are equipped with a variety of sensors like lidar, radar, cameras, ultrasonic, temperature sensors, pressure sensors…. These sensors are used for collecting data about vehicle's surroundings such vehicle status and road conditions.
- Navigation tools; vehicle can navigate on Net for having many services like more information about roads, updating applications and uploading new applications.
- Energy management system, Vehicle utilizes energy management technologies for reducing energy consumptions.
- Computing and storage units, used for processing and saving a large amount of data.
- Artificial intelligence and machine learning modules; used for analyzing data and making intelligent decisions.
- Control system; offers an intelligent vehicle control by managing various aspects of the vehicle's operation like braking, steering, and propulsion.

- Connectivity modules; provides advanced technologies that allow vehicle to everything communications.
- Autonomous driving system;

Using these components, vehicle can generate a large amount of data, process and analyze it to make intelligent decisions. In addition, it can share and disseminate data in real time.

3.3. Vehicle to x communications

IoV offers a seamless connectivity between vehicle and other objects creating different types of communication including Vehicle to vehicle communication, Vehicle to infrastructures communication, Vehicle to roadside units, vehicle to sensors, and vehicle to pedestrian. These five types are illustrated in Fig 2.10.

- Vehicle to vehicle communication (V2V), vehicle can use dedicated short-range communication (DSRC) through the 802.11p/WAVE standards or cellular communication technologies (4G LTE, 5G) to communicate with other vehicles for sharing information about road conditions, speed, direction, and breaking. This communication helps vehicle to predict actions of nearby vehicles and avoid collisions.
- Vehicle to infrastructure (V2I) is done through Wi-Fi (802.11a/b/g/n) or cellular communication technologies for offering a dynamic link between vehicle and surrounding environment.
- Vehicle to roadside unit (V2R) refers to the communication between vehicles and road side units that are located along roads like bus stations, traffic cameras, and traffic lights using 802.11p/WAVE. V2R communication can offer real-time information and services including signal timing information, available parking spaces, and traffic conditions.
- Vehicle to sensors (V2S), presents the communication between vehicles and sensors like radar, lidar, and cameras using Ethernet, Wi-Fi or Media Oriented System Transport .Through this communication, vehicle can collect real time information about its surroundings such air quality and weather conditions. These information help drivers to react to environment changes and to take intelligent actions. V2S has an important role for improving efficiency and safety in various driving conditions.
- Vehicle to personal devices (V2P), through Bluetooth, Wi-Fi, and other wireless communication technologies, vehicle can communicate and exchange information with personal devices like smart phones and tablets.

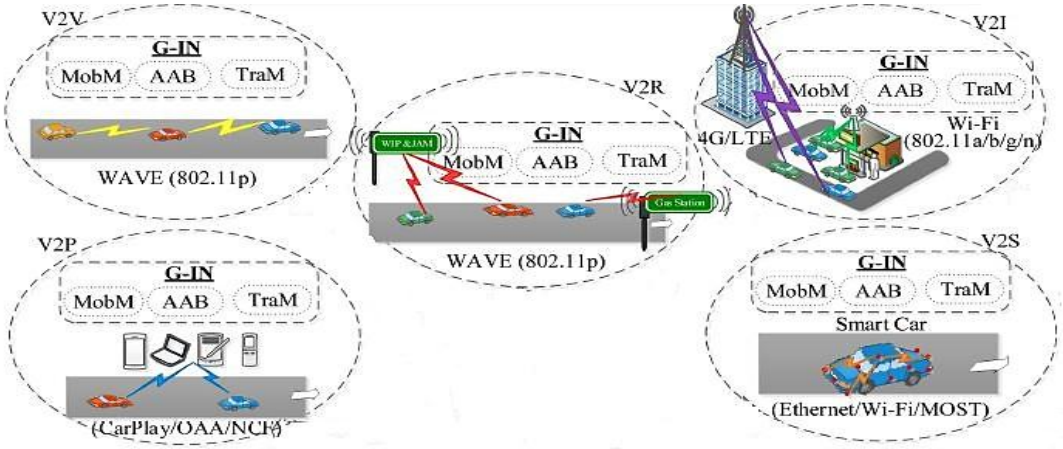

Figure 1. 11 Types of communication in IoV [176].

3.4. IoV objectives

The main objectives of IoV is to offer a more connected, more efficient, more intelligent, and safer transportation system. Integrating IoV in smart city can bring a wide variety of benefits. IoV can reduce road accidents, energy consumption, and carbon emissions. It improves air quality, service quality, driving behaviors, traffic and parking management in the city. It also provides vehicle's diagnostic and maintenance in real time.

With the use of smart parking system, vehicles can reserve free spaces in real time that leads to reduced price, time, air pollution, and minimize the unnecessary movement of vehicles. Smart traffic management (STM); IoV offers an intelligent traffic management system by identifying traffic patterns, congestion points, and potential bottlenecks, based on these information, STM can proactively adjust the allocation of lanes and dynamically optimize traffic signal time. Energy consumption; IoV revolutionises energy usage by building a seamlessly interconnected vehicle environment. This connectivity minimizes fuel consumption. IoV offers a real time information about traffic conditions, optimal routes, and even energy-saving driving techniques that help vehicles to make intelligent decisions and leads to have an efficient energy usage. Maintenance in real time, using vehicle smart sensors' vehicle can sends notifications about its health status and its performance in real time. With the use of data analytics and machine learning, IoV can provide a proactive maintenance. The real time maintenance can saves vehicle components' like lights, brakes, and tires and can prevent unexpected breakdowns.

3.5. IoV applications

Researchers developed a variety of vehicular applications that make driving experience more comfort, more connected, and more intelligent. Applications like CarPlay, Android Auto, BMW Connected, Ford Pass, My Chevrolet, Waze, Plug Share, Gas Buddy, Nissan Connect Service, Volvo on Call, Mercedes me, and Audi connect are some specific applications for

smart vehicles. BMW Connect Drive serves as an example of how IoV technologies improves driving experience by giving vehicle owners connectivity and real time information. BMW offers remote services like locking/unlocking vehicle, vehicle status, and navigation assistance. Tesla is another example that enables self-driving, self-controlling, and navigating vehicles. Tesla can receive software updates allowing manufactures to add new features remotely to enhance vehicle's performances. CarPlay provides an infotainment system with access to music, navigation, and other applications. Audi Connect offers a suite of connected services such real time traffic information, remote vehicle monitoring, and remote control.

There are applications that plays the role of bridge between smart homes and smart vehicles. Amazon Alexa Auto is one of these applications that can be integrated in smart vehicles. It is an extension of Amazon Alexa application, allows drivers to send messages, make calls, navigate, and control smart home devices.

Modern cities around the world such as Singapore, Los Angeles, and Sydney work hard to improve citizen's quality life. Singapore is one of modern cities that achieve remarkable advancements in its transportation systems using smart traffic lights, electronic road pricing (ERP), real time traffic monitoring, smart parking systems, mass rapid transit (MRT), adaptive response to incidents, and public transport management.

4. Concepts

4.1. Cloud Computing

Instead of installing applications in devices and wasting time and cost. Cloud Computing is a common effective technology that offers a variety of services. CC can provide a three category of services Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These services are presented in [4]. SaaS provides software through the Internet that are available for any device. PaaS gives a platform on which users can built applications and services, PaaS allows users to develop, run, and manage applications. IaaS offers online access to virtualized computing and storing resources.

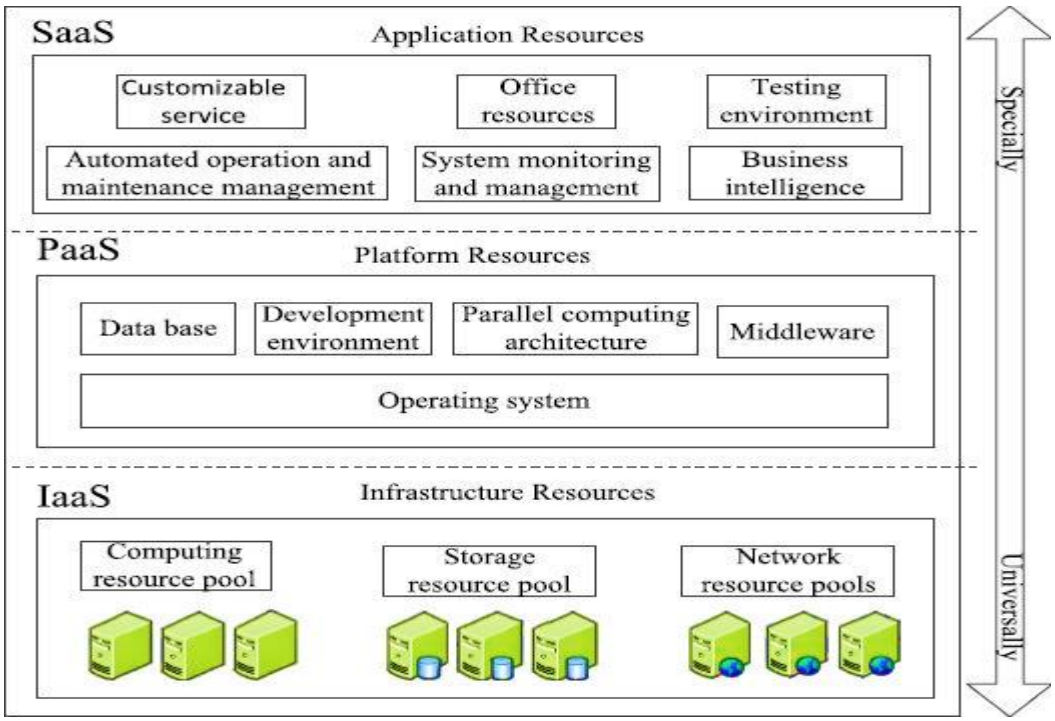

Figure 1. 12 The hierarchical model for cloud computing [8]

CC can be public, private, and hybrid Cloud. In Public Cloud, any users can access and utilize services offered by the cloud. Private Cloud in this type, only authorized users can benefit from services and resources. Hybrid Cloud is a combination of private and public cloud, some services are available for all users and specific services kept private for a limited number of users.

Integrating CC with IoV can bring many benefits including the availability of services at any time and from anywhere, a higher level of reliability, unlimited storage and computing capacity, improved collaboration; users can collaborate with each other that's enhance productivity, low maintenance cost; the cost of hardware and software maintenance is decreased by using CC, and dynamic resources utilization.

With the rapid evolution of IoV, cloud computing cannot handle with the huge amount of data coming from various objects located at different place in the world. In addition, cloud is far from end users. Therefore, it was necessary of creating new small-scale clouds like cloudlet, fog, and edge computing. Choosing one of these types depends on where you are and what you need.

Fog computing was first coined by Banomi et al from Cisco, situated between IoT objects and CC. It can be linked to devices called fog nodes like routers, switches, controllers, and servers.

FC brings cloud services closer to IoV objects. Due to FC close proximity, data can be processed and stored more quickly, more effectively, and with less latency.

Edge computing is so similar to fog computing and has the same goal of moving services from CC to the edge of network that reduce latency. However, edge computing brings services as more closely as possible to the end users. While Fog computing is situated between the edge computing and the cloud. FC can help EC for analyzing and filtering data and classify them to useful and irrelevant data.

The term of Cloudlet was first introduced by Satyanarayanan et al. It is a small scale of cloud, well connected to the Internet, and has the same objective of fog and edge; being so closer to users. Cloudlet is suitable for environments that require real time data computing and low latency like vehicular environment.

4.2. Software Defined Network

Day by day, the number of connected objects grow rapidly and the traditional network fails to meet the needs of modern cities (as illustrated in table 2.3). Software Defined network is an emerging approach that solves the limitations of traditional network.

Table 1. 3 Traditional network Vs. SDN [179].

Traditional Network	**SDN**
Distributed architecture	Centralized architecture
Manual devices' configuration	Automatic devices' configuration
Static network	Dynamic network
Closed interface	Open interface
Takes a long time response	Takes a short time response
Data and control planes are implemented in the same device	Data and control planes are separated
All network packets have the same priority	Specific network packets can be blocked or can have more priority
High maintenance cost	Low maintenance cost
It is difficult to have a global network view	It is so easier to have a global view of the network
Low availability	High availability

Unlike traditional network, SDN is characterized by the decoupling of the control plane from data forwarding plane (figure 11). This separation simplifies the network management, optimizes network resources, and makes the network more scalable, more efficient, and more flexible.

As shown in the following figure, the SDN architecture is divided into three layers; Application layer, control layer, and infrastructure layer. Application layer is responsible for defining the network functions, policies, and services. Control layer manages and controls network's behavior. Infrastructure layer is responsible for forwarding data from one device to another. These layers communicate with each other using northbound API and southbound API.

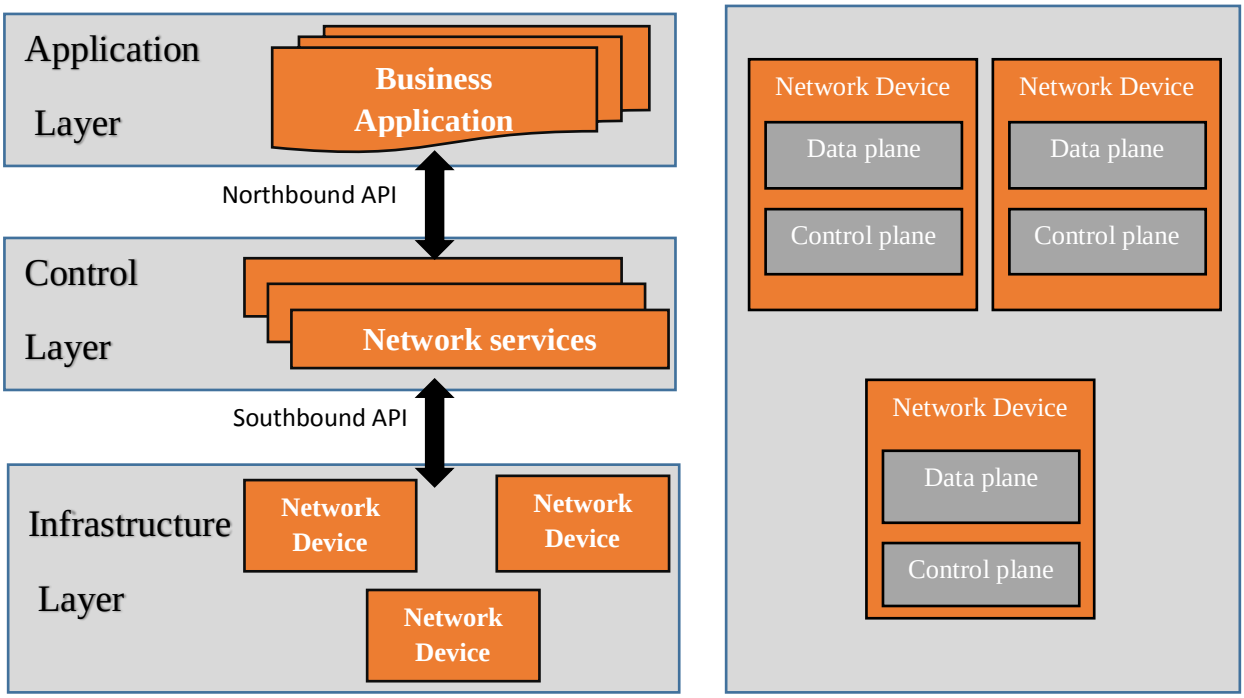

Figure 1. 13 Traditional architecture Vs SDN architecture [177].

The integration of SDN in IoV can provides a wide range of benefits. SDN offers an intelligent and a dynamic network management, control and configuration. It provides a quicker responses time to users, a high data transfer, a high connectivity between objects from heterogeneous networks, a real time allocation of resources, and an efficient data routing. The dynamic network control helps to having a better level of security. SDN can also adapt the network according to business needs and without the need for manual adjustments .SDN do not only simplify the network management and control but also open the door to innovation services and applications.

5. IoV Challenges

Certain IoV characteristics like incredible speed of vehicles, dynamic topology, high mobility, variety of the environment, non-uniform distribution of vehicles, poor of network connectivity, large network, IoV Communication types, and openness of IoV present several challenges including data management, vehicle management, scalability, interoperability, power consumption, and security.

- Data management; due to the diversity of data sources and the enormous volume of data produced by connected objects, data need to be stored, analyzed, and managed in real time.
- Vehicle management; large number of smart vehicles move rapidly from one place to another place, this makes hard to configure, and maintain vehicles.
- Scalability; as the number of connected objects grows rapidly, it is so difficult to control and manage IoV network.
- Interoperability; the ability of different objects in heterogeneous network such as vehicles, homes, and industries to seamlessly and effectively communicate and collaborate with each other.
- Power consumption,
- Security; Security is one of the biggest challenges of IoV; data and vehicles need to be protected from malicious attacks.

6. Conclusion

SC offers many benefits making citizen's life smarter. Objects in SC share and disseminate information between them, this information need to be protected from malicious devices. A security failure can make disasters in smart cities in terms of economical loses and human life lost. In the next chapter, we treat the security aspect in the IoV network.

Chapter Two: Security of Internet of vehicles in Smart City

1. Introduction

The communication among various objects in the IoV environment gives the opportunity to malicious objects to intercept, modify, delete or even to insert fake information during communication that can cause disasters in route. In this chapter, we present various security aspects, threats and attacks related to IoV environment.

2. Security requirements

The communication and the cooperation between vehicles and objects can create security challenges; an illegal vehicle can act as a legitimate vehicle and cause disasters in smart city. In this section, we discuss the IoV security requirements including authentication, confidentiality, availability, privacy, and non-repudiation. It is so important to ensure these requirements for having a safe, comfortable, and enjoyable driving in transportation system.

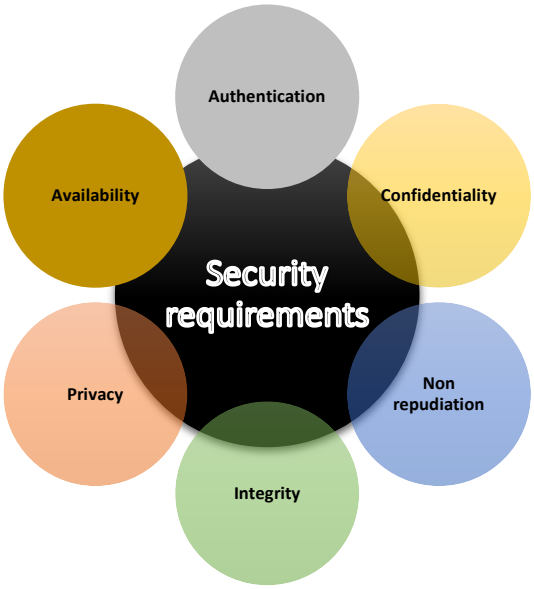

Figure 2. 1 IoV Security requirements [115].

2.1. Authentication

Two security requirements can be implemented together authentication and authorization for building a trust among interconnected objects. Authentication is the process of identifying vehicles, it gives the answer of "Who is the vehicle identity? ", and "Does this identity represent itself?" However, authorization refers to the mechanism of determining if a vehicle has the authority to access to smart city resources', answering the question of "does the vehicle have the right to access resources ?".

Authentication plays an important role for keeping IoV network more secure allowing only authenticated vehicles to communicate and interact with smart city objects' as well as decline malicious devices.

Several techniques are used for creating authentication schemes such as: Biometric authentication (human physical or behavioral features) [78] [79] [80], smart card [63][62][81][82], ID/Password [60] [45] [82] , hash functions [83] [62] [84] , pre shared secret keys [18] [85] [86], and public key cryptosystems [87] [88] [89].

2.2. Confidentiality

Confidentiality is a set of rules that restrict the access to data, used to protect sensitive information from unauthorized access. According to Hammer and Scheider [90], Confidentiality is a concept of ensuring that only destined vehicles can read, listen, and record information.

Most security schemes use diverse data encryption methods to achieve confidentiality. Symmetric encryption is a well-known approach like AES (Advanced Encryption Standard) [91], and Blowfish [92][93], it uses a common secret key for encrypting and decrypting data [86], this key needs to be kept private during communication. Asymmetric encryption is the use of key pairs (public and private) for encrypting and decrypting messages. Example of asymmetric cryptography; RSA (Rivest Shamir Adleman) [94][95], DSA (Digital Signature Algorithm) [104], and Diffie Hellman [102] [103]. Digital signatures, Identity-based encryption [101], and Homomorphic encryption [100].

2.3. Non repudiation

Non-repudiation is the mechanism that makes vehicles unable to deny their actions or their behaviors in the network. For example, vehicle cannot refute that is the sender of message. Most security schemes use digital signatures inside IoV data to provide the non-repudiation. Some vehicular network approaches related to non-repudiation are presented in these papers [96][97][98][99].

2.4. Integrity

Integrity ensures that data transmitted between vehicles and objects are not modified during transmission. Only the authorized vehicles are able to alert messages.

Integrity is an important aspect for building a safe connected vehicle in smart cities. To guarantee the integrity of information, the received message should be verified using

different technics like message authentication codes (MACs) [105] [107] and digital signature [106].

2.5. Availability

Availability makes services available at any time and everywhere even in emergencies. In the vehicular system, a few seconds of delay can make message insignificant. It is so important to stay connected and continue to operate efficiency, not just being connected.

The high availability depends on network architecture, connectivity, regular maintenance, and service management. The IoV requires strong infrastructure and strategic planning in order to ensure high availability using distributed network architecture, virtualization, real time management and maintenance. The distributed network architecture reduces the risk of centralized failures. The real time management plays a crucial role for detecting network problem and resolving it [112]. Virtualization offers an efficient use of physical resources, and allows a dynamic resource allocation [109]. Predictive maintenance can improve availability by identifying potential issues before they escalate [111]. Sumra et al provided a summary of different proposed techniques for the availability in the vehicular network [108]. Zenni et al exploited network coding for data availability in vehicular networks [110].

2.6. Privacy

Privacy refers to the protection of vehicle's personnel information. It means that is impossible for malicious object to determine whether two different messages are coming from the same vehicle or not.

Various methods are used to preserve privacy in IoV. Anonymity and pseudonym can be implemented in IoV framework to enhancing privacy [113] [114] [75][31]. Vehicles and other objects can communicate using pseudonyms instead their real identities [19]. These pseudonyms should be managed using an efficient protocol to avoiding the long-term tracking.

Table 2. 1 Security requirements in vehicular networks.

Requirements	What	Why	How	Papers
Authentication	Process of identifying and authorizing vehicles to participate in communication.	Confirms if a vehicle is legitimate or not.	-Id/Password. -Pre-shared key. -Public key cryptosystem. -Biometric. -Smart card. -Hash function.	[45] [60] [82] [18] [85] [86] [87] [88] [89] [22] [78] [79][80] [29] [62] [63] [81] [82] [62] [83] [84]
Confidentiality	Set of rules that limit access to IoV information.	-Protecting IoV data during transmission. -Preventing unauthorized access to sensitive IoV data.	-Symmetric encryption. -Asymmetric encryption. -Hash functions. -Digital signatures. -Identity based encryption. -Homomorphic encryption.	[91] [92] [93] [86] [94] [95] [104] [104] [101] [100]
Integrity	Process of protecting IoV messages from any change during the transmission.	Preventing unauthorized vehicles to modify IoV information.	- Controlling the physical environment. - Using hash functions. - MAC. - Digital signatures.	[26] [27] [28] [105] [107] [106]

Privacy	Assures that the information between vehicles is trustworthy	Protecting vehicle's information from exposure in IoV environments.	- An anonymous authentication.	[21] [30] [22] [31]. [113] [114] [75].
Availability	Mechanism of making IoV resources available when needed.	Guarantees the resources' availability.	- Distributed architecture. - Predictive maintenance. - Virtualization. - Real time management.	[23] [111]. [109]. [112].
Non repudiation	Mechanise of proving that the vehicle is the sender of message or document.	Assures that the vehicle cannot refute something.	- Blockchain. - Digital Signatures.	[36] [37] [96][97][98][99]

3. Most serious IoV attacks

The IoV system are exposed to different types of attacks. As shown in figure 2. 2, we classify the attacks and threats on IoV communications into six different categories including, attacks against authentication, attacks against confidentiality, attacks against non-repudiation, attacks against integrity, attacks against availability, and attacks against privacy.

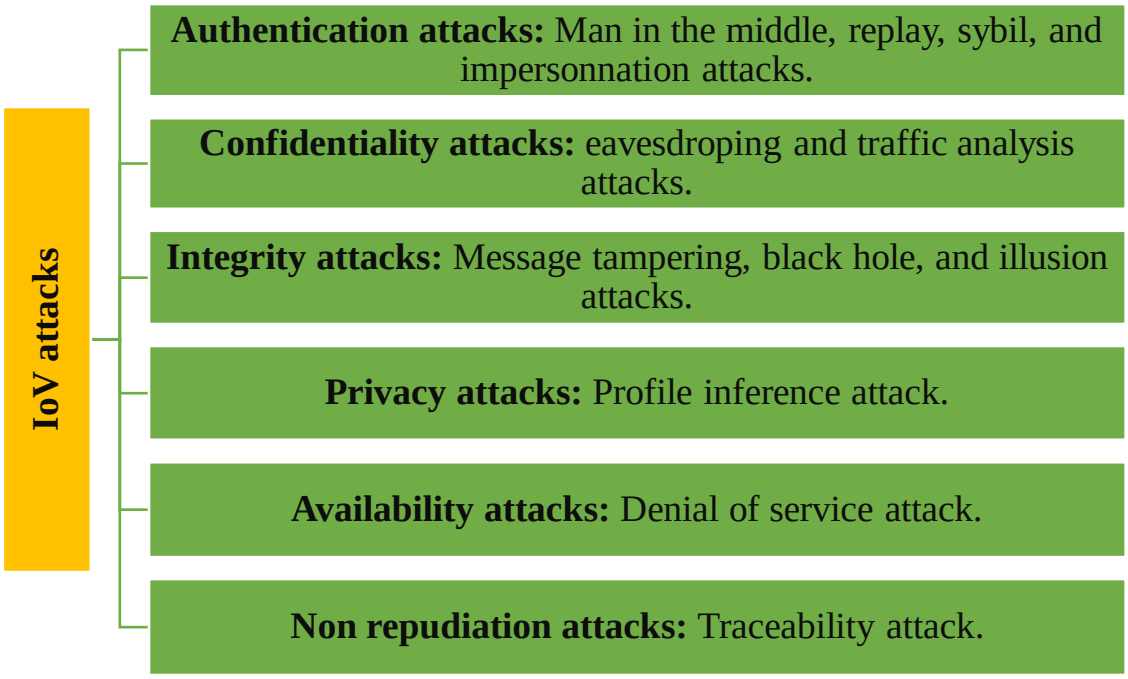

Figure 2. 2 IoV attacks.

3.1. Authentication attacks

3.1.1. Sybil attack

In Sybil attack, a malicious object can generate more than one identity for a single vehicle and give a sense that multiple vehicles are there [115]. He/It can use these false identities to send incorrect information to legitimate objects that affect vehicles decisions.

Malicious object tries to get a large number of identities to send multiple messages (about traffic or route decisions) from one object with multiple identities; the Vehicle receiver believes that messages are send by different objects, so he makes decision according to these messages. This decision is so beneficial to malicious object; he can redirect vehicles to another place.

There are several countermeasures against this type of attack including Digital Signature combined with anonymous certificates [37], Distributed Aggregate privacy-preserving authentication [38], Group Signature [39], Identity based cryptography [22], Tamper-proof

device(TPD), One-time identity based aggregate signature [20] **[40],** identity symmetric scheme [117], and Payload-based mutual authentication Protocol [22].

In [116] Mustafa et al discussed different approaches for the Sybil attack in the vehicular network. Jiantao et li used trajectory as an identity of vehicle to achieve Sybil resistant authentication for IoV [117].

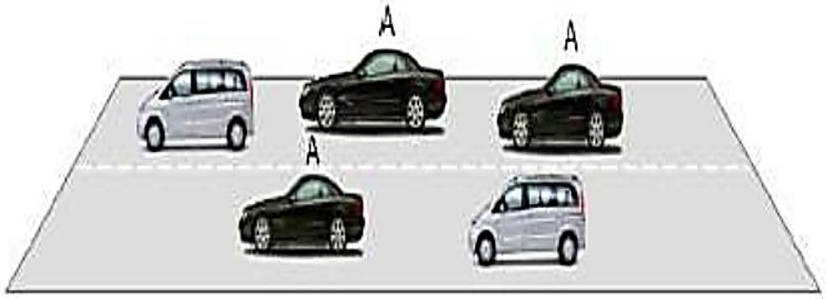

Figure 2. 3 Sybil Attack [68].

3.1.2. Man in the middle attack

Man in the middle attack is the most popular attack in IoV system. It is considered as a real time attack; It happens during the transmission of messages between objects for displaying and modifying the information before the legitimate vehicle receiving it.

A malicious object MO can spoof the identities of two legitimate vehicles (V1 and V2) involved in a network and he passes V1 for V2 and vice versa. This type of attack can make serious consequences in IoV, it can take the control of the communication channel between V1 and V2 [119], intercept, modify, change or replace target victims' communication traffic. Moreover, victims believe that the communication channel is protected [120].

Different solutions are proposed against Man in the Middle attack like mutual authentication [44], Blockchain [121], biometric update [29], time synchronization [30], password [122] [21], and bloom filter based on SDN [46].

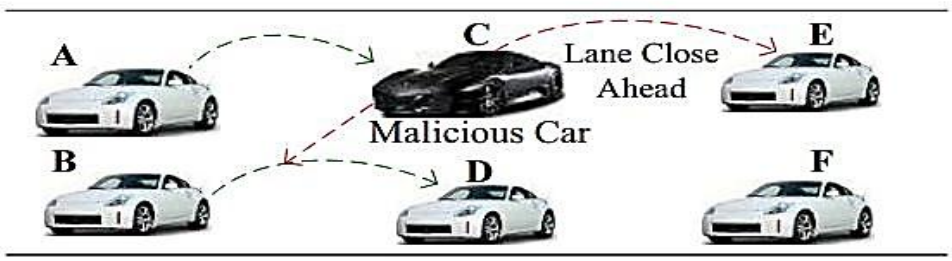

Figure 2. 4 Man in the Middle Attack [69].

3.1.3. Impersonation and forging attack

In this type of attack, a malicious object can change his/it identity to modify the content of message then he sends this message to vehicles. This impersonation can create chaos, traffic jam, and accidents.

Many solutions proposed against the impersonation and forging attack, including linear search algorithm and binary search algorithm [48], keys based on shared secret m_i [52], password and hush functions applied on the secret key [51][62], bloom filter and the binary search techniques [24].

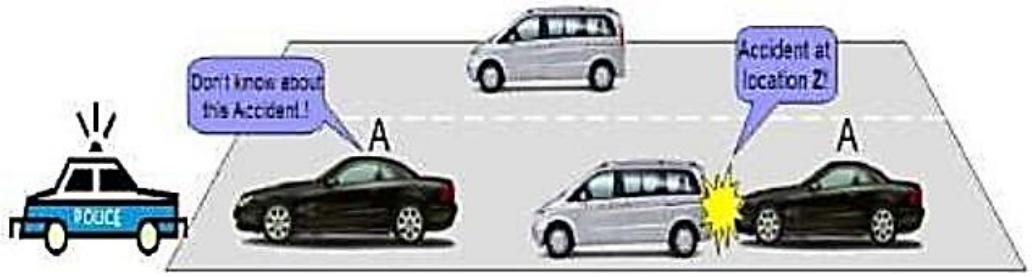

Figure 2. 5 Impersonation Attack [68].

3.1.4. Replay attack

It consists of intercepting message and resending it as it to have the right as the legal user. This attack aims to have an illegal access to IoV services and resources. To prevent this attack, there are many countermeasures including robust reset speed synchronization control of a connected vehicle [54], timestamp [59] [121] [122], and random numbers [47] [29].

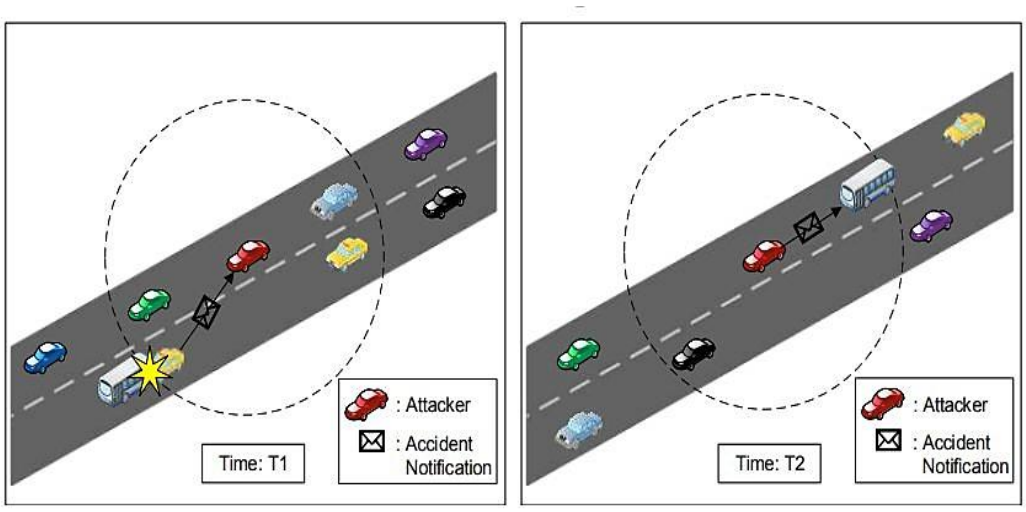

Figure 2. 6 Replay Attack [70].

3.2. Confidentiality attacks

3.2.1. Eavesdropping attack

The eavesdropping attack works by listening and intercepting the communication between vehicles in IoV environment in order to gain unauthorized access to vehicle message. Many solutions are used to defend against this attack. Sun et al used shared key and ID-based encryption for protecting sensitive information [129]. Lei et al used one time identity based group key for cryptography mix zone to prevent eavesdropping attack [130]. Hu et al used group signature to ensure confidentiality [131]. Qian Kang et al used cipher text policy attribute based encryption (CP-ABE) to ensure confidentiality [132].

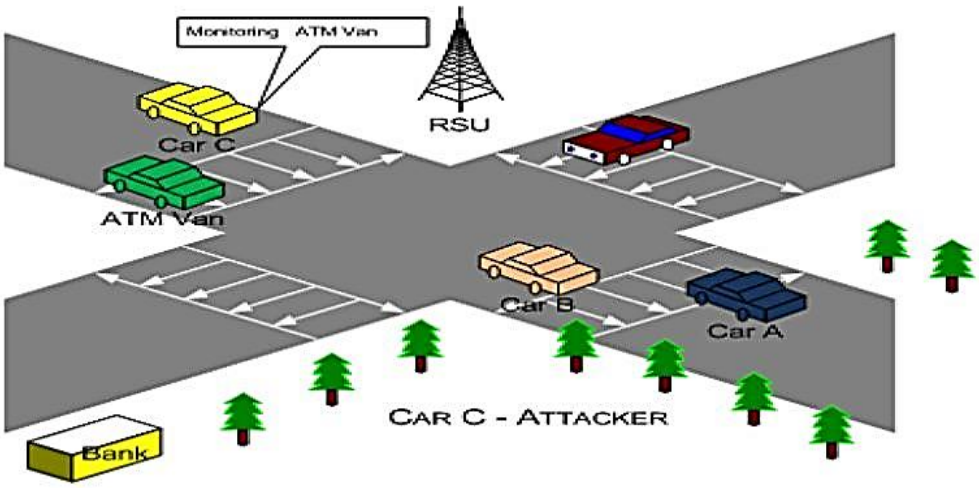

Figure 2. 7 Eavesdropping Attack [71].

3.2.2. Traffic analysis attack

The traffic analysis attack is characterized by the interception and the analysis of communication between vehicles for collecting as much information as possible [133] [136]. This information is used for malicious activities, ranging from tracking specific vehicles to planning sophisticated attacks.

Protecting the IoV environment against traffic analysis attack necessitates robust security strategies like the use of encryption and anonymization, the integration of traffic padding [135], session keys [49], intrusion detection system, and dummy traffic analysis [134].

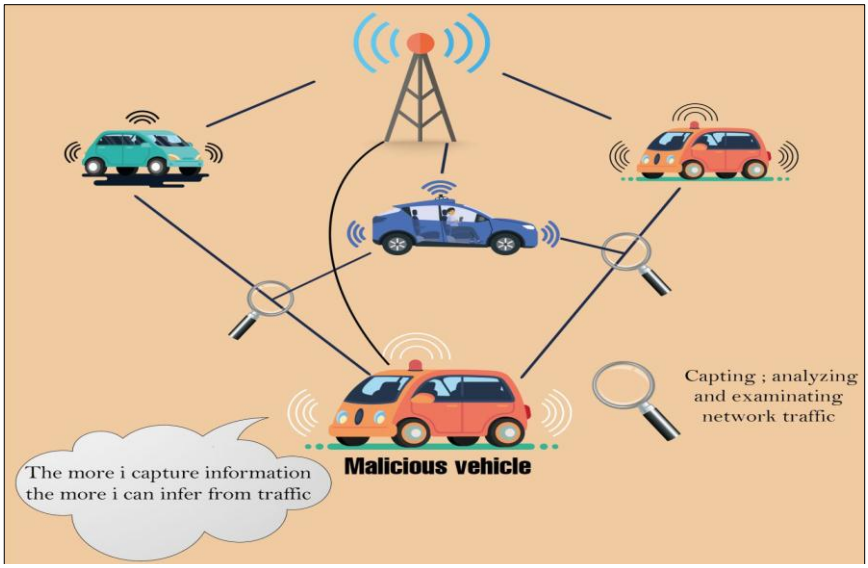

Figure 2. 8 Traffic Analysis Attack.

3.3. Non repudiation attacks

3.3.1. Traceability attack

This attack occurs when a malicious vehicle intentionally disrupts or obfuscates the traceability of events inside the IoV network. There are several countermeasure to such attacks like digital signature to confirm the sender of messages and to prevent malicious vehicles from tampering with or forging event data [137]. Intrusion detection system (IDS) for detecting and identifying the abnormal or malicious activities [138]. Timestamp for establishing a chronological order of events, making it difficult for vehicles to deny their actions [139]. Blockchain for recording transactions and communications [138] [139]. Biological password [140].

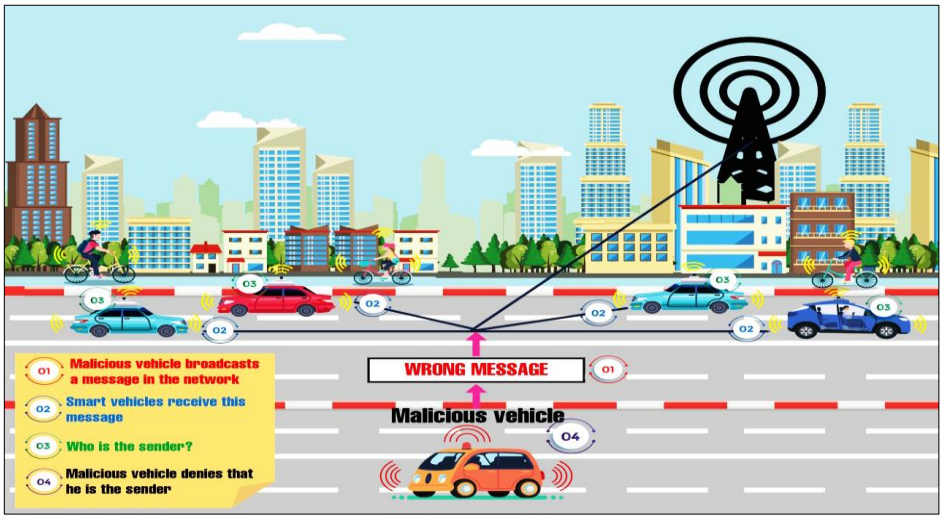

Figure 2. 9 Traceability Attack.

3.4. Integrity attacks

3.4.1. Message tampering attack

Message tampering attack refers to the unauthorized modification or suppression of message exchanged between vehicles and other objects during the communication process [141]. The main goal of this attack are sharing false information, disrupting traffic flow, and having unauthorized access in the IoV ecosystem.

To defend against message tampering attack, it is important to implement robust security measures. TangleCV [142]. A group of signature is proposed in to detect the tampered messages [147].

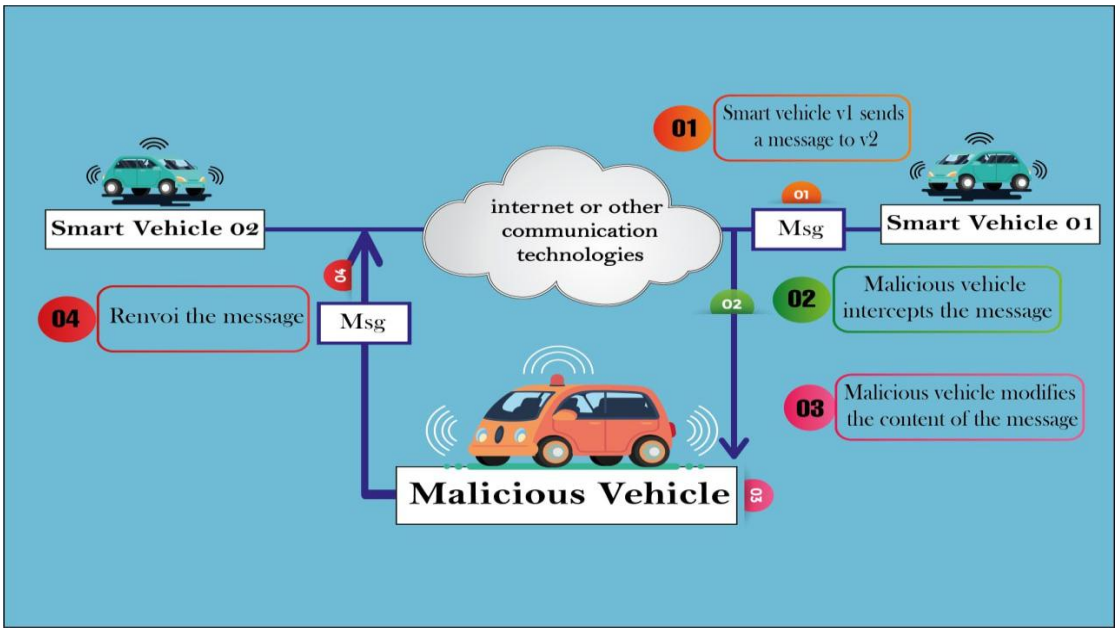

Figure 2. 10 Message Tampering Attack.

3.4.2. Black hole attack

In this type of attack, a malicious object collects and discards data packets without transmitting them to their intended destination creating a “Block Hole” in the network in which data is disappeared. Preventing data from reaching its desired destination can leads to services disruption affecting the overall performance and scalability of IoV network.

Several solutions can be used to reduce the risk of black hole. Abul et al proposed an efficient solution for preventing BHA in vehicular network by computing a dynamic threshold value that is used to identify malicious BHA and broadcasting a forged route request packet (RREQ) to confirming BHA [143]. Saptarshi et al used a trusty dynamic software agent (TDSA) and basic probabilistic approach for detecting BHA [144]. Jhon et al proposed an

approach to mitigate BHA through route backtracking and noticing discrepancies in statistics reported by intermediate nodes [145].

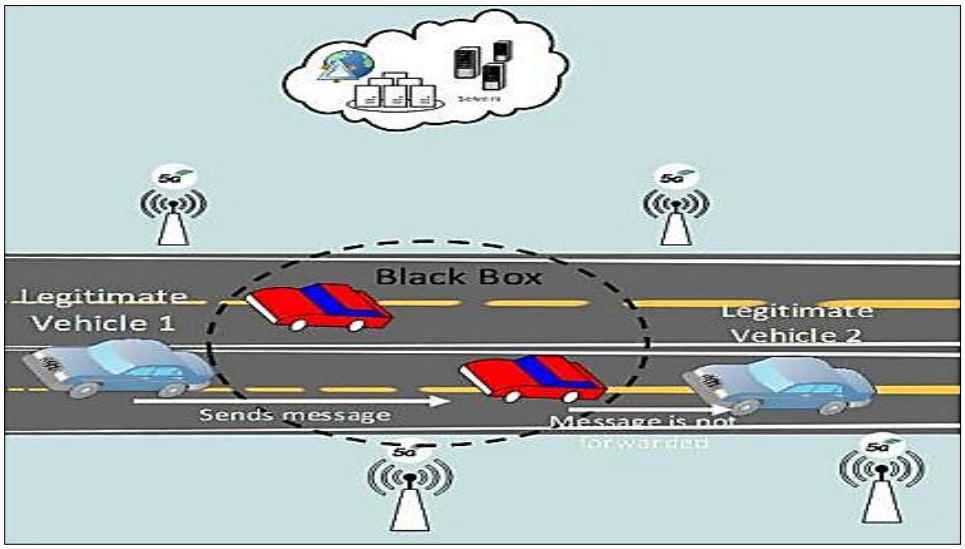

Figure 2. 11 Black Hole Attack [72].

3.4.3. Illusion attack

Illusion attack consists of generating false or useless information and place it in the IoV network. This can lead to misinformation, confusion, or disruption in the IoV ecosystem. This attack can make serious consequences including traffic congestion, malicious diversions, accidents.

Reducing the risk of illusion attacks necessitates a combination of security measures to ensure the integrity of data transmitted between objects. Implementing robust encryption mechanisms. Employing tamper proof hardware to avoiding the physical tampering. Regularly update firmware and software on infrastructures and vehicles. Naj et al proposed Plausibility validation network (PVN) [148]. Dhurandher et al proposed Reputation plausibility checks [149].

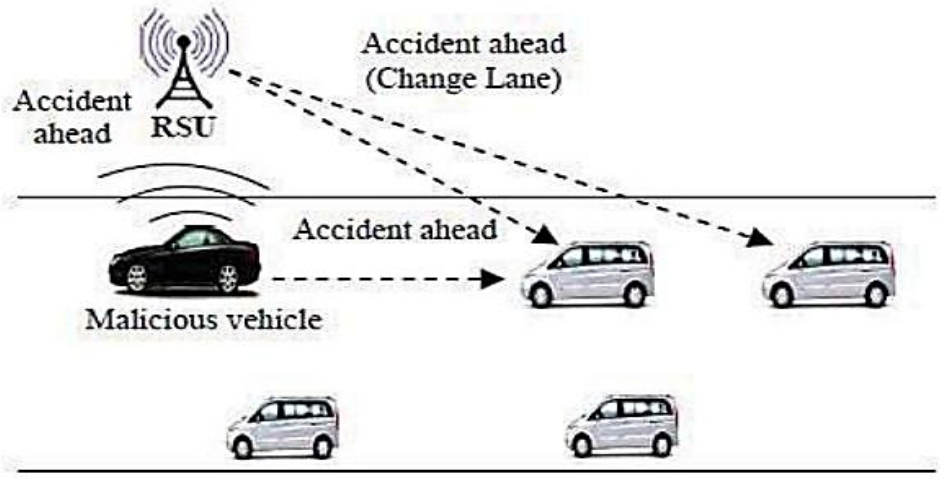

Figure 2. 12 Illusion Attack [73].

3.5. Availability attacks

3.5.1. Denial of services attack

The Denial of service attacker tries to overload the IoV network with a large amount of traffic in order to distribute the normal function of IoV objects and networks. DoS attack can create delays, chaos, congestion, and accidents.

It is important to implement strong security measures against DoS like deploying firewalls, traffic monitoring [150][151], robust authentication and authorization mechanism, rate limiting [152], load balancing [155], and regular security audits and penetration testing. Robust authentication and authorization mechanisms for guarantee that only authenticated and authorized objects can access the IoV network, this can minimize the risk of DoS attack. Load balancing for distributing incoming network traffic across multiple servers to prevent a single point of failure. Rate limiting; defining the maximum number of messages and requests that an object can send to the IoV network. Zoleikha et al proposed a real-time scheme for diagnostics of DoS attack. This scheme consists of a group of observers designed via sliding mode theory and adaptive observer theory [153]. Amandeep et al provided an effective solution to mitigating DoS attack by combining statistical logistic model and machine learning method [154]. Munazza et al proposed an efficient solution for detecting and preventing DoS attack by verifying the number of packets injected into the network and the average time of a communication session between objects [155]. Mahmoud et al provided an efficient scheme to prevent DoS by using a modular square root-based [156].

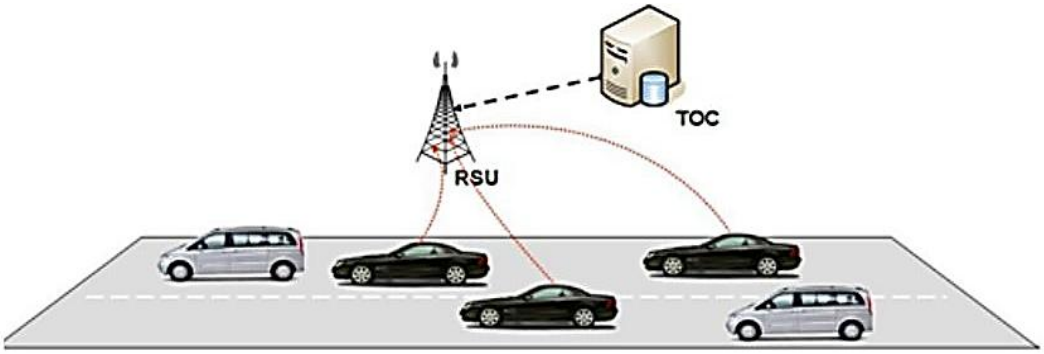

Figure 2. 13 Denial of Services Attack [73].

3.6. Privacy attacks

3.6.1. Profile inference attack

A malicious object analyzes data produced by vehicles and their interactions with the IoV network in order to inferring sensitive information. This inference can be used for various reasons including surveillance, identity theft, sabotage, blackmail, and financial gain.

To protect IoV systems against profile inference attack, it is essential to implement robust security measures like multi factor authentication (MFA) [79], anonymization, pseudonymization [75], biometric authentication [157], certificates, notifications and hardware token. MFA provides an additional layer of security against this attack by requiring vehicles to provide two forms of authentications before being able to access to the IoV system. Notifications; vehicles can get notifications to complete the authentication process. Anonymizaion; data should be anonymized to make it difficult for a malicious vehicle to associate it with particular vehicles or objects. Data minimization; saving the unnecessary data or the too detailed data might lead to the inference of sensitive information, so it is important to gathering and saving only the necessary data.

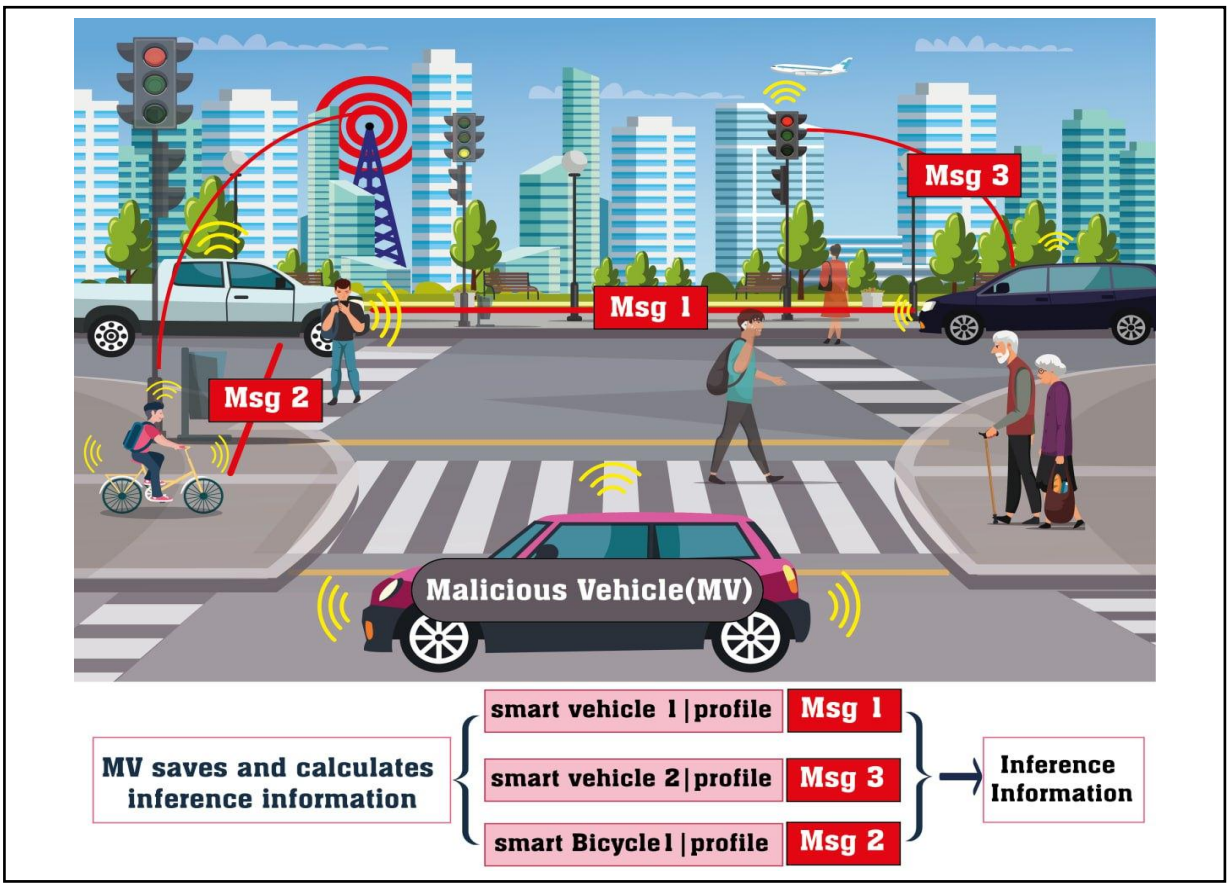

Figure 2. 14 Profile Inference Attack.

The following table represents the most serious vehicular network attacks and the corresponding countermeasures.

Table 2. 2 Most serious vehicular networks attacks and countermeasures

Attack	Category	Type of attack	Impact on IoV	Countermeasures	Papers
Sybil Attack	Attack against authentication	Active and insider	Medium	- Digital Signature combined with anonymous certificates. - Authentication with privacy preserving based on distributed aggregate. - Group signature. - Identity based cryptography. - Tamper-proof device. - Aggregate signature based on one-time identity. - Mutual authentication based on payload. - Distrusted and localized approach.	[37] [38] [39] [22] [21] [40] [42] [53]
Man in the Middle Attack	Attack against authentication	Active, Insider and monitoring	High	- Mutual authentication. - Password. - Biometric update. - Time synchronization - Blockchain. - Bloom filter based on SDN (Software Defines Network). - Symmetric polynomials and keys are generated in mobile router and relay router.	[44] [21,122] [29] [30] [121] [46] [47]

Impersonation Attack	Attack against authentication	Active, insider, malicious	Medium	-Linear search algorithm and binary search algorithm. - Keys based on shared secret m_i - Password and hush functions applied on the secret key. -Bloom filter and the binary search techniques.	[48] [52] [51][62] [24]
Replay Attack	Attack against authentication	Active	High	- Robust reset speed synchronization control - The use of Timestamp. - Random numbers. [29] - Verifying the received data in correlation with the data received.	[54] [55] [47][29] [56]
Eavesdropping Attack	Attack against confidentiality	Passive	Medium	- Session keys. - ID-based encryption - One time identity based group key. - Group signature. - CP-ABE.	[58] [129] [130] [131] [132]
Traffic Analysis Attack	Attack against confidentiality	Passive	Medium	- Dummy traffic delivery. -Traffic padding. - Session keys.	[134] [135] [49]
Traceability Attack	Attack against non repudiation	Passive	Medium	- Digital signature. - Intrusion detection system. - Timestamp. - Blockchain.	[137] [138] [139] [138,139, 140]
Message Tampering Attack	Attack against Integrity	Active	High	-TangleCV. - Signatures. - Group of signatures.	[142] [146] [147]
Black Hole Attack	Attack against Integrity	Active	High	-Trusty dynamic software agent and basic probabilistic. -Nodes reports. -Dynamic threshold value and RREQ.	[144] [145] [143]
Illusion Attack	Attack against Integrity	Malicious, insider	High	- Plausibility validation network (PVN). - Reputation plausibility checks.	[148] [149]
Denial of Services Attack	Attack against availability	Active, insider, malicious	High	- Statistical logistic model and Machine learning techniques. - Bloom-filter-based IP-CHOCK detection. - Real-time detection of denial-of-service attacks - Traffic monitoring. - Rate limiting. - Load balancing.	[154] [76] [77] [150][151] [152] [155]
Profile Inference Attack	Attack against privacy	Passive	Medium	- MFA. - Anonymization and pseudonyzation. - Biometric authentication.	[79] [75] [157]

4. Related works

Many researchers have developed various security schemes for ensuring secure data transmission in vehicular network. In this section, we present related work of security network schemes. Each scheme has a communication mode, cryptographic technics, and its level of security and performance.

Recently IoV has gained significant attention in research aiming to enhance trust and security within vehicular communication networks. However, a unified authentication and confidentiality protocol has not been designed yet.

Shao et al [39], developed a threshold anonymous authentication and confidentiality protocol for vehicular network in a decentralized group model. This protocol achieves an efficient anonymity, revocation, and traceability by the use of a group signatures and AES algorithm for the symmetric encryption. Nevertheless, the protocol consumes a high communication cost and does not support batch verification.

Na Ruan et al [58] proposed a parallel broadcast authentication protocol (PBAP) for IoV. The protocol is inherited from multi-level μTesla. PBAP improves network security and energy conservation for a direct communication between vehicles and wireless sensor networks. Nerveless, PBAP is not immune to distributed denial of services attacks.

Lui et al [59], developed a privacy-preserving authentication scheme (PPDAS) based on trusted computing and bilinear pairing. This scheme provides a secure communication between vehicles. It used two steps for improving the legitimacy of vehicles; vehicle identity verification followed by reputation evaluating. The confidentiality is ensured with the symmetric encryption. The correctness of PPDAS is demonstrated using BAN logic. However, PPDAS is vulnerable to insider attacks, and consumes a high communication cost.

In [60] Jiang et al proposed a two factor authentication protocol for IoV. This protocol used password and physical unclonable function (PUF) to prevent an unauthorized access to user's device and to provide anonymity, untraceability, and desynchronization resilience. However, Jiang et al protocol's supports just two kinds of communication V2V and V2RSU. In addition, it does not support key updates.

Kain Fan et al [61] proposed a mutual authentication for IoV by using a modular exponential technique and hash functions. This protocol enables people to traveling efficiently and smartly. Kain Fan et al used tag anonymous to protect data and to prevent malicious users to tracking legal users. Kain Fan et al used BAN logic to indicate that the protocol is logically secured. However, the confidentiality is not considered in this protocol.

Ying et al in [62] proposed an anonymous authentication protocol for secure vehicular networks (ASC) in which vehicles identities' are generated by smart card. These identities are changed

dynamically in order to avoiding malicious user to target legal vehicles. Ying et al compared ASC protocol with other protocols [65][66][67] and showed that ASC can satisfy anonymity and unlinkability and can resist to impersonation attack, smart card loss, offline password guessing attack, and RSU compromised attack. However Chien et al [63] demonstrated that ASC protocol is vulnerable to offline identity guessing attacks and takes a long time for computing. To solve these problems, Chien et al proposed a secure authentication protocol by optimizing the steps of authentication process that reduced the time cost of computing compared to ASC. Chien et al proved that their protocol is more secure than the original protocol and resists against various attacks such as replay attack. Nerveless other attacks like man in the middle and DDoS remain unaddressed.

Alshusukhi et al [64] proposed an authentication protocol for vehicular networks based on ECC. One of the main concepts of this protocol is that the initial public parameters of the system are preloaded in each TPD of RSU instead of TPD of OBU in order to achieve privacy preserving and security properties. However, this protocol employs a large number of ECC operations that leads to high computational costs.

Table 2. 3 Related work for IoV security network.

Schema	Network model	Goals	Methods and tools used	Performances (+) and limitations (-)
Shao et al [39]	Consists of Vehicles, RSUs, Tracing Manager (TM), and Central Authority (CA).	Creating an effective threshold anonymous authentication mechanism for vehicular network.	*Group Signature scheme. *Bilinear paring. *Decisional Diffie Helman.	+An Anonymous authentication. -High communication cost. -Infectiveness.
Na et al [58]	Consists of Vehicles, Sensor Nodes (SN), Cluster Head Node, RSU, Internet servers	Improving network security and energy conservation in WSN/IoV communications.	*Inherited from uTesla.	+Improves energy conservation. -Vulnerable to DoS attack.
Lui et al [59]	Comprises of TA , fixed RSUs, and vehicles equipped with OBU and TPM.	Enhancing the security and the privacy for V2V communication.	*Bilinear paring. *CBC-HMAC AES. *One way hash function SAH-1. *Omnet ++. *BAN logic.	+Offers a dual authentication between vehicles. + Improves privacy protection. - Increases traffic delay. -Vulnerable to insider attacks. -Does not offer untracebelity.
Jiang et al [60]	Comprises of Data Center (DC), User (U_i), and Vehicle Senser (VS_u).	Ensuring two factor security; untraceability and anonymity.	*Physical unclonable function (PUF). *Password. *Authentication and key agreement.	+Supports untraceability. +Ensures anonymity. -Does not apply key updates.

Kai Fan et al [61]	Consists of Vehicles, RFID tags, readers, and semi-reliable cloud.	Ensuring an efficient authentication scheme for IoV.	*Modular exponential. *Hash functions. *Flag. *BAN logic.	+Secure against Dos attacks. +Computing cost is reduced. +Avoiding malicious tracking from external attackers. -Confidentiality is not considered.
Ying et al [62]	Consists of TA, RSU, and Vehicles.	Creating an anonymous and lightweight authentication protocol for vehicular networks.	*Smart card. *VanetMobiSim. *OPNET.	+Satisfied the unlinkability. - Vulnerable to offline identity guessing attacks, replay attack, stolen smart card, and location spoofing attacks.
Chien et al [63]	Consists of TA, RSU, and Vehicles.	Solving ASC problems to having an optimized and a secure authentication protocol for vehicular network.	*Hash functions. *Modular exponentiation.	+More secure compared to ASC. +Secured against replay attack. - Vulnerable to man in the middle and DDoS attacks. - High computation cost. -Man in the middle attack and DDoS attacks remain unaddressed.
Alshudukhi et al [64]	Consists of Trusted Authority,RSUs, and Vehicles.	Achieving authentication with conditional privacy preserving scheme.	*ECC *Hash functions. *Miracl cryptographic library.	+Resistance to man in the middle and replay attacks. -High computational costs.

IoV uses several cryptographic methods to ensure that vehicles communicate securely. One common approach is the **password based method**, which relies on user-generated passwords. This method is simple, easy to deploy, and cost-effective; however, it suffers from weak security, is vulnerable to theft, and lacks scalability, making it unsuitable for large-scale IoV networks. Another approach is the **biometric method**, which authenticates users based on their unique physiological or behavioral traits, such as fingerprints or facial recognition. While this method offers higher security and greater convenience for drivers, it involves relatively high implementation costs and requires strong protection for stored biometric data. Consequently, despite its advantages, it is also not ideal for large IoV networks. **Symmetric encryption techniques**, such as AES (Advanced Encryption Standard), ensure fast processing and low computational overhead through shared keys but face significant challenges related to key distribution and scalability. In large IoV networks, each vehicle would be required to manage an enormous number of secret keys, making real-time operation infeasible. **Asymmetric encryption methods**, like RSA (Rivest–Shamir–Adleman), provide improved scalability and enhanced security through public/private key mechanisms but impose substantial computational overhead, which is unsuitable for resource-constrained and latency-sensitive vehicular systems. **Blockchain** is a decentralized and tamper-proof digital ledger that records and verifies transactions across a distributed network. It ensures transparency and traceability but introduces high processing, storage, and latency issues. In contrast, **Elliptic Curve Cryptography (ECC)** offers strong security with short keys, low computational overhead, and fast authentication, making it the most efficient and suitable cryptographic solution for dynamic IoV environments

5. Conclusion

SC offers many benefits making citizen's life smarter. Objects in SC share and disseminate information between them, this information need to be protected from malicious devices. A security failure can make disasters in smart cities in terms of economical loses and human life lost.

In the next chapter, we present our contribution to enhancing both authentication and confidentiality in the IoV. Our contribution introduces a comprehensive security IoV framework designed to ensure that only valid and authorized vehicles can communicate within the IoV system. Additionally, our approach incorporates advanced encryption technique using ECC to protect sensitive data from being tampered.

Part II

Chapter Three: Security proposal schemes

Chapter Four: Evaluation and results

Chapter Three: Security proposal schemes

1. Introduction

In this chapter, we describe our security proposal schemes including authentication, and confidentiality schemes. First, we present the different basic knowledge and notions related to cryptographic techniques that we studied to curry out this work. Then, we present our proposal network model; we define the network elements followed by their functions and services. After that, we provide the detailed explanation of our proposed security schemes with the different phases.

2. Preliminaries

In this section, we introduce the basic notions concerning the cryptography methods used in our protocol including definition, function, and basic operations.

2.1 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) was first proposed by Miller [123] and Kolbitz [124]. It is a kind of public key cryptosystem based on the algebraic structure of elliptic curves over finite fields [128]. Elliptic curves can be defined by the equation:

$$\boldsymbol{y^2 = x^3 + ax + b \ (mod\ p)} \quad \textbf{3-1}$$

where $\boldsymbol{a, b, x, y \in F_p}$ and

$$\boldsymbol{4a^3 + 27\, b^2 \ (mod\ p) \neq 0} \quad \textbf{3-2}$$

In which:

- $\boldsymbol{F_p}$ is a finite field and $\boldsymbol{p}$ is a prime number that indicates the order of F_p.
- The variables x and y represent points on the curve.
- a and b are constants that define the specific shape of the elliptic curve.

To ensure that the curve is non singular, the curve must satisfy the condition presented in the equation 3-2. This condition makes the curve smooth and suitable for cryptographic applications.

The following figure presents an example of elliptic curve for two equations:

$$\boldsymbol{y^2 = x^3 - 4x + 1} \quad \textbf{3-3}$$

$$\boldsymbol{y^2 = x^3 - 5x + 5} \quad \textbf{3-4}$$

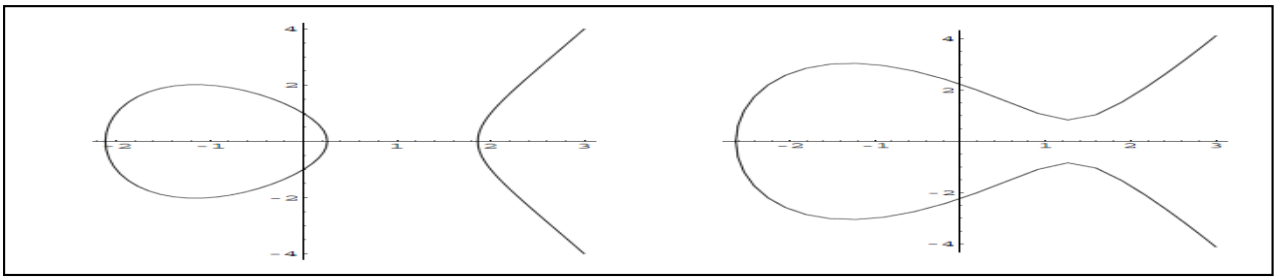

Figure 3. 1 Graphs of elliptic curves y2 = x3 - 4x+1 (on the left) and y2 = x3 - 5x + 5 (on the right) over R [126].

In the paper [125], Omondi described the essentials arithmetic operations used in elliptic-curve cryptography; point addition, point doubling, and scalar point multiplication.

- **Point addition**

The addition of two points A and B on an elliptic curve over $\boldsymbol{F_p}$ is achieved by drawing a line through A and B, the line will intersect the elliptic curve at exactly one point D', reflecting D' across the x-axis yields D which is the result of the addition A+B as presented in figure 3.2.

$$\boldsymbol{A + B = D} \qquad \textbf{3-5}$$

where A and B are distinct ($\boldsymbol{A \neq B \neq \emptyset}$).

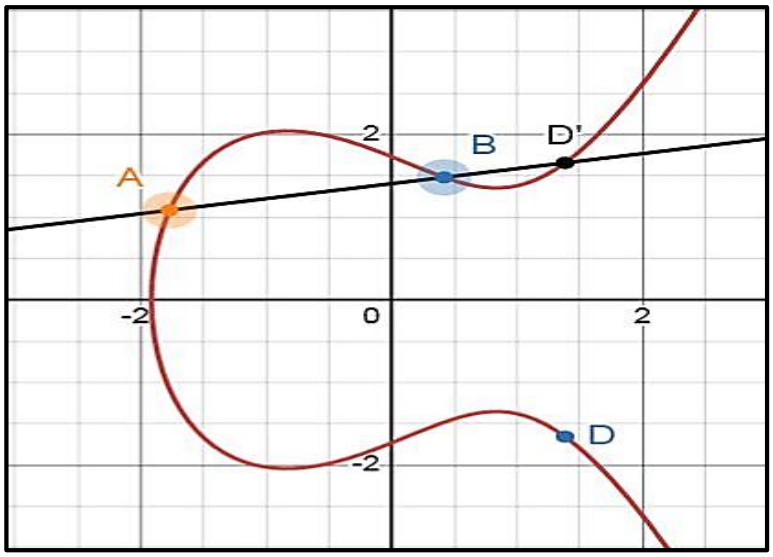

Figure 3. 2 Addition points.

- **Point doubling**

The point doubling is representing by the addition of a point with itself $\boldsymbol{2A = A + A}$. Point doubling can be visualized by drawing a tangent line at the point A which intersects the elliptic

curve at exactly one point D', reflecting this intersection point D' across the x-axis yields the doubled point D as illustrated in the following figure.

$$A + A = D \qquad 3\text{-}6$$

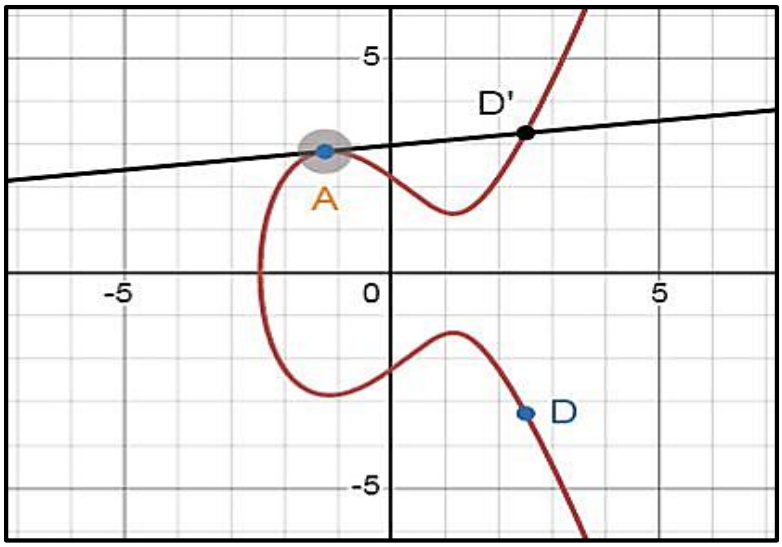

Figure 3. 3 Point doubling.

- **Point scalar Multiplication**

Point scalar multiplication is the process of multiplying a point **A** on an elliptic curve by a scalar value **K** where $K \in Z_p^*$, and **K>0** resulting a new point D**.** This process is achieved through a repeated addition of A to itself K times.

$$K.A = A + A + \cdots + A\ (K\ times) = \mathbf{D}. \qquad 3\text{-}7$$

Scalar multiplication is the core mathematical operation in ECC that makes it efficient and secure. It allows ECC to run effectively on objects with limited processing and storing capabilities.

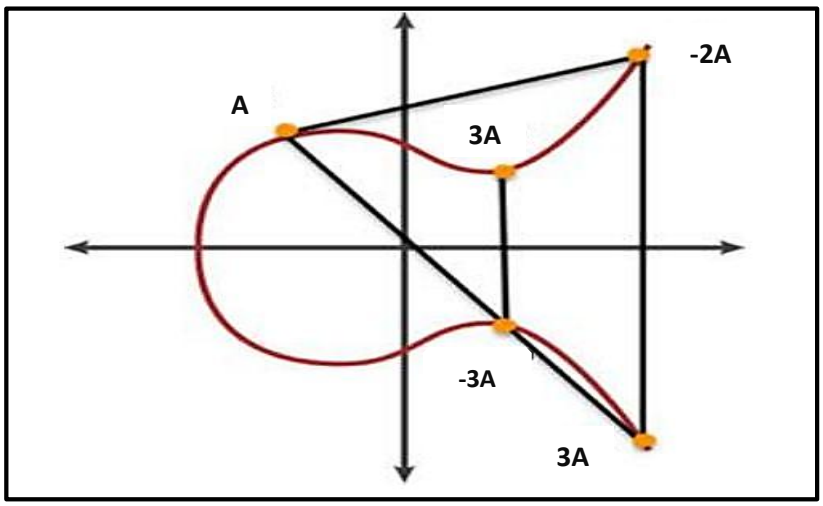

Figure 3. 4 Point scalar multiplication

Compared to previous cryptographic methods, ECC offers a high-level security by using the difficulty of solving certain mathematical problems related to elliptic curves. For example, A and B two points on the elliptic curve, where A = K.B, it is computationally hard to find the scalar K, even we have A and B, it is difficult to determine K. ECC utilizes smaller keys size, supports very fast key generation and fast encryption/decryption and uses less memory and CPU cycles compared to RSA. For example, 160 bit key in ECC is considered to be as secured as 1024 bit key in RSA [127]. Due to these advantages, ECC is well suited for wireless communications, like mobile phones and smart cards [128].

3. Security Proposal schemes

As vehicle increasingly rely on communication networks, the need for robust security framework becomes paramount to secure vehicles' identities and data confidentiality. Designing authentication and confidentiality schemes is a crucial for maintaining secure and reliable communication within the network. Authentication ensures that only legitimate vehicles can access the IoV system. Confidentiality protects sensitive data against eavesdropping and unauthorized decryption of data. By designing these schemes effectively, IoV system can achieve high level of security. Balancing security with system's performance needs, which is essential for the safe operation of connected vehicles. In this section, we present our proposal network model, authentication and Confidentiality schemes.

3.1 Network model for IoV

As shown in figure 3.5, our proposal network model has four principal entities including security cloud center, cloud data center, network center, and physical world. These entities collaborate with each other in order to provide a secure network communication. Table 3.1 summaries the network functions and services of each entity.

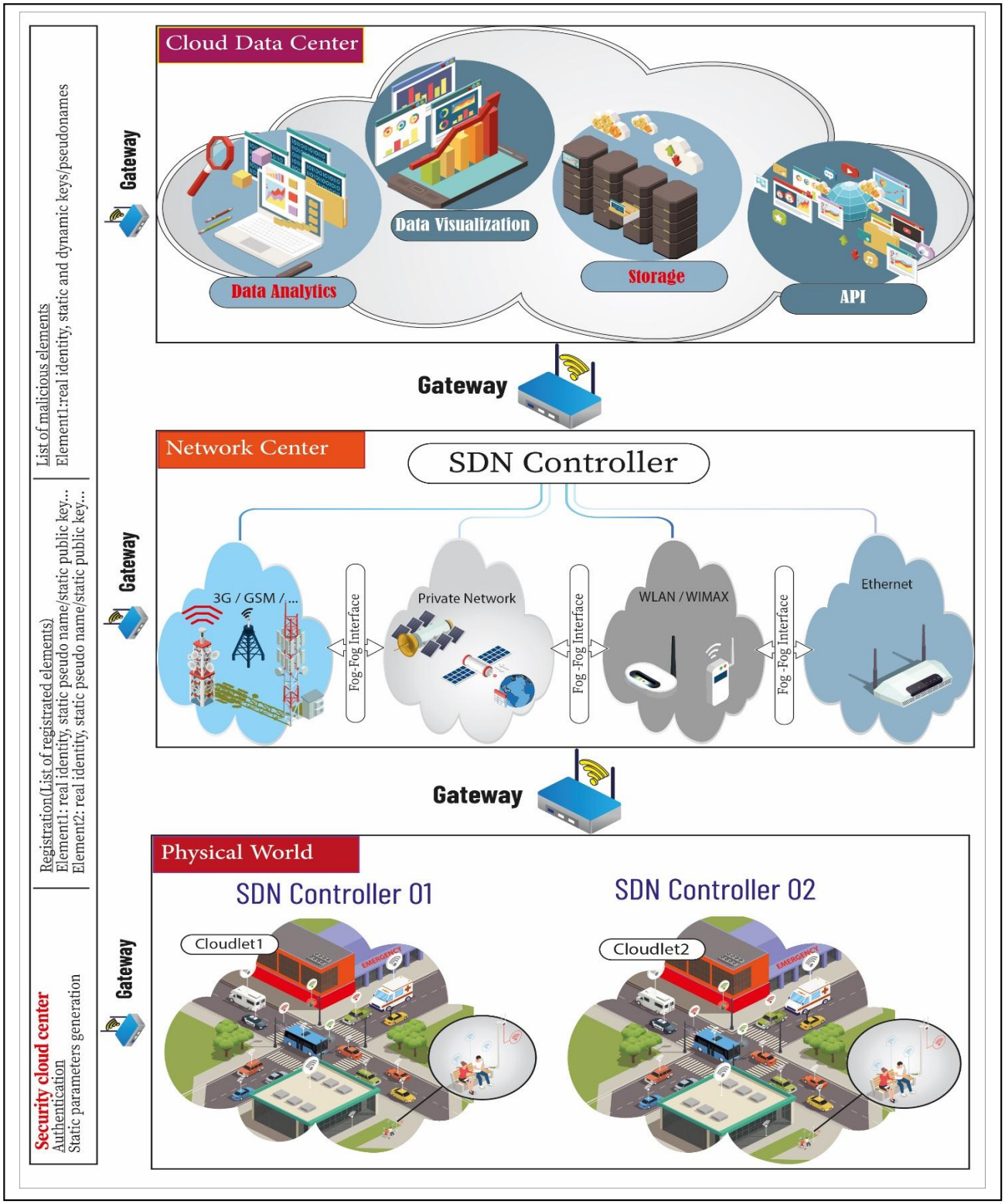

Figure 3. 5 The global architecture of IoV Network [173].

- **Cloud Data Center:**

The Cloud Data Center (CDC) is an efficient platform for smart vehicles. It offers smart applications, data analytics, storage, and computing services. It also defines strategies including graphs, flowcharts, tables, and diagrams designed to process complex data,

helping smart vehicles to make quick and intelligent decisions. Graphs facilitates real data monitoring and analysis, enabling fast detection of traffic patterns and trends. Tables store and classify data systematically, allowing quick retrieval and efficient processing of vehicular information. Flowcharts is an important tool for visualizing and understanding the complex process and decision making pathways involved in data processing. Diagrams enable smart vehicles to make better decisions by organizing data to clarify routes, identify conditions, and highlight potential hazards, thereby improving situational awareness and enhancing driving safety.

- **Security Cloud Center:**

The Security Cloud Center (SCC) is considered as a trusted cloud that has a high computation and storage capabilities. SCC has the responsibility of ensuring all security tasks of the whole system. SCC generates the static security parameters of the global system, attributes certificates, and collaborates with all cloudlets for detecting malicious objects and preventing them to communicate with other objects.

- **Network Center:**

Network center (NC) is the middleware between objects and CDC. NC is responsible for offering the access to virtual and real networks, ensuring the connectivity between objects using various technologies like GSM, WiMax, WLAN, 5G, and Wi-Fi. It provides seamless communication across smart objects, maintains traffic prioritising, manages, and controls dynamic network topology changes caused by vehicle movement. NC also reduces the functionality destined to CDC by analyzing, filtering, processing, and storing data received from objects and then determining the best network to transfer data using SDN. SDN manages how data is directed, routed, and prioritized as it travels across the network, offering a quick data forwarding by choosing the optimal path and adapting to the dynamic topology created by vehicle movement. SND ensures that the network continue working even in emergency situations.

- **Physical world:**

The physical world (PhyW) consists of several objects including smart sensors, smart actuators, smart phones, smart watches, smart chips, smart vehicles, smart trucks, smart bicycles, smart ambulances, and smart garbage cars. The main objective of these objects is to collecting data including weather conditions, traffic Jams, localization and data environment with the help of various technologies like GPS (Global Positioning System),

WSN (Wireless Sensor Network), RFID (Radio-Frequency Identification) and RFID sensor Network, this Data will be transferred to NC through the gateway.

All objects are clustered in groups of ***Cloudlet***. These clusters have a wide range of coverage and are used to offer security services and to quickly provide Cloud computing services; data storage, data processing and connectivity to mobile devices within close geographical proximity with low latency. All objects must join the cluster to get authenticated and to have the security parameters enabling it to communicate with all objects situated in the same cluster.

The cloudlet's objects are controlled with SDN controller. We consider a multiple of SDN controllers in our proposal model to achieve the availability of the system; in case of SDN controller is damaged or compromised, another SDN controller can take its place. Each SDN controller is responsible for forwarding, managing, and controlling data transmitted in its domain.

Cloudlet analyzes vast amounts of data collected from various resources in order to inform smart vehicles about touristic information, construction zones, local events, road, traffic, and weather conditions. It can offer intelligent services like parking payment; facilitating automatic payment without physical tickets or cash.

Table 3. 1 IoV network tasks and services

Elements	**Network tasks**	**Features offered to the network**
CDC	-Provides smart applications, statistics, decisions, storage and processing services.	Scalability - Availability - Reliability
SCC	-Occupied for all security tasks.	Security functions (Authentication, Authorization, and Confidentiality)
NC	-Considered as an access point. -Provides Network Connectivity. -Interacts with physical world. -Determines the best network to transfer data. -Makes fast decisions.	Connectivity - Flexibility - Availability - Scalability - Efficient

	-Forwards and controls messages using SDN network. -Reduces the functionality destined to CDC by analyzing, filtering, processing and storing data.		
PhyW	**SDN**	-Manages and controllers all objects that belong to its scope. -Provides a secure data Routing.	Flexibility - Management - Reliability - Scalability
	Cloudlet	-Quickly provides Cloud Computing services. -Offers security services by generating the permanent secret parameters.	Availability Security functions (Validation, Authentication, and Confidentiality)
	Vehicles	-Collect information from the environment devices. -Communicate with different objects.	Connectivity

3.2 Authentication Proposal schemes

Authentication schemes are essential for verifying the identities of communicating entities, ensuring that only legitimate objects can participate in the network. In this section, we present our authentication proposal schemes. We have two schemes; the first one is for authentication between objects situated in different domains, and the second scheme is for authentication between objects in the same domain. We consider that SCC and Cloudlet as Trusted Units in which SCC plays the role of the administrator and the manager of IoV networks and Cloudlet is the mobile Cloud that offers security parameters to devices belong to its domain. Table 3.2 illustrates the security functions and services of each element in the network.

Table 3. 2 Secure IoV network services

Elements	Security Functions	Security Services
Security Cloud Center (SCC)	-Generates the static secret parameters of the global system. -Registers all network elements with their real identities.(element, real identity, Static pseudo identity, public key) -Collaborates with Cloudlet in order to revoke malicious vehicles. -Reveals the real identities of malicious element.	Authentication Authorization Confidentiality
Cloudlet	-Generates the secret Cloudlet parameters. -Attributes dynamic secret parameters of the Cloudlet domain. -Registers all Cloudlet elements with their pseudo identities (pseudo names, public keys…). -Collaborates with SCC to detect malicious vehicles in case of misbehaviour.	Authentication Validation Confidentiality
Vehicle	-Has a Tamper Proof Device (TPD), used to store the vehicle's private data and provides the cryptographic processing capabilities. -Uses dynamic identity to communicate with other objects situated in the same Cloudlet. -Uses static identity to communicate with other objects situated in heterogeneous domains. -Collaborates with Cloudlet to get authenticated and to update the list of revoked vehicles.	Authentication Confidentiality

All network entities must register in SCC that generates the secret static parameters of the system. SCC maintains a list of registered elements including Cloudlet, RSU, vehicles, bicycles, and trucks and has the responsibility for revealing the real identities of malicious elements. Figure 3.6 illustrates how an element is registered in SCC.

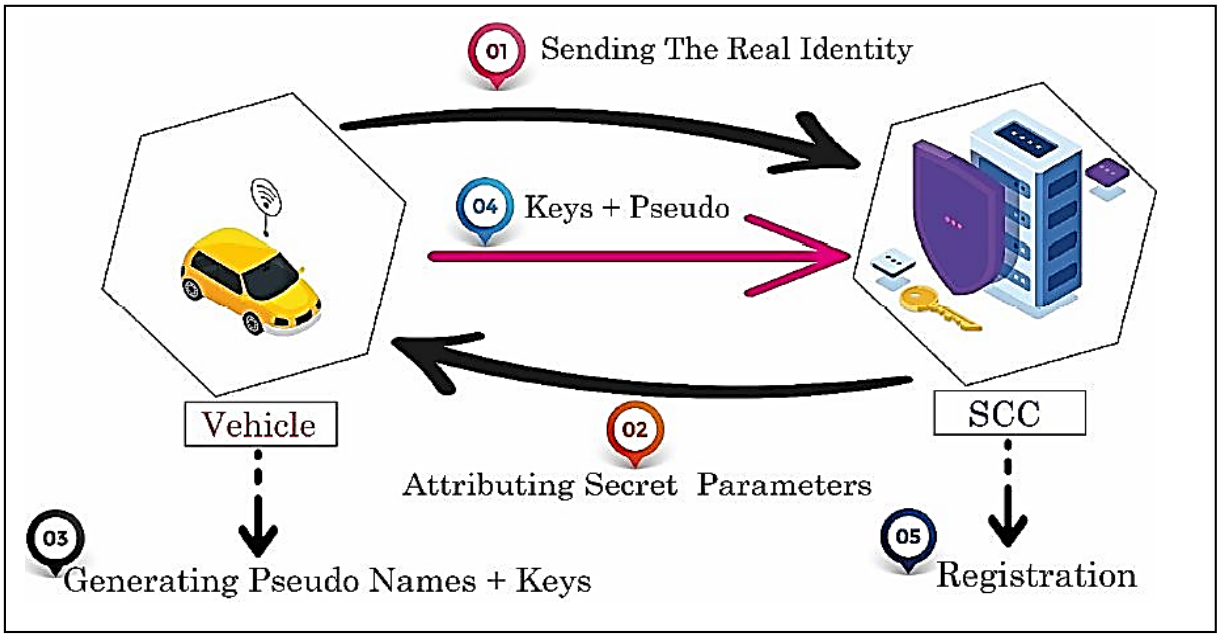

Figure 3. 6 Registration to SCC [173].

Each Cloudlet manages all vehicles that belong to its scope by generating the secret Cloudlet parameters and providing a real time registration. These parameters are then used by vehicle to generate dynamic keys and dynamic pseudo name enabling it to communicate with other devices that situated in the same Cloudlet as shown in figure 3.7.

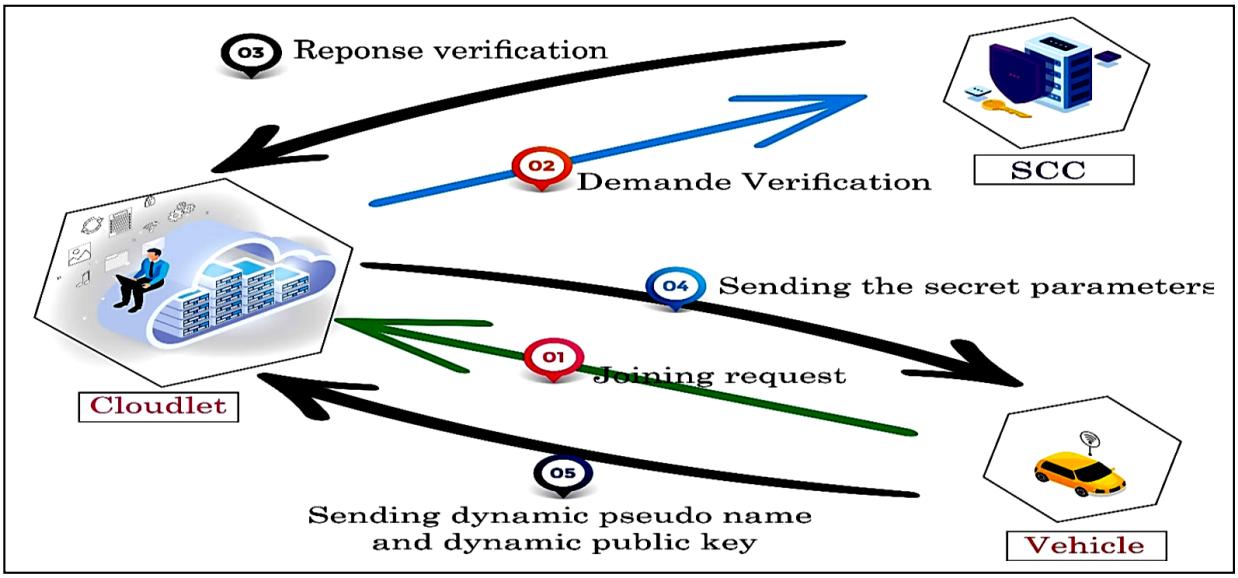

Figure 3. 7 Mutual authentication between vehicles and Cloudlet [173].

In order to ensure the availability of the system, SCC can create a virtual Cloudlet in case of one of Cloudlet is compromised or damaged. That increases the network security and system performance.

When a vehicle $\boldsymbol{V_1}$ want to communicate for the first time with other object (for example vehicle $\boldsymbol{V_2}$), it must join the cluster "**Cloudlet**" by sending an encrypted message with vehicle's

static keys. Then Cloudlet authenticates the vehicle V_1 after verifying the legitimacy of the vehicle with the help of SCC and then sends the secret parameters to the vehicle V_1. V_1 uses these parameters to generate the dynamic Keys and the pseudo name. Finally, V_1 can communicate with V_2 after the mutual authentication process between V_1 and V_2 as shown in the following figure.

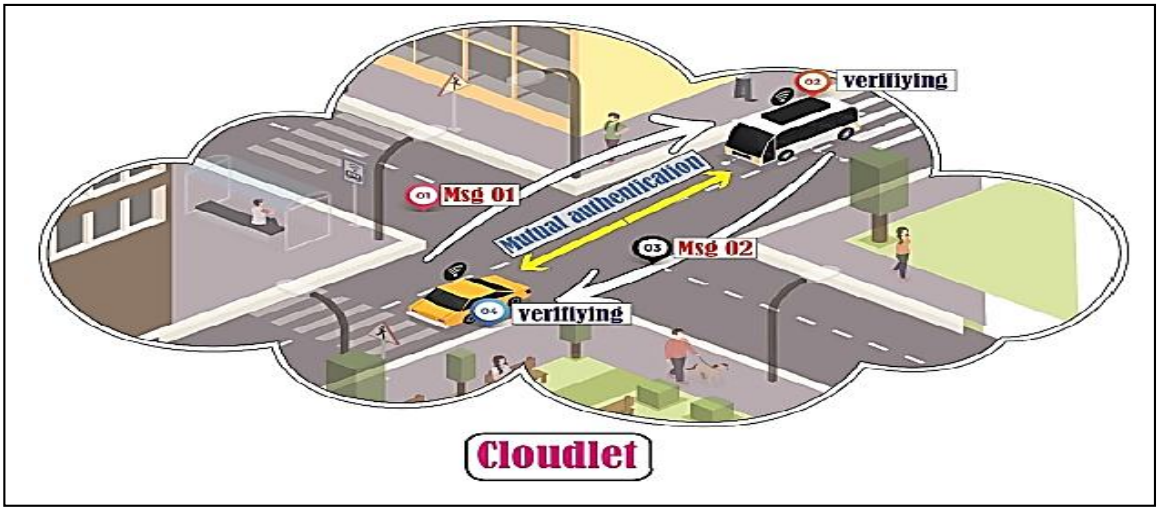

Figure 3. 8 Mutual authentication between vehicles in the same domain [173].

We have two modes of communication. The first is for heterogeneous communication using static keys and the second is for communication between objects in the same Cloudlet domain using dynamic keys. Our Authentication protocol has four stages of operations as follows:

3.2.1 Registration in SCC:

The following process is executed by all devices before any communication and in offline mode. As presented in figure 3.9 the registration process contains two phases: System setup and pseudo identity generation.

a) System setups

SCC establishes the initial parameters of the system using these steps:

1. Selecting an elliptic curve **E (a,b)** defined by the equation 3-1.
2. Selecting the cyclic addition group **G**, where **P** is the generator of the group and **Q** is the order of the group.
3. Selecting a random number $SK \in Z_p^*$ as a secret key then calculate

$$PK = SK \,.\, P \quad \textbf{3-8}$$

4. Selecting a secure hash functions H_i
5. Publishing the public parameters to all elements $\{E(a,b), p, P, PK, H_i\}$

b) Pseudo identity and Keys generation

TPD of each element selects a random number $SK_e \in Z_p^*$ and a current time CT_i then calculates: $PK_e = SK_e . P$ **3- 9**

and $PID_e = (RID_e \oplus H_1 (PK_e, SK_e))$ **3-10**

Each device broadcasts the (PID_e, PK_e) to all objects.

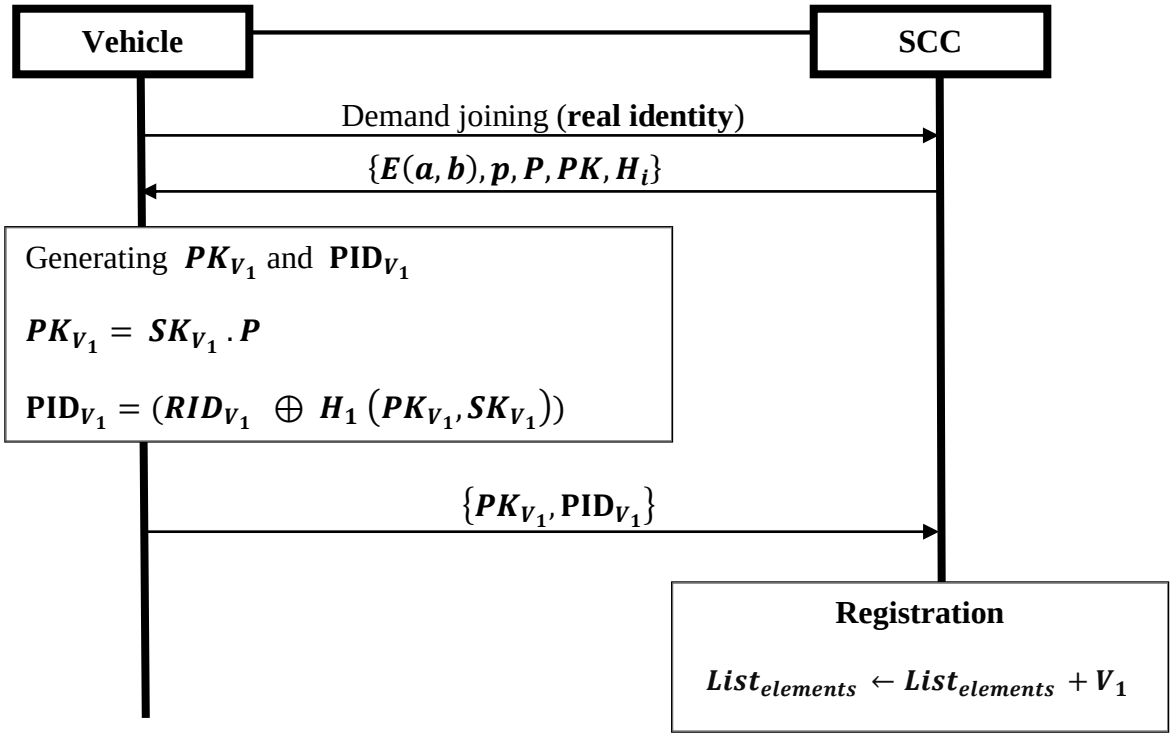

Figure 3. 9 Registration phase in SCC.

3.2.2 Mutual Authentication between heterogeneous elements:

This process is executed by heterogeneous elements such as Cloudlet to SCC, Cloudlet to Cloudlet, Cloudlet to SDN, SDN to SDN, Fog to Fog, Vehicle to Cloudlet for the first time, and vehicle to objects that belong to different domains. Heterogeneous elements mean that the elements are not situated in the same domain. The authentication process has two steps message signing and message verification as shown in figure 3.10.

a) Message signing

When an object for example V_1 wants to communicate with another object situated in other domain.V_1 executes the process below:

1. V_1 chooses a random number $U \in Z_p^*$.
2. V_1 computes $E_{V_1} = U . P$ **3-11**
3. V_1 calculates x and y where:

$$x = H_2\left(U.PK_{Cloudlet_i}, m_i, T_i\right) \quad \textbf{3-12}$$

and $$y = x.SK_{V_1} \quad \textbf{3-13}$$

4. V_1 sends $\{E_{V_1}, \mathbf{PK_{V_1}}, m_i, T_i, \mathbf{y}\}$ to Cloudlet.

b) Message verification

Upon receiving $\{E_{V_1}, \mathbf{PK_{V_1}}, m_i, T_i, \mathbf{y}\}$, Cloudlet checks the validity of V_1 by:

1. Cloudlet computes $E'_{V_1} = SK_{Cloudlet_i}.E_{V_1}$ **3- 14**

2. Cloudlet calculates x' and y' where:

$$x' = H_2\left(E'_{V_1}, m_i, T_i\right) \quad \textbf{3-15}$$

and $$y' = x'.PK_{V_1} \quad \textbf{3-16}$$

3. If $y' \neq y.P$ Cloudlet rejects the authentication message and contacts SCC to indicate that V_1 is a malicious vehicle. Otherwise, vehicle is a legitimate object and it can communicate with Cloudlet.

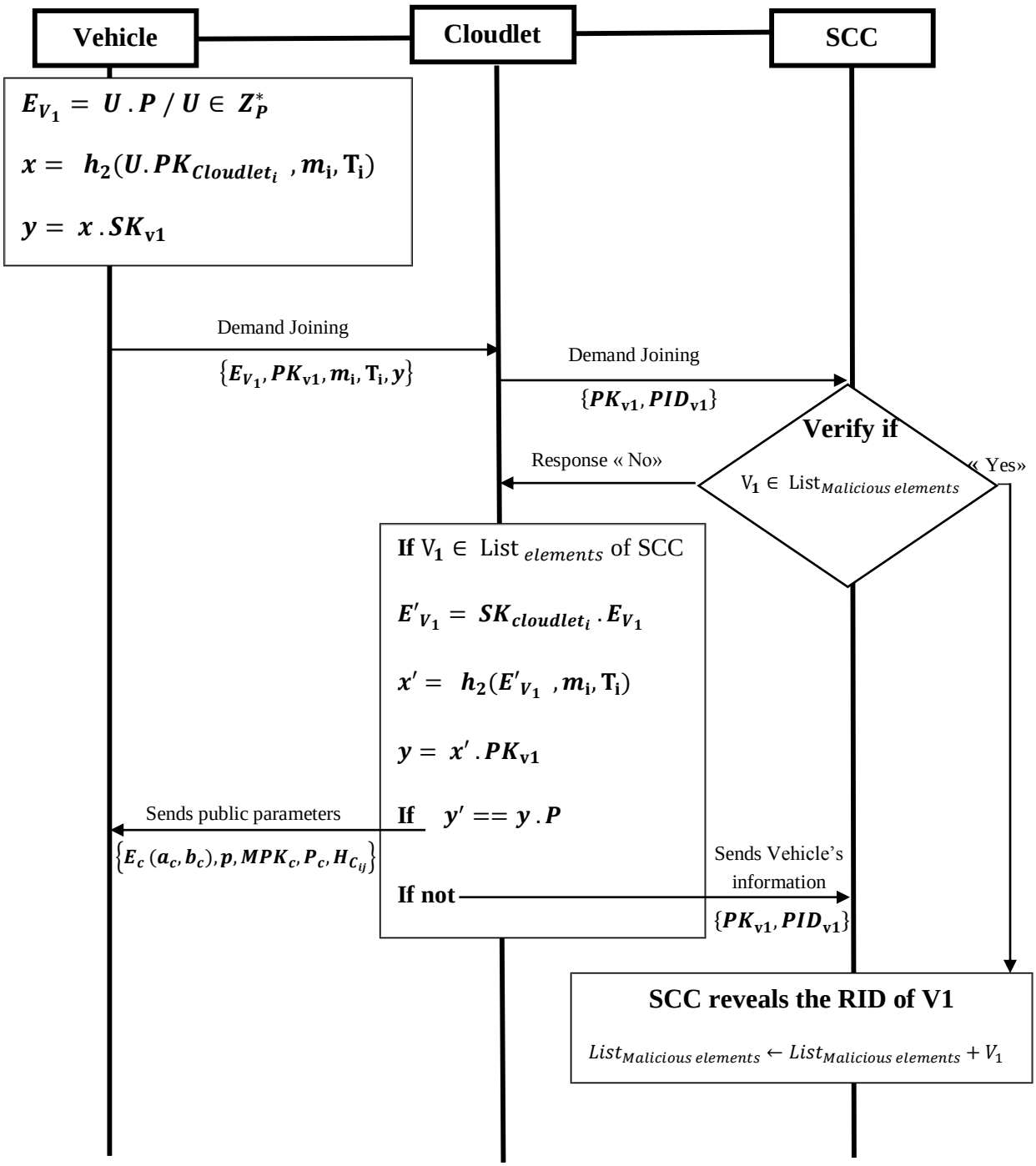

Figure 3. 10 Message flow in mutual authentication between heterogeneous elements.

3.2.3 Registration in Cloudlet domain:

First Cloudlet generates the initial parameters of its domain then it selects an elliptic curve $\mathbf{E_c\ (a_c,b_c)}$ defined by the equation $\mathbf{(y^2 = x^3 + a_c x + b_c)\ mod\ p}$ **3-17** , a secure hush functions $H_{c_{ij}}$ and chooses the cyclic addition group $\mathbf{G_c}$, when $\mathbf{P_c}$ is the generator of the group and $\mathbf{Q_c}$ is the order of the group. After that it selects a random master Key

$\mathbf{MSK}_{c_i} \in Z_q^*$ and calculates $\mathbf{MPK}_{c_i} = \mathbf{MSK}_{c_i} . \mathbf{P_c}$ **3-18**. Finally, Cloudlet publishes the public parameters $\{E_C(a_c, b_c), p, q, P_c, MPK_c, H_{c_{ij}}\}$ to all devices that belong to its domain. When a vehicle V_1 comes across a zone covered by Cloudlet, it must execute the previous process (Mutual Authentication between heterogeneous elements) as illustrated in figure 3.10 to get authenticated by Cloudlet and to be able to communicate with all devices situated in the same cloudlet. After Mutual authentication process, if V_1 is a malicious object, Cloudlet sends (PID_{V_1}, PK_{V_1}) to SCC that reveals the real identity of V_1 and $\mathbf{V_1} \in \mathbf{List}_{\text{malicious elements}}$. Otherwise, V_1 will be a member of this Cloudlet after executing the following steps to get the dynamic identity.

1. V_1 a selects random number $S_{CV_1} \in Z_q^*$ and calculates:

$CSK_{V_1} = SK_{V_1} . S_{CV_1}$ **3-19** as a vehicle's private key,

$CPK_{V_1} = CSK_{V_1} . P_c$ **3-20** as a vehicle's public key, and

$CID_{V_1} = h_{c_{11}} (RID_{V_1} , CSK_{V_1})$ **3-21** as a vehicle's dynamic identity.

2. V_1 sends (CID_{V_1}, CPK_{V_1}) to Cloudlet.

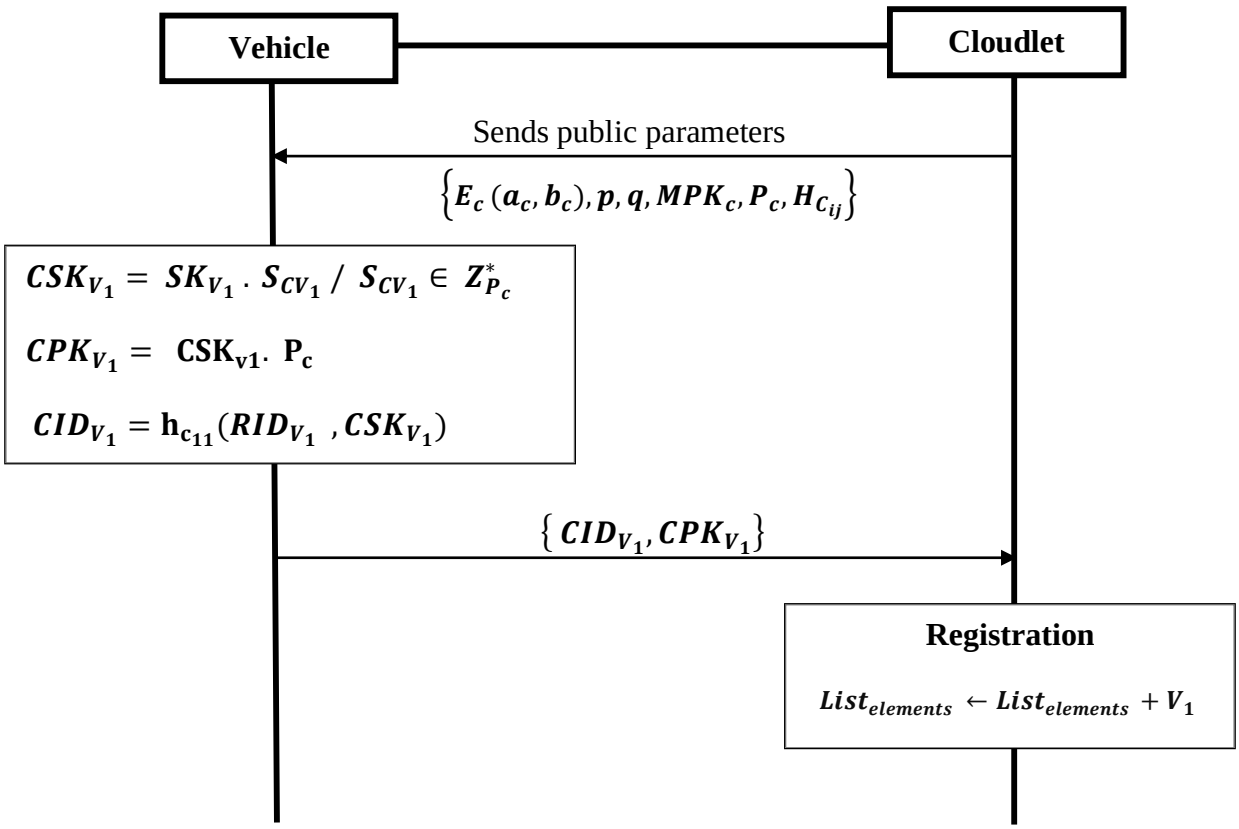

Figure 3. 11 Registration in Cloudlet domain.

3.2.4 Mutual Authentication between elements in the same domain (Cloudlet):

The following process enables two objects situated in the same domain to verify each other's identity before the exchange of data, ensuring that both objects in communication are legitimate participants in the network.

- When V_1 want to communicate with V_2, it sends an authentication message AM where

$$AM = \boldsymbol{CSK_{V_1}} . \boldsymbol{h_{c_{11}}}(\boldsymbol{CID_{V_1}}, \boldsymbol{CPK_{V_1}}, \boldsymbol{m_i}, \boldsymbol{CT_i}) \quad \textbf{3-22}$$

And $\{\boldsymbol{AM}, \boldsymbol{CID_{V_1}}, \boldsymbol{CPK_{V_1}}, \boldsymbol{m_i}, \boldsymbol{CT_i}\}$ to V_2.

- V_2 can check the validity of the message by calculating:

$$AM . \boldsymbol{P_c} = \boldsymbol{P_c} . \boldsymbol{CSK_{V_1}} . \boldsymbol{h_{c_{11}}}(\boldsymbol{CID_{V_1}}, \boldsymbol{CPK_{V_1}}, \boldsymbol{m_i}, \boldsymbol{CT_i}) \quad \textbf{3-23}$$

$$AM . \boldsymbol{P_c} = \boldsymbol{CPK_{V_1}} . \boldsymbol{h_{c_{11}}}(\boldsymbol{CID_{V_1}}, \boldsymbol{CPK_{V_1}}, \boldsymbol{m_i}, \boldsymbol{CT_i}) \quad \textbf{3-24}$$

$$AM' = \boldsymbol{CPK_{V_1}} . \boldsymbol{h_{c_{11}}}(\boldsymbol{CID_{V_1}}, \boldsymbol{CPK_{V_1}}, \boldsymbol{m_i}, \boldsymbol{CT_i}) \quad \textbf{3-25}$$

- V_2 compares this result $(AM . P)$ with AM'.

If $\boldsymbol{AM' = AM . P_c}$ V_1 is a legal element and the communication between V_1 and V_2 starts. Otherwise $\mathbf{V_2}$ informs Cloudlet that $\mathbf{V_1}$ is a malicious vehicle by sending $\{\boldsymbol{CID_{V_1}}, \boldsymbol{CPK_{V_1}}\}$.

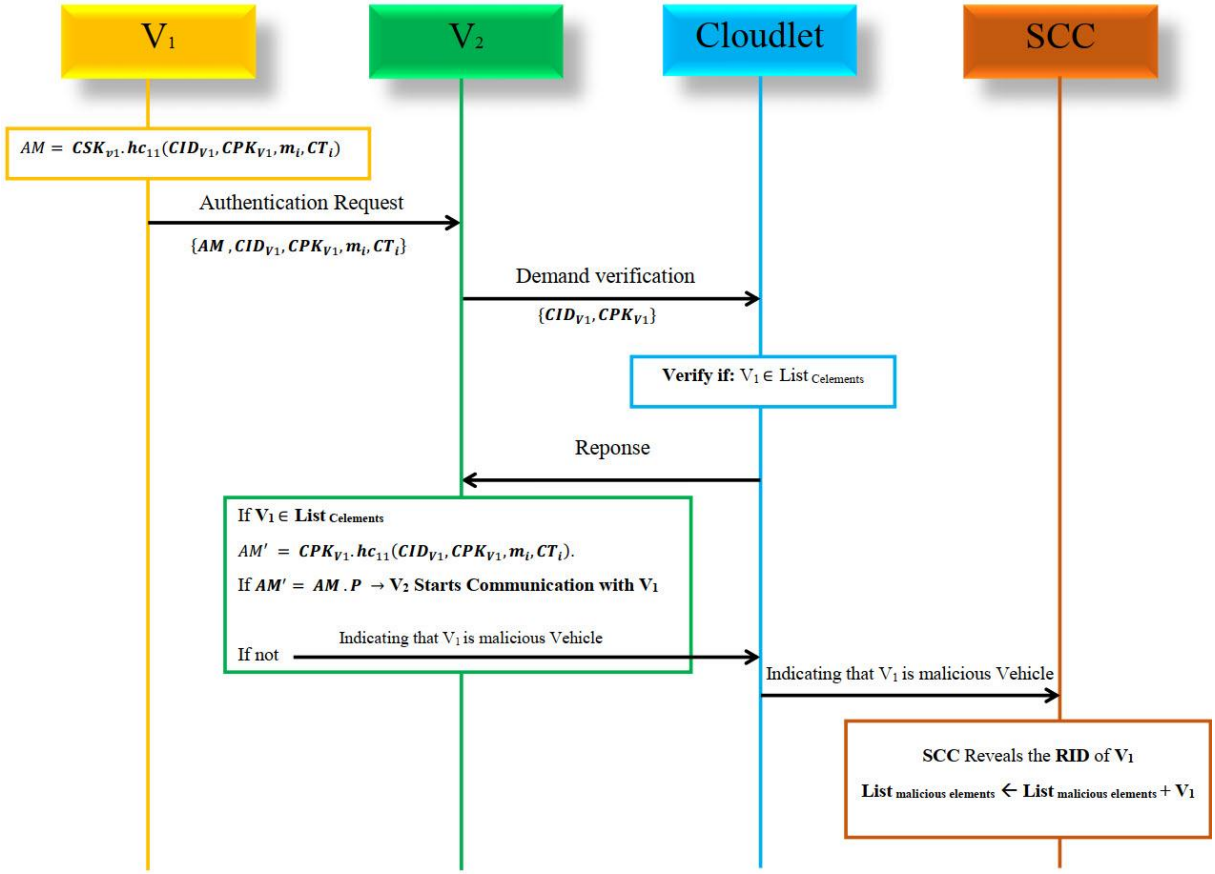

Figure 3. 12 Message flow in mutual authentication between elements situated in the same domain [173].

3.3 Confidentiality schemes

With the rapid growth of technology, strong data encryption method is the major challenges among researchers. To protect data from unauthorized elements, we propose a confidentiality schemes for two types of messages; Communication messages and Broadcasting messages.

We use ECC method to encrypt and decrypt messages. First, messages should be transformed in a points of E (a,b). If messages are not mapped to points of the elliptic curve, the encryption with ECC cannot be done.

3.3.1. V2X Communication messages:

After the mutual authentication between objects (for example: V_1 and V_2), V_1 and V_2 share a set of messages between them. These messages will be reading only by V2. We propose the following process to ensure the confidentiality of communication messages.

a. Encryption:

- V_1 generates the communication message **CM_i**.
- **CM_i** should be mapped into a point on the elliptic curve.

- V_1 selects a random number $\boldsymbol{R} \in \boldsymbol{Z_q^*}$ and computes

$$\boldsymbol{C_1 = R \,.\, P} \qquad \textbf{3-26}$$

- V_1 calculates $\boldsymbol{C_2 = P_{CM_i} \oplus CPK_{v_2}.R}$ **3-27**
- V_1 sends $\{\boldsymbol{C_1, C_2}\}$ to V_2

b. Decryption:

- V_2 calculates $\boldsymbol{K = C_1 \,.\, CSK_{v_2}}$ **3-28**
- V_2 computes $\boldsymbol{C_2 \oplus K = (P_{CM_i} \oplus CPK_{v_2}.R) \oplus R \,.\, P \,.\, CSK_{v_1}}$ **3- 29**

$$\boldsymbol{C_2 \oplus K = P_{CMi}} \qquad \textbf{3- 30}$$

- V2 Decodes $\boldsymbol{P_{CMi}}$ on $\mathbf{CM_i}$

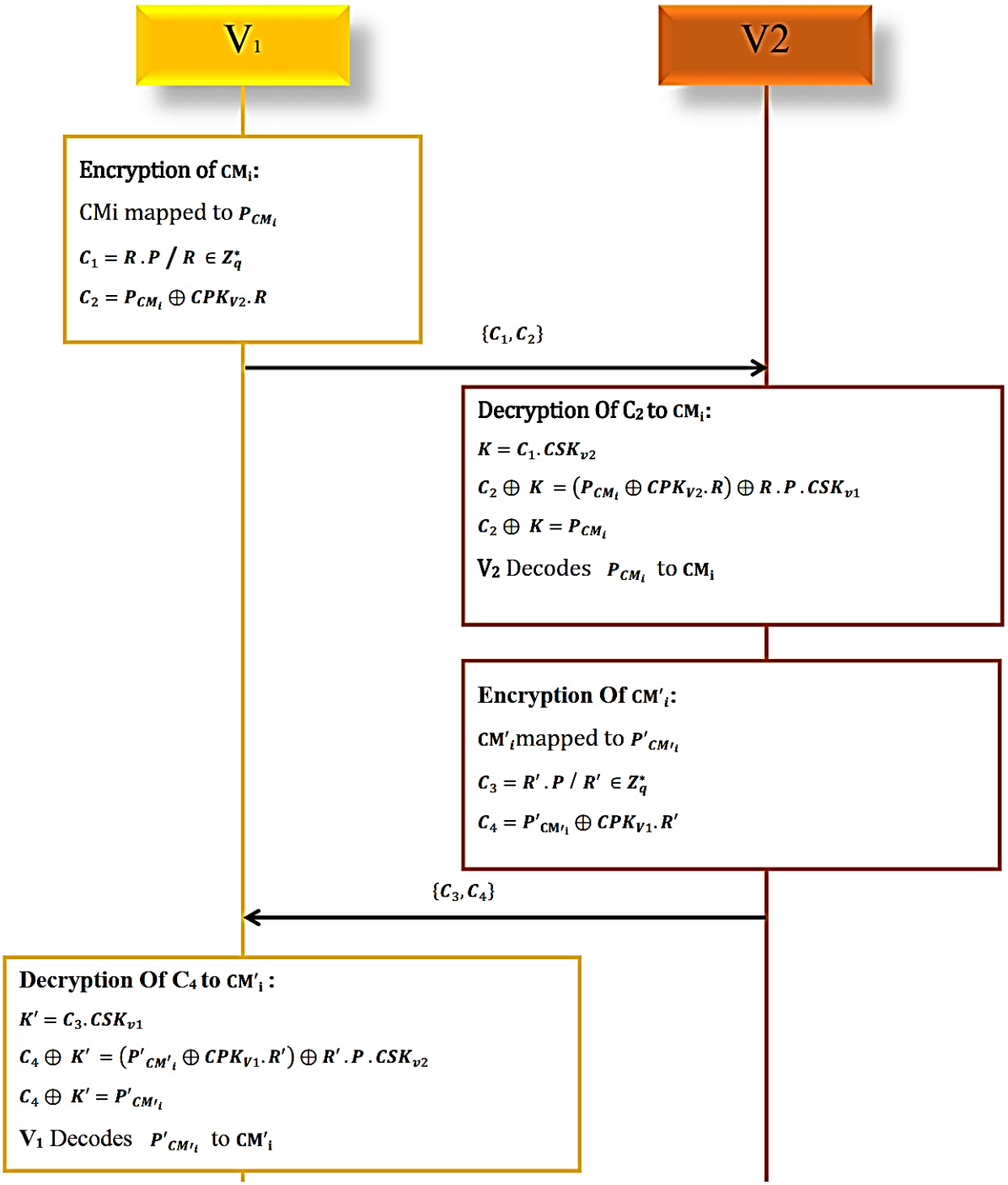

Figure 3. 13 Message flow of V2X communication phase [173].

3.3.2. V2X Broadcasting messages:

An object V_1 can broadcast information with a group of objects that belong to its domain. This information should be accessible for reading only with objects addressed to it. To guarantee this requirement, V_1 executes the following steps:

a. Preparing of the group:

- V_1 sends a demand of creating a group of communication to Cloudlet. The demand contains pseudo identities and public keys of participating elements.
- Cloudlet verifies the legitimacy of V_1 and participating elements.
- Cloudlet Selects an elliptic curve $\boldsymbol{E}\left(\boldsymbol{a_{gr}}, \boldsymbol{b_{gr}}\right)$defined by the equation

$$(\boldsymbol{y^2 = x^3 + a_{gr}x + b_{gr}}) \textbf{ mod p} \text{ for groups.}$$

- Cloudlet creates a group by generating a pseudo identity $\boldsymbol{ID_{gr_i}}$ and a symmetric key $\boldsymbol{K_{gr_i}}$.

$$\boldsymbol{K_{gr_i} = S_{gr_i} . P} \quad \textbf{3- 31 Where: } \boldsymbol{S_{gr_i}} \text{ is a random number in } \boldsymbol{Z^*_{gr_q}}$$

$$\boldsymbol{ID_{gr_i} = PID_{cloudlet} \oplus h_{gr_i}(PK_{cloudlet}, K_{gr_i})} \quad \textbf{3-32}$$

- Cloudlet sends $\boldsymbol{ID_{gr_i}}$ and $\boldsymbol{K_{gr_i}}$ to all participating elements in secure way.

b. Broadcasting:

- When V_1 receives $\mathbf{ID_{gr}}$ and $\mathbf{K_{gr}}$, it generates the broadcasting message $\mathbf{BM_i}$ and produces:

$$\boldsymbol{Verf_{gr_i} = h_{gr_i}(K_{gr_i}, T_{gr_i})} \quad \textbf{3-33}$$

$$\boldsymbol{C_{gr_i} = P_{BM_i} \oplus K_{gr_i} . P} \quad \textbf{3-34}$$

- V_1 sends $\{\boldsymbol{Verf_{gr_i}, C_{gr_i}, T_{gr_i}}\}$ to the group.

c. Receiving:

- $\boldsymbol{E_i}$ receives $\{\boldsymbol{Verf_{gr_i}, C_{gr_i}, T_{gr_i}}\}$.
- $\boldsymbol{E_i}$ first checks the freshness of timestamp; if $\boldsymbol{T_{gr_i}}$ is invalid, $\boldsymbol{E_i}$ rejects the message, otherwise, $\boldsymbol{E_i}$ calculates

$$\boldsymbol{Verf'_{gr_i} = h_{gr_i}(K_{gr_i}, T_{gr_i})} \quad \textbf{3-35}$$

- If $\boldsymbol{Verf'_{gr_i} == Verf_{gr_i}}$, $\boldsymbol{E_i}$ decrypts the message by computing:

$$\boldsymbol{C_{gr_i} \oplus K_{gr_i} . P = P_{BM_i}} \quad \textbf{3-36}$$

Otherwise, $\boldsymbol{E_i}$ rejects the message.

Note: the identifier $\boldsymbol{ID_{gr_i}}$ and $\boldsymbol{K_{gr_i}}$ will be update when an element leaves the group to provide a high security broadcasting.

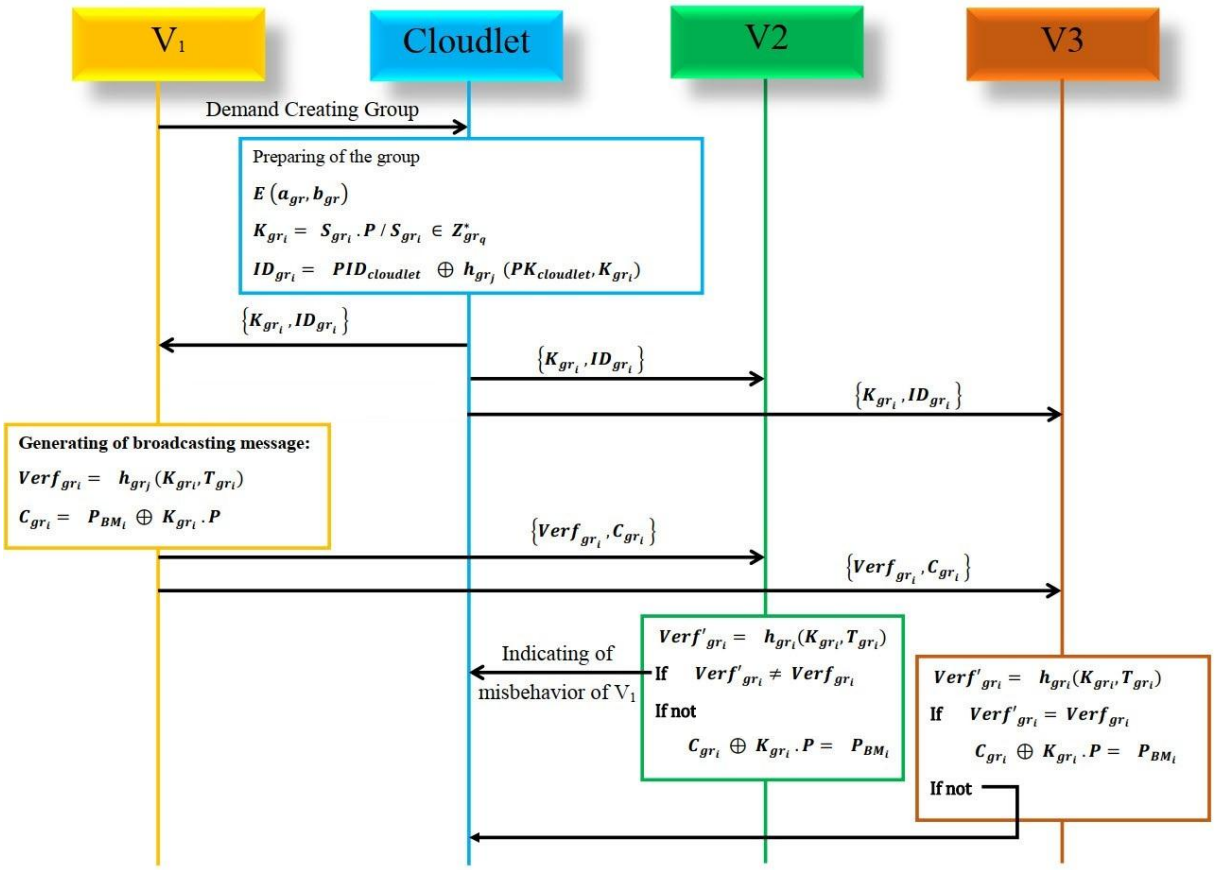

Figure 3. 14 Message flow of broadcasting message [173].

4. Conclusion

In this chapter, we presented our proposal security architecture by defining the network elements and the role of each element in the network. Then we described the authentication schemes for two mode of communication; heterogeneous communication using static keys, and communication between objects in the same domain using dynamic keys. After that, we presented our proposal confidentiality schemes for two types of communications V2X communication messages and broadcasting messages. Our proposed schemes aim to balance security and efficiency, taking into consideration the specific constrains of vehicular networks including high mobility, connectivity, and limited bandwidth. We evaluate our proposal security schemes in the next chapter.

Chapter Four*:* Evaluation and results

1. Introduction

In this chapter, we evaluate and analyze our proposed security schemes to ensure their robustness and effectiveness. We began by providing detailed description of automated validation Internet Security Protocol and Analysis (AVISPA) and Burrows Abadi Needham Logic (BAN Logic) tools. Then, we use the formal and informal security analysis to prove that our schemes are secured against various attacks. Finally, we analyze our proposal schemes in terms of storage cost, communication cost, and computation cost.

2. Tools

To validate our security proposal schemes, we use the widely accepted tools AVISPA and BAN logic. In this subsection, we describe these tools by providing definitions, characteristics, and objectives.

2.1 AVISPA

The Automated Validation Internet Security Protocol and Analysis (AVISPA) is a commonly used verification tool for cryptographic protocols (AVISPA-Project). It is funded by the European commission under the information society technologies program, operating within the fifth framework program, started on January 1st, 2003 [25].

AVISPA is considered as a state of the art tool for Internet security protocols [32]. It is used for detecting whether the protocol is safe or unsafe against various attacks. AVISPA supports High Level Protocol Specification Language (HLPSL) that is an extensive, modular, and formal language [33]. HLPSL is translated into an Intermediate Format (IF) by HLPSL2IF translator to put it on the four backends in order to generate the Output Format (OF) as shown in figure 4.1.

AVISPA integrates four different back-ends. The first backend is On the fly Model Checker (OFMC) that offers a tree based symbolic technique to explore the state space in a demand-driven way [34]. The second backend called, Constraint-Logic based Attack Searcher (CL-AtSe) provides a translation from any protocol written in as translation relation in IF to a set of constraints to detect attacks in the specified protocol. The third backend SAT-based-Model Checker (SATMC) generates propositional formulae. Tree Automata based Four Security Protocol Analyzer (TA4SP) is the last backend that uses the regular tree language to discover approximation of intruder knowledge [35].

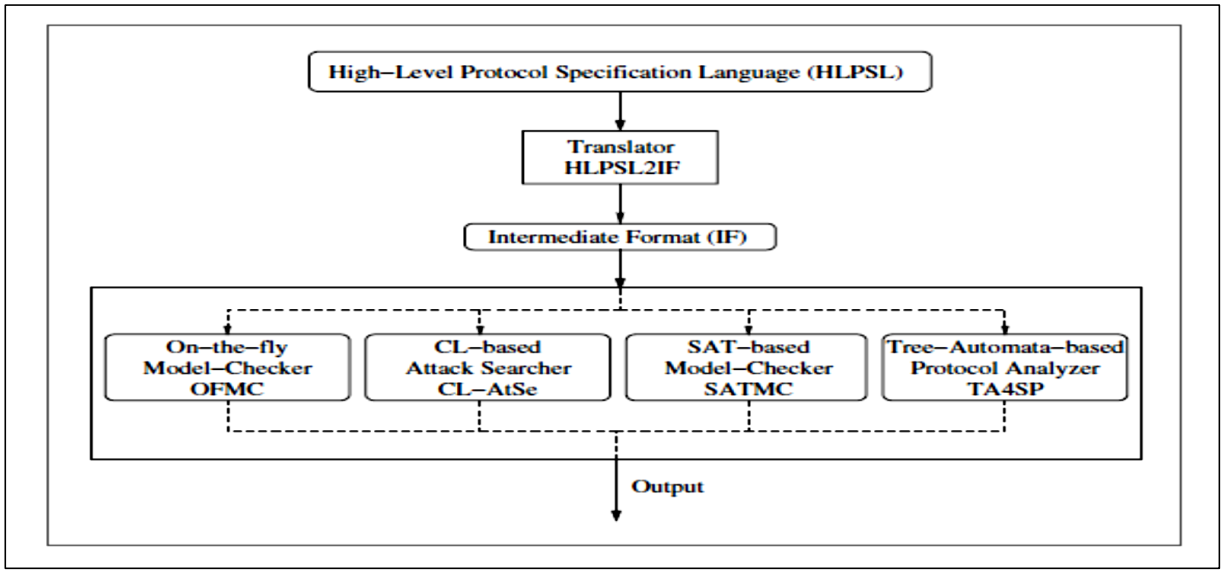

Figure 4. 1 The architecture of AVISPA tool [32].

2.2 BAN logic

BAN logic introduced by Burrows, Abadi and Needham [43], an epistemic logic for analyzing protocols [41] used in many platforms like: Mobile Ad hoc networks [50], Named Data Networking [57], Security Analysis Grid Protocol for MANET [74], Future IoT Applications [158] and Wireless Medical Sensor Network [159]. It focus on the logic of beliefs that provides a set of rules used to determine whether the exchanged messages are trustworthy secured against attacks. Each message is represented by a logical formula using BAN symbols and notations [160]. We use Ban Logic to verify the message source, message freshness and the origin's trustworthiness.

3. Formal and informal security analysis

In this section, we present the formal and informal security analysis of our proposed schemes to thoroughly examine their resilience against potential threats.

3.1.Formal security analysis

3.1.1. AVISPA

AVISPA is a role oriented language in which each IoV participant plays a role during the execution. The basic roles of our proposed protocol are: vehicle, cloudlet and SCC that communicate with each other using Snd() and Rcv() operations to send and receive messages over Dolev-Yao(dy) channel. The composition roles: goal and environment, and sessions represent participants and environment conditions.

The simulation result of our proposed protocol is shown in Figure 4.2 and Figure 4.3 under the two backends: OFMC and CL-AtSe.

As to TA4SP and SATMC backends, they do not support the XOR operation.

Figure 4. 2 AVISPA simulation results using OFMC [173].

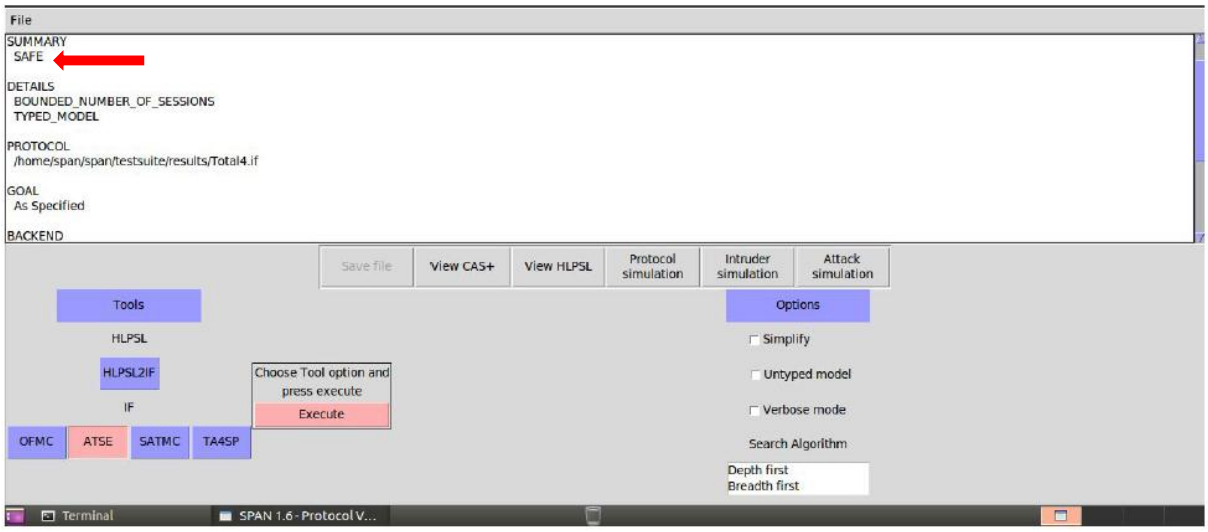

Figure 4. 3 AVISPA simulation results using CL-AtSe [173].

3.1.2. BAN logic

In this section, we first define the principal goals that should be achieved by our scheme. Then this scheme is idealized to BAN logic language. Next, we define the various

assumptions, and finally we apply constructs and postulates in order to achieve the goals mentioned in the first step.

Table 4. 1 The basic ban logic notations.

Notations	**Meaning**
SCC, V_i, $Cloudlet_j$	The main participants in our proposed protocol.
$Cloudlet_j \mid \equiv V_i$	$Cloudlet_j$ believes V_i
$V_i \mid \equiv Cloudlet_j$	V_i believes $Cloudlet_j$.
$Cloudlet_j \triangleleft M$	$Cloudlet_j$ sees M.
$V_i \triangleleft M$	V_i sees M.
$V_i \mid\sim M$	V_i sent M.
$\#(M)$	The message M is fresh.
$V_i \overset{SK}{\longleftrightarrow} Cloudlet_j$	V_i and $Cloudlet_j$ communicate by SK
$Cloudlet_j \underset{e}{\Rightarrow} V_i$	$Cloudlet_j$ has the ability to control V_i
$(M)_{SK}$	The message M is hashing by SK
$\{M\}K$	M is encrypted using secret key K
#(X, Y)	The pair of X and Y are fresh
$\frac{Rule\ 1}{Rule\ 2}$	Rule2 comes from Rule1

The main rules of BAN logic are presented as follows [174]:

a. Message-meaning:

This rule helps to explain the origin of the message. In symmetric keys; if P believes that P and Q shares a secret Key K and P sees $\{\boldsymbol{M}\}_{\boldsymbol{K}}$, then P believes that Q once said M as shown in the equation below:

$$\frac{P|\equiv P\overset{K}{\leftrightarrow}Q,P\lhd\{M\}_K}{P|\equiv Q|\sim M} \qquad \textbf{4-1}$$

The following equation presents the message-meaning rule for asymmetric keys; if P believes that the key K is the public key of Q and P received the message M signed by the private key K^{-1} of Q then P believes that M is sent by Q.

$$\frac{P|\equiv P\overset{K}{\rightarrow}Q,P\lhd\{M\}_{K^{-1}}}{P|\equiv Q|\sim M} \qquad \textbf{4-2}$$

b. Freshness:

This rule states that any message with a fresh component is also fresh. That means if P believes that X is fresh then P believes that the pair of (X, Y) are fresh.

$$\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)} \qquad \textbf{4-}3$$

c. Nonce-verification:

This rule helps to check that a message is fresh and if the sender still believe in it. That means if P believes that M is fresh and P believes that Q once sees X, then P believes that Q believes M.

$$\frac{P|\equiv\#(M),P|\equiv Q|\sim M}{P|\equiv Q|\equiv M} \qquad \textbf{4-4}$$

d. Jurisdiction:

It should be trusted that a principal has an authority on M, i.e. if P believes that Q has jurisdiction over M and Q believes M then P believes M.

$$\frac{P|\equiv Q|\overset{f}{\Rightarrow}M,\ \ P|\equiv Q|\equiv M}{P|\equiv M} \qquad \textbf{4-5}$$

Our proposed protocol need to achieve the following goals: / Security goals

Goal 1: $Cloudlet_j|\equiv\{E_{V_1},\mathrm{PK}_{V_1},\ m_i,T_i,\mathrm{y}\}$

Goal 2: $E_l|\equiv AM_{v_i}$

The idealized form of the authentication phase of the proposed protocol is given by:

M1: $V_i \longrightarrow Cloudlet_j : \{E_{V_1}, \mathrm{PK}_{V_1}, m_i, T_i, \mathrm{y}\}$

M2: $V_i \longrightarrow E_l : \{AM_{v_i}, \mathrm{CID}_{V_i}, \mathrm{CPK}_{V_i}, m_i, CT_i\}$

The following are the assumptions made to achieve the previous goals:

A1: $Cloudlet_j| \equiv \# E_{V_1}$

A2: $Cloudlet_j| \equiv \xrightarrow{PK_{V_i}} V_i$

A3: $Cloudlet_j| \equiv V_i \overset{d}{\Rightarrow} \{E_{V_1}, \mathrm{PK}_{V_1}, m_i, T_i, \mathrm{y}\}$

A4: $E_l| \equiv \#AM_{v_i}$

A5: $E_l| \equiv \xrightarrow{CPK_{V_i}} V_i$

A6: $E_l| \equiv \xrightarrow{CID_{V_i}} V_i$

A7: $E_l| \equiv V_i \overset{d}{\Rightarrow} \{AM_{v_i}, \mathrm{CID}_{V_i}, \mathrm{CPK}_{V_i}, m_i, CT_i\}$

The above assumptions and postulates are applied to the idealized form M1 and M2 to achieve the defined goals as follows.

For M1: $V_i \longrightarrow Cloudlet_j: \{E_{V_1}, \mathrm{PK}_{V_1}, m_i, T_i, \mathrm{y}\}$

- According to the seeing construct, we get:

P1: $Cloudlet_j \triangleleft \{E_{V_1}, \mathrm{PK}_{V_1}, m_i, T_i, \mathrm{y}\}$

- According to the assumption A2, P1 and message meaning rule (in this order), we get:

P2: $Cloudlet_j| \equiv V_i |\sim \{E_{V_1}, \mathrm{PK}_{V_1}, m_i, T_i, \mathrm{y}\}$

- According to A1 and freshness rule, we get:

P3: $Cloudlet_j | \equiv \# \{E_{V_1}, \mathrm{PK}_{V_1}, m_i, T_i, \mathrm{y}\}$

- According to P3, P2 and nonce verification rule, we get:

P4: $Cloudlet_j| \equiv V_i | \equiv \{E_{V_1}, \mathrm{PK}_{V_1}, m_i, T_i, \mathrm{y}\}$

- According to A3, P4 and jurisdiction rule, we get:

P5: $Cloudlet_j| \equiv \{E_{V_1}, \mathrm{PK}_{V_1}, m_i, T_i, \mathrm{y}\}$ **Goal 1**

For M2: $V_i \longrightarrow E_l : \{ AM_{v_i}, \mathrm{CID}_{\mathrm{V_i}}, \mathrm{CPK}_{\mathrm{V_i}}, m_i, CT_i \}$

Element E_l (may be another vehicle or another object situated in the same domain of V_i) sees the $\{ AM_{v_i}, \mathrm{CID}_{\mathrm{V_i}}, \mathrm{CPK}_{\mathrm{V_i}}, m_i, CT_i \}$, we get:

P6: $E_l \lhd \{ AM_{v_i}, \mathrm{CID}_{\mathrm{V_i}}, \mathrm{CPK}_{\mathrm{V_i}}, m_i, CT_i \}$

- According to the assumption A5, P6 and message meaning rule, we get:

P7: $E_l \mid \equiv V_i \mid\sim \{ AM_{v_i}, \mathrm{CID}_{\mathrm{V_i}}, \mathrm{CPK}_{\mathrm{V_i}}, m_i, CT_i \}$

- According to A4 and freshness rule, we get:

P8: $E_l \mid \equiv \# \{ AM_{v_i}, \mathrm{CID}_{\mathrm{V_i}}, \mathrm{CPK}_{\mathrm{V_i}}, m_i, CT_i \}$

- According to P8, P7 and nonce verification rule, we get:

P9: $E_l \mid \equiv V_i \mid \equiv \{ AM_{v_i}, \mathrm{CID}_{\mathrm{V_i}}, \mathrm{CPK}_{\mathrm{V_i}}, m_i, CT_i \}$

- According to A7, P9 and jurisdiction rule, we get:

P10: $E_l \mid \equiv \{ AM_{v_i}, \mathrm{CID}_{\mathrm{V_i}}, \mathrm{CPK}_{\mathrm{V_i}}, m_i, CT_i \}$ **Goal 2**

The precedent derivations shows that our proposed protocol achieve all the defined goals.

3.2.Informal security analysis

- **Man in the middle attack**

We suppose that A can intercept the messages over a public channel. A cannot generate the authentication request messages {y, AM} because A cannot guess the random value U and cannot calculate the secret value of V_i ($\mathrm{CSK}_{\mathrm{V_i}}$). So our protocol is secure against man in the middle attack.

- **Replay attack**

The replay attack consists of an attacker A intercepting the exchanged messages {$\mathrm{E}_{\mathrm{V_i}}$, PKV_i, m_i, T_i, y} and {$\mathrm{CID}_{\mathrm{V_i}}, \mathrm{CPK}_{\mathrm{V_i}}$, m_i, CT_i} in the authentication process over a public channel to have the same right as the user. Our protocol is able to prevent replay attack because the receiver checks first the freshness of the timestamps (T_i, CT_i), also all messages are protected with random value U and the secret keys ($\mathrm{CSK}_{\mathrm{V_i}}$, $\mathrm{SK}_{\mathrm{V_i}}$).

- **Eavesdropping attack**

Eavesdropping attack means that an attacker A has the ability to access to the communication or broadcasting messages ($\{C_1, C_2\}, \{\mathrm{Verif}_{\mathrm{gr}_i}, C_{\mathrm{gr}_i}\}$) and reading the data. In our protocol, if attacker A obtains the communication messages {C_1, C_2}, he cannot

calculate K where $K = C_1.CSK_{V_2}$ because he has not the private key CSK_{V_2} and he cannot generate it; CSK_{V_2} is the multiplication of the two random secret values SK_{V_2} and S_{cv_2}. In the case of broadcasting messages, if A has C_{gr_i}, he cannot decrypt the message because K_{gr_i} ($K_{gr_i} = S_{gr_i}.P$) is a secret symmetric key and S_{gr_i} is a random value. So our protocol can prevent eavesdropping attack.

- **Traffic analysis**

Vehicles use dynamic pseudo identities for communication, so an attacker A will not able to know who is connected with who, which is one of the main goals of this type of attack. Also in our proposal network model, each SDN controller manages and controls all packets forwarded in its domain. For example, V_1 want to send a message to an object O_1. SDN controller chooses the optimal path that is not the same path for the next message between V_1 and O_1. This makes it difficult for an attacker to discover the structure of the network. This is another goal of this type of attack.

- **Impersonation attack**

If an attacker impersonates a registered vehicle or an object, he should create the legal authentication message of this vehicle $\{E_{v_i}, PK_{v_i}, m_i, T_i, y\}$ and it is impossible because he cannot compute y without having the random secret value U. Even if the attacker A has the real authentication request $\{E_{v_i}, PKV_i, m_i, T_i, y\}$, he cannot calculate $CSK_{v_i}.CSK_i$ which is the multiplication of SK_{v_i} to S_{cv_i} and is used also for decrypting messages.

- **Spoofing attack**

In our proposed schemes, if an attacker A wants to pretend to be another element, for example a vehicle V_1, he should calculate E_{v_1} and AM. To calculate E_{v_1} and AM, A has to know U and CSK_{v_1} which is impossible. U and CSK_{v_1} are only known by the vehicle. Also as A has not CSK_{v_1}, he cannot decrypt messages. Therefore, A will not be able to access data that is the main goal of this type of attack. Thus, our protocol is secure against spoofing attack.

- **Masquerading attack**

Our proposed protocol can resist against masquerading attack because the authentication of an object requires signatures: $x = h_2(U.PK_{cloudlet_1}, m_i, T_i)$ and $AM = CSK_{v_1}.h_{c_{11}}(CID_{v_1}, CPK_{v_1}, m_i, CT_i)$ for mutual authentication between heterogeneous elements and

mutual authentication between elements in the same domain respectively. A cannot compute x and AM.

- **Sybil attack**

In case of static identity and keys, an attacker A cannot generate more than one identity. Because each object should register in SCC with its real identity and before any authentication between cloudlet and vehicle, cloudlet collaborates with SCC to verify if PK_{v_1} and PID_{v_1} exist in the list of registered objects or not. In case of dynamic identities and dynamic keys, each object registers in cloudlet domain to have dynamic parameters to calculate CID_{v_1} and CPK_{v_1}. Cloudlet registers CID_{v_1} and CPK_{v_1} with the static PK_{v_1} and PID_{v_1} of this vehicle. If an attacker A generates more than one $\{CID_{v_i}, CPK_{v_i}\}$ then sends messages to V1 like a multiple senders. Before the mutual authentication between V_2 and senders, V_2 coordinates with cloudlet for verifying if $\{CID_{v_i}, CPK_{v_i}\}$ of senders exist in the registered objects of cloudlet or not. We conclude that an attacker A cannot communicate with multiple identities. Our proposed schemes successfully prevent the Sybil attack.

- **Profile inference attack**

In eavesdropping attack, the attacker A listens to network communication in order to gain access to private information. So ensuring privacy is an important issue in IoV. In our proposed protocol, vehicle does not use its real identity for communication, it uses pseudo static and dynamic identities:

$$PID_{v_1} = (RID_{v_1} \oplus h_1 (PK_{v_1}, SK_{v_1})) \text{ and } CID_{v_1} = h_{c_{11}} (RID_{v_1}, CSKv1)$$

It is impossible for an attacker A to know the real identity of vehicle, because it cannot obtain the random secret values SK_{v_1} and CSK_{v_1}. Also to read messages, A should have SK_{v_1} and CSK_{v_1} which is impossible. So the privacy protection of our proposed protocol is guaranteed.

- **Denial of service attack**

The main goal of this type of attack is to make the network unavailable. So if an attacker A sends several bogus requests to the cloudlet, the cloudlet will be unavailable. In this case, SDN controller will redirected vehicles to the nearest cloudlet. So proposed protocol can prevent denial of service attack.

- **Anonymity**

The messages transmitted between IoV objects in the authentication process are protected with: random value U, secret keys (CSK_{v_1}, SK_{v_1}), hush functions, and XOR operations, also objects use dynamic pseudo identities. So an attacker A cannot obtain the real identities of IoV objects. Thus, our protocol provides the anonymity of IoV objects.

4. Performance analysis

In this section, we present the performance analysis in terms of storage cost, communication cost, and computation cost.

4.1.Storage cost

We considered that all the elliptical curve points with 224 bits, one way hash functions give a 128 bits output, scalar random number, and timestamps take 64 bits. Private Keys are considered as scalar values and Public Keys are considered as points. So for an object like vehicle, we need to store static elements {public Key, private key, and object's identity} and dynamic elements {public Key, private key, and object's identity} that occupy $2 \times (224 + 64 + 32) = 640\ bits$. For dynamic elements, each object updates its dynamic elements and stores only the new elements.

4.2.Communication cost

The communication cost depends on the number of bits transmitted between devices during conversation. Our proposed protocol have two types of authentication requests. The first request is for mutual authentication between heterogeneous objects $\{\boldsymbol{E_{V_1}}, \mathbf{PK_{V_1}}, \boldsymbol{m_i}, \boldsymbol{T_i}, \mathbf{y}\}$ that occupies $224 + 224 + 64 + 64 + 64 = 640\ bits$. The second request is for mutual authentication between objects suited in the same domain $\{AM = \boldsymbol{CSK_{v1}} . \boldsymbol{hc_{11}}(\boldsymbol{CID_{V1}}, \boldsymbol{CPK_{V1}}, \boldsymbol{m_i}, \boldsymbol{CT_i})\}$ and $\{(\boldsymbol{CID_{V1}}, \boldsymbol{CPK_{V1}}, \boldsymbol{m_i}, \boldsymbol{CT_i})\}$ which take $(128 + 32 + 224 + 64 + 64) + (32 + 224 + 64 + 64) = 896 bits$.

Our proposed protocol have two types of communication messages; V2X communication message and V2X broadcasting message. For V2X communication message, Vehicle sends $\{\boldsymbol{C_1}, \boldsymbol{C_2}\}$ that occupies $224 + 224 = 448\ bits$. For V2X broadcasting message, Vehicle sends $\{\boldsymbol{Verf_{gr_i}}, \boldsymbol{C_{gr_i}}, \boldsymbol{T_{gr_i}}\}$ which take $64 + 224 + 64 = 352 bits$.

4.3.Computation cost

The following notations are used to represent the running time of the cryptographic operations. The other operations are ignored due to their trivial computational cost.

- T_m: The running time of an elliptic curve point multiplication.
- T_b: The running time of a bilinear pairing operation.
- T_h: The running time of a general hash function operation.
- T_{mas}: The running time of a modular addition/subtraction.
- T_{mm}: the running time of a modular multiplication operation.

The computational costs of vehicle, Cloudlet, and other objects in the authentication phase are as follows:

- For the mutual authentication between heterogeneous elements:
  $3T_m + T_h$ are needed for vehicle and $3T_m + T_h$ are needed for cloudlet.
- For the mutual authentication between elements situated in the same domain:
  $T_m + T_h$ and $2T_m + T_h$ are needed for vehicle and another object separately.

The computational costs of vehicle, Cloudlet, and other objects in the communication phase are as follows:

- For V2X communication message:
  $2\ T_m$ is needed for the sender and T_m is needed for the receiver.
- For V2X broadcasting message:
  $T_m + T_h$ are needed for the cloudlet.
  $T_m + T_h$ are needed for broadcasting and $T_m + T_h$ are needed for the receiver.

4.4.Comparison with other schemes

As the computation cost is a very important aspect in IoV, we present the computation comparison between our protocol and related works in Table 4.2. In the Liu et al. scheme [59], the mutual authentication between two objects takes $T_m + 4T_h$ for generating the authentication request of object and objects 2 takes $2T_m + 4T_h$ for verification. Chien et al. scheme [63] takes $3T_m + 4T_h$ and $T_m + 4T_h$ for authentication request and verification respectively. The authentication request in Alshudukhi et al. scheme [64] takes $T_m + 2T_h$ and $T_m + 2T_h$ verification request of V1 and $2T_m + T_h$ for verification. As illustrated in Table 4.2 Our protocol takes less cost comparing to these schemes.

Table 4. 2 Computation cost comparison [173]

Schemes	Authentication request cost	Authentication verification cost
Lui et al. [59]	$T_m + 4T_h$	$2\ T_m + 4\ T_h$
Chien et al. [63]	$3T_m + 4\ T_h$	$T_m + 4\ T_h$
Alshudukhi et al. [64]	$T_m + 2T_h$	$T_m + 2\ T_h$
Our	$T_m + T_h$	$2T_m + T_h$

Xu et al proposed a lightweight and secure multi messages and multi receiver messages scheme for the Internet of vehicles [175]. In this paper [175], the sender vehicle signcrypts the message and sends the cipher text to other vehicles or RSUs. $3T_m + T_h$ are needed for the sender to accomplish this process. The receiver (vehicle or RSU) unsigncrypts the cipher text to obtain the traffic related information, and this process needs $4T_m + 3T_h$ to be achieved. However, in our protocol, the sender needs $2T_m$ for encrypting the message and the receiver needs $2T_m$ decrypting the message.

5. Conclusion

In this chapter, we evaluated our proposal authentication and confidentiality schemes. We demonstrated that our proposal authentication schemes allow only authenticated vehicles to communicate with others and declines malicious objects by using mutual authentication schemes between elements. The first is between elements in heterogeneous domains and the second is between elements situated in the same domain. These schemes are based on the secret values (SK_{v_i}, U) and CSK_{v_i} where $CSK_{v_i} = SK_{v_i} S_{cv_i}$. The malicious vehicle A cannot guess the secret random values $SK_{v_i}, U,$ and S_{cv_i}. Even if A has PK_{v_1} and CPK_{v_1}, it is very hard and nearly impossible to deduce these secret random values. The confidentiality of shared messages between vehicles is maintained by the use of private key CSK_{v_i} and the secret random value R. The receiver cannot decrypt the message. For the broadcasting messages, a malicious vehicle A cannot decrypt the broadcasting messages BM_i because A cannot generate the symmetric key K_{gr_i} where $K_{gr_i} = S_{gr_i}.P$. A cannot deduce the random secret value S_{gr_i}. We used AVISPA and BAN logic to illustrate that our protocol is secure against attacks. Finally, we provided the performance analysis in terms of storage cost, communication cost, and computation cost.

By integrating lightweight encryption methods and robust authentication mechanisms, our proposal schemes ensure robust protection against potential threats without posing significant computational overhead.

General Conclusion

General Conclusion

Smart cities are designed to improve urban living by leveraging advanced technologies and intelligent systems to optimize infrastructure, enhance sustainability, and provide a better public services for citizens. The core of smart cities is build around the internet of things (IoT). IoT represents a transformative and expansive network of interconnected devices, sensors, and systems that communicate and exchange data seamlessly to enhance efficiency, convenience, and innovation across a myriad of sectors including healthcare, manufacturing, transportation, and home automation. By enabling devices to collect, share, and analyze data in real time, IoT facilitates smarter decisions, predictive maintenance, and the automation of routine tasks, thereby driving significant advancements in technology and improving overall quality of life. Building upon the foundational principals of IoT, the Internet of vehicles (IoV) focus on integrating intelligent transportation systems with vehicular networks, allowing vehicles to interact not only with each other but also with infrastructure components such as traffic lights, road signs, and even pedestrians' mobile devices. This interconnected ecosystem aims to enhance traffic management, increase road safety, reduce congestion, and provide enriched driving experiences through features like autonomous driving, real time navigation updates, and vehicle to everything (V2X) communication. However, the adoption of IoV introduces significant challenges, particularly in ensuring secure and efficient communication between objects. Authentication mechanisms between vehicles and connected objects are critical to prevent malicious object to act as a legitimate object. Additionally, maintaining data confidentiality is paramount to protect sensitive information transmitted across the network from potential threats. The open and dynamic nature of IoV network makes it susceptible to diverse attacks such as man in the middle attack, impersonation attack, eavesdropping attack, and traffic analysis attack. To effectively mitigate these vulnerabilities and enhance the overall security posture of IoV systems, our proposed schemes introduced robust mechanisms designed to ensure high level of security in both authentication and data confidentiality.

In this thesis, we proposed a secure proposal schemes based on elliptic curve cryptography. Our proposed schemes effectively balance security and efficiency, which is particularly critical in Internet of vehicles environment where vehicles are continuously and rapidly moving from one place to another. By offering robust security schemes with optimized performances and Comparing to Lui et al scheme [59], Chien et al scheme [63], and Alshudukhi scheme [64], our approach ensures that authentication between objects and data confidentiality are maintained

without introducing significant latency or computation overhead. This delicate equilibrium allows seamless and secure communication between vehicle and other objects.

Publications

1- **A Network Model for Internet of vehicles based on SDN and Cloud Computing.** In: 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakesh, Morocco, 2018.

2- **A Security Proposal for IoT integrated with SDN and Cloud.** In: 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakesh, Morocco, 2018.

3- **An Overview of Internet of Vehicles (IoV): Concepts, Security requirements and threat models.** In:4th International Conference on Embedded Systems in Telecommunications and Instrumentation (ICESTI'19), October 28-30, 2019, Annaba, Algeria.ICESTI'19 Conference (28-30 October 2019).

4- **Security of internet of vehicles in smart cities: authentication and confidentiality aspects.** In: International Journal of Internet Technology and Secured Transactions, 2024, Vol.13 No.3, pp.232 – 269.

References

[1] Statista team. “Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 (in billions)”. (accessed April, 2023). https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ .

[2] RAMAPRASAD, Arkalgud, SÁNCHEZ-ORTIZ, Aurora, et SYN, Thant. A unified definition of a smart city. In : International Conference on Electronic Government. Cham: Springer International Publishing, 2017. p. 13-24.

[3] Abderahman Rejeb, Karim Rejeb, Steve Simske , Horst Treiblmaier, and Suhaiza Zailani, “The big picture on the internet of things and the smart city: a review of what we know and what we need to know ”. In: Internet of Things, Elsevier, 2022, vol. 19, p. 100565

[4] Renata Paola Dameri, “Smart City Definition, Goals and Performance”. In: Smart City Implementation. Progress in IS. 16 September 2016. Springer International Publishing, 2016. p. 1-22

[5] Keshavarzi Golnaz, YildirimYalcin, et Arefi Mahyar. “Does scale matter? An overview of the “smart cities” literature”. In: Sustainable Cities and Society (Elsevier), 2021, vol. 74, p. 103151.

[6] Zaidan A.A., Zaidan, B.B., Qahtan, M.Y., Albahri O.S., A. S. Albahri, Mussab Alaa, Jumaah F. M. , Mohammed Talal, Tan K. L., Shir W.L., Lim C.K., “A survey on communication components for IoT-based technologies in smart homes”. In: Telecommun Systems Journal (Springer), vol. 69, p 1–25 (2018).

[7] Ding Dan, Cooper Rory A., Paul F. Pasquina, Lavinia Fici-Pasquina, “Sensor technology for smart homes”. In: Maturitas Journal (Elsevier), vol. 69, no 2, p. 131-136 (2011).

[8] Tian Shuo, Yang Wenbo, LE grange Jehane Michael, Peng Wang, Wei Huang, and Zhewei Ye, “Smart healthcare: making medical care more intelligent”. In: Global Health Journal (Science Direct) , vol. 3, no 3, p. 62-65 (2019).

[9] Haluk Demirkan, "A Smart Healthcare Systems Framework," in IT Professional Journal (IEEE), vol. 15, no. 5, pp. 38-45, Sept.-Oct. (2013).

[10] Bayindir Ramazan, Colak Ilhami, Fulli Gianluca, and Demirtas Kenan, "Smart grid technologies and applications. Renewable and sustainable energy reviews". In: Renewable and Sustainable Energy Reviews Journal (Elsevier), vol. 66, p. 499-516. (2016).

[11] Dileep Gjre, "A survey on smart grid technologies and applications". In: Renewable energy Journal (Elsevier), vol. 146, p. 2589-2625. (2020)

[12] Tanwar Sudeep, Tyagi Sudhanshu, and Kumar Sachin. "The role of internet of things and smart grid for the development of a smart city". In : Intelligent Communication and Computational Technologies: Proceedings of Internet of Things for Technological Development, IoT4TD 2017. (Springer Singapore), vol. 19, p. 23-33 (2018).

[13] Wang, W., Ren, L., Chen, L., & Ding, Y. (2019). Intrusion detection and security calculation in industrial cloud storage based on an improved dynamic immune algorithm. Information Sciences, 2019, vol. 501, p. 543-557.

[14] ZHU, Zhi-Ting, YU, Ming-Hua, et RIEZEBOS, Peter. A research framework of smart education. Smart learning environments, 2016, vol. 3, p. 1-17.

[15] BAJAJ, Richa et SHARMA, Vidushi. Smart Education with artificial intelligence based determination of learning styles. Procedia computer science, 2018, vol. 132, p. 834-842.

[16] CHEN, Baotong, WAN, Jiafu, SHU, Lei, et al. Smart factory of industry 4.0: Key technologies, application case, and challenges. Ieee Access, 2017, vol. 6, p. 6505-6519.

[17] SHI, Zhan, XIE, Yongping, XUE, Wei, et al. Smart factory in Industry 4.0. Systems Research and Behavioral Science, 2020, vol. 37, no 4, p. 607-617.

[18] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 57, no. 6, pp. 3357–3368, 2008.

[19] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous Authentication scheme with strong privacy preservation for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 7, pp. 3589–3603, 2010.

[20] ZHAO, Yanan, HOU, Yingzhe, WANG, Lili, et al. An efficient certificateless aggregate signature scheme for the Internet of Vehicles. Transactions on Emerging Telecommunications Technologies, 2020, vol. 31, no 5, p. e3708.

[21] ISLAM, SK Hafizul, OBAIDAT, Mohammad S., VIJAYAKUMAR, Pandi, et al. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Generation Computer Systems, 2018, vol. 84, p. 216-227.

[22] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, 2015.

[23] LUAN, Tom H., CAI, Lin X., CHEN, Jiming, et al. Engineering a distributed infrastructure for large-scale cost-effective content dissemination over urban vehicular networks. IEEE Transactions on Vehicular Technology, 2013, vol. 63, no 3, p. 1419-1435.

[24] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Specs: Secure and privacy enhancing communications schemes for vanets," Ad Hoc Networks, vol. 9, no. 2, pp. 189–203, 2011

[25] GLOUCHE, Yann, GENET, Thomas, HEEN, Olivier, et al. A security protocol animator tool for AVISPA. In : ARTIST2 workshop on security specification and verification of embedded systems, Pisa. 2006. p. 1-7.

[26] T. H. Luan, X. S. Shen, and F. Bai, "Integrity-oriented content transmission in highway vehicular ad hoc networks," in 2013 Proceedings IEEE INFOCOM. IEEE, 2013, pp. 2562–2570.

[27] J. Yoo and J. H. Yi, "Code-based authentication scheme for lightweight integrity checking of smart vehicles," IEEE Access, vol. 6, pp. 46 731–46 741, 2018.

[28] CUI, Jie, TAO, Xuefei, ZHANG, Jing, et al. HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs. Vehicular communications, 2018, vol. 14, p. 15-25.

[29] MA, Ruhui, CAO, Jin, FENG, Dengguo, et al. A secure authentication scheme for remote diagnosis and maintenance in Internet of Vehicles. In : 2020 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2020. p. 1-7.

[30] JO, Hyo Jin, KIM, In Seok, et LEE, Dong Hoon. Reliable cooperative authentication for vehicular networks. IEEE Transactions on Intelligent Transportation Systems, 2017, vol. 19, no 4, p. 1065-1079.

[31] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 8, pp. 2627–2637, 2018.

[32] VIGANO, Luca. Automated security protocol analysis with the AVISPA tool. Electronic Notes in Theoretical Computer Science, 2006, vol. 155, p. 61-86.

[33] AR, Rizwana Shaikh et DEVANE, Satish. Formal Verification of Payment protocol using AVISPA. 2010.

[34] DAS, Ashok Kumar, CHATTERJEE, Santanu, et SING, Jamuna Kanta. Formal security analysis and verification of a password-based user authentication scheme for hierarchical wireless sensor networks. International Journal of Trust Management in Computing and Communications, 2014, vol. 2, no 1, p. 78-102.

[35] LIU, Nan, ZHU, Wen-ye, et ZHU, Yue-fei. Security protocol analysis based on rewriting approximation. In : 2009 Second International Symposium on Electronic Commerce and Security. IEEE, 2009. p. 318-322.

[36] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles," IEEE Transactions on Vehicular Technology, vol. 67, no. 11, pp. 11 169–11 180, 2018.

[37] S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal, "Vehicle authentication via monolithically certified public key and attributes," Wireless Networks, vol. 22, no. 3, pp. 879–896, 2016.

[38] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, 2016.

[39] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for vanets," IEEE Transactions on vehicular technology, vol. 65, no. 3, pp. 1711–1720, 2015.

[40] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy preserving vehicular communication authentication with hierarchical aggregation and fast response," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, 2015.

[41] TEEPE, Wouter. On BAN logic and hash functions or: how an unjustified inference rule causes problems. Autonomous Agents and Multi-Agent Systems, 2009, vol. 19, p. 76-88.

[42] M. Jan, P. Nanda, M. Usman, and X. He, "Pawn: a payload-based mutual authentication scheme for wireless sensor networks," Concurrency and computation: Practice and experience, vol. 29, no. 17, p. e3986, 2017.

[43] BURROUGHS, M., ABADI, M., et NEEDHAM, R. A logic of authentication. Proceedings of the Royal Society of London, 1989, p. 233-271.

[44] VASUDEV, Harsha, DESHPANDE, Varad, DAS, Debasis, et al. A lightweight mutual authentication protocol for V2V communication in internet of vehicles. IEEE Transactions on Vehicular Technology, 2020, vol. 69, no 6, p. 6709-6717.

[45] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," Peer to-peer Networking and Applications, vol. 9, no. 1, pp. 223–244, 2016.

[46] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing sdn infrastructure of iot–fog networks from mitm attacks," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1156–1164, 2017.

[47] S. Céspedes, S. Taha, and X. Shen, “A multihop-authenticated proxy mobile ip scheme for asymmetric vanets,” IEEE Transactions on Vehicular Technology, vol. 62, no. 7, pp. 3271–3286, 2013.

[48] A.Wasef and X. Shen, “Emap: Expedite message authentication protocol for vehicular ad hoc networks,” IEEE transactions on Mobile Computing, vol. 12, no. 1, pp. 78–89, 2011.

[49] WANG, Neng-Wen, HUANG, Yueh-Min, et CHEN, Wei-Ming. A novel secure communication scheme in vehicular ad hoc networks. Computer communications, 2008, vol. 31, no 12, p. 2827-2837.

[50] SAXENA, Mihir et DUA, Amit. Security solutions against attacks in mobile ad hoc networks and their verification using BAN logic. In : 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS). IEEE, 2017. p. 3188-3193.

[51] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, “Provably secure user authentication and key agreement scheme for wireless sensor networks,” Security and Communication Networks, vol. 9, no. 16, pp. 3670–3687, 2016.

[52] T. W. Chim, S. Yiu, L. C. Hui, and V. O. Li, “Security and privacy issues for inter-vehicle communications in vanets,” in 2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops. IEEE, 2009, pp. 1–3.

[53] B. Xiao, B. Yu, and C. Gao, “Detection and localization of sybil nodes in vanets,” in Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks. ACM, 2006, pp. 1–8

[54] XU, Xiangyang, LI, Xiang, DONG, Peng, et al. Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack. IEEE Transactions on Vehicular Technology, 2020, vol. 70, no 6, p. 5524-5536.

[55] H. Liu, Y. Sun, Y. Xu, R. Xu, and Z. Wei, “A secure lattice-based anonymous authentication scheme for vanets,” Journal of the Chinese Institute of Engineers, vol. 42, no. 1, pp. 66–73, 2019.

[56] M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. ACM, 2005, pp. 11–21.

[57] FEI, Yuan, ZHU, Huibiao, et VINH, Phan Cong. Security analysis of the access control solution of NDN using BAN logic. Mobile Networks and Applications, 2020, vol. 25, p. 1162-1173.

[58] Na Ruan, Mengyuan Li and Jie Li, “A novel broadcast authentication protocol for internet of vehicles.” In: Peer-to-Peer Networking and Applications journal (Springer), Volume: 10, Issue: 6, pp 1331-1343 (August 2016).

[59] LIU, Yanbing, WANG, Yuhang, et CHANG, Guanghui. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm. IEEE Transactions on Intelligent Transportation Systems, 2017, vol. 18, no 10, p. 2740-2749

[60] JIANG, Qi, ZHANG, Xin, ZHANG, Ning, et al. Two-factor authentication protocol using physical unclonable function for IoV. I: 2019 IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 2019. p. 195-200.

[61] Fan, K., Jiang, W., Luo, Q., Li, H., & Yang, Y. (2019). Cloud-based RFID mutual authentication scheme for efficient privacypreserving in IoV. Journal of the Franklin Institute.

[62] YING, Bidi et NAYAK, Amiya. Anonymous and lightweight authentication for secure vehicular networks. IEEE Transactions on Vehicular Technology, 2017, vol. 66, no 12, p. 10626-10636.

[63] CHEN, Chien-Ming, XIANG, Bin, LIU, Yining, et al. A secure authentication protocol for internet of vehicles. Ieee Access, 2019, vol. 7, p. 12047-12057

[64] J. S. Alshudukhi, Z. G. Al-Mekhlafi and B. A. Mohammed, "A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography," in IEEE Access, vol. 9, pp. 15633-15642, 2021.

[65] MUN, Hyeran, HAN, Kyusuk, LEE, Yan Sun, et al. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. Mathematical and Computer Modelling, 2012, vol. 55, no 1-2, p. 214-222

[66] ZHAO, Dawei, PENG, Haipeng, LI, Lixiang, et al. A secure and effective anonymous authentication scheme for roaming service in global mobility networks. Wireless Personal Communications, 2014, vol. 78, p. 247-269

[67] HE, Debiao, ZEADALLY, Sherali, XU, Baowen, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no 12, p. 2681-2691.

[68] RAWAT, Ajay, SHARMA, Santosh, et SUSHIL, Rama. VANET: Security attacks and its possible solutions. Journal of Information and Operations Management, 2012, vol. 3, no 1, p. 301-304.

[69] AL-KAHTANI, Mohammed Saeed. Survey on security attacks in vehicular ad hoc networks (VANETs). In : 2012 6th international conference on signal processing and communication systems. IEEE, 2012. p. 1-9

[70] Fatih Sakiz and Sevil Ben, "A servey of attacks and Detection Mechanisms on Intelligent transportation Systems: VANETs and IoV." In: Journal of ad hoc networks (Elseiver), Volume: 61, pp 33-50 (June 2017).

[71] UPADHYAYA, Ajay N. et SHAH, J. S. Attacks on vanet security. Int J Comp Eng Tech, 2018, vol. 9, no 1, p. 8-19.

[72] OSIBO, Benjamin Kwapong, ZHANG, Chengbo, XIA, Changsen, et al. Security and privacy in 5G internet of vehicles (IoV) environment. Journal on Internet of Things, 2021, vol. 3, no 2, p. 77.

[73] ZAIDI, Taskeen et FAISAL, Syed. An overview: Various attacks in VANET. In : 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018. p. 1-6.

[74] HAN, Shuai et JIAO, Wencheng. Security analysis of GRID protocol for MANET based on BAN logic. Proceedings of Information Science and Cloud Computing—PoS (ISCC 2017), Sissa Medialab, Guangzhou, China, 2018, p. 042.

[75] RAJPUT, Ubaidullah, ABBAS, Fizza, EUN, Hasoo, et al. A two level privacy preserving pseudonymous authentication protocol for VANET. In : 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2015. p. 643-650.

[76] K. Verma, H. Hasbullah, and A. Kumar, "An efficient defense method against udp spoofed flooding traffic of denial of service (dos) attacks in vanet," in 2013 3rd IEEE International Advance Computing Conference (IACC). IEEE, 2013, pp. 550–555.

[77] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in ieee 802.11 p vehicular networks," IEEE Communications letters, vol. 18, no. 1, pp. 110–113, 2013.

[78] JIANG, Qi, ZHANG, Xin, ZHANG, Ning, et al. Three-factor authentication protocol using physical unclonable function for IoV. Computer Communications, 2021, vol. 173, p. 45-55.

[79] JIANG, Qi, ZHANG, Ning, NI, Jianbing, et al. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. IEEE Transactions on Vehicular Technology, 2020, vol. 69, no 9, p. 9390-9401.

[80] XIE, Qi et HUANG, Juanjuan. Improvement of a Conditional Privacy-Preserving and Desynchronization-Resistant Authentication Protocol for IoV. Applied Sciences, 2024, vol. 14, no 6, p. 2451.

[81] BERLATO, Stefano, CENTENARO, Marco, et RANISE, Silvio. Smart card-based identity management protocols for V2V and V2I communications in CCAM: a systematic literature review. IEEE Transactions on Intelligent Transportation Systems, 2021, vol. 23, no 8, p. 10086-10103.

[82] Blidi Yang and Amiya nayak, "Anonymous and lighweight authentication for secure Vehicular Networks." In: IEEE Transactions on Vehicular technology journal, Volume: 66, Issue: 12, pp 10626-10636 (24 August 2017).

[83] VASUDEV, Harsha et DAS, Debasis. P2-SHARP: privacy preserving secure hash based authentication and revelation protocol in IoVs. Computer Networks, 2021, vol. 191, p. 107989.

[84] VIGHNESH, N. V., KAVITA, N., URS, Shalini R., et al. A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks. In : 2011 IEEE Symposium on Wireless Technology and Applications (ISWTA). IEEE, 2011. p. 96-101.

[85] CHAUDHRY, Shehzad Ashraf. Combating identity de-synchronization: An improved lightweight symmetric key based authentication scheme for IoV. 2021.

[86] GOUMIDI, Hadjer, HAROUS, Saad, ALIOUAT, Zibouda, et al. Lightweight secure authentication and key distribution scheme for vehicular cloud computing. Symmetry, 2021, vol. 13, no 3, p. 484.

[87] TAN, Hengchuan, MA, Maode, LABIOD, Houda, et al. A secure and authenticated key management protocol (SA-KMP) for vehicular networks. IEEE Transactions on Vehicular Technology, 2016, vol. 65, no 12, p. 9570-9584.

[88] CHUANG, Ming-Chin et LEE, Jeng-Farn. TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks. IEEE systems journal, 2013, vol. 8, no 3, p. 749-758.

[89] KANUMALLI, Satya Sandeep, CH, Anuradha, et MURTY, Patanala Sri Rama Chandra. Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach. International Journal of Advanced Computer Science and Applications, 2020, vol. 11, no 1.

[90] HAMMER, Johs Hansen et SCHNEIDER, Gerardo. On the definition and policies of confidentiality. In : Third International Symposium on Information Assurance and Security. IEEE, 2007. p. 337-342.

[91] SHARON, S., SURIYA PRABA, T., ANUSHIADEVI, R., et al. Privacy-preserving authentication scheme using reduced-advanced encryption standard for vehicular ad hoc network. In : Applications and Techniques in Information Security: 10th International Conference, ATIS 2019, Thanjavur, India, November 22–24, 2019, Proceedings 10. Springer Singapore, 2019. p. 254-265.

[92] SELVI, Muthukumar et RAMAKRISHNAN, B. Prioritized and secured data dissemination technique in VANET based on optimal blowfish algorithm and signcryption method. International Journal of Computer Networks and Applications (IJCNA), 2015, vol. 2, no 4, p. 165-172.

[93] SELVI, M. et RAMAKRISHNAN, B. Secured message broadcasting in VANET using blowfish algorithm with oppositional deer hunting optimization. International Journal of Computer Network and Information Security, 2021, vol. 13, no 2, p. 39.

[94] ROY, Debasish et DAS, Prodipto. A modified RSA cryptography algorithm for security enhancement in vehicular ad hoc networks. In : Proceedings of the International Conference on Computing and Communication Systems: I3CS 2016, NEHU, Shillong, India. Springer Singapore, 2018. p. 641-653.

[95] SHEKHAR MONDAL, Himadri, TARIQ HASAN, Md, MAHBUB HOSSAIN, Md, et al. A RSA-based efficient dynamic secure algorithm for ensuring data security. In : Proceedings of International Joint Conference on Computational Intelligence: IJCCI 2018. Springer Singapore, 2020. p. 643-653.

[96] CHEN, Chin-Ling, CHIANG, Mao-Lun, PENG, Chun-Cheng, et al. A secure mutual authentication scheme with non-repudiation for vehicular ad hoc networks. International Journal of Communication Systems, 2017, vol. 30, no 6, p. e3081.

[97] LI, Jie, LU, Huang, et GUIZANI, Mohsen. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE transactions on parallel and distributed systems, 2014, vol. 26, no 4, p. 938-948.

[98] BRADAI, Amira et AFIFI, Hossam. A framework using IBC achieving non-repudiation and privacy in vehicular network. In : 2011 Conference on Network and Information Systems Security. IEEE, 2011. p. 1-6.

[99] HEGDE, Nayana et MANVI, Sunilkumar S. Thesis Proposal Summary: Key Management Authentication and Non Repudiation for Information Transaction in Vehicular Cloud Environments. In : 2016 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM). IEEE, 2016. p. 157-160.

[100] PREMA, N. K. Efficient secure aggregation in VANETs using fully homomorphic encryption (FHE). Mobile Networks and Applications, 2019, vol. 24, no 2, p. 434-442.

[101] HORNG, Shi-Jinn, LU, Cheng-Chung, et ZHOU, Wanlei. An identity-based and revocable data-sharing scheme in VANETs. IEEE Transactions on Vehicular Technology, 2020, vol. 69, no 12, p. 15933-15946.

[102] VIVEK SRIDHAR MALLYA, P. V., AJITH, Aparna, SANGEETHA, T. R., et al. Implementation of differential privacy using Diffie–Hellman and AES algorithm. In: Inventive Communication and Computational Technologies: Proceedings of ICICCT 2019. Springer Singapore, 2020. p. 143-152.

[103] LUO, Jingtang, YAO, Shiying, ZHANG, Jiamin, et al. A secure and anonymous communication scheme for charging information in vehicle-to-grid. IEEE Access, 2020, vol. 8, p. 126733-126742.

[104] LIU, Xinxin, JIA, Zhijuan, XU, Erfeng, et al. A privacy protection scheme in vanets based on group signature. In : Trusted Computing and Information Security: 12th Chinese Conference, CTCIS 2018, Wuhan, China, October 18, 2018, Revised Selected Papers 12. Springer Singapore, 2019. p. 286-300.

[105] AFTAB, Muhammad Usman, HUSSAIN, Mehdi, LINDGREN, Anders, et al. Towards a distributed ledger based verifiable trusted protocol for VANET. In : 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2). IEEE, 2021. p. 1-6.

[106] ELKHALIL, Ahmed, ZHANG, Jiashu, et ELHABOB, Rashad. An efficient heterogeneous blockchain-based online/offline signcryption systems for internet of vehicles. Cluster Computing, 2021, p. 1-18.

[107] ABHISHEK, Nalam Venkata, AMAN, Muhammad Naveed, LIM, Teng Joon, et al. Drive: Detecting malicious roadside units in the internet of vehicles with low latency data integrity. IEEE Internet of Things Journal, 2021, vol. 9, no 5, p. 3270-3281.

[108] SUMRA, Irshad Ahmed, HASBULLAH, Halabi Bin, et al. Effects of attackers and attacks on availability requirement in vehicular network: a survey. In : 2014 International Conference on Computer and Information Sciences (ICCOINS). IEEE, 2014. p. 1-6.

[109] ZHENG, Qiang, ZHENG, Kan, ZHANG, Haijun, et al. Delay-optimal virtualized radio resource scheduling in software-defined vehicular networks via stochastic learning. IEEE Transactions on Vehicular Technology, 2016, vol. 65, no 10, p. 7857-7867.

[110] FENG, Zhenni, ZHU, Yanmin, ZHANG, Qian, et al. Exploiting network coding for data availability in vehicular networks: Issues and Opportunities. In : 2012 8th International Conference on Mobile Ad-hoc and Sensor Networks (MSN). IEEE, 2012. p. 24-30.

[111] CHUKWUDI, Isinka Joseph, ZAMAN, Nafees, RAHIM, Md Abdur, et al. An Ensemble Deep Learning Model for Vehicular Engine Health Prediction. IEEE Access, 2024, vol. 12, p. 63433-63451.

[112] SONG, Wenjie, YANG, Yi, FU, Mengyin, et al. Real-time obstacles detection and status classification for collision warning in a vehicle active safety system. IEEE Transactions on intelligent transportation systems, 2017, vol. 19, no 3, p. 758-773.

[113] QURESHI, Kashif Naseer, SHAHZAD, Luqman, ABDELMABOUD, Abdelzahir, et al. A blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the internet of vehicles. Applied Sciences, 2022, vol. 12, no 1, p. 476.

[114] Cui, Jie, Wenyu Xu, Hong Zhong, Jing Zhang, Yan Xu, and Lu Liu. 2018. "Privacy-Preserving Authentication Using a Double Pseudonym for Internet of Vehicles" Sensors, vol. 18, no 5, p. 1453

[115] Abdus Samad, Shadab Alam, Mohammed Shuaib and Mohammed Ubaidullah Bokhari., "Internet of vehicles (IoV) Requirements, attacks and Countermeasures." In : Proceedings of 12th INDIACom; INDIACom-2018; 5th international conference on "computing for sustainable global development" IEEE conference, New Delhi. (14th – 16th March 2018). p. 1-4.

[116] HAMDI, Mustafa Maad, DHAFER, Majeed, MUSTAFA, Ahmed Shamil, et al. Effect Sybil attack on security Authentication Service in VANET. In : 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2022. p. 1-6

[117] KHALIL, Mohamed et AZER, Marianne A. Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks. In : 2018 Wireless Days (WD). IEEE, 2018. p. 184-186.

[118] LI, Jiangtao, SONG, Zhaoheng, LI, Yufeng, et al. Trajectory as an identity: Privacy-preserving and Sybil-resistant authentication for Internet of vehicles. Security and Communication Networks, 2021, vol. 2021, p. 1-10.

[119] FERRAG, Mohamed Amine, MAGLARAS, Leandros A., JANICKE, Helge, et al. Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks, 2017, vol. 2017. no 1, p. 6562953.

[120] Mauro Conti, Nicola Dragoni and Viktor Lesyek, "A Survey of Man in nthe Middle Attacks." In: IEEE Communication Surveys and Tutorials Journal, Volume: 18, Issue: 3, pp 2027-2051 (29 March 2016).

[121] LI, Lun, LIU, Jiqiang, CHENG, Lichen, et al. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Transactions on Intelligent Transportation Systems, 2018, vol. 19, no 7, p. 2204-2220.

[122] KHALID, Haqi, HASHIM, Shaiful Jahari, AHMAD, Sharifah Mumtazah Syed, et al. New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles. In : 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, 2020. p. 1-7.

[123] MILLER, Victor S. Use of elliptic curves in cryptography. In : Conference on the theory and application of cryptographic techniques. Berlin, Heidelberg : Springer Berlin Heidelberg, 1985. p. 417-426.

[124] KOBLITZ, Neal. Elliptic curve cryptosystems. Mathematics of computation, 1987, vol. 48, no 177, p. 203-209.

[125] OMONDI, Amos R. et R OMONDI, Amos. Elliptic-Curve Basics. Cryptography Arithmetic: Algorithms and Hardware Architectures, 2020, p. 225-241.

[126] PRENEEL, Bart, VERBAUWHEDE, Ingrid, et BATINA, Lejla. Arithmetic and Architectures for Secure Hardware Implementations of Public-Key Cryptography. 2005. doctoral thesis. Leuven

[127] NIMBHORKAR, Sonali U. et MALIK, L. G. A survey on elliptic curve cryptography (ECC). International Journal of Advanced Studies in Computers, Science and Engineering, 2012, vol. 1, no 1, p. 1-5.

[128] AMARA, Moncef et SIAD, Amar. Elliptic curve cryptography and its applications. In: International workshop on systems, signal processing and their applications, WOSSPA. IEEE, 2011. p. 247-250.

[129] SUN, Jinyuan, ZHANG, Chi, ZHANG, Yanchao, et al. An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Transactions on Parallel and Distributed Systems, 2010, vol. 21, no 9, p. 1227-1239.

[130] ZHANG, Lei. OTIBAAGKA: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 2017, vol. 12, no 12, p. 2998-3010.

[131] XIONG, Hu, ZHU, Guobin, CHEN, Zhong, et al. Efficient communication scheme with confidentiality and privacy for vehicular networks. Computers & Electrical Engineering, 2013, vol. 39, no 6, p. 1717-1725.

[132] KANG, Qian, LIU, Xuejiao, YAO, Yiyang, et al. Efficient authentication and access control of message dissemination over vehicular ad hoc network. Neurocomputing, 2016, vol. 181, p. 132-138.

[133] MEJRI, Mohamed Nidhal. Securing vehicular networks against denial of service attacks. 2016. Thèse de doctorat. Université Sorbonne Paris Cité; École nationale d'ingénieurs de Tunis (Tunisie).

[134] HUANG, Xumin, YU, Rong, PAN, Miao, et al. Secure roadside unit hotspot against eavesdropping based traffic analysis in edge computing based internet of vehicles. IEEE Access, 2018, vol. 6, p. 62371-62383.

[135] MIRZAEE, Siavash et JIANG, Letian. Fast confidentiality-preserving authentication for vehicular ad hoc networks. Journal of Shanghai Jiaotong University (Science), 2019, vol. 24, p. 31-40.

[136] SUMRA, Irshad Ahmed, HASBULLAH, Halabi Bin, et ABMANAN, Jamalul-lail Bin. Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey. In: Vehicular Ad-hoc Networks for Smart Cities: First International Workshop, 2014. Singapore: Springer Singapore, 2014. p. 51-61.

[137] PENG, Xiong. A novel authentication protocol for vehicle network. In : 2016 3rd International Conference on Systems and Informatics (ICSAI). IEEE, 2016. p. 664-668.

[138] KRISHNA, A. Mohan et TYAGI, Amit Kumar. Intrusion detection in intelligent transportation system and its applications using blockchain technology. In : 2020 international conference on emerging trends in information technology and engineering (IC-ETITE). IEEE, 2020. p. 1-8.

[139] SHIH, Chi-Sheng, HSIEH, Wei-Yu, et KAO, Chia-Lung. Traceability for Vehicular Network Real-Time Messaging Based on Blockchain Technology. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 2019, vol. 10, no 4, p. 1-21.

[140] WANG, Fei, XU, Yongjun, ZHANG, Hanwen, et al. 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Transactions on Vehicular Technology, 2015, vol. 65, no 2, p. 896-911.

[141] VERMA, Amandeep, SAHA, Rahul, KUMAR, Gulshan, et al. The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions. Applied Sciences, 2021, vol. 11, no 10, p. 4682.

[142] RATHORE, Heena, SAMANT, Abhay, et JADLIWALA, Murtuza. TangleCV: A distributed ledger technique for secure message sharing in connected vehicles. ACM Transactions on Cyber-Physical Systems, 2020, vol. 5, no 1, p. 1-25.

[143] MALIK, Abdul, KHAN, Muhammad Zahid, FAISAL, Mohammad, et al. An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. Sensors, 2022, vol. 22, no 5, p. 1897.

[144] MITRA, Saptarshi, JANA, Bappaditya, et PORAY, Jayanta. A novel scheme to detect and remove black hole attack in cognitive radio vehicular ad hoc networks (CR-VANETs). In: 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE). IEEE, 2016. p. 1-5.

[145] TOBIN, John, THORPE, Christina, et MURPHY, Liam. An approach to mitigate black hole attacks on vehicular wireless networks. In : 2017 IEEE 85th vehicular technology conference (VTC Spring). IEEE, 2017. p. 1-7.

[146] FUNDERBURG, L. Ellen, REN, Huimin, et LEE, Im-Yeong. Pairing-free signatures with insider-attack resistance for vehicular ad-hoc networks (VANETs). IEEE Access, 2021, vol. 9, p. 159587-159597.

[147] GUO, Jinhua, BAUGH, John P., et WANG, Shengquan. A group signature based secure and privacy-preserving vehicular communication framework. In : 2007 Mobile Networking for Vehicular Environments. IEEE, 2007. p. 103-108.

[148] Nai-Wei lo, Hsiao-Chien Tsai, “Illusion Attack on VANET Applications – A Message Plausibility Problem" , IEEE Globecom Workshops, pp.1- 8, 2007.

[149] DHURANDHER, Sanjay K., OBAIDAT, Mohammad S., JAISWAL, Amrit, et al. Vehicular security through reputation and plausibility checks. IEEE Systems Journal, 2013, vol. 8, no 2, p. 384-394.

[150] TAIE, Shereen A. et TAHA, Sanaa. A novel secured traffic monitoring system for VANET. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2017. p. 176-182.

[151] ROY, Ayan et MADRIA, Sanjay. Distributed incentive-based secured traffic monitoring in vanets. In : 2020 21st IEEE International Conference on Mobile Data Management (MDM). IEEE, 2020. p. 49-58.

[152] ALSULAIM, Noura Adel, ALOLAQI, Raghad Abdullah, et ALHUMAIDAN, Reem Yaseen. Proposed solutions to detect and prevent DoS attacks on VANETs system. In : 2020 3rd international conference on computer applications & information security (ICCAIS). IEEE, 2020. p. 1-6.

[153] BIRON, Zoleikha Abdollahi, DEY, Satadru, et PISU, Pierluigi. Real-time detection and estimation of denial of service attack in connected vehicle systems. IEEE Transactions on Intelligent Transportation Systems, 2018, vol. 19, no 12, p. 3893-3902.

[154] VERMA, Amandeep, SAHA, Rahul, KUMAR, Gulshan, et al. PREVIR: Fortifying Vehicular Networks against Denial of Service Attacks. IEEE Access, 2024, vol. 12, p. 48301-48320.

[155] SHABBIR, Munazza, KHAN, Muazzam A., KHAN, Umair Shafiq, et al. Detection and prevention of distributed denial of service attacks in VANETs. In : 2016 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2016. p. 970-974.

[156] AL-SHAREEDA, Mahmood A. et MANICKAM, Selvakumar. Msr-dos: Modular square root-based scheme to resist denial of service (dos) attacks in 5g-enabled vehicular networks. IEEE Access, 2022, vol. 10, p. 120606-120615.

[157] ALHARTHI, Abdullah, NI, Qiang, et JIANG, Richard. A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. Ieee Access, 2021, vol. 9, p. 87299-87309.

[158] CHALLA, Sravani, WAZID, Mohammad, DAS, Ashok Kumar, et al. Secure signature-based authenticated key establishment scheme for future IoT applications. Ieee Access, 2017, vol. 5, p. 3028-3043.

[159] AMIN, Ruhul, ISLAM, SK Hafizul, BISWAS, G. P., et al. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Generation Computer Systems, 2018, vol. 80, p. 483-495.

[160] SIERRA, José M., HERNÁNDEZ, Julio C., ALCAIDE, Almudena, et al. Validating the Use of BAN LOGIC. In : International conference on computational science and its applications. Berlin, Heidelberg : Springer Berlin Heidelberg, 2004. p. 851-858.

[161] EINARSSON, Atli F., PATREKSSON, Patrekur, HAMDAQA, Mohammad, et al. SmarthomeML: Towards a domain-specific modeling language for creating smart home applications. In : 2017 IEEE International Congress on Internet of Things (ICIOT). IEEE, 2017. p. 82-88.

[162] SHCHERBINA, Anna, MATTSSON, C. Mikael, WAGGOTT, Daryl, et al. Accuracy in wrist-worn, sensor-based measurements of heart rate and energy expenditure in a diverse cohort. Journal of personalized medicine, 2017, vol. 7, no 2, p. 3.

[163] SONGKRAM, Noawanit. Virtual smart classroom to enhance 21 st century skills in learning and innovation for higher education learners. In : 2017 Tenth international conference on mobile computing and ubiquitous network (ICMU). IEEE, 2017. p. 1-4.

[164] CHOI, Baek-Young, SONG, Sejun, et ZAMAN, Rafida. Smart Education: Opportunities and challenges induced by COVID-19 pandemic:[A survey-based study]. In : 2020 IEEE International Smart Cities Conference (ISC2). IEEE, 2020. p. 1-8.

[165] ISLAM, Monjurul, MAZLAN, Nurul Hijja, AL MURSHIDI, Ghadah, et al. UAE university students' experiences of virtual classroom learning during Covid 19. Smart Learning Environments, 2023, vol. 10, no 1, p. 5.

[166] MAITI, Monica, PRIYAADHARSHINI, M., et VINAYAGA SUNDARAM, B. Augmented reality in virtual classroom for higher education during COVID-19 pandemic. In : Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3. Springer International Publishing, 2021. p. 399-418.

[167] DHAL, Shraddha, SAMANTARAY, Swati, et SATAPATHY, Suresh Chandra. From chalk boards to smart boards: An integration of IoT into educational environment during Covid-19 pandemic. In : Intelligent Data Engineering and Analytics: Proceedings of the 9th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA 2021). Singapore : Springer Nature Singapore, 2022. p. 301-309.

[168] AL-QIRIM, Nabeel, MESMARI, Ahlam, MAZROEEI, Khawlah, et al. Developing teaching scenarios in the classroom using interactive smart board ecosystem. In : 4th IEEE International Conference on Digital Ecosystems and Technologies. IEEE, 2010. p. 525-530.

[169] AMIN, Samina, UDDIN, M. Irfan, MASHWANI, Wali Khan, et al. Developing a personalized E-learning and MOOC recommender system in IoT-enabled smart education. IEEE Access, 2023, vol. 11, p. 136437-136455.

[170] KEPUSKA, Veton et BOHOUTA, Gamal. Next-generation of virtual personal assistants (microsoft cortana, apple siri, amazon alexa and google home). In : 2018 IEEE 8th annual computing and communication workshop and conference (CCWC). IEEE, 2018. p. 99-103.

[171] MTSHALI, Progress et KHUBISA, Freedom. A smart home appliance control system for physically disabled people. In : 2019 Conference on Information Communications Technology and Society (ICTAS). IEEE, 2019. p. 1-5.

[172] PENG, Chen-Yen et CHEN, Rung-Chin. Voice recognition by Google Home and Raspberry Pi for smart socket control. In : 2018 Tenth International Conference on Advanced Computational Intelligence (ICACI). IEEE, 2018. p. 324-329.

[173] SAHBI, Roumissa, GHANEMI, Salim, et FERRAG, Mohamed Amine. Security of internet of vehicles in smart cities: authentication and confidentiality aspects. International Journal of Internet Technology and Secured Transactions, 2024, vol. 13, no 3, p. 232-269.

[174] BURROWS, Michael, ABADI, Martin, et NEEDHAM, Roger. A logic of authentication. ACM Transactions on Computer Systems (TOCS), 1990, vol. 8, no 1, p. 18-36.

[175] XU, Guishuang, YIN, Xinchun, et LI, Xincheng. Lightweight and Secure Multi-Message Multi-Receiver Certificateless Signcryption Scheme for the Internet of Vehicles. Electronics, 2023, vol. 12, no 24, p. 4908.

[176] SHARMA, Nishant, CHAUHAN, Naveen, et CHAND, Narottam. Security challenges in Internet of Vehicles (IoV) environment. In : 2018 first international conference on secure cyber computing and communication (ICSCCC). IEEE, 2018. p. 203-207.

[177] JAHROMI, Hamed Z. et DELANEY, Declan T. An application awareness framework based on SDN and machine learning: Defining the roadmap and challenges. In : 2018 10th international conference on communication software and networks (ICCSN). IEEE, 2018. p. 411-416.

[178] HAKIMI, Arif, YUSOF, Kamaludin Mohamad, AZIZAN, Muhammad Afizi, et al. A survey on internet of vehicle (iov): A pplications & comparison of vanets, iov and sdn-iov. ELEKTRIKA-Journal of Electrical Engineering, 2021, vol. 20, no 3, p. 26-31.

[179] SINGH, Ashutosh Kumar et SRIVASTAVA, Shashank. A survey and classification of controller placement problem in SDN. International Journal of Network Management, 2018, vol. 28, no 3, p. e2018.