Software Requirement Specification Document for Certificateless Signcryption Scheme for Securing Internet of Vehicles

Kirollos Emad, Omar Maged, Adham Ahmed, Mariam Khaled
Supervised by: Dr. Sahar Abdelrahman, Eng. Mohamed khaled

April 8, 2024

Table 1: Document version history

Version	Date	Reason for Change
1.0	9-Jan-2024	SRS First version's specifications are defined.
1.1	11-Jan-2024	abstract modifications added more details to the problem statement section .
1.2	12-Jan-2024	busniess context updated
1.3	13-Jan-2024	System overview was modified
1.4	14-Jan-2024	Use case and Class diagram modified

GitHub: https://github.com/kirollos2009063/Certificateless-Signcryption-Scheme-for-Securing-Internet-of-V

Contents

Abstract

The operational basis of the Internet of Vehicles (IoV) is made up of vehicular ad hoc networks, or VANETs, which allow cars to act as networked nodes on the open Internet. Nonetheless, IoV is still susceptible to security risks including impersonation and illegal access to private data. . This paper aims to strengthen the security architecture of IoV by analyzing and improving different algorithms, with a particular focus on elliptic curve algorithms.The goal is to strengthen IoV against new threats in this dynamic vehicle network, making sure that security breaches are prevented and that resilience is increased.

1 Introduction

1.1 Purpose of this document

This document outlines the goals, requirements, and development processes for this project. Furthermore , it serves as a roadmap for the developers delivering insights into the software implementation methodologies vital to reinforcing the security architecture of Vehicular Ad Hoc Networks (VANETs) inside the Internet of Vehicles (IoV). This document is to guide the development team toward the effective fulfillment of our project goals by outlining the essential features and standards, guaranteeing a reliable and secure Internet of Vehicles environment.

1.2 Scope of this document

This document explores the details of the "Certificateless Signcryption Scheme for Securing Internet of Vehicles." It offers a perceptive examination of systems similar to our project, highlighting the overview, extent, and background of our system design. The goals of our research, which are centered on improving security in the Internet of Vehicles (IoV) Vehicular Ad Hoc Networks (VANETs), are explained, and the features of the expected users are explored. It also includes a detailed description of our Certificateless Signcryption Scheme's functional and nonfunctional requirements, design constraints, and fundamental class diagram. In overall, we consider operational scenarios that provide insight into our system's possible practical uses. The last section of the document presents a time plan that outlines the expected milestones and schedule for the creation and implementation of the "Certificateless Signcryption Scheme for Securing Internet of Vehicles."

1.3 Business Context [1]

Regarding the "Certificateless Signcryption Scheme for Securing Internet of Vehicles," our project is a valuable resource for companies who have a significant involvement in vehicle operations , Through the reinforcement of the security architecture in Vehicular Ad Hoc Networks (VANETs), this project creates a strong barrier that protects critical vehicle communication. Our initiative, which is the only one of its kind in this field, offers new results that will increase operational dependability and trustworthiness. Considering the significance of security in the market, our project takes a leading position by providing incomparable security measures that directly improve the effectiveness and safety of vehicle operations, therefore improving the market for vehicular

security.In the context of future plans to construct smart nations, our project is critical in guaranteeing safe communication channels between vehicles, traffic control systems, police stations, and hospitals. This strong security architecture helps to protect the integrity and confidentiality of interactions among these important components of smart villages, which improves overall security measures.

2 Similar Systems

2.1 Academic

2.1.1 A Secure Authentication Protocol for Internet of Vehicles [2]

In internet of vehicles (IoV) vehicles share messages among themselves ,but the way they share data isn't safe , so it's important to find a way to verify their identities in order to protect the driver's privacy , The researchers found weaknesses in an authentication protocol that was already in place and that was suggested for IoV by Ying et al. consisting of vulnerability to replay attacks, location spoofing, offline identity guessing, and inefficient authentication times , so they decided to address these issues and enhance the authentication protocol to improve security and performance.The researchers focused on comparing their patched protocol with related protocols by comparing the performance and storage costs they reached that their patched protocol is more secure and efficient .One of the key drawbacks of this paper is that they didn't use any data sets or simulation tools for validation or testing

2.1.2 Cryptographic Solution-Based Secure Elliptic Curve Cryptography Enabled Radio Frequency Identification Mutual Authentication Protocol for Internet of Vehicles: [3]

The paper focuses on addressing the security and privacy concerns related to RFID technology in IoV by proposing a secure authentication protocol To provide increased security in the Internet of Vehicles (IoV), the researchers proposed a secure RFID authentication system using Elliptic-Curve Cryptography (ECC). Through AVISPA tool simulations, they verified this protocol, demonstrating its resistance to different types of assaults and reduced computing expenses in comparison to other approaches. To further strengthen the overall security of the IoV network, they also built a revolutionary Blockchain-based security framework. The paper's findings demonstrate how well the suggested ECC-enabled RFID authentication protocol handles security issues with the Internet of Vehicles (IoV). Based on ECC-based lightweight operations, AVISPA simulations confirm that the protocol achieves Mutual Authentication, Availability, and protection against security risks including DoS, Replays, and Cloning Attacks. To further strengthen IoV network security, the study also presents a blockchain-based security architecture that estimates the network's expansion in terms of transactions over time , this paper needs the suggested blockchain-based security framework to be put into practice and the assessment of the framework's performance

2.1.3 RTED-SD: A Real-Time Edge Detection Scheme for Sybil DDoS in the Internet of Vehicles: [4]

The Sybil Denial of Service (DoS) Attack is considered to be one of the biggest obstacles to the security of the Internet of Vehicles it involves fake identities flooding system and disrupting essential services , the advancement they made to solve this issue involves Entropy theory is used to Sybil DDoS detection in IoV, a real-time deviation detection algorithm is developed, and a tem-

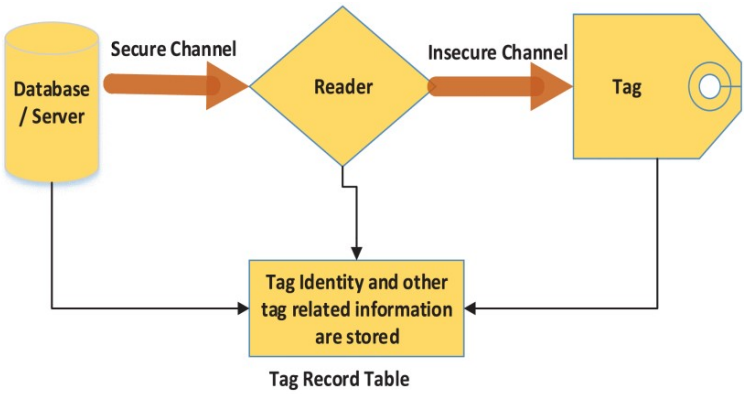

Figure 1: Primary components of RFID system

poral index is introduced to assess detection algorithms in IoV. The researchers used a simulation tool F2MD and various data-sets :

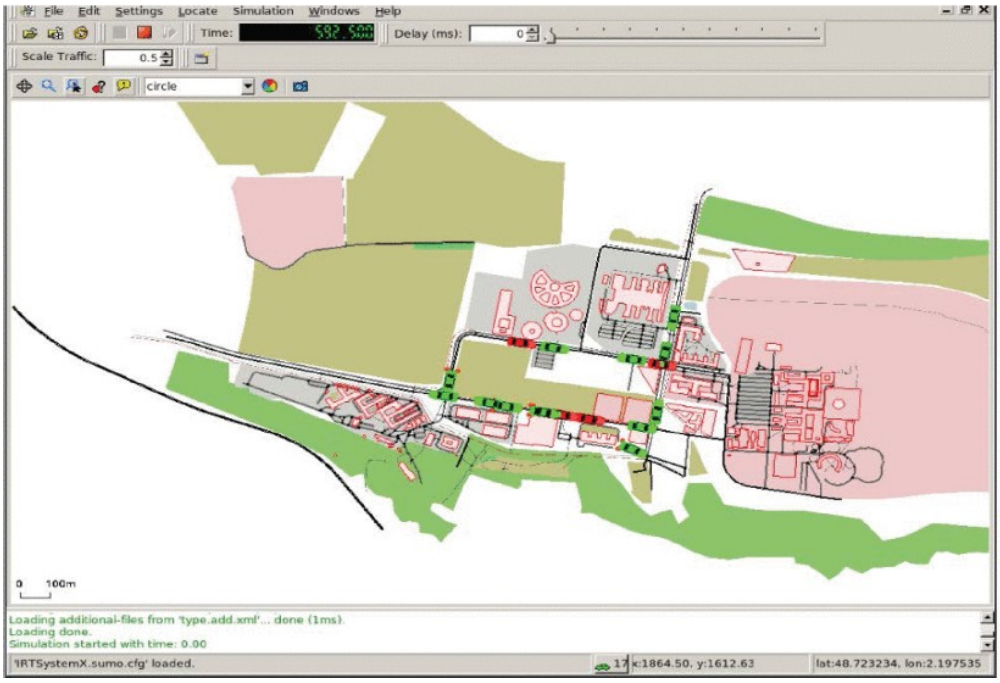

Figure 2: The F2MD Sybil DDoS simulation

Dataset	Attack Occur Index (number)	Attack Occur Time (s)	w	k	Alarm Index (number)	Alarm Time (s)	**Alarm Delay (s)**	Sliding Window Start Time (s)	Sliding Window Duration (s)	**TFOR (%)**
1	40007	25207.89177	15	5	40058	25223.186332	**15.294559**	24907.813790	315.372542	**4.8497%**
			15	4	40043	25213.186332	**5.294559**	24903.830426	309.355906	**1.7115%**
			10	5	40041	25212.902349	**5.010576**	24903.813790	309.088559	**1.6211%**
			10	4	40031	25211.891773	**4.000000**	24903.505428	308.386345	**1.2971%**
			5	5	40018	25210.186332	**2.294559**	24902.875142	307.311190	**0.7467%**
			5	4	40013	25209.391773	**1.500000**	24902.813790	306.577983	**0.4893%**
2	40001	28800.00998	15	5	40034	28807.370778	**7.360797**	28586.466523	220.904255	**3.3321%**
			15	4	40019	28805.227412	**5.217431**	28586.130745	219.096667	**2.3813%**
			10	5	40021	28805.509981	**5.500000**	28586.209806	219.300175	**2.5080%**
			10	4	40011	28803.370778	**3.360797**	28585.914162	217.456616	**1.5455%**
			5	5	40016	28804.509981	**4.500000**	28586.121505	218.388476	**2.0605%**
			5	4	40011	28803.370778	**3.360797**	28585.914162	217.456616	**1.5455%**
3	40002	50404.62356	15	5	40047	50413.602763	**8.979199**	50105.876584	307.726179	**2.9179%**
			15	4	40032	50412.087129	**7.463565**	50105.150275	306.936854	**2.4316%**
			10	5	40027	50411.087129	**6.463565**	50104.708453	306.378676	**2.1097%**
			10	4	40017	50409.087129	**4.463565**	50104.264428	304.822701	**1.4643%**
			5	5	40016	50408.623564	**4.000000**	50104.258284	304.365280	**1.3142%**
			5	4	40011	50407.623564	**3.000000**	50103.998904	303.624660	**0.9881%**
4	40001	54004.84526	15	5	40018	54010.845264	**6.000000**	53341.680349	669.164915	**0.8966%**
			15	4	40003	54005.845264	**1.000000**	53340.541266	665.303998	**0.1503%**
			10	5	40012	54008.845264	**4.000000**	53341.355652	667.489612	**0.5993%**
			10	4	40002	54005.345264	**0.500000**	53340.515882	664.829382	**0.0752%**
			5	5	40017	54010.345264	**5.500000**	53341.678005	668.667259	**0.8225%**
			5	4	40012	54008.845264	**4.000000**	53341.355652	667.489612	**0.5993%**
Average							**4.919332**			**1.6024%**

Figure 3: TFOR of different Sybil DDoS attacks using FQDC

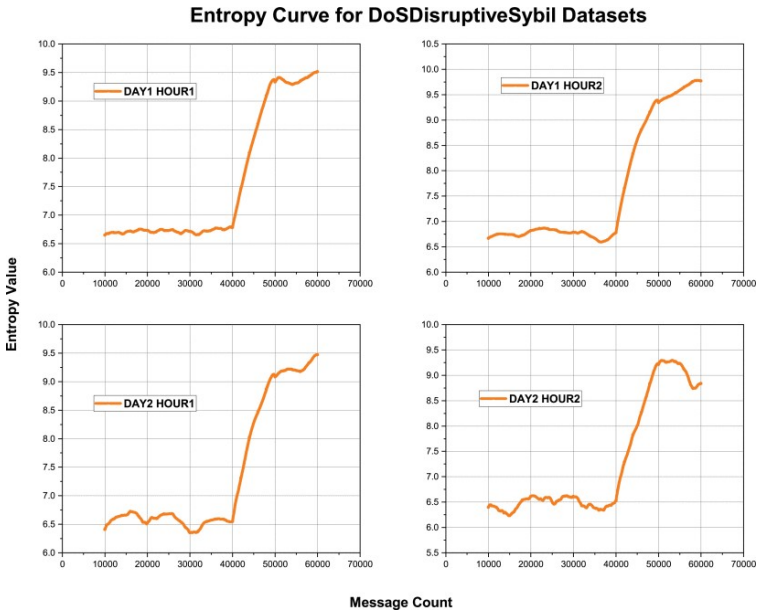

Figure 4: TFOR of different Sybil DDoS attacks using FQDC

Based on their methodologies and evaluation using multiple data sets and the F2MD simulation framework, the researchers revealed: Their simulations showed effective anomalous behavior identification throughout various traffic hours, with a particular preference for Distributed Denial of Service (DDoS) assaults also had the ability to recognize Sybil DDoS attempts and sound an alert for them in an average of 4.9193 seconds after the attacks got underway.While the research does an outstanding job applying their recommended scheme alongside their successful detection conclusions, they could have made a stronger case for the superiority or uniqueness of their scheme via a comparison analysis with other DDoS detection approaches or with modern technologies already in use.

3 System Description

3.1 Problem Statement

1.Key Escrow Vulnerability: Data security and privacy are severely compromised by the cryptographic design that is currently in place. Key escrow is a flaw in traditional cryptography where copies of cryptographic keys are kept by a trusted third party. This situation puts the integrity and confidentiality of the sent data at risk of compromise if the trusted third party is exposed. Unauthorized entities might then be able to access the saved keys.
2.Dynamic Nature of Vehicles: Since cars are always moving, their dynamic nature makes it more difficult to secure communication using conventional digital certificates. since of their large number and ever-changing nature, vehicles require a more flexible and effective security system since it becomes logistically difficult to keep track of so many certificates.
3.Data Integrity and Unauthorized Modification: Malicious actors may attempt to alter data

without authorization during transmission. Maintaining the validity and integrity of data transferred is essential in order to stop illegal changes that might endanger the trustworthiness and security of vehicular communication.

4. (DoS) Vulnerability: Denial of Service (DoS) attacks puts the vehicular communication system at risk of interfering with continuous vehicle-to-vehicle communication and maybe causing defects in the network's general operation.

3.2 System Overview

The system main goal is securing the communication process between vehicles as shown in the figure (5), which is successfully achieved by using certificateless signcryption, generating private and public key for each vehicle using the elliptic curve algorithm. The system will ensure the security (confidentiality, integrity, authenticity) of the transmitted communication between the vehicles.

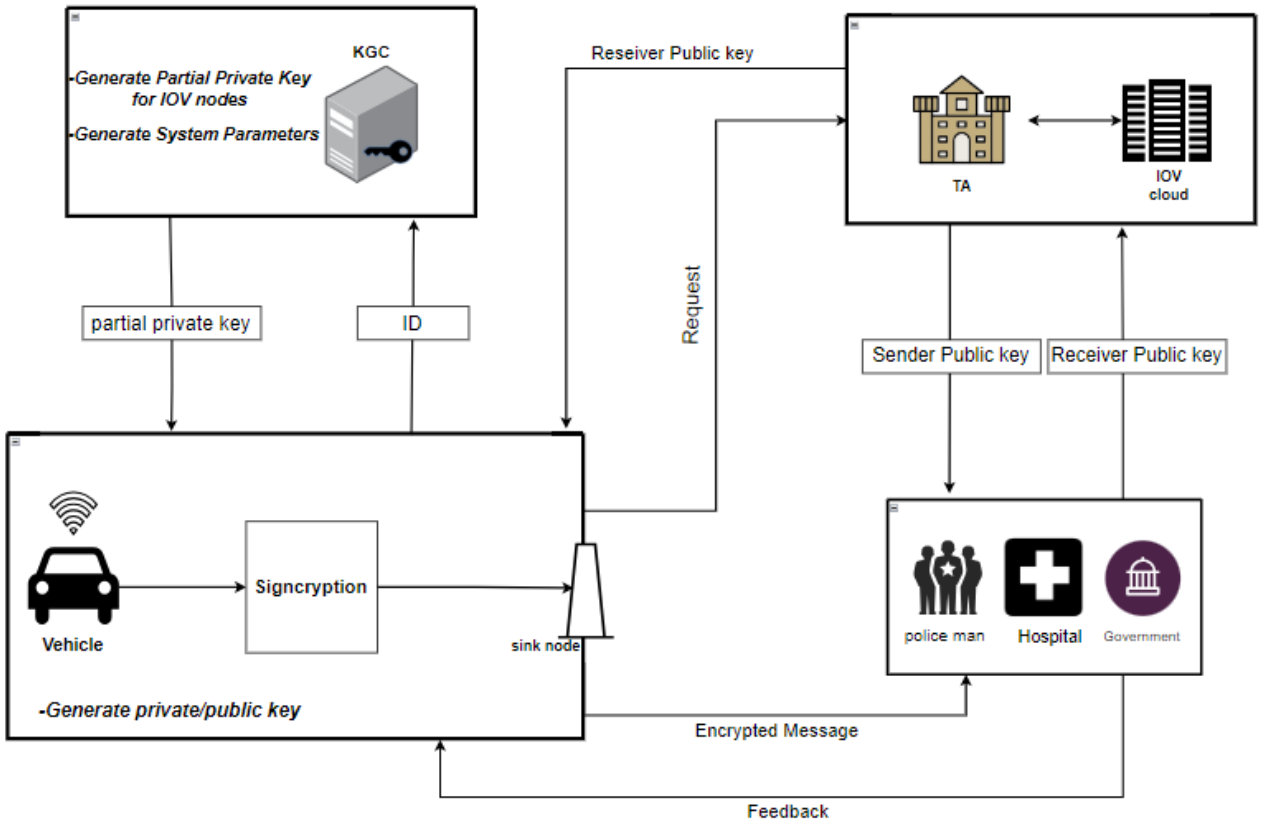

Figure 5: Overview Diagram

3.2.1 Vehicle

The vehicle's safe interaction plays out methodically in the complex movement of the Internet of Vehicles (IoV). To initiate communication, the Vehicle provides the Key Generation Center (KGC)

with its Identification (ID) and (OD). In response, the KGC creates a unique partial private key for the vehicle And the Vehicle generate signcrypted messages .

3.2.2 Key Generation Center

3.2.3 RSU

In the Internet of Vehicles (IoV) network, the Roadside Unit (RSU) plays a vital role as a gateway that connects disparate components in an integrated manner. It establishes itself as a crucial infrastructure element by serving as a main means of facilitating seamless communication between entities inside the Internet of Vehicles. The RSU plays a crucial part in preserving the dependability and effectiveness of the IoV network by accomplishing this and guaranteeing the safe movement of information from one entity to another. Transmitting messages to the intended IoV component, the RSU ensures that the data is successfully and securely sent. Due to its diverse capabilities, which guarantee data security and add to the overall resilience of the IoV, the RSU is positioned as a crucial part of the complex network.

3.2.4 Trust authority (TA)

A mechanism to safely store the public key is started by the vehicle when it creates one. The vehicle talks with the Trusted Authority (TA), delivering the freshly produced public key to be kept in a secure environment within the IoV cloud. A request is then sent to the TA by the car when it uses signcryption and requires the recipient's public key. In order to successfully complete the signcryption process and guarantee the confidentiality and integrity of vehicular communications, the TA serves as a secure key repository and retrieves and sends the necessary public key.

3.3 System Scope

To improve the security of communication in the Internet of Vehicles (IoV), we are committed to developing a sophisticated cryptographic method that solves the key escrow issue and guarantees recipient anonymity, confidentiality, and unforgeability. Our method, which makes use of well-known elliptic curve techniques, is expected to perform better than current approaches in terms of compute and communication expenses. We will use the OMNeT++ simulation program, which is well-known for modeling computer systems and communication networks, to assess the effectiveness and performance of our novel strategy. The context diagram represents the envisioned system context, which captures the complex interactions in the IoV ecosystem. This is a major step towards creating a new standard for safe communication in dynamic vehicular networks.

3.4 System Context

In order to provide secure communication in the Internet of Vehicles (IoV), the Certificateless Signcryption system functions inside a dynamic framework. Vehicles provide plaintext messages and private and public keys to the system in this scenario. Following that, it sends acknowledgements together with the encrypted communications to the cars. Concurrently, vehicles communicate their identity data (ID and OD) to the Key Generation Center (KGC). The KGC, in turn, reacts by delivering a partial key to the vehicle, enabling it to independently construct its unique set of public and

private keys. Within the IoV environment, a reliable and effective mechanism for safe communication is ensured by this complex procedure.The TA obtains and sends the required public key in its function.

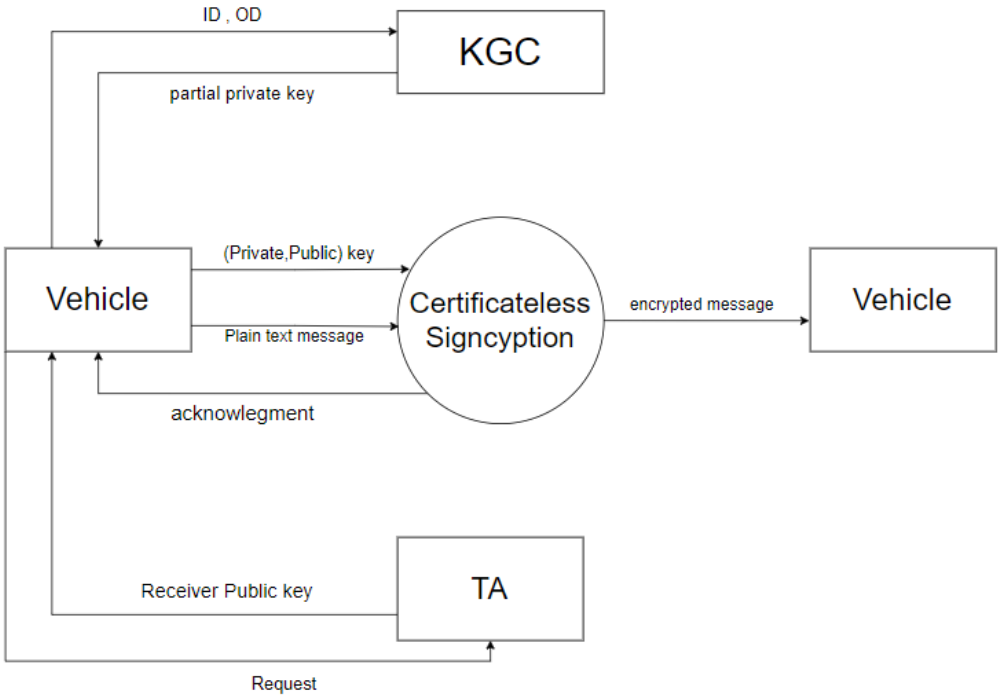

Figure 6: context diagram

3.5 Objectives

• Set up a Channel of Secure Communication
• Ensure the Exchange of Trustworthy Messages.
•Enable smooth communication with the Key Generation Center (KGC) and establish an efficient feedback system.
• Respond to errors or transmission issues with the proper feedback
• Use the Key Generation Center to create and distribute a partial private key.
• Fortify security by ensuring the authenticity of communication entities .

3.6 User Characteristics

• users with varying professional backgrounds, such as engineers, researchers, and administrators, are seeking employment in vehicular networks.
• Drivers and passengers utilizing vehicles connected to the IoV.
• Users interested in secure communication and data exchange within the IoV network.

4 Functional Requirements

4.1 System functions

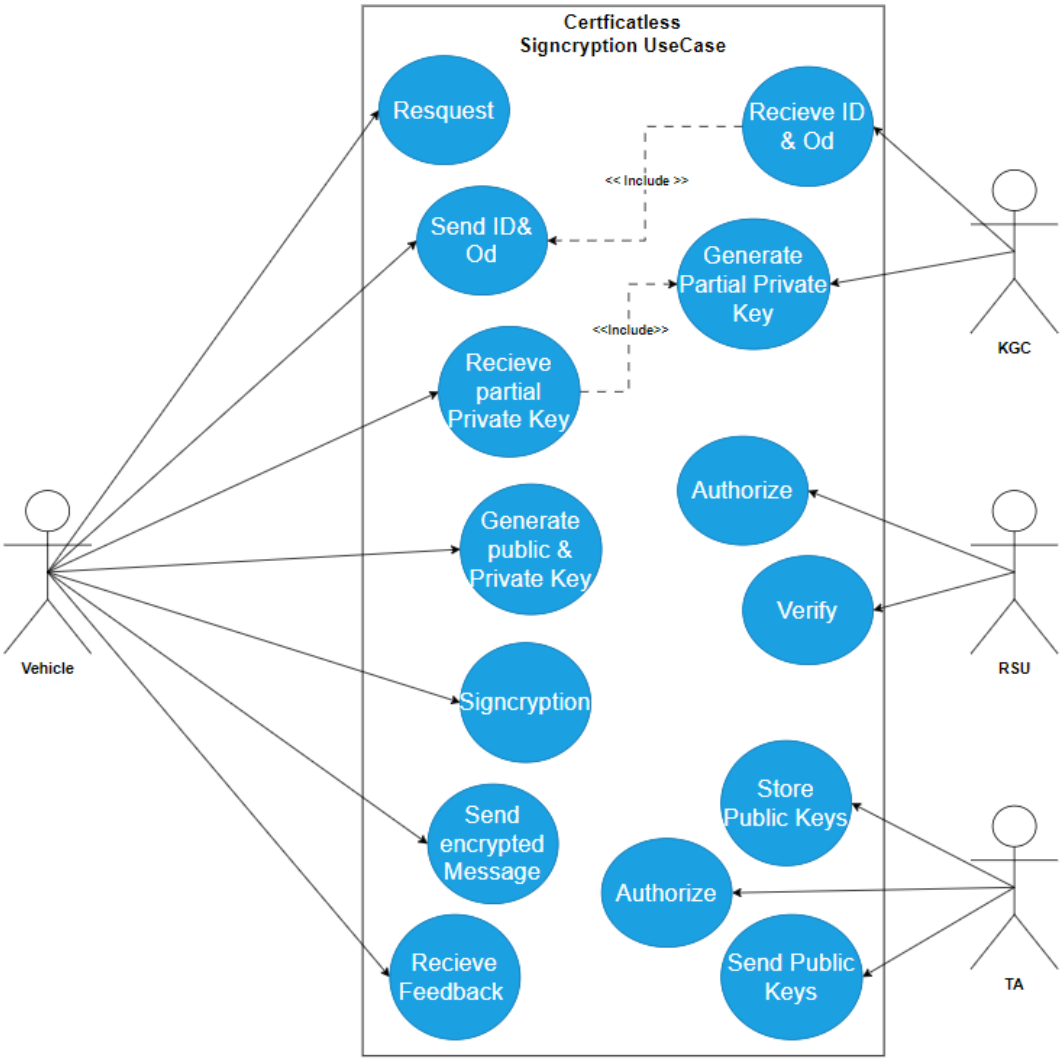

Figure 7: Use Case diagram

ID:1. The TA should securely store the generated public by vehicles through IOV cloud .

ID:2. TA must obtain and provide the recipient's public key in order to facilitate proper signcryption.

ID:3. The KGC will provide a partial private key linked to the ID and Od that was obtained.

ID:4. The KGC will distribute the relevant partial private key for the received ID.

ID:5. The vehicle should sends its ID and OD to the KGC .

ID:6. The vehicle should reach out for secure communication on its own behalf by generating its own private and public key .

ID:7. The vehicle must effectively create signcrypted messages inside the IoV network using public and private keys.
ID:8. The vehicle transmit its identity information(Public ,private key) to the RSU

ID:9. The vehicle should transmits the public keys to the Trusted Authority (TA) for cloud storage.

ID:10. The vehicle "The sender" requests the public key of the intended recipient from the TA.

ID:11. The RSU should make sure that the message is transmitted successfully to the vehicle .

ID:12. The RSU send the partial private key from the kGC to the vehicle .

4.2 Detailed Functional Specification[5]

Table 2: Signcryption process Description

Attribute	Description
Name	Signcryption
Code	ID:7
Priority	High
Critical	During transmission, guarantee that there is secure communication and data integrity.
Description	Using the public and private keys that are supplied, the function will preform signcryption on messages that are received.
Input	To be sign-crypted message Keys: Public, Private.
Output	Signcrypted Message.
Pre-condition	The vehicle signcrypt the message before being transmitted
Post-condition	Successfully signcrypted message ready for safeguarded transmission.
Dependency	Valid messages and accessible public and private keys are prerequisites for the Signcryption Process.
Risk	disrupted connection.

Table 3: Generate partial private key

Attribute	Description
Name	Generate partial private key
Code	ID:3
Priority	High
Critical	Generate partial private keys for users.
Description	The KGC will produce an equivalent partial private key to the user to make his own private and public key .
Input	User ID,Od
Output	partial Private key
Pre-condition	The Key Generation Center provided the system with an authenticated user ID.
Post-condition	The user ID-associated partial private key have been successfully produced.
Dependency	The availability of the Key Generation Center and an authorized user ID.
Risk	If the user ID has been altered or compromised, insecure keys might be generated,which could be risky.A concern during the key generation process might be connection disruptions.

Table 4: Transmitting PPK to the vehicle

Attribute	Description
Name	Transmitting PPK to the vehicle
Code	ID:12
Priority	High
Critical	Enabling the vehicle to generate its public key and private key
Description	The KGC generate the partial private key using some of elliptic curve functionalities then sends it to the vehicle with associated ID
Input	Partial Private Key
Output	Successfully assigning the vehicle with its Partial Private Key came from the KGC
Pre-condition	The KGC generate the partial private key of the vehicle
Post-condition	successfully partial private key is received by the intended vehicle to compute its own Keys
Dependency	accuracy partial private key generation function
Risk	A threat might happen if the transmission of the PPK was vulnerable

Table 5: Storing public key in IOV cloud

Attribute	Description
Name	Storing public key in IOV cloud
Code	ID:1
Priority	High
Critical	Ensures the authenticity of the recipient's public key .
Description	user generate public key and store it in the TA's iov cloud By taking this step, the TA makes it possible for the vehicle to communicate securely with any entity
Input	Vehicle public key.
Output	Successfully stored
Pre-condition	After the vehicle generate its public key,it transfer it to the TA
Post-condition	User's public key stored
Dependency	the authenticity of public key received
Risk	compromised public key may occur while the transmission of the public key that was sent by the user

5 Design Constraints[6]

5.1 Hardware Limitations

Our system adapted for restricted computing power, memory, and energy resources in recognition of vehicle limits. Adapted to the ever-changing dynamics of vehicles, it functions effectively within these hardware constraints, guaranteeing top performance in a variety of IoV scenarios

5.2 Other Constraints as appropriate

Beyond hardware and cryptography issues, our study tackles issues like variable network conditions and sporadic connection in the Internet of Vehicles. This flexibility demonstrates our dedication to a robust and flexible system by ensuring efficient functioning in real-world vehicle conditions.

6 Non-functional Requirements [7]

6.1 performance:

- In real time Processing: To provide quick and responsive communication, the system should be able to complete signcryption procedures in less than a second.

- Simulation Effectiveness: When assessing the suggested cryptographic method, simulation tools such as OMNeT++ should function effectively.

6.2 Scalability:

- Vehicle Network Load: The system should be able to keep up with the traffic in dynamic vehicular networks without compromising functionality.

6.3 Reliability:

- Message Delivery:To reduce the possibility of transmission errors, the system must guarantee dependable and secure message delivery between the vehicle and the server.

6.4 Usability:

- User-Friendly Feedback: To improve the user experience overall, the system's feedback mechanism should give users clear and straightforward information.

7 Data Design

For the purpose of simulating and evaluating the performance of the suggested system in the context of the Internet of Vehicles (IoV), the project makes use of the OMNeT++ simulator. Through the use of OMNeT++, the project seeks to assess the algorithms and functions in a regulated virtual environment, enabling thorough testing and analysis of the efficacy and robustness of the Certificateless Signcryption Scheme against new developments.

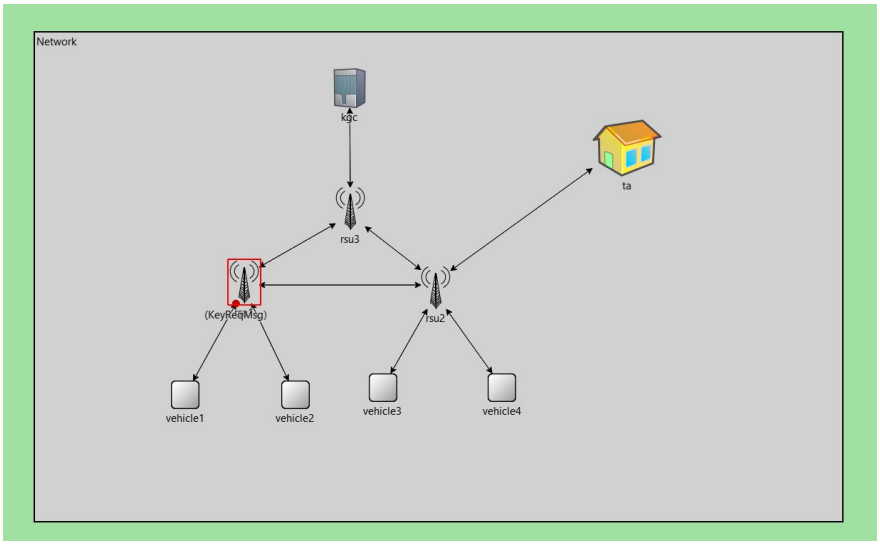

Figure 8: OMNeT++ Simulator

8 Preliminary Object-Oriented Domain Analysis

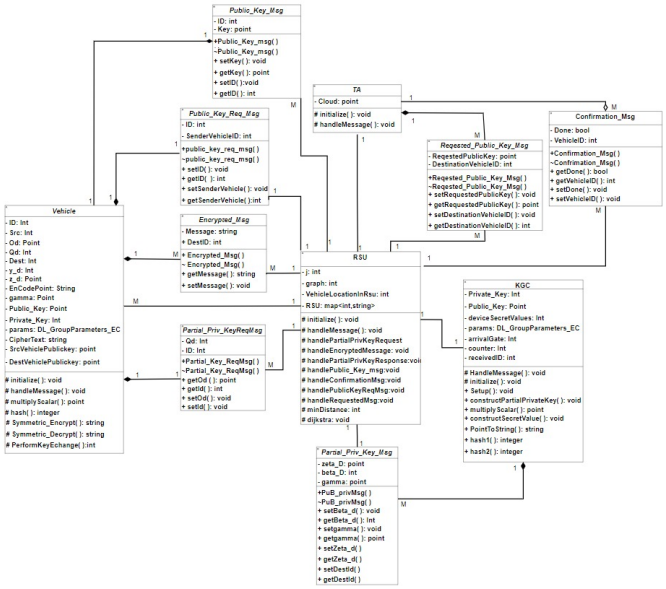

Figure 9: Class Diagram

9 Operational Scenarios

Scenario(1)"*Secure Vehicle-to-Vehicle Communication*": A secure communication exchange is required between two automobiles in the Internet of automobiles (IoV). By using the suggested signcryption strategy, the system ensures security and integrity while facilitating secure communi-

cation.

Scenario(2)"*Key Generation for New Vehicles*":A new vehiclehas to set up secure connection when it joins the IoV ecosystem. To engage in secure exchanges, the new vehicle receives a unique partial private key from the Key Generation Center (KGC).

Scenario(3)"*RSU Verification and Authorization*": Messages are received by a Roadside Unit (RSU) from servers and vehicles. By verifying and approving the identities of these communicating entities, the RSU improves the overall security of the vehicular network by making sure that only genuine and allowed communications are handled.

Scenario(4)"*Real-time Signcryption Processing":*Vehicles constantly share information in a dynamic traffic setting. By quickly signing and sending communications, the system shows off its real-time computing power and keeps the vehicular network safe and functional.

10 Project Plan

Table 6: Document version history

Task name	**Start date**	**End date**	**duration**
Researching	20-Oct-2023	15-Nov-2023	25 days
Proposal document	9-Nov -2023	15-Nov-2023	6 days.
Code and simulation	20-Dec-2023	15-Jan-2024	26 days
SRS Document	29-Dec-2023	15-Jan-2024	17 days
SDD preparation	20-jan-2024	20-Feb-2024	30 days

11 Appendices

11.1 Definitions, Acronyms, Abbreviations

Table 7: **Abbreviations**

VANETs:	Vehicular Ad Hoc Networks
KGC	SRS First version's specifications are defined.
RSU	Roadside Unit
UI	User Interface
hv,hw,hx,hy	Irreversible Hash Functions
η	Parameter
γ	Public Key
$\mathscr{E}_I$, $\mathscr{D}_I$	Encryption and Decryption Algorithms
Ξ	Global Parameter Set
δ_d	Partial Private Key

11.2 Supportive Documents

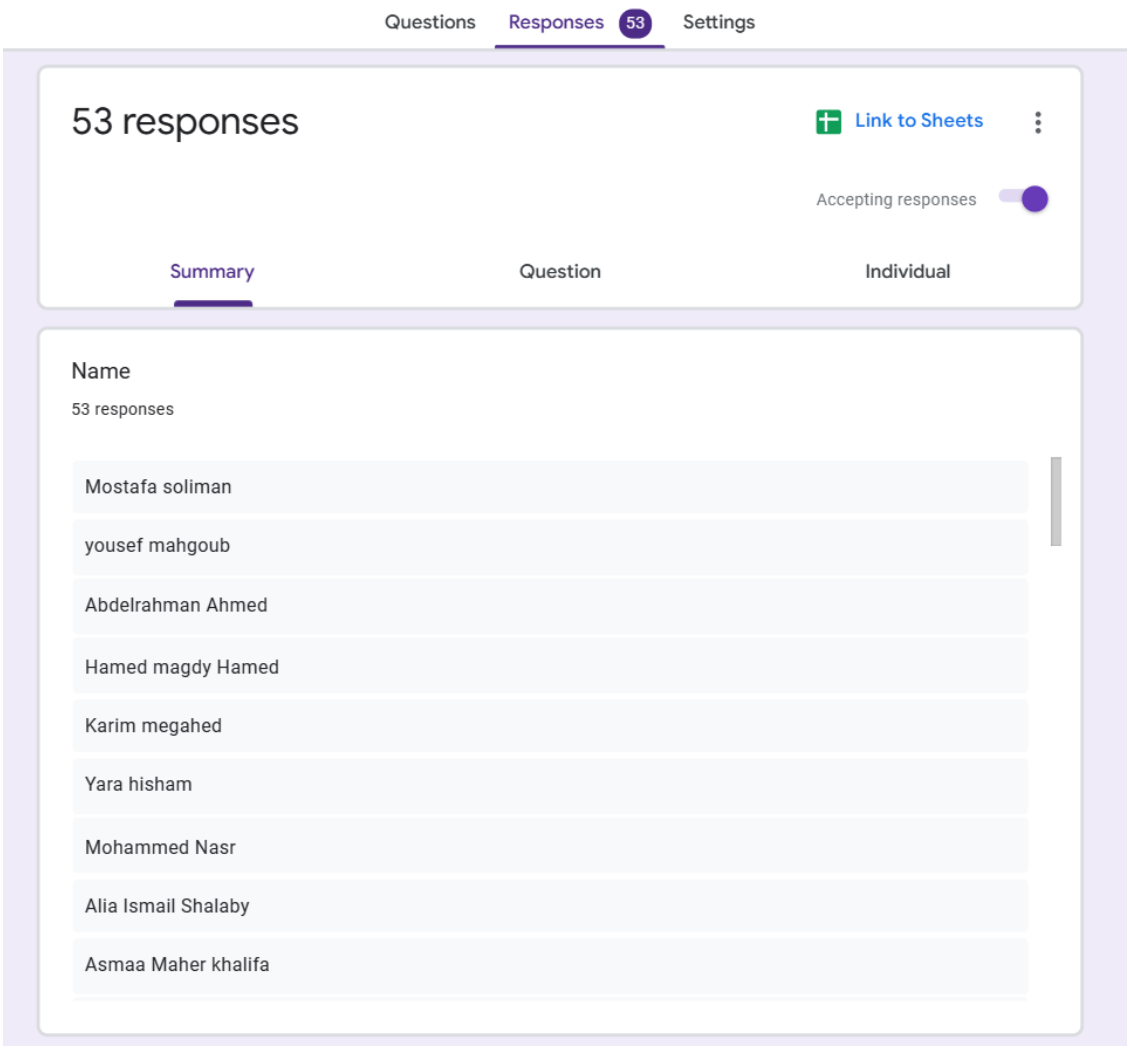

Figure 10: survey

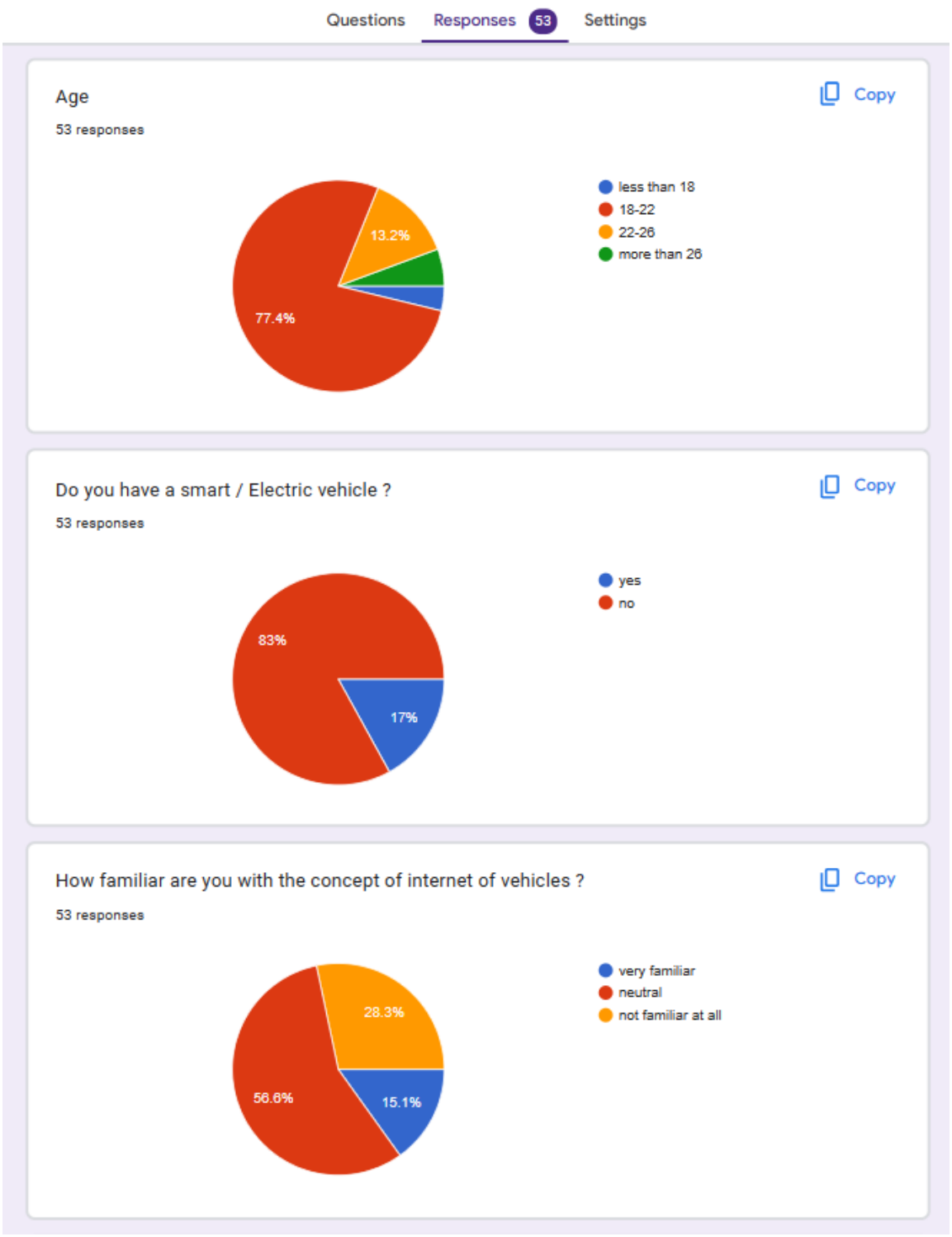

Figure 11: survey

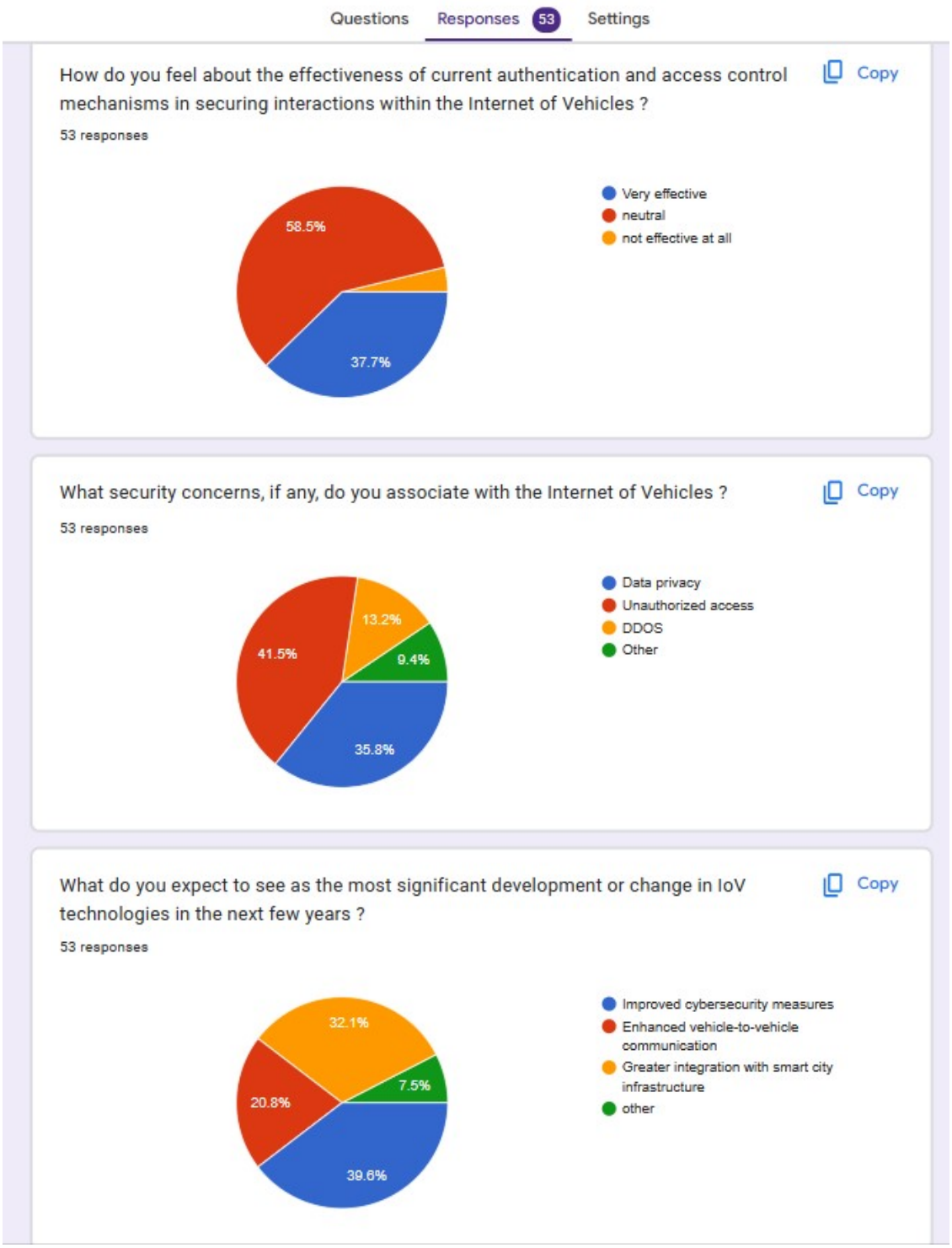

Figure 12: survey

Figure 13: survey

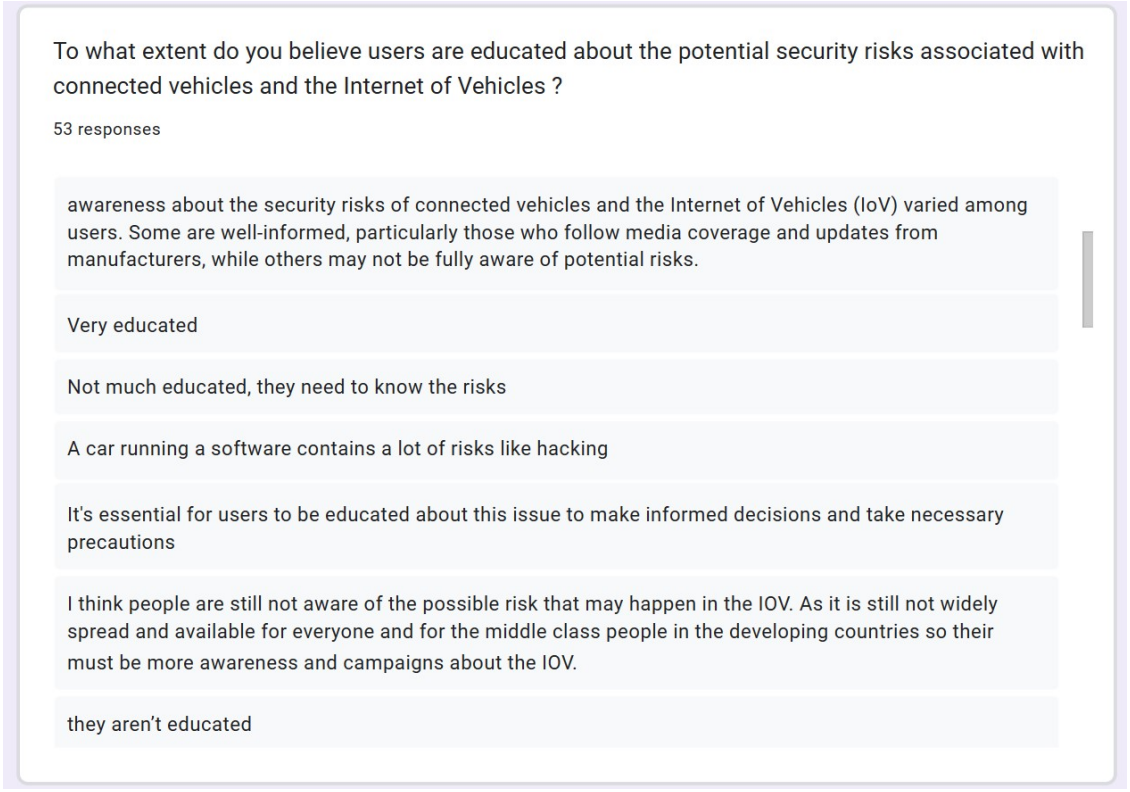

Figure 14: survey

References

[1] Li-Minn Ang, Kah Phooi Seng, Gerald K Ijemaru, et al. "Deployment of IoV for smart cities: Applications, architecture, and challenges". In: *IEEE access* 7 (acessed 8 jan 2024).

[2] Chien-Ming Chen, Bin Xiang, Yining Liu, et al. "A secure authentication protocol for internet of vehicles". In: *Ieee Access* 7 ((Accessed 12 november 2023)).

[3] Surbhi Sharma, Baijnath Kaushik, Mohammad Khalid Imam Rahmani, et al. "Cryptographic solution-based secure elliptic curve cryptography enabled radio frequency identification mutual authentication protocol for internet of vehicles". In: *IEEE Access* 9 ((Accessed 12 november 2023)).

[4] Jiabin Li, Zhi Xue, Changlian Li, et al. "RTED-SD: A real-time edge detection scheme for sybil DDoS in the internet of vehicles". In: *IEEE Access* 9 (accessed 2023 11 november).

[5] Shirin Abbasi, Amir Masoud Rahmani, Ali Balador, et al. "Internet of Vehicles: Architecture, services, and applications". In: *International Journal of Communication Systems* 34.10 ((accessed jan 12 2024)).

[6] Minghui LiWang, Shijie Dai, Zhibin Gao, et al. "A computation offloading incentive mechanism with delay and cost constraints under 5G satellite-ground IoV architecture". In: *IEEE Wireless Communications* 26.4 (jan 13 2024), pp. 124–132.

[7] Rita Rocha de Sousa. "Real-time data analytics for Non-Functional Requirements satisfaction". PhD thesis. Instituto Politecnico do Porto (Portugal), (accessed 2024 11 jan).