UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Nwaokolo Anita Onyinye

A Comparison of Privacy Enhancing Technologies in Internet of Vehicle Systems

Master's Thesis (30 ECTS)

Supervisor: Prof Raimundas Matulevičius, PhD
Co-supervisor: Abasi-amefon Obot Affia, Msc

Tartu 2020

A Comparison of Privacy Enhancing Technologies in Internet of Vehicle Systems

Abstract:
The evolution of internet of things (IoT) is driving conventional vehicle ad-hoc networks into the internet of vehicles (IoV). IoV has shown great relevance in helping to improve traffic efficiency by easing traffic congestion. Vehicles can easily exchange information with other vehicles and infrastructure in the same environment as they are. However, the exchange of information in IoV introduces privacy challenges to vehicle owners. Private data of these IoV users are being leaked unintentionally to the system, some systems even send user's data to a third party system and most times the user's are not aware of such message exchange with their private data.

It is possible for a honest but curious IoV user to identify vehicles and track user's location by analysing messages exchanged between systems. Messages exchanged between these systems carry some form of vehicular identification and in turn can be used to trace an owner via location profiling.

This thesis follows a structured approach towards mitigating this privacy leakage by applying the privacy enhancing technologies (PETs) identified in this thesis paper (encryption and attribute based credential), to help in protecting the information exchanged between each IoV's involved in communication. This approach is beneficial to system entities compliance in privacy frameworks and also helps in identifying the most effective PET by comparing the state and condition of each data objects identified in the system.

Keywords: Autonomous Vehicles (AV), Intelligent Transportation System (ITS), Internet of Vehicle(IoV), BPMN, PE-BPMN, Privacy Enhancing Technology (PETs).

CERCS:
T-120 Systems engineering, computer technology

Võrdlus eraelu puutumatust soodustavate tehnoloogiatega autosüsteemide Internetis

Lühikokkuvõte:

„Asjade interneti (IoT) areng viib tavapärased sõidukite sihtotstarbelised võrgud sõidukite internetti (IoV). IoV on näidanud üles suurt tähtsust liikluse tõhususe parandamisel liiklusummikuid leevendades. Sõidukid saavad hõlpsalt vahetada teavet teiste sõidukite ja infrastruktuuriga samas keskkonnas, kus nad on. IoV-s toimuv teabevahetus tähendab sõidukite omanikele siiski privaatsusprobleeme. Nende IoV kasutajate privaatseid andmeid lekitatakse süsteemi tahtmatult, mõned süsteemid saadavad kasutaja andmeid isegi kolmanda osapoole süsteemi ja enamasti pole kasutaja sellisest sõnumivahetusest oma privaatsete andmetega teadlik.

Ausal, kuid uudishimulikul IoV-kasutajal on võimalik sõidukid tuvastada ja kasutaja asukohta jälgida, analüüsides süsteemide vahel vahetatud sõnumeid. Nende osapoolte vahetatavatel teadetel on mingisugune sõidukitunnus ja neid saab omakorda kasutada omaniku jälgimiseks asukohaprofiili kaudu.

Käesolevas lõputöös järgitakse nimetatud privaatsuse lekke leevendamiseks struktureeritud lähenemisviisi, rakendades privaatsust suurendavaid tehnoloogiaid (PET), mis on tuvastatud töös encryption and attribute based credential, et aidata kaitsta IoV suhtluses osalenud osapoolte vahelist teavet. See lähenemisviis on kasulik süsteemi üksuste vastavuse tagamiseks privaatsusraamistikes ja aitab ka kõige tõhusama PET-i kindlaks teha, võrreldes kõigi süsteemis tuvastatud andmeobjektide olekut ja seisundit. ”

Märksõnad: autonoomsed sõidukid (AV), arukas transpordisüsteem, IoV, BPMN, PE-BPMN, privaatsust suurendav tehnoloogia (PET).

CERCS: T120 Süsteemitehnoloogia, arvutitehnoloogia

Contents

List of Figures

List of Tables

List of Abbreviations

ABC	Attribute Based Credential
AV	Autonomous Vehicle
AIK	Attestation Identity Key
AVP	Automated Valet Parking
BPMN	Business Process Model and Notation
CSP	Car Sharing Provider
CTS	Cyber Transportation System
FHE	Fully Homomorphic Encryption
GPS	Global Positioning System
ICT	Information and Communication Technology
IoT	Internet of Things
IoV	Internet of Vehicles
ITS	Intelligent Transportation System
IVC	Inter-vehicular Communication
PHE	Partially Homomorphic Encryption
PE-BPMN	Privacy Enhanced-Business Process Model and Notation
PETs	Privacy Enhancing Technologies
PII	Personal Identifiable Information
PLT	Parking Lot Terminal
PSP	Parking Service Provider
SHE	Somewhat Homomorphic Encryption
TA	Trusted Authority

RQ	Research Question
RL	Revocation List
RSU	Road Side Unit
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything

1 Introduction

Research into the established area of the intelligent transportation system (ITS) is evolving into the internet of vehicles (IoV), a fast-moving research area, fuelled in part by rapid changes based on cyber-physical systems [4].

With the rapid development of IoV, the application of the vehicle network has been developed from the primary stage of entertainment navigation services to the intermediate stage marked by travel induction and energy-saving driving. In IoV, traffic information and distribution means that the vehicle can navigate and complete its own state via environmental recognition through GPS, sensors and other devices in a huge superimposed interactive network composed of road network, communication network and location network. The collection of information, through computer technology, is analyzed and processed to support vehicle collaborative safety applications and traffic management [39].

1.1 Motivation

Internet of vehicles (IoV) has emerged as term to describe vehicles connected through the internet [43]. IoV interconnects humans within and around vehicles, intelligent systems on board vehicles, and various cyber-physical systems in urban environments, by integrating vehicles, sensors, and mobile devices into a global network, thus enabling various services to be delivered to vehicles and humans on board and around vehicles[40].

However, these services brings about various privacy implications to individuals especially when addressing the benefits it provides. The continuous collection and exchange of messages or data between vehicles enables IoV to improve transportation efficiency such as traffic congestions. However, the exchange of these messages between each vehicles or infrastructure may carry sensitive information. Controlling the enormous information collected by these systems from being abused is critical to mitigating privacy leakage [27]. Therefore privacy protection on personal data exchanged by any system has become an important factor in the continuous development of connected vehicles transportation system. The implementation of PETs to an entire system first of all helps to identify the data leakage point in the system. By doing this, it would help developers,policy makers etc to design and analyse implementation solution by translating these requirements into functional specifications and therefore to system processes [2].

1.2 Problem Description

The continuing evolution of internet of vehicles has ushered in a new era of interconnected intelligent systems, which certainly has been a quantitative leap in safety of road transport. These systems enable the exchange of information between different applications, and the subsequent analysis to improving the safety of drivers and eases travel and comfort in road travel [11]. These systems are driven by a substantial amount of data, mostly data obtained from diverse sources, such as smart card, GPS, sensors, video detector, social medias [42], smart phones, and passengers (or users). With the development of cloud based infrastructure, cloud computing, wireless communication and connected autonomous vehicles, the issue of individual privacy becomes questioned.

IoV technology gives way to privacy challenges such as location and personal identifiable information being visible to all infrastructures involved in information processing in IoV. Privacy of a legitimate user is the most significant attribute in order to avoid traceability of an honest IoV user[3]. This thesis hopes to address this privacy issue by applying PETs solutions to data exchanged and used between systems so that it is impossible for an honest IoV user to trace,link or identify an individual via data collected by each infrastructure in IoV. Furthermore, the analysis and comparison on each PETs solutions would further provide a result of which PET solution is the best for mitigating privacy issues/leakage in IoV.

1.3 Research Question

For the purpose of this thesis paper, the main research question that would be answered is:

What PET solution is best for mitigating privacy leakage in internet of vehicles (IoV)?

The main research question would be broken down further to the following research questions:

- RQ1: How can we identify the business objects in IoV? To answer this question, we analyse the system context for an IoV scenario using any modelling language.
- RQ2: How can the identified PETs analysed in this paper be applied to the related data object in IoV system context? To answer this question, we analyse the model for the IoV scenario from RQ1 and apply the identified PETs to the models to give a privacy enhanced model.

- RQ3: How can we evaluate the privacy of the related data object in IoV system context after the PETs application? To answer this question, we analyse the privacy enhanced BPMN model and use the information disclosure table to identify the extent to which the privacy enhanced model is visible. After that we use the result from the information disclosure table to carry out a privacy goal analysis.

- RQ4: What is the usefulness of our solution? To answer this question, we outline the outcomes of our approach and through validation detail the potential usefulness of our approach when implemented in real-life business cases.

1.4 Scope

The framework of the entire thesis is focused on identifying the privacy issues in IoV, applying PETs solution to mitigate the issue and comparing the outcome of the PET solution applied. This section provides specific boundaries and scope of this paper:

1. Privacy enhancing technologies: The objective of PETs is to protect personal data and ensure the users of technology that their information is confidential. PETs aim to minimize personal data collected and used by service providers and merchants. For the purpose of this research work, we would be focusing on encryption and attribute based credential (ABC). We limit our PETs to encryption and ABC because we need to understand fully the fundamentals of how each technologies operates and what is needed from each PETs to achieve our desired privacy properties.

2. Privacy enhanced- BPMN and BPMN: This is a BPMN language for capturing PET-related activities in order to study the flow of private information and ease the communication of privacy concerns and requirements among stakeholders [30]. The essence of using BPMN and PE-BPMN is to capture data objects, data collection, data usage and information flow between the system entities.

3. Internet of vehicles (IoV): The various systems components that are involved with IoV example the Autonomous Vehicles, Road Side Units etc. Identifying various IoV context is crucial for our paper. Understanding the various systems involved helps us address certain privacy concerns of individuals.

For example, the introduction of a third party system raises the concern of the kind of individual information that is being shared with the third party system.

1.5 Thesis Contribution

This thesis describes in details how our private information is being collected in IoV. Our contribution is as follows:

1. Analysing the various IoV scenarios in details to understand how information is being collected and used. In doing this, we can address some of the privacy concerns in an IoV.

2. Applying Protection mechanism to each IoV scenario to see how privacy goals are satisfied based on protection mechanism characteristics. In doing this, we understand the conditions and state of each protected data objects in an IoV to fulfil certain privacy characteristics.

3. Comparing each protection mechanism to identify the best protection mechanism for the system context. By doing this, we can understand the conditions each data objects fulfils, which helps us to select the best PETs for our IoV.

1.6 Structure of Work

The remainder of this paper is organised as follows:

- Chapter 1: This chapter introduces the research for this paper which includes motivation, problem description, scope, research question and thesis contribution.

- Chapter 2: This chapter provides an overview of various studies done that are related to PETs and IoV. It gives details on the PETs studied in this paper, their principles and privacy outcome. Furthermore, it provides information on modelling process of Privacy Enhancing-BPMN by illustrating 3 generic models of a privacyless system process and a privacy enhanced process. It discusses also the PET evaluation method using a visibility matrix.

- Chapter 3: This chapter provides information on the research method and introduces our learning model for this thesis paper. The learning model is

based on a selected scenario using IoV, illustrated with the BPMN and PE-BPMN modelling language. We evaluate two kinds of model, the privacyless model illustrated with BPMN and the privacy enhanced model illustrated with PE-BPMN.

- Chapter 4: This chapter evaluates the effectiveness of the PET applied in chapter 3 and evaluates the overall privacy of the data objects in the system. It gives an analysis of both privacyless model and privacy enhanced model to show the gap between the two models in terms of privacy properties achieved. Also a comparison of both PETs based on the specific conditions identified by our analysis leads us to determine which PETs achieves more privacy property in the system.
- Chapter 5: This chapter introduces our validation model and procedure and evaluates the privacy properties of the system based on the PETs combination
- Chapter 6: This chapter summarizes the entire thesis paper, answers the research question and gives a final conclusion.

2 Literature Review and Background

In this section, we identify existing research that is in scope of privacy enhancing technologies (PETs), and how it can be applied to IoV. This chapter introduces IoV, and identifies the major privacy issues associated with IoV, understanding the PETs applied in this thesis research, highlighting the privacy properties achieved by each PETs by looking into various literature studies and identifying the research Gaps. For more information about paper selection process please refer to Appendix A.

2.1 Internet Of Vehicles

The concept of Internet of Thing (IoT) is to equip real world objects with computing, processing, and communicating capabilities to enable socializing between them. Internet of vehicles (IoV) is an adherent of IoT that has realized significant advancements using communication technologies. Vehicles connected through Internet are capable of sharing information that can substantially enhance the quality of traffic on roads [34].

According to Kombate et al. [23], the implementation of an IoV environment have to be based on a certain number of aspects:

1. Thorough analysis of a scenario driven methodology visualized to shape some portion of the future of internet-connected vehicles, such as: intelligent traffic management, safety and emergency management, eco-driving for energy-efficiency.

2. Autonomic algorithm to improve operation of internet-connected vehicles, in terms of safety and traffic management, green targeted criteria, as well as for enabling services from the vehicular extended internet

3. Versatile data acquisition and aggregation from various internet connected vehicles, directly and indirectly (even through networks of social type),

4. Driver, vehicle and environment modelling for inferring collective and yet individualized knowledge that can be used in context handling; producing outputs on a per-scenario basis for optimizing the performance of internet connected vehicles.

5. Service-oriented effective solutions for a massively large networked system, developed by different organizations and spread across the world, used by

millions of vehicles and comprising huge numbers of sensing and computing devices with (basic) communication capabilities, a complete functional and system architecture for IoV, based on existing standards and providing extensions when necessary.

2.2 Privacy Enhancing Technologies

Privacy enhancing technologies are means to protect privacy of the individual or the information contained within. [21]. In this research paper by David and Isabel[10], they described existing privacy-enhancing technologies based on taxonomies to review the state of the art in smart cities around the world. The first taxonomy presented was in smart city applications and the technologies that enable them. The smart application includes smart mobility (transportation), smart utilities (such as smart energy, smart grid etc.), smart buildings, smart public services, smart governance etc, smart economy, smart health care etc. The second taxonomy was on privacy, which was divided into five types that show which kind of user information is exposed. The five types of privacy includes; privacy of location, privacy of state of body and mind, privacy of social life, privacy of behavior & action, privacy of media. They also identified the building blocks for PETs that have been developed over the past few decades which includes:

1. Process-Oriented Privacy Protection: This addresses the process of developing and operating privacy-friendly systems and are thus applicable to most technologies. This includes privacy by design, privacy engineering requirement, testing and verification, transparency, consent and controls, privacy architectures.

2. Data-Oriented Privacy Protection: This includes data minimization, data anonymization, differential privacy, encryption (identity based and attribute based encryption), homomorphic encryption, zero-knowledge proofs, anonymous/pseudonym digital credential, secret sharing, secure multiparty computation etc.

3. No Privacy without Security: Security and privacy are closely related terms and effective privacy protection is almost impossible without security.

From the findings, they concluded that different technologies have similar privacy solutions which indicates the possibility of generic privacy patterns. These patterns can contribute to the implementation of many tailored privacy solutions found in

the literature. For the purpose of this paper, emphasis would be laid on encryption and attribute based credential (ABC). The reason for this selection is because both PETs exhibit a vast difference in terms of operation, architecture (systems involved) and application. Hence, the need to study the underlying objectives of each PETs would help us identify and understand each PETs as they are when applied to data.

2.2.1 Attribute Based Credential

Attribute-based credentials are cryptographic schemes designed to enhance user privacy. These schemes can be used for constructing anonymous proofs of the ownership of personal attributes. The attributes can represent any information about a user, e.g., age, citizenship or birthplace. Out of five entities, the user, issuer and verifier are considered to be core entities, while the revocation authority and inspector are optional entities

1. **User:** The user enrolls into the system by requesting a credential and demonstrating the possession of certain attributes (anonymously)[13].

2. **Issuer:** An issuer is an infrastructure-based (trusted) identity provider also known as an attribute authority[12]; An Issuer issues credentials to users, thereby vouching for the correctness of the information contained in the credential.

3. **Verifier:** The verifier protects access to a resource or service that it offers by imposing restrictions on the credentials that users must own and the information from these credentials that users must present in order to access the service.

4. **Revocation Authority:** The revocation authority is responsible for revoking issued credentials, so that these credentials can no longer be used to generate a presentation token.

In an ABC system, the following phases are distinguished:

1. **Setup:** It is performed only once by each entity of the system. A trusted authority generates all public and secret global parameters used by the entities of the system. At the end of this phase, the issuer is ready to release credentials to users and the verifier is ready to validate such credentials.

2. **Issuance:** An issuer can issue a credential without being related to any existing credential owned by the user [12]. Before issuing a credential, the Issuer may have to authenticate the user, which it may do using privacy-ABCs, using a different online mechanism (e.g., username and password), or using out-of-band communication (e.g., by requiring the user to physically present herself at the issuer's office) [5]. The issuer public key is used by verifiers to verify the authenticity of presentation tokens[33].

3. **Presentation:** it is one of the most important stages from the ABC life-cycle. Verifiers request a credential and users provide it (or a presentation token derived from it) to be later verified [12].

4. **Revocation:** Credentials are revoked by the revocation authority, which is also responsible for making available updated revocation information[12].

5. **Inspection:** An Inspector is a trusted authority who can de-anonymize presentation tokens under specific circumstances. To make use of this feature, the verifier must specify in the presentation policy which Inspector should be able to recover which attribute(s) under which circumstances. The user is therefore aware of the de-anonymization options when the token is generated and actively participates to make this possible; therefore the user can make a conscious decision based on her trust in the Inspector[5]. There are scenarios in which it is necessary to de-anonymize the credential holder. This is achieved by performing token inspection [12].

Table 1 provides a summary of the privacy properties achievable by ABC based on studies done. All privacy properties can be achieved by ABC depending on the condition and environment present. For instance some conditions might not support revocation or minimal information disclosure due to systems involved. Depending on what we are presented with can we then evaluate the privacy properties. For an ideal condition ABC can achieve all properties.

Privacy Property	Definition	Reference
Anonymity	The user's identity stays hidden during verification of attribute ownership.	[9, 13, 17, 18]
Unlinkability	The issuer cannot link an issued credential to the presentation of such credential and different presentation tokens cannot be linked to the same user. This feature prevents from user profiling.	[8, 12, 13, 17, 19, 24]
Minimal information disclosure	Presentation tokens do not leak any data either from the attributes to be verified nor from the remaining ones included in the credential.	[12, 13, 16, 17, 18, 24]
Revocation	Invalid, lost, stolen or expired credentials are revocable.	[7, 12, 17]

Table 1. Privacy Properties achieved by ABC

2.2.2 Encryption

More generally, encryption is the science of privacy. It is about the construction and analyses of protocols that overcomes the authority of adversaries through information security such as integrity, confidentiality and authentication. There are two types of encryption techniques: symmetric and asymmetric encryption. In symmetric encryption, both sender and receiver have the same key for encryption and decryption and in asymmetric the sender and receiver have different keys (public key and private key) for encryption and decryption [35]. Public-key encryption would seem to be inherently asymmetric, in that only messages sent to a user can be encrypted using the user's public key [14]. Once information has been encrypted with the public key, nobody but the holder of the private key can decrypt it. In reverse, if the private key is used for encryption, anyone with the public key can decrypt it. It is very hard to derive the private key from the public key, this is because the private key does not need to be exchanged, public key encryption is much more secure than earlier techniques, so it can be used for applications such as internet commerce [6].

Table 2 provides information of the privacy properties that are being achieved by encryption.

Privacy-Property	Definition	Reference
Confidentiality	It is designed to avoid private data or information from getting to unauthorized people. Data encryption is a user known method of ensuring confidentiality.	[15, 31]
Anonymity	Hiding identity. A system cannot tell an identity from the sender of a message.	[1, 25, 32, 38, 41]

Table 2. Privacy Properties Achieved by Encryption

2.3 PE-BPMN

Privacy-enhanced BPMN (PE-BPMN) is a BPMN language for capturing PET-related activities in order to study the flow of private information and ease the communication of privacy concerns and requirements among stakeholders[30]. PE-BPMN provides constructs to specify privacy enhancing technologies to be used on process models. Extension of the BPMN concrete syntax to add PETs is done using stereotypes, which are the representatives of privacy enhancing technology groups. Therefore, considering privacy in business process starts with fixing the general goal and stereotype and then making decisions to select the PETs. Table 3 summarizes all concrete stereotypes as adapted from [30]. Unprotected data element is considered as data whereas shares, encrypted data or protected data emphasize that there is some form of protection.

PE-BPMN defines stereotypes for different tasks in privacy enhancing technologies so that they can be included in the BPMN model. There are two message flow stereotypes: $CommunicationProtection$ is a general goal stereotype and denotes any protected communication, whereas $SecureChannel$ is a channel that protects confidentiality and integrity of the communication. Another concrete instantiation of $CommunicationProtection$ could be something to mark anonymous communication [37]. We illustrate a privacyless model and a privacy enhanced model based on concrete stereotypes as described in Table 3.

Concrete Stereotype	General Stereotype	Input	Output
$PKencryption$	$ProtectConfidentiality$	2:data, public key	1:encrypted data
$PKdecryption$	$OpenConfidentiality$	2:encrypted data, secret key	1: data
$PKcomputation$	$PETComputation$	1-infinity: encrypted data or data	1: encrypted data

Table 3. Example stereotypes, their input–output types and number (or range) of input and output data objects (Adapted from [30])

Figure 1 shows communication exchange involving data-set between two parties (party 1 and party 2). Party 1 inputs data into the system and party 2 receives the data. Party 2 computes the data with another data 2 and produces the result of the computation. The result is then sent to party 1 who receives it and updates its database with it.

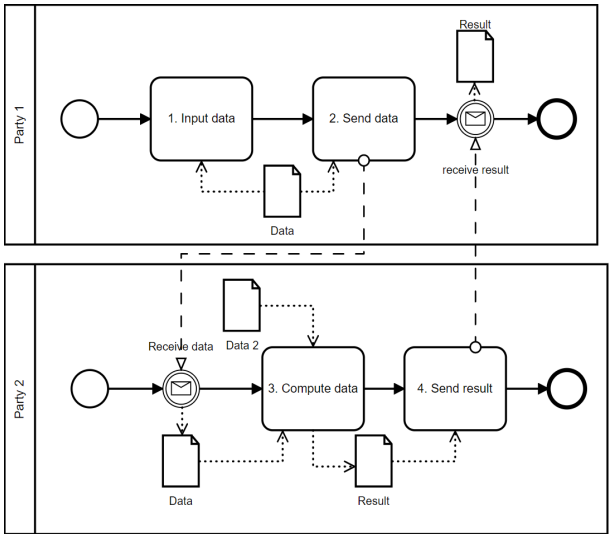

Figure 1. Privacyless model: Basic Communication Scenario Between Party 1 and party 2 adapted from Pullonen, et al [30]

2.4 Privacy Enhanced Model with Concrete Stereotyped Technologies

Concrete technologies introduce different limitations, therefore considering privacy in business process starts with fixing the general goal and stereotypes and then making decisions to select PETs [30]. For the purpose of this paper, emphasis for PETs chosen is being laid on encryption and attribute based credential (ABC).

2.4.1 Public Key Encryption

Public key cryptography uses two pairs of key (public key and private key) for encryption and decryption. The model in Figure 2 introduces a generic PE-BPMN for public key encryption.

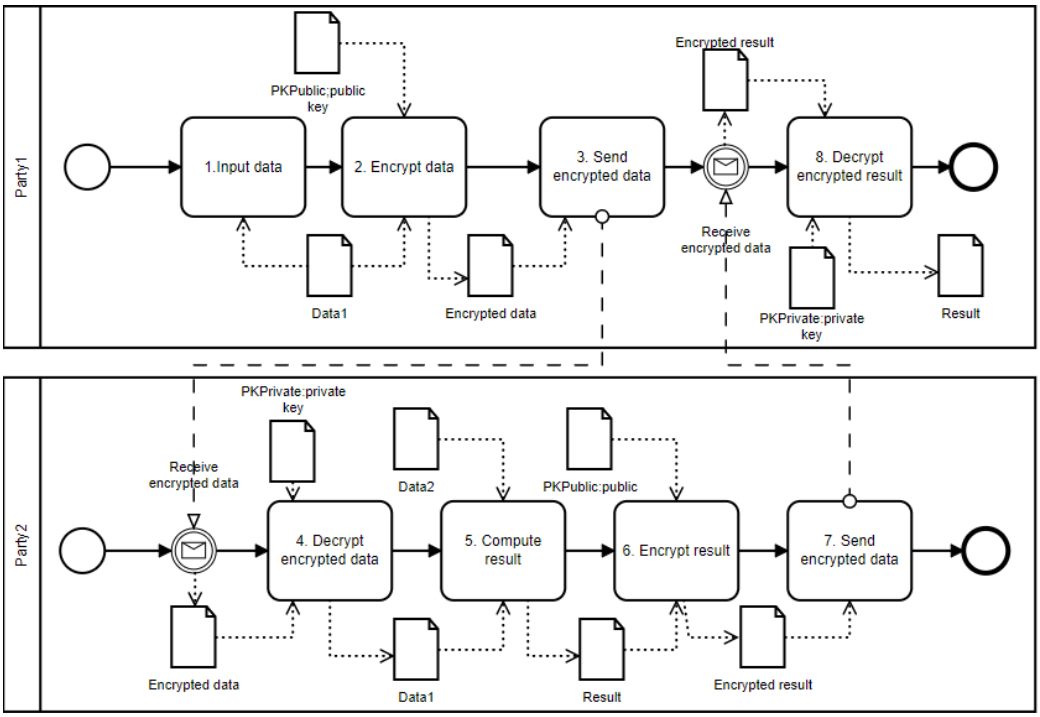

Figure 2. Generic Model Encryption Scenario Between Party 1 and party 2 adapted from Pullonen et al.[30]

In Figure 2, we see two parties (party 1 and party 2) exchange encrypted data between themselves where party 1 encrypts data1 with the public key of party 2 and sends out the encrypted data to party 2: $PKEncryption$. Party 2 receives the data and with its corresponding private key decrypts the encrypted data:

$PKDecryption$ and compute the result intended. Party 2 then encrypts the result with party 1's public key:$PKEncryption$ and sends the encrypted result to party 1 who in turn decrypts the encrypted result with its private key:$PKDecryption$ to produce an un-encrypted result.

Also performing homomorphic encryption is also possible. Here, computation is carried out on encrypted data to produce an encrypted result. The scenario description in Figure 3 is still very much the same as Figure 2, only that party 1 encrypts the data with its secret key and sends the encrypted data to party 2. party 2 is given the ability to carry out computation on encrypted data. Here, we introduce $PKComputation$ as the concrete stereotype.

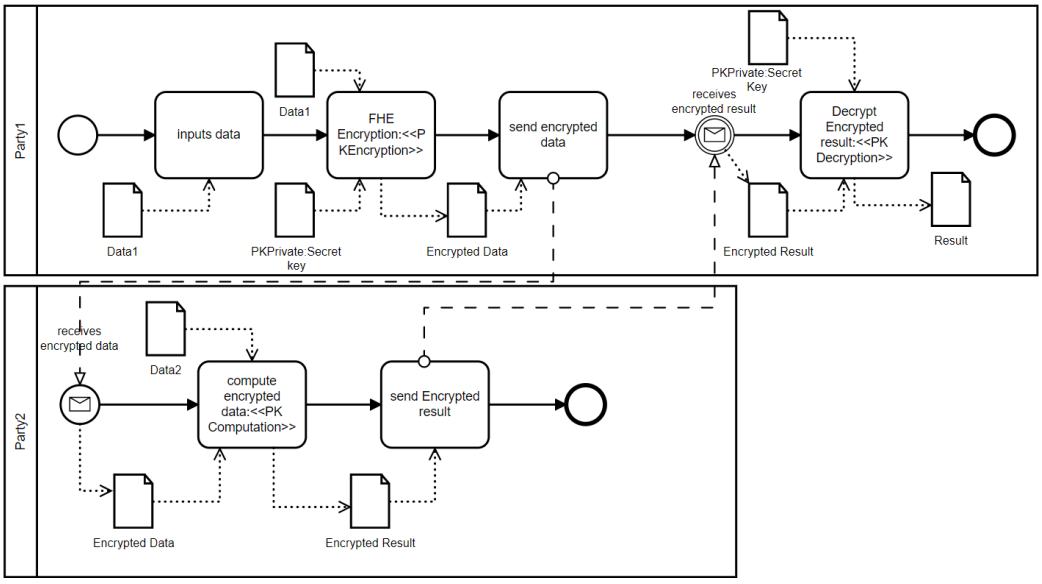

Figure 3. Generic Model Fully Homomorphic Encryption Scenario Between Party 1 and party 2 adapted from Pullonen et al.[30]

2.4.2 Attribute Based Credentials (ABC)

In ABC systems, users obtain credentials (specific pieces of information) from an issuer. Each credential contains a set of attributes linked to the user. Based on those credentials, users create presentation tokens that are used to prove the possession of such credentials without disclosing any further information [13]. ABC technologies have been designed to enhance users' privacy [12]. Figure 4 shows a generic ABC model where a user requests for enrollment with an Issuer.

The issuer generates a credential for the user based on proof of attributes provided by the user anonymously and signs it with its public key $PKEncryption$. When the user wants to request a service, the user generates a presentation token that includes only the needed attributes and the issuer's public signature. The service provider verifies an validates the user based on the issuer's public signature before accepting any service to authenticate the user.

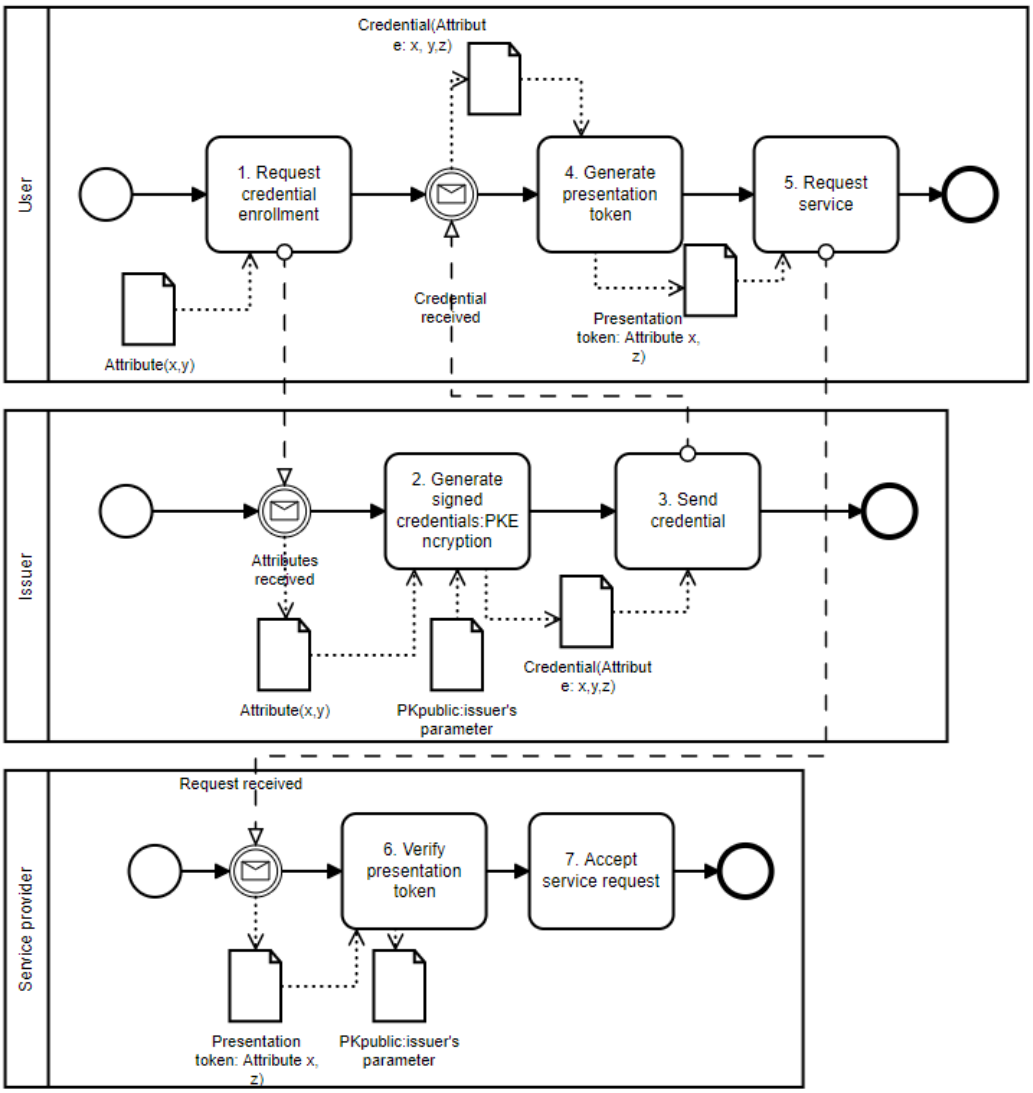

Figure 4. Generic Model ABC

2.5 Information Disclosure Analysis

Information is considered disclosed when it is accessible by another party, regardless of authorization level. For the purposes of PE-BPMN, we consider an object to be disclosed if it is received or intercepted by another party regardless of intent or policy [30]. Information disclosure analysis is supported by three types of disclosure tables: visibility matrix, communication matrix and data dependency matrix. For this thesis, we would be dealing with only visibility matrix. This is because visibility matrix gives an overview of data that is visible, hidden or accessible which is important to discover information leakage.

A visibility matrix gives an overview of the data objects that each actor possesses at some point along the process. It also describes the extent of data visibility to each actor. The actors learn the contents of data sent to them or computed by them,but some data objects hide the actual data that they encode (e.g., through encryption or sharing). We consider technologies that provide data confidentiality protection and PET computations that give protected outputs as producing the data objects that hide their underlying content. The three visibility ratings are *Visible (V)*, *Hidden (H)*, *Accessible (A)*. We consider *Accessible (A)* also as Hidden (H) for the purpose of privacy evaluation in this work. Accessible is considered as hidden because at some point when the actor possess the data object, it is "protected" by some PET mechanism. The only time the data object is visible is when the actor meets the access specification requirements. Also when we do a final visibility score on the data object, we do not want the scoring to be complicated by considering three ratings. Hence Accessible (A) would be considered as Hidden (H), so our final evaluation lies between Visibility (V) and Hidden (H). The visibility ratings of data object are as follows:

1. *Visible (V):* This indicates that an object is owned or obtained at some point by an actor and is fully readable.An object is visible if it is not protected[30].

2. *Hidden (H):* This tells us that a data object is owned or obtained by an actor at some point but its contents are unreadable as it is protected by some PET mechanism (e.g.,encryption) and the party does not meet the access specification requirements to recover the protected data. Hence, all hidden data is something that is not disclosed to the given stakeholder [30].

In addition to the above ratings, for ABC we introduce new visibility ratings that satisfies the ABC properties. The visibility ratings are as follows:

1. *Authenticate (A):* This tell us that a data object that is owned by an actor at some point in the system is protected by a system's signature example an Issuer.

2. *Verified (R):* This tells us that the data object owned by an actor at some point in the system has been verified by a service provider.

3. *Visible (V):* This indicates that an object is owned or obtained at some point by an actor and is fully readable. An object is visible if it is not protected[30].

2.6 Related Works on Privacy Enhancing Technologies in IoV

Various studies on the application of the main PETs applied in this paper (encryption and attribute based credential) to internet of vehicles would be analysed. We would present the approach of each studies cited in this paper and their final evaluation of each PETs.

2.6.1 Privacy and Integrity Considerations in Hyper-connected Autonomous Vehicles

In this paper by Karnouskos and Kerschbaum [22], they discussed the feasibility of ensuring integrity while preserving privacy in a hyper-connected vehicle scenario. In their approach, they illustrated an exemplary case study on real-time vehicle interactions pertaining to map updates exemplifying the combination of privacy-enhancing technologies with integrity-protecting mechanisms. They identified objective challenges in hyper-connected vehicles and provided an overview of techniques. With these information on objective challenges and an overview of techniques, they applied it to their use-case (illustrated vehicle real-time map updates). They identified deployment challenges as limitation. Such deployment challenges includes; social debate about privacy and parameter setting due to conflicting objectives between data use and privacy, flexibility of cryptographic protocols through the design of compilers for cryptographic protocol and secure issuance and key management.

2.6.2 An autonomous privacy-preserving authentication scheme for intelligent transportation systems

In this paper by Sucasas et al.[36], they discussed the challenges faced with intelligent transportation system applications such as authentication of transmitted

messages where user's identity and location are sent in plain text. They identified a solution by using cryptographic pseudonyms which are termed computationally efficient solutions for preserving the privacy of vehicles' location. However, the limitation of this solution is that vehicles and trusted authority (TA) have to be in permanent contact which could lead to issues like network congestion or be infeasible in some situations due to the lack or scarcity of deployed infrastructure.

They addressed this limitations by proposing an autonomous privacy-preserving authentication scheme, where vehicles only need to contact the TA once; afterward, they can renew their pseudonyms by themselves without communicating with the TA. They illustrated a use case in traffic monitoring and road safety application. According to them, a privacy-preserving authentication scheme for traffic monitoring and road safety applications should satisfy the requirements described in Table 4.

Privacy Property	Definition
Efficient message authentication	The origin of the messages should be efficiently authenticated since traffic monitoring and road safety applications are delay sensitive.
Data integrity	The message should not be modified by unauthorized or unknown means during transmission.
Non-repudiation	Any entity cannot deny any previous data transmission.
Conditional privacy	Only the TA can link pseudonyms to real identities, which can be triggered in case of misbehavior.
Efficient revocation	The TA can publish a revocation list (RL) of pseudonyms, which can be discarded by vehicles. The revocation list size has to be scalable.
Unlinkability	The different pseudonyms of the same vehicle cannot be linked.
Forward unlinkability	After a vehicle is included in the revocation list, its future data transmissions are traceable but the past activities are still untraceable.

Table 4. Privacy-preserving authentication scheme for traffic monitoring and road safety applications

2.7 Research Gap

Various studies have tried to show the significance of employing privacy enhancing technologies to protect the privacy of individuals in internet of vehicle systems, but there are limitations and setbacks of the various identified solutions provided by PETs. In this study by Karnouskos and Florian [22], they identified about three limitations in ensuring that privacy is preserved in a system. The limitations are in line with deployment challenges where there is social debate about privacy and parameter setting due to conflicting objectives between data use and privacy. Another limitation identified was the update of cryptographic protocols. The drawback of computation on encrypted data is that it is rather difficult to change the protocol, hence the need for flexibility of cryptograhpic protocols. Also the issue of secure issuance and key management that relies on cryptography needs to deal with the key management problem. Keys and identities need to be securely issued, revoked, and renewed (life cycle management).

2.8 Summary

This chapter highlighted the various privacy issues associated with internet of vehicle. The two main PETs (encryption and attribute based credential) that would be discussed in this thesis paper was analyzed. We identified the various privacy properties and requirements that each PETs should satisfy when applied. Furthermore, future research areas, opportunities and challenges of PETs in IoV were discussed.

3 Privacy Evaluation Approach

In this chapter, we introduce a proposed approach that would be used to achieve our desired results. Subsequent subsections in the chapter would be based on the illustration of an IoV scenario that would serve as our learning model for this thesis paper. The privacy enhanced model is also illustrated in this chapter. For complete illustration of privacyless and privacy enhanced model please refer to Appendix B.

3.1 Proposed Approach

We present the proposed approach that would be used for this thesis paper. Each step identified in this approach is an important step towards achieving our end result. The goal of this chapter is to successfully identify the important data objects from the business process of the IoV scenario. The activity of modelling the business process for our IoV scenario would be illustrated using BPMN model. The approach is as follows:

1. Identify data objects from an IoV use case: Based on selective IoV scenarios illustrated into business process model, we identify the important data objects associated with the system. The process of data object identification is done using an appropriate modelling language. This IoV scenario serves as our learning model for this thesis paper.

2. Apply privacy enhancing technology (PETs) to data objects : This process has to with applying the identified PETs in this paper (encryption and ABC) to the data objects identified in (1). By applying PETs to the data object in the identified system context for our IoV scenario, we can evaluate the state and condition of the data object across each system.

3. PET privacy evaluation: This activity analyses the protected data object from (2) by considering the state and condition of the data object across each system entities. By evaluating the state of the data object using a visibility matrix, we can analyse the condition of each data object and determine how each PET applied to it is being effective through the privacy properties achieved. This evaluation is done based on the generic principles and conditions of each PETs analysed in this paper.

4. PET comparison: This activity focuses on analysing the PET evaluation table and based on certain principles and conditions provided, we evaluate

each PETs by determining the privacy properties based on the conditions set and achieved by each PETs on the data objects.

3.2 Learning Model: Automated Valet Parking

We introduce our learning model for this thesis paper. The IoV context for the learning model is the Automated Valet Parking (AVP). We would illustrate a part of the AVP process through BPMN modelling. The models would include a privacyless model that shows the important data objects transmitted between system entities and the issues associated with the system privacy; a privacy enhanced model (encryption and ABC) that shows the effects of the applied PETs to the system. All process models for the IoV scenario are illustrated fully in Appendix B.

An Automated Valet Parking (AVP) [20, 29] allows users to leave their vehicles at the drop-off area, e.g., the foyer of a hotel and the departure layer of the airport, and activate the AVP application on the smartphone for valet parking. AVs connect with the nearby parking lots to find vacant parking space, self-drive to the parking lots, and park themselves at the vacant space. Due to the development of advanced sensing, communication and control technologies, parking space discovery and vehicle parking are completely automatic and problem-free for AVs [29]. The entities involved in this use case scenario includes:

1. **Autonomous Vehicle (user device):** For the purpose of model, the user device would be classified as the AV system components.

2. **Parking Service Provider (PSP):** The PSP is a group of online servers that provide parking services for users. These services are offered by a parking service company under subscription services [20].

3. **Parking Lot Terminal (PLT):** The PLT is a terminal deployed by the owner of the parking lot. It is responsible for organising and managing the parking lot through IoT devices (e.g. cameras and sensors). [20].

3.2.1 Privacyless Model: AVP

Figure 5, shows the privacyless model for an AVP scenario. For a more complete privacyless model please refer to Appendix B. Also note that the privacyless analysis is done based on the presented model in Figure 5. In this model, there are three system entities involved with providing the user a service. The user presents multiple data that are relevant to the service but also visible at all ends through

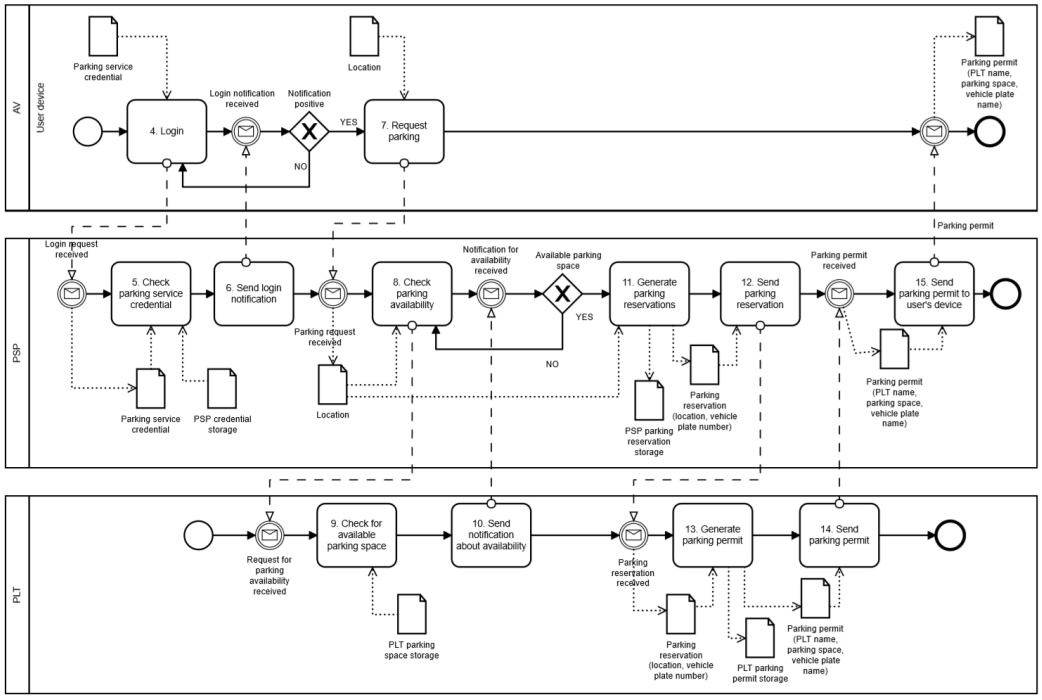

Figure 5. Privacyless Model: Automated Valet Parking Information Usage

communication channels and system entities. At the point of authentication with the PSP, the user needs to present the parking service credential which is visible to the PSP system. When the user request for parking service from the PSP, the location of the user is visible at all ends in the system entities. Likewise the parking reservation and parking permit exchanged between the PSP, PLT and the user. All data objects and its values are visible at all system entities.

The implication of such a data exchange in a privacyless system is as follows:

1. The user can be identified from the system using any data object parameter such as the parking service credential or parking parking permit presented to the system or presented by the system.

2. The messages such as location, parking reservation, and parking permit etc. transmitted between the systems can be linked back to the user.

3. Due to visibility of information across all systems, user's identity can be forged or stolen based on specific credential usage example the parking service credential. The data objects sent across the system do not have

any form of entity identification, hence messages sent across system can be tampered with. For instance the parking permit information can be changed by an honest IoV user and sent to the user.

4. When a user decides to change their credentials, there is no assurance that the previous credential is being revoked by the system. Hence, it is possible for an honest IoV user to keep using the credential even after the change.

Data Object Identification: In Figure 5, there are at least three system entities involved in the communication process. The user device provides the basis of interaction between the user and the parking service provider (PSP). The parking service provider (PSP) has a direct interaction with the parking lot terminal (PLT) and the user. The Parking Terminal is a third party system entity in this context. From the scenario described in Figure 5 we identify the IoV system assets and data object in Table 5

System Assets	Data Object Identification
AV (User Device)	Provide basis of interaction with PSP and user
PSP, PSP credential storage	Collect user registration data, store PSP credential, carry out login procedure, use customer's location to process parking reservation
PLT, PLT parking storage	Use customer's information provided by PSP to generate parking permit,store parking permit
AV (OBU)	Use parking permit to gain entrance into PLT

Table 5. Data Object Identification

3.3 Privacy Enhanced Model: AVP

We apply the PETs identified in this paper (encryption and ABC), to the process model illustrated in Figure 5. The application of PETs to the system is to enhance the user's privacy by protecting the data objects that is being passed across the system. Further analysis on the privacy enhanced model for the system process is discussed based on the state and condition of the objects as it passes through the system. The privacy properties that are intended to be achieved by encryption and ABC can be exemplified in Table 1 and Table 2.

3.3.1 Privacy Enhanced Model: Encryption

The model in Figure 6 shows the application of encryption mechanism to the data object identified in Table 5. This process was achieved by illustrating the PE-BPMN model of the IoV system. For a more complete encryption process please refer to Appendix B. Also note that the encryption analysis is done on the model presented in Figure 6 hence the privacy properties are going to be elicited based on the presented model.

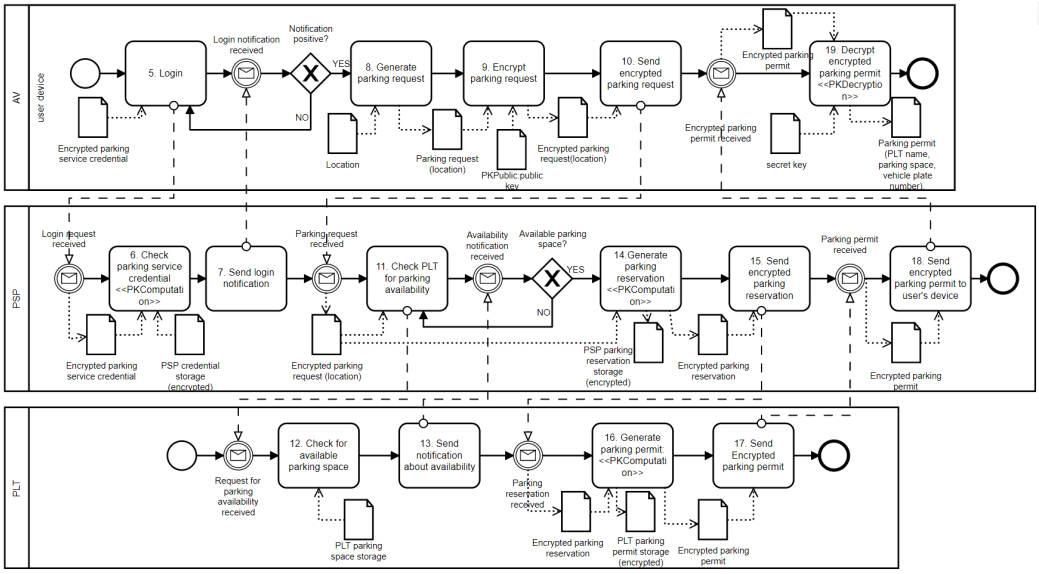

Figure 6. Privacy Enhanced Model for AVP: Encryption[30]

We assume that each system have computational capabilities to process the encrypted data objects passed across the systems in every activity that encrypted data object needs to be processed to generate a new encrypted data object, we identify this using the $PKComputation$ stereotype.

In the encryption model in Figure 6, we notice the parking service credential is protected during authentication with the PSP. Hence, the protected parking service credential hides its value from the PSP. Also, when the user generates a parking request to the PSP, the user encrypts it with their own secret key.

The PSP receives the encrypted parking request and perform some computations on the encrypted parking request to generate an encrypted parking reservation: $PKComputation$ that is then sent to the PLT. The PLT receives the encrypted parking reservation from the PSP and also performs some computations

on the encrypted parking reservation to generate an encrypted parking permit: $PKComputation$ that is sent to the PSP and the user. The user can then decrypt the parking permit with his secret key.

Throughout this process, the values of the encrypted data object passed across each system is hidden. This is due to the application of encryption to the data object and the computational $PKComputation$ capability on encrypted data object by the systems (PLT and PSP). This mechanism preserves the privacy of the data object and as such Data confidentiality is achieved. There is a clear contrast between the privacyless model in Figure 5 and the privacy enhanced model in Figure 6. All data presented by the system in Figure 6 are entirely unreadable by the system because of the encryption mechanism applied to the data objects. This changes the overall privacy of the data objects in the system. Only the user can decrypt the encrypted data because the user possess the secret key.

3.3.2 Privacy Enhanced Model: ABC

For more complete information about ABC for the AVP scenario please see Appendix B. Also note that ABC analysis is done on the model presented in Figure 7, hence the privacy properties are going to be elicited based on the presented model.

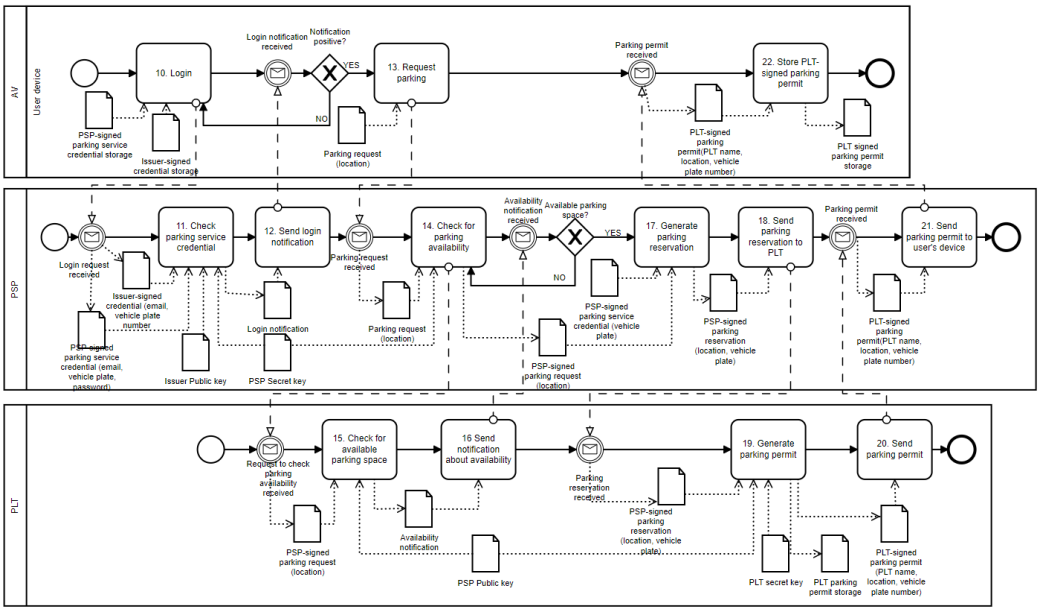

Figure 7. Privacy Enhanced Model for AVP:ABC

We assume an ABC scenario where the user obtains a valid credential from the issuer and presents parts of the attributes associated with the signed credential to the PSP system. Figure 7 illustrates the usage of the user's credential where the user presents it directly to the PSP with only as much needed information. The PSP verifies the user's credential based on the issuer's public signature and authenticates the user to access its service if the credential provided by the user is valid. As the user request for the parking service from the PSP, the user presents location information which the PSP uses to generate a parking reservation based on parking availability by the PLT and a parking permit. Although the location of the user is visible to the PSP, the presentation of it is done anonymously by the user. The user provides needed information to the system based on certain selected attributes from the signed credential. Also the word "signed" means that whatever issuer issued the credential to the user, the validity of the credential is based on that issuer's signature. With this, service providers can freely validate the user of the attributes by verifying with the issuer's public parameter or public signature. From the model in Figure 7 we notice how each data objects passing through the system is being assigned a signature by the system entities (PSP, PLT). This provides a sort of uniqueness in identification. This means that based on some type of mathematical computations or algorithm, the values provided from the signatures and attributes are unique to a particular person. Also, the signature represents validity of the information provided by the user or any of the systems.

3.4 Summary

This chapter introduces our proposed approach and illustrates our learning model for IoV scenario using BPMN. We illustrate a privacyless model for the IoV scenario and based on our scenario, we identified the different important data objects associated with the system and analyse the issue associated with the privacyless system. The privacy enhanced model for the IoV scenario was introduced for both the ABC and encryption and a brief analysis of the activities between the data objects across the system is done.

4 PET Privacy Evaluation

We evaluate the effectiveness of the PETs applied to the BPMN model in Chapter 3. This process would be done using a visibility matrix and then a privacy evaluation table to illustrate the privacy goals achieved by each PETs. The evaluation procedure is carried out on the privacyless model Figure 5 as well as the privacy enhanced models in Figure 6 and Figure 7 to show how effective each PETs applied was.

4.1 Privacyless model privacy property analysis

We analyse the privacy property of the applied PETs by following a visibility analysis on the PET applied models to produce a visibility matrix for our privacy property evaluation. This visibility process is carried out to evaluate the state of the data. By doing this, it is possible to analyse which privacy goal for each PET as laid out in Table 1 and Table 2 are achieved. This method can be exemplified in Table 6 and Table 7. The visibility matrix for the privacyless model in Table 6 shows the data object and at all points of interactions are visible to the IoV system entities. Therefore in our privacy evaluation in Table 7 for our privacyless model, no privacy property is achieved. We use a visibility score to get the final state of the data object across the system based on the consistency of the state of the data object.

The analysis of the privacyless model can be found below:

1. The parking service credential is believed to contain the user's identity which is visible to all system entities. Hence the user's identity is exposed across the system and the anonymity property is not achieved.

2. The messages (such as location, parking reservation, and parking permit etc.) transmitted between the systems can be linked back to the user. The property of unlinkability is not achieved in the system.

3. Messages transmitted across the systems can be modified by a honest IoV user during transmission. For instance parking permit can be intercepted between the PLT and the PSP and the data can be altered. Hence data integrity is not achievable in the system.

System Entity	D1	D2	D3	D4
User Device (AV)	V	V		V
On Board Unit (AV)				V
Parking Service Provider (PSP)	V	V	V	V
Parking Lot Terminal (PLT)			V	V
Visibility Score on Each Data Object	V	V	V	V

Table 6. Information Disclosure Analysis for AVP privacyless scenario. Denotations for data objects include; Parking Service Credential: $D1$, Parking Request: $D2$, Parking Reservation: $D3$, Parking Permit: $D4$.

Business Asset	Visibility Score	Privacy Property	PET Applied
D2	V	None	None
D3	V	None	None
D4	V	None	None
D5	V	None	None

Table 7. Privacy evaluation for privacyless model. Denotations for data objects include; $D1$: Parking Service Credential, $D2$: Parking Request, $D3$: Parking Reservation, $D4$: Parking Permit.

4.2 Encryption PET Privacy Property Analysis

The visibility matrix table for encryption in Table 8 shows that the contents of the data object identified in the IoV system is hidden. It also shows the states of each data objects across the system entities.

1. At the point of login with the PSP, the user presents an encrypted parking service credential. The credential is checked by the PSP based on its computational $PKComputation$ capabilities. The contents of the data is therefore unknown to the PSP and thus data privacy is preserved. The privacy property accomplished here is anonymity (the user's identity is unknown to the PSP), confidentiality (the PSP performs computations on the encrypted data without decrypting it).

2. The user makes a parking request and encrypts it before sending it out to the PSP. The PSP performs computations:$PKComputation$ on the encrypted parking request to generate the encrypted parking reservation. The contents of both the parking request and parking reservation is therefore unknown to the PSP. The privacy property accomplished here is confidentiality.

3. When the PSP sends out the encrypted parking reservation to the PLT, the PLT also performs computation:$PKComputation$ to generate the encrypted parking permit. The contents of both the encrypted parking reservation and encrypted parking permit are unknown to the PSP hence privacy of the encrypted parking permit and encrypted parking reservation is preserved at the PLT's end. The privacy property achieved here is confidentiality.

System Entity	D1	D2	D3	D4	D5
User Device (AV)	H	V	H		H
On Board Unit (AV)					H
Parking Service Provider(PSP)	H		H	H	H
Parking Lot Terminal (PLT)				H	H
Visibility Score on Each Data Object	H	V	H	H	H

Table 8. Visibility Analysis for AVP Scenario with encryption applied. Denotations for data objects include;$D1$: Encrypted parking service credential, $D2$: Parking request(location), $D3$: Encrypted parking request, $D4$: Encrypted parking reservation, $D5$: Encrypted parking permit.

Data Object	Visibility Score	PET Applied	Privacy Property
D1	H	Homomorphic Encryption	Anonymity, Confidentiality
D2	V	None	None
D3	H	Homomorphic Encryption	Confidentiality
D4	H	Homomorphic Encryption	Confidentiality
D5	H	Homomorphic Encryption	Confidentiality

Table 9. Privacy evaluation with encryption applied. Denotations for data objects include; Encrypted parking service credential: $D1$, Parking request: $D2$, Encrypted parking request: $D3$, Encrypted parking reservation: $D4$, Encrypted parking permit: $D5$.

4.3 Attribute Based Credential PET Privacy Property Analysis

The visibility matrix for ABC in Table 10 shows the state of the data objects when ABC mechanism is applied. As stated earlier in Section 2.5, the visibility matrix for ABC would be different from that of the normal identified ones in Section 2.5. This is because ABC does not provide confidentiality so the visibility rating *Hidden (H)* would not be ideal for ABC.

However, the major identified states of data objects when ABC is applied is *Authentication (A)* and *Verification (R)*. This would serve as our visibility rating for ABC in this thesis paper. *Visible (V)* would remain the same in the case a data object does not match *Authentication (A)* and *Verification (R)*. The privacy evaluation table (see Table 11) shows the condition of each data objects as it passes through the system. This analysis presented in this paper is done based on the presented ABC model (see Figure 7).

1. When the user requests login with the PSP using the issuer-signed credential and parking service credential, the PSP verifies the user's credentials with the issuer public key and authenticates the user to access the service if the credential is valid. By doing this, the user is able to prove ownership of some attributes requested by the PSP. The user does this anonymously and also discloses minimal information to the PSP. The privacy properties achieved here are minimal disclosure (the user is able to prove ownership of certain attributes without revealing too much information), anonymity (the PSP cannot identify the user from the presented attributes).

2. When the user requests a parking service with the PSP, the user does so anonymously and only with the intended location. The property of anonymity and minimal disclosure is achieved here. Although, the location is visible because no form of protection mechanism is applied to it.

3. Upon the receiving the parking service request, the PSP signs the request with its secret key and sends this signed request to the PLT to check for an available parking space. The property of, minimal disclosure (only the location is revealed by the user and the PSP to the PLT) and anonymity (The PSP and the PLT cannot identify the user from the attribute received) is achieved.

4. The PLT in turn delivers an availability notification to the PSP. The PSP then generates a signed parking reservation and sends this to the PLT. The

PLT then generates a signed parking permit and sends this to the PSP. The property of anonymity (the PSP and PLT cannot identify the user) is achieved here.

System	D1	D2	D3	D4	D5	D6
User Device	A	V			A	A
PSP	A, R	V	A	A	A	A, R
PLT			A, R	A, R	A	
Visibility Score on Each Data Object	A, R	V	A, R	A, R	A	A, R

Table 10. Visibility Analysis for AVP Scenario with ABC applied. Denotations for data objects include; PSP-signed Parking service credential:$D1$, Parking Request (location):$D2$, PSP-signed Parking Request:$D3$, PSP-signed Parking reservation:$D4$, PLT-signed Parking permit: $D5$, Issuer-signed Credential: $D6$.

Data Object	Visibility Score	Privacy Property	PET Applied
D1	A, R	Minimal disclosure, anonymity	ABC Computation, ABC authentication
D2	V	Minimal disclosure, anonymity	ABC
D3	A, R	Minimal disclosure and anonymity	ABC computation
D4	A, R	Anonymity	ABC computation
D5	A	Anonymity	ABC computation
D6	A, R	Anonymity, Minimal disclosure	ABC authentication

Table 11. Privacy evaluation with ABC applied. Denotations for data objects include; PSP-signed Parking service credential: $D1$, Parking Request: $D2$, PSP-signed Parking Request:$D3$, PSP-signed Parking reservation: $D4$, PLT-signed Parking permit: $D5$, Issuer-signed Credential: $D6$.

4.4 PET privacy property comparison

We compare the two PETs (encryption and ABC) identified in this paper under the context of our learning model (AVP). The reason for this comparison is to :

1. Analyse the performance of the two technologies (encryption and ABC) because clearly each technology serves a purpose and achieves certain privacy properties.

2. Analyse certain conditions each technologies operate under to achieve certain privacy properties. For instance, not all systems are capable of performing computational operations on encrypted data and also not all systems can perform revocation of credentials.

3. Select the best PET based on a proposed approach in identifying each points analysed above.

We identify the privacy properties achieved by ABC and encryption. By analysing our evaluation table we extract the privacy properties achieved by each PET from the privacy evaluation tables (see Table 11 and Table 9). The visibility matrix presents us with an evaluation that tells us the state of the data object (visible, hidden, authenticated or verified) as it passes through the systems, but the privacy evaluation gives details of important conditions of the data object at each system entities. For example, in the ABC model Figure 7, even though the parking request (location), is visible at the PSP's end the property of minimal disclosure and anonymity is achieved. Hence, for each data object to satisfy or meet each privacy properties, certain conditions must be met. Table 12 shows a PET comparison between encryption and ABC based on the privacy evaluation table.

Privacy properties	Condition 1	Condition 2	ABC data object	Encryption data object
Anonymity	Demonstrate possession of certain attributes without reviewing identity	Hiding identity	Satisfies condition 1 and2 data object involved are D1,D2,D3,D4,D5, D6	Satisfies condition 2 data object involved: D1
Zero knowledge proof	Obtain a signature from an issuer on a set of attributes so that the issuer is not able to see the values of the signed attributes	Prove the knowledge of a secret to a verifier without revealing it.	None	None
Confidentiality	Protecting data from unauthorized access by unauthorized persons	None	None	Satisfies condition1 data objects involved are D1,D2,D3,D4,D5
Minimal disclosure	Credentials do not leak any data either from the attributes to be verified	None	Satisfies condition 1 data object involved are D1,D2,D3,D6	None
Unlinkability	Presentation token cannot be traced back to the issued credential	Different presentation tokens cannot be linked to the same user	None	None
Revocation	When user changes attributes, credentials can be revoked	New presentation tokens can be verified after revocation	None	None

Table 12. PET comparison

4.4.1 Limitations and Recommendations

From Table 12, we can see that ABC and encryption both satisfies different equal privacy properties, although some of the data object (e.g location) in ABC are visible example location data. This doesn't mean that because a data object is visible then it does not satisfy any privacy property. Upon thorough analysis, we can say that location data presented was done anonymously by the user and no other information aside the location was disclosed. Hence, even in its visible state,

some privacy properties can be achieved depending on the conditions presented by the IoV system. Also, revocation of credentials is possible in a situation where the user decides to change attributes in the credential due to certain reasons such as the credential being compromised. In our model (Figure 7), the condition for credential revocation did not arise.

More privacy properties such as unlinkability, conditional anonymity, zero knowledge proof (ZPK), forward privacy and backward privacy etc. can be provided by ABC. In our ABC learning model Figure 7, the method presented is a generic ABC application of credential issuance and usage. The addition of a presentation token derivation by the user from their credential could enhance the effectiveness of privacy on the data object in the system to achieve the following:

1. Unlinkability: This has two instances: first, ensuring that the use of a presentation token cannot be traced back to the issued credential (issuance-show unlinkability). Second, different presentation tokens cannot be linked to the same user (multi show unlinkability) [13]. Our model fails to achieve this property because no presentation token was generated by the user at any point across the systems.

2. Pseudonyms: Users can create presentation tokens containing pseudonyms that are unlinkable to one another [13]. In our ABC model, since no presentation token was generated, it may not be possible to create pseudonyms.

3. Forward and backward privacy: The revocation of a credential does not affect the unlinkability of previously signed messages. Also, when the identity of the sender of a particular message is recovered through the identity resolution procedure, then the privacy of other messages signed by the same sender remains guaranteed [28]. In the case of our ABC model Figure 7, the revocation of a credential will affect unlinkability because this property was not achieved in the first instance. If an identity resolution procedure is being carried out, the privacy of other messages signed by the same sender is not guaranteed. This is because the sender can be linked directly to that message.

4. Zero Knowledge Proof (ZKP): ZKPs are a special form of cryptographic digital signatures that enable a user to obtain a signature from an issuer on a set of attributes without the issuer being able to see the values of the signed attributes. It is also the ability of a user to prove the knowledge of a secret to a verifier without revealing it. In our ABC model, the verifier can see the sets of attributes presented by the user. Hence this property is not achieved.

In the encryption model, although confidentiality and anonymity seems to be the only privacy properties achieved more properties can be achieved based on different cryptographic schemes like identity based encryption (IBE), attribute based encryption (ABE) etc. Although other cryptographic mechanism that achieves several other privacy properties such as differential privacy etc. exists, a combination of ABC and encryption could improve the overall privacy of data objects in the system.

4.5 Summary

This chapter evaluates the effectiveness of our identified PETs solution. It gives an analysis of both the privacyless model Figure 5 and privacy enhanced models Figure 6 and Figure 7 to show the gap between the two models in terms of privacy properties achieved. Also a comparison of both PETs based on the specific conditions identified by our analysis leads us to determine which PETs achieves more privacy property in the system.

5 Validation

In this Section 5 another IoV scenario that would be considered as a validation model is introduced. More illustration of the validation model can be found in Appendix C. The privacy analysis is done based on the presented models (Figure 9 and Figure 10).

5.1 Validation Procedure

The validation procedure aims to highlight the privacy properties achieved by combining the two PETs under different conditions, showing the effectiveness of each PETs as it is applied to a data object. We determine why each PET is most suitable to the data object. The reason for the combination of both PETs is to achieve an effective privacy preserving IoV, this would lead us to achieving more privacy properties by taking into considerations our approach to deeply understand the state and condition of each data object at any given point in time in the system.

Also several privacy experts made efforts to validate mainly the attribute based credential for our learning model. With that foundation, more ABC techniques such as generation of a presentation token and generation of pseudonyms from presentation tokens were considered in our validation model. Although some privacy properties (such as forward and backward privacy) which doesn't really take into account the business process of the IoV system can also be achieved. These privacy properties takes into consideration unforeseen events such as the need to recover identity of a stolen car. Although not explicitly discussed in our validation model, backward and forward privacy can be achieved going by our validation model as the only limitation has to be that an event to warrant such privacy properties needs to arise.

5.2 Validation Scenario: Car Sharing

Car-Sharing systems, which allow people to rent vehicle for short periods of time, are a complementary to private vehicle ownership. They are attractive to customers who make only occasional use of a vehicle, as well as others who would like occasional access to a vehicle of a different type than they use day-to-day [26].

5.2.1 Privacyless BPMN Model for Car sharing

For more complete information about the car sharing model, please see Appendix C.

The model in Figure 8 provides information of an "after trip" using a car sharing service. This model involves two system entities (car sharing provider and user's bank) and a user. The user communicates directly with the car sharing provider (CSP) and presents the trip information (such as duration and location of the user's final destination) to the CSP. With this information (duration), the CSP computes an amount that would be charged on the user's card. The CSP charges the amount on the user's card and sends the payment transaction generated as a result of the charged amount to the user's bank. The user's bank processes the payment and notifies both the CSP (as a credit transaction) and the user (as a debit transaction) about the payment.

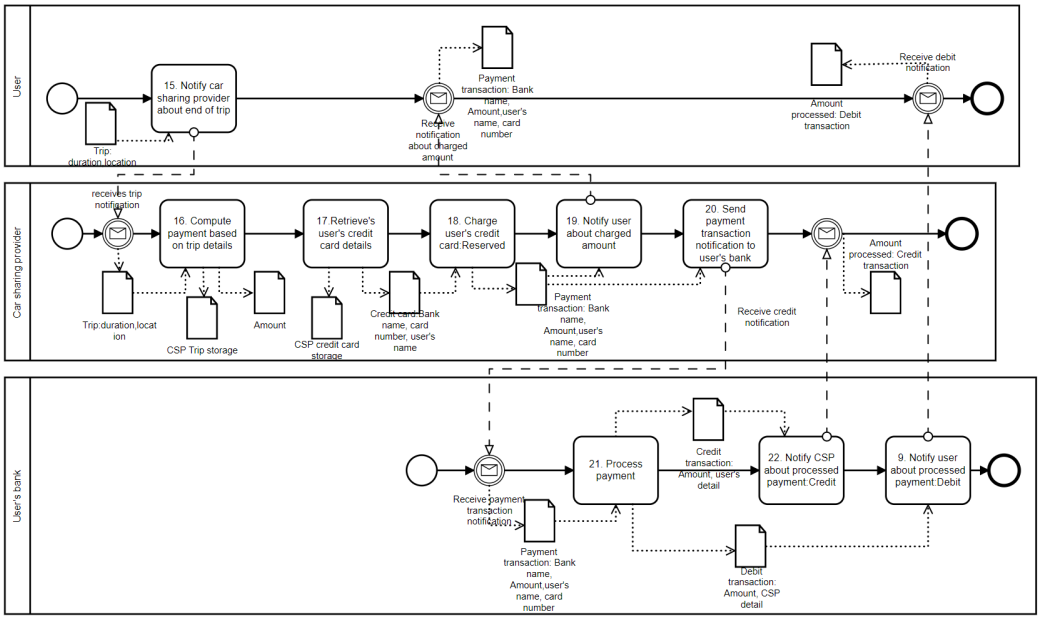

Figure 8. Privacyless Model: Car Sharing (After Trip)

5.2.2 Data Object Identification

In the model Figure 8, there are at least three system entities involved in the communication process. The user interacts directly with the car sharing provider (CSP), while the CSP interacts with both the user and the user's bank. In this case, the user's bank is a third party system entity because the CSP relays information about the user to the bank. The Table 13 identifies the system assets and the supporting data object

System Assets	Data Object Identification
User's device	Provide basis of interaction with car sharing provider. Has access to user's details such as registration data for enrollment at the CSP
CSP, CSP login storage	Collect user registration data, store CSP login, carry out login procedure, use customer's location to find vehicles, access customer's driver's license and credit card information, communicates payment transaction to user's bank
User's Bank	Access customer's information from payment transaction details, send debit and credit transactions to customer and CSP respectively

Table 13. Data Object Identification

5.2.3 Privacy Enhanced Model

We present two privacy enhanced model for our validation based on the combination of both PETs discussed in this model. In the model Figure 9, we notice an upgrade from the previous ABC learning model illustrated. We assume the user has issuer-signed credentials and generates a presentation token based on the issuer-signed credential to register with the CSP. The presentation token generated by the user contains the issuer's signature and a single attribute from the user's credentials. The CSP verifies the credential based on the issuer's public key. When the CSP generates the login details, it is signed with its private key.

In the second model, the user communicates directly with the car sharing provider (CSP) and presents trip information (such as duration and location of the user's final destination). With this information (duration), the CSP computes an amount that would be charged on the user's card. The CSP charges the user's card and sends a notification to the user. The payment transaction produced is encrypted with the bank's public key: $PKEncryption$ and sent to the bank. The bank receives the payment transaction from the CSP and decrypts it with private/secret key to reveal the payment transaction in its unencrypted form. The bank then process payment and encrypt the payment notifications (debit and credit transaction) respectively for the user and CSP with their respective public keys. So the bank sends out the encrypted debit transaction to the user and encrypted credit transaction to the CSP. The user decrypts the encrypted debit transaction with their private/secret key and the CSP decrypts its encrypted debit transaction with its private/secret key.

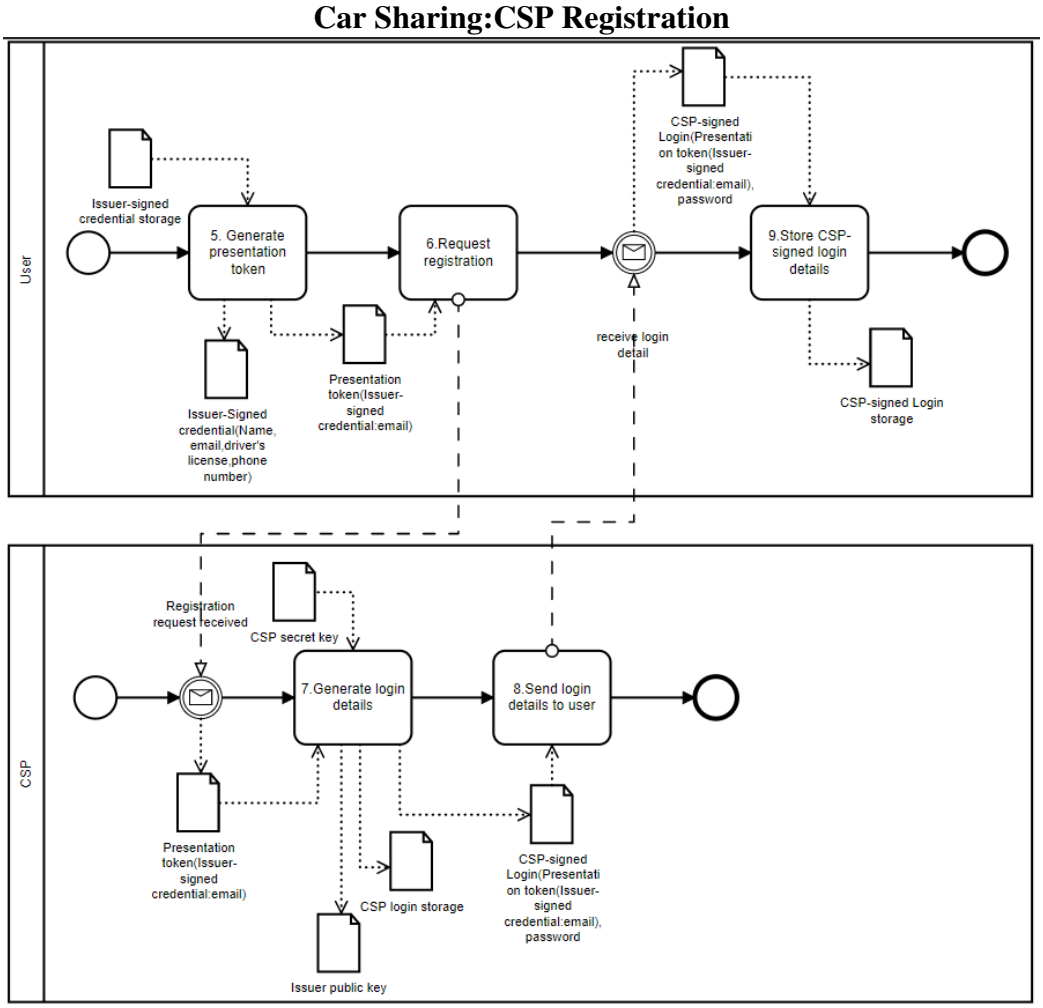

Figure 9. Privacy Enhanced Model: Car Sharing

Both models in Figures 9 and 10 illustrate the combination of both PETs (encryption and ABC) to the system to improve the overall effectiveness of the data object privacy in the system. However, in the case of the payment process to the bank the user's privacy is not preserved at the bank's end. This is because the bank can see the data object values (payment transaction) that is being sent by the CSP. In this case the bank does not possess computational capabilities due to verification of important information from the user such as:user's account balance, correct account details sent etc. The bank needs this information to carryout the payment process. For instance if the user does not have sufficient balance, the bank

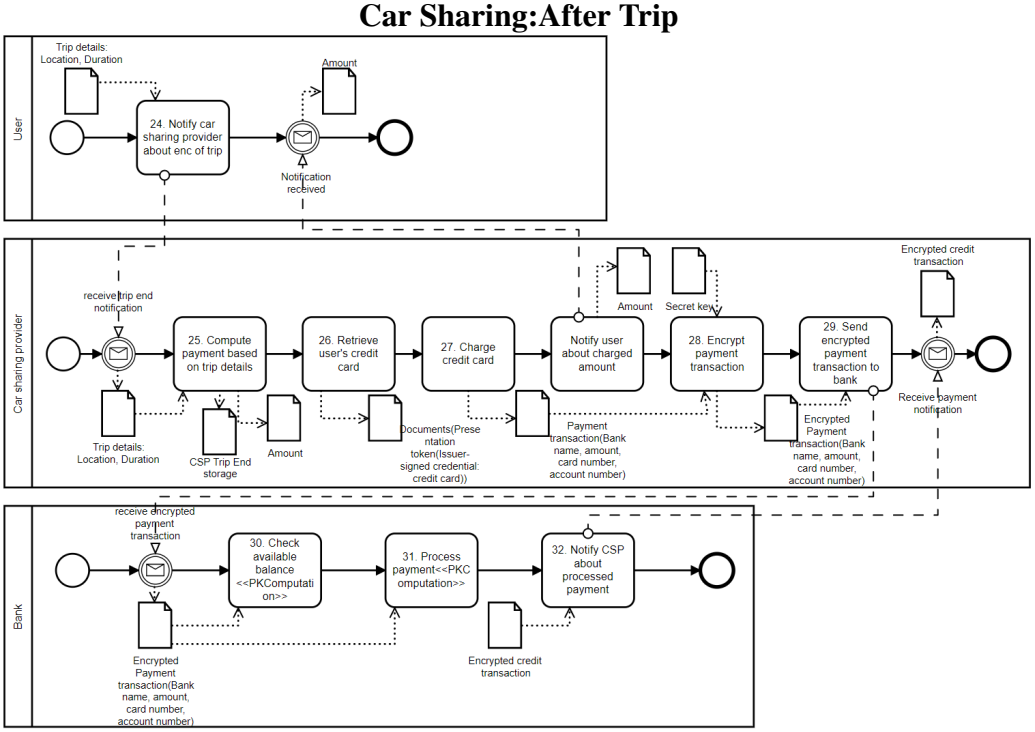

Figure 10. Privacy Enhanced Model: Car Sharing

can immediately reject the transaction.

5.2.4 PET Privacy Evaluation

The visibility matrix for the car sharing scenario in Table 14, shows the visible, authenticated and verified contents of the data object identified in the IoV system. The privacy evaluation in Table 15 shows the state of the condition of each data object. In our evaluation, we would be highlighting each PET mechanism applied and why it was being applied. Furthermore, a standard PET comparison would be done between both PETs and we would be highlighting certain limitations of each PETs and recommendations for future research work.

1. We assume an issuer's-signed credential is being issued to the user to present to a service provider. The presentation token generated from the signed credential presents only the required attributes requested by the system. The privacy property of minimal disclosure (only needed attributes are disclosed), anonymity (the CSP cannot identify the user from the presented attributes),

unlinkability (the presentation token cannot be traced back to the issued credential and the presentation token cannot be linked backed to the same user) is achieved. We applied ABC here because we want to selectively authenticate the attributes presented by the user without revealing additional information to the CSP.

2. The CSP-signed login detail is used to authenticate the user to access the service of the provider. The privacy property of anonymity, minimal information disclosure is achieved here. Anonymity is achieved because the CSP cannot identify the user from the information given, minimal information disclosure is achieved because only the needed information was provided by the user. We applied ABC here because we want to selectively authenticate the attributes presented by the user without revealing additional information to the CSP.

3. Encrypted payment transaction, debit and credit transaction both achieve the privacy property of confidentiality. The CSP encrypts the payment transaction before it is being sent to the user's bank for processing. The bank decrypts the payment transaction and processes payment for the CSP. After payment processing, the bank notifies the CSP and the user of the respective encrypted credit and encrypted debit transaction. The privacy property achieved here is confidentiality. Anonymity is not achieved here because the bank can identify the user from the data object values (payment transaction). We applied encryption here because the CSP needed to send very sensitive and much needed information of the user across an untrusted channel to a third party entity (user's bank). All information sent to the third party (user's bank) is needed by the third party to process transaction so selective presentation of attribute by the CSP cannot be used.

System	D1	D2	D3	D4	D5	D6	D7	D8
User	A	A	V			A	H	
CSP	A, R	A, R	V	H	H	A, R		V
User's bank				H	H		H	V
Visibility Score on Each Data Object	A, R	A, R	V	H	H	A, R	H	V

Table 14. Visibility matrix for privacy enhanced car sharing model. Denotations for data objects include;$D1$: Presentation Token, $D2$: CSP-signed Login, $D3$: Trip End Details, $D4$: Encrypted Payment Transaction, $D5$: Encrypted Credit Transaction, $D6$: Issuer-signed credential, $D7$: Encrypted debit transaction, $D8$: Payment transaction

Business Asset	Visibility Score	Privacy Property	PET Applied
D1	A, R	Minimal disclosure, anonymity, unlinkability	ABC authentication, ABC computation
D2	A, R	Anonymity	ABC authentication, ABC computation
D3	V	None	None
D4	H	Confidentiality	Public key encryption
D5	H	Confidentiality	Public key encryption
D6	A, R	Revocation, anonymity	ABC authentication
D7	H	Confidentiality	Public key encryption
D8	V	None	None

Table 15. Privacy Evaluation Table:Car Sharing

5.2.5 Privacy Comparison

From the PET comparison Table 16, we see a slightly higher privacy property achieved and still by ABC. Although some of these other properties not achieved right now is due to the limitations in the IoV context we are dealing with. In a complete scenario as seen in Appendix C, revocation on a credential is possible. Zero knowledge proof is not possible with our system because the issuer can see all the attributes values in our enrollment data (please refer to Appendix C).

Also, in the encryption Figure 10, we see the payment transaction being visible at the bank's end. This is because the bank needs to see the information contained in the payment transaction before payment processing is done so as to avoid the bank accepting transactions that are not valid (such as insufficient amount in the

Privacy Properties	Condition 1	Condition 2	Encryption	ABC
Anonymity	Demonstrate possession of attributes without reviewing identity	Hiding Identity	Satisfies 2,data object involved D4	Satisfies 1 and 2,data object involved D1,D2,D6
Confidentiality	Protecting data from unauthorized access by unauthorized persons	None	Satisfies 1 data object involved D4,D5,D6	Satisfies 1 data object involved include D1 and D2
Unlinkability	Presentation token cannot be traced back to the issued credential	Different presentation tokens cannot be linked to the same use	None	Satisfies 1 data object involved D1
Pseudonyms	Users can create presentation tokens containing pseudonyms that are unlinkable to one another	None	None	Satisfies 1 data object involved D1
Zero Knowledge proof	Obtain a signature from an issuer without the issuer being able to see the values of the signed attributes	Prove the knowledge of a secret to a verifier without revealing it	None	None
Revocation	When user changes attributes,credentials can be revoked	New presentation tokens can be verified after revocation	None	Satisfies 1,data object involved D6

Table 16. PET comparison for Car Sharing scenario

account). Also, even if the bank were to be able to perform computations on an encrypted data, it cannot send the debit transaction to the user because the CSP would use its secret key to encrypt the data, and the user would need the CSP's secret key to decrypt the data, hence the feasibility of the bank performing computations on an encrypted data may not be practical.

5.2.6 Limitations of Validation Model

In our validation model (Figure 9 and Figure 10), we combined the PETs (encryption and ABC) involved in this paper to evaluate the overall privacy of the system achieved. As stated in our recommendation in Section 4.4.1, the addition of the presentation token improved the privacy of the system. Although, there are still some limitations of this technology in application to our validation model:

1. Forward and backward privacy is achievable with our model if the need arises, in our model there was no need for the forward or backward privacy as the need for it did not arise or was not part of the scenario.

2. The banking scenario does not present us with the practicality of performing computations on encrypted data due to reliance on external gateway information (such as important payment processing details). Hence, confidentiality is not being achieved at the banks end.

5.3 Difference Between Learning Model and Validation Model

The difference between both models would be classified under the following; privacy properties achieved, IoV context and PETs applied. In general, certain conditions have to occur for each privacy property to surface. The following differences are observed when our learning model (AVP) is compared to our validation model (car sharing):

1. IoV context: The two scenarios are different and as such there might not be any need to achieve some of the privacy properties. For instance in the AVP model, there was no need to generate pseudonyms because: there was no presentation token generated and secondly even if we do generate a presentation token, the presentation of the token is done only once (during PSP registration). Whereas in our validation model (car sharing), we had the presentation tokens presented to the car sharing provider (during registration with the CSP) so it is possible to generate a pseudonym . So the possibility to get the pseudonym property is much achievable in the second model.

2. The first model is a learning model for this thesis work. It forms the framework of how each PETs works when applied. With that basic understanding, the validation model gives us an in depth knowledge of the PETs. For instance in the ABC for our learning model (Figure 7), we noticed a more generic framework description of how ABC generally works. However, in

our validation model (Figure 9) we notice the upgrade of the ABC technology. Also, in our learning model for encryption (Figure 6), we noticed that all systems are capable of performing computations on encrypted data. However, in our validation model for encryption (Figure 10), the banking system cannot perform computation on encrypted data. This is due to the difference in the data object provided.

3. The validation model takes the combination of both PETs and apply it to the data objects of the entire system. We see the need for encryption and the need for ABC. Encryption protects the sensitive data that passes across the communication channels that is not protected. The illustration of ABC here shows that selective attributes can be passed out for authentication without revealing much information. The overall privacy of the system can be even greater with more research and study. For instance achieving the ZKP, the system would have to come up with a way to ensure that the user's attributes are not visible to the issuer.

4. There are a lot of environmental and structural complexities in the IoV context. Our two models (learning and validation) projects this different environmental and structural complexities and as such we can see the different underlying objectives of the PETs when applied to the system. For instance in our validation model for encryption (Figure 10) , we can see that not all the systems in the IoV context can perform computation on an encrypted data object. Whereas, our learning model for encryption (Figure 6) shows that all systems in the IoV context can perform computation on encrypted data.

5.4 Threats to Validity

The major threat to validity of this research work is lack of our underlying model subjected to optimization. The IoV environment under which PETs are applied is very complex and dynamic and as such leaves a huge gap between our model and real life scenario. This gap is showed in the privacy result achieved by both the learning models Figure 6 and Figure 7 and the validation models Figure 10 and Figure 9 where we notice that the two different IoV scenario illustrated in this paper requires different data objects, system entities and most importantly different conditions for each privacy properties to be achieved.

5.5 Analysis of our Approach

In the context of our learning model Figure 6 and Figure 7 and validation model Figure 9 and Figure 10, location privacy is of utmost importance as the location can reveal an individual's identity as identified by both the learning and validation model. Other information such as vehicle plate number, credit card details, and driver's license are also sensitive information as they may reveal user's identity. Our approach is based on analysing and evaluating the state of these sensitive information we term as data object. We provide information of an overview of the analysis carried out with our approach:

1. Preservation evaluation: Based on our approach, one can identify the asset being preserved is data objects. Our approach also outlines the data objects (such as driver's license, registration data etc.) being preserved and identifies what is protected or preserved and what is not protected or preserved. In our encryption model Figure 6, we can see from our evaluation that the user's identity was preserved during authentication process with the PSP. The user identity is the data attribute that is being preserved. Also in our ABC model Figure 7 we can see that no PET protection was applied to the parking request.

2. Condition evaluation: By applying our method, it is possible to analyse the outcome of a particular situation under some given conditions in a system. For our case, by analysing the models (both privacyless and privacy enhanced models), one can identify under some given conditions what is possible to be achieved at the end. For instance in the ABC model Figure 7, with the user's possession of an issuer's-signed credential, identity forgery can be prevented and the user can remain anonymous when authenticating with the systems.

3. Compliance: It is possible to determine generally weather a system is being compliant to a privacy framework like ENISA. By analysing the evaluation table in a quick glance (Table 12), some privacy features related to ENISA privacy framework can be identified.

4. Evaluating the suitable PET for the scenario: By employing our method, a user can directly compare several PETs to determine the best under different conditions being presented. For example, in our IoV scenario, after several evaluation of ABC and encryption (Table 12), it is possible to determine which PET technique is the best for the scenario presented.

5. Business benefit: With the evolution in IoT, businesses are tasked strictly with keeping privacy of individual data especially service providers that operate cloud-based database. In our case, the PSP and PLT can be assumed as cloud based service providers that collects individual information for processing. To this effect, these cloud-based service providers need a breakdown of how user privacy can be achieved from point of collection to point of processing. It provides them with a clear concept and visualisation and also as mentioned earlier help them get to standard for some privacy frameworks.

5.6 Summary

The chapter provides us with another IoV scenario that is considered as a validation model and based on our research approach, we evaluate the privacy properties achieved when the two PETs involved in this paper (encryption and ABC) are combined. Furthermore, based on the validation of our learning model by privacy experts we developed further our validation model to take into consideration more characteristics so as to achieve an effective privacy system.

6 Conclusion

This chapter summarizes the thesis paper which includes limitations of our research, answer to the research question, proposal for future work and concluding remarks.

6.1 Limitation of Research

The limitations of this research work are as follows:

1. Unlike internet of things, internet of vehicle is highly dynamic. The privacy properties that can be achieved in an IoV scenario is not entirely generic. Our IoV scenarios presents us with privacy properties slightly different from the other because current conditions were being taken into considerations. However, for the privacy implementation of an IoV system different possible conditions (both the main business process and unforeseen conditions such as the need to identify a criminal or recover a stolen vehicle) has to be put into considerations.

2. This thesis research focuses on only the protection of data objects collected from individuals or user's. The system assets that supports the business data objects in this case (for example the communication channel and the data object storage) are not considered due to several complexities and derailment from the focus of this paper. However, for system implementation purpose the system assets have to be considered for more privacy effectiveness provided by our PETs.

3. Laying emphasis on privacy alone does not achieve much result. There is a need to include security as well because the two (privacy and security) go hand in hand.

6.2 Answer to Research Questions

This section provides the answers to the research question in Section 1.3.

- RQ1. *How can we identify business objects in IoV?*
  The identification of business objects in IoV was done based on an IoV use case (scenario). The business process of the scenario was studied and a BPMN model of the IoV scenario was done. The BPMN model provided the base for important data object identification in the IoV scenario. The

privacyless BPMN models illustrated in our research work helps us with the identification of our data objects. According to our models, the data objects vary depending on the IoV scenario. For instance in our learning model, the data objects identified (Table 5) were slightly different from the data objects identified in our validation model (Table 13). Likewise other use-cases not mentioned in this paper for instance a ticketing system for transportation.

- RQ2. *How can the identified PETs analysed in this paper be applied to the related data object in IoV system context?*
  As stated earlier the BPMN model of our IoV scenario provided a base for important data object identification. Hence in the PET-related case, a privacy enhanced BPMN would be our base for analysing PET-related activities taking place in the IoV system. PE-BPMN constructs and specifies PETs that can be used on process models. In our case, we are confined to the application of PETs to our data objects which is quite crucial since we are dealing with very sensitive private data.

- RQ3. *How can we evaluate the privacy of the related data object in IoV system context after the PETs application?*
  Evaluating the privacy of the data related objects comes in two different stages: identifying the state of the object in the system and understanding the condition of the object in the system. The visibility matrix table helps us to identify the state of the object (see Table 14) in the system which is a crucial aspect to our final analysis and conditional evaluation. By understanding the condition of a given data object at a particular point in time in a system, it is possible to evaluate the privacy properties of the system. This is one of the limitations of our research work not being able to identify all possible conditions pertaining to IoV. Hence when comparing the state and condition of each data object, it is possible to evaluate the effectiveness of the PETs applied.

- RQ4. *What is the usefulness of our solution?*
  By implementation our solution and taking into considerations that this research work is purely theoretical, we achieve a head start when planning on implementing privacy into a system. Also, emphasis is being laid on the critical evaluation of data object which can give us edge in several privacy frameworks to analyse what privacy property can be achieved.

6.3 Concluding Remarks

The development of this research work was guided by the main research question "**What PET solution is best for mitigating privacy leakage in IoV?**". This research work implemented various approach such as IoV business process identification (scenario), data object identification, IoV privacy enhanced business process identification, PET evaluation to analyse our entire IoV system.

By identifying the IoV business process, we focused on a particular system context to provide detailed step by step information flow and communication process of the entire system. We also identified the system entities involved in the business process which gave us an understanding of how a third party system is involved in the entire communication process, how our data is being collected, how our data collected is being used and shared between systems etc. By understanding this IoV framework, we then went ahead to identify the data objects collected by the system. The data objects collected by the system are highly personal and sensitive data hence the reason for our third approach. The privacy enhanced business process model shows the PET-related activities in the system. In our case, not much emphasis is not being laid on the system assets but rather our focus is on data objects collected by the system. The application of PETs to these data objects erases the privacy concerns of individuals and also protects individual from unnecessary identification, document forgery and linkability. However, each PETs applied to our data objects achieved some privacy properties that somehow protects the user. However in our validation model, the need to combine both PETs is to achieve more privacy properties and evaluate the effectiveness of the combination. The next approach was to evaluate the privacy enhanced business process model by identifying the state of the data object in the system and evaluating the condition of the data objects upon the which the state reflects. By doing this, we achieve a more concrete reason of why a privacy property is achieved. The condition of the data object matters a lot because it gives the final evaluation of the PET effectiveness.

6.4 Proposals for Future Work

As discussed in the previous sections, emphasis is being laid on privacy protection on data objects. A lot of privacy concerns on the data objects are being raised daily and this constitutes the basis of several privacy framework. As a proposal for future work, the overall implementation of privacy in an IoV context should take into considerations unforeseen circumstances rather than just the business process.

Also, the concept of ABC that was introduced in this paper is on a generic level,

as a future proposal for research more holistic approach of ABC and encryption should be considered to achieve an effective privacy preservation of a system.

References

[1] Al-Hazaimeh, O.M., Alhindawi, N., Otoum, N.A.: A novel video encryption algorithm-based on speaker voice as the public key. In: 2014 IEEE International Conference on Control Science and Systems Engineering. pp. 180–184. IEEE (2014)

[2] Alghanim, A.A., Rahman, S.M.M., Hossain, M.A.: Privacy analysis of smart city healthcare services. In: 2017 IEEE International Symposium on Multimedia (ISM). pp. 394–398. IEEE (2017)

[3] Ali, Q.E., Ahmad, N., Malik, A.H., Ali, G., Rehman, W.U.: Issues, challenges, and research opportunities in intelligent transport system for security and privacy. Applied Sciences **8**(10), 1964 (2018)

[4] Bao, S., Cao, Y., Lei, A., Asuquo, P., Cruickshank, H., Sun, Z., Huth, M.: Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems. IEEE Access **7**, 80390–80403 (2019)

[5] Bichsel, P., Camenisch, J., Dubovitskaya, M., Enderlein, R., Krenn, S., Krontiris, I., Lehmann, A., Neven, G., Nielsen, J.D., Paquin, C., et al.: D2. 2 architecture for attribute-based credential technologies-final version. ABC4TRUST project deliverable. Available online at https://abc4trust. eu/index. php/pub (2014)

[6] Bunn, S.: Data encryption. Parliamentary Office of Science and Technology (2006), `https://www.parliament.uk/documents/post/postpn270.pdf`

[7] Büttner, C., Huss, S.A.: Attribute-based authorization tickets for car-to-x communication. In: 2016 IEEE Conference on Communications and Network Security (CNS). pp. 234–242. IEEE (2016)

[8] Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., Zwingelberg, H.: D2. 1 architecture for attribute-based credential technologies-version. Tech. rep., Technical report, ABC4Trust Consortium (December 2011), https://abc4trust ... (2011)

[9] Cha, S.C., Hsu, T.Y., Xiang, Y., Yeh, K.H.: Privacy enhancing technologies in the internet of things: Perspectives and challenges. IEEE Internet of Things Journal **6**(2), 2159–2187 (2018)

[10] Eckhoff, D., Wagner, I.: Privacy in the smart city—applications, technologies, challenges, and solutions. IEEE Communications Surveys & Tutorials **20**(1), 489–516 (2017)

[11] Fernandez, S., Ito, T.: Driver classification for intelligent transportation systems using fuzzy logic. In: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). pp. 1212–1216. IEEE (2016)

[12] de Fuentes, J.M., González-Manzano, L., Serna-Olvera, J., Veseli, F.: Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities. Personal and Ubiquitous Computing **21**(5), 869–891 (2017)

[13] de Fuentes, J.M., Gonzalez-Manzano, L., Solanas, A., Veseli, F.: Attribute-based credentials for privacy-aware smart health services in iot-based smart cities. Computer **51**(7), 44–53 (2018)

[14] Galil, Z., Haber, S., Yung, M.: Symmetric public-key encryption. In: Conference on the Theory and Application of Cryptographic Techniques. pp. 128–137. Springer (1985)

[15] Gunjal, Y.S., Gunjal, M.S., Tambe, A.R.: Hybrid attribute based encryption and customizable authorization in cloud computing. In: 2018 International Conference On Advances in Communication and Computing Technology (ICACCT). pp. 187–190. IEEE (2018)

[16] Guo, N., Jin, Y., Yim, K.: Anonymous credential-based privacy-preserving identity verification for business processes. In: 2014 Eighth international conference on innovative mobile and internet services in ubiquitous computing. pp. 554–559. IEEE (2014)

[17] Hajny, J., Malina, L.: Unlinkable attribute-based credentials with practical revocation on smart-cards. In: International Conference on Smart Card Research and Advanced Applications. pp. 62–76. Springer (2012)

[18] Hajny, J., Malina, L., Dzurenda, P.: Practical privacy-enhancing technologies. In: 2015 38th International Conference on Telecommunications and Signal Processing (TSP). pp. 60–64. IEEE (2015)

[19] Han, J., Chen, L., Schneider, S., Treharne, H., Wesemeyer, S.: Privacy-preserving electronic ticket scheme with attribute-based credentials. IEEE Transactions on Dependable and Secure Computing (2019)

[20] Huang, C., Lu, R., Lin, X., Shen, X.: Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles. IEEE Transactions on Vehicular Technology **67**(11), 11169–11180 (2018)

[21] Kang, Y., Lee, H., Chun, K., Song, J.: Classification of privacy enhancing technologies on life-cycle of information. In: The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007). pp. 66–70. IEEE (2007)

[22] Karnouskos, S., Kerschbaum, F.: Privacy and integrity considerations in hyperconnected autonomous vehicles. Proceedings of the IEEE **106**(1), 160–170 (2017)

[23] Kombate, D., et al.: The internet of vehicles based on 5g communications. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). pp. 445–448. IEEE (2016)

[24] Koning, M., Korenhof, P., Alpár, G., Hoepman, J.H.: The abc of abc: An analysis of attribute-based credentials in the light of data protection, privacy and identity (2014)

[25] Ma, M., He, D., Kumar, N., Choo, K.K.R., Chen, J.: Certificateless searchable public key encryption scheme for industrial internet of things. IEEE Transactions on Industrial Informatics **14**(2), 759–767 (2017)

[26] Maaser, M., Ortmann, S.: Providing granted rights with anonymous certificates. In: 2008 15th IEEE International Conference on Electronics, Circuits and Systems. pp. 890–893. IEEE (2008)

[27] Neisse, R., Baldini, G., Steri, G., Miyake, Y., Kiyomoto, S., Biswas, A.R.: An agent-based framework for informed consent in the internet of things. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). pp. 789–794. IEEE (2015)

[28] Neven, G., Baldini, G., Camenisch, J., Neisse, R.: Privacy-preserving attribute-based credentials in cooperative intelligent transport systems. In: 2017 IEEE Vehicular Networking Conference (VNC). pp. 131–138. IEEE (2017)

[29] Ni, J., Lin, X., Shen, X.: Toward privacy-preserving valet parking in autonomous driving era. IEEE Transactions on Vehicular Technology **68**(3), 2893–2905 (2019)

[30] Pullonen, P., Tom, J., Matulevičius, R., Toots, A.: Privacy-enhanced bpmn: enabling data privacy analysis in business processes models. Software & Systems Modeling pp. 1–30 (2019)

[31] Qi, F., Li, K., Tang, Z.: A multi-authority attribute-based encryption scheme with attribute hierarchy. In: 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC). pp. 607–613. IEEE (2017)

[32] Ren, Y., Wang, S., Zhang, X., Qian, Z.: Fully secure anonymous identity-based encryption under simple assumptions. In: 2010 International Conference on Multimedia Information Networking and Security. pp. 428–432. IEEE (2010)

[33] Serna-Olvera, J.M.: A trust-driven privacy architecture for vehicular ad-hoc networks (2013)

[34] Silva, R., Iqbal, R.: Ethical implications of social internet of vehicles systems. IEEE Internet of Things Journal **6**(1), 517–531 (2018)

[35] Singh, K.J., Manimegalai, R.: Evolution of encryption techniques and data security mechanisms. World Applied Sciences Journal **33**(10), 1597–1613 (2015)

[36] Sucasas, V., Mantas, G., Saghezchi, F.B., Radwan, A., Rodriguez, J.: An autonomous privacy-preserving authentication scheme for intelligent transportation systems. Computers & Security **60**, 193–205 (2016)

[37] Toots, A., Tuuling, R., Yerokhin, M., Dumas, M., García-Bañuelos, L., Laud, P., Matulevičius, R., Pankova, A., Pettai, M., Pullonen, P., et al.: Business process privacy analysis in pleak. In: International Conference on Fundamental Approaches to Software Engineering. pp. 306–312. Springer (2019)

[38] Wang, Q., Qiu, X., Zhang, Q., Tang, C.: Key privacy in mceliece public key cryptosystem. In: 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. pp. 824–828. IEEE (2011)

[39] Wang, Z., Huo, W., Yu, P., Qi, L., Cao, N.: Research on vehicle taillight detection and semantic recognition based on internet of vehicle. In: 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). pp. 147–1473. IEEE (2018)

[40] Yang, F., Wang, S., Li, J., Liu, Z., Sun, Q.: An overview of internet of vehicles. China communications **11**(10), 1–15 (2014)

[41] Zhang, M., Wang, S., Zhang, P., He, L., Li, X., Zhou, S.: Protecting data privacy for permissioned blockchains using identity-based encryption. In: 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). pp. 602–605. IEEE (2019)

[42] Zhu, L., Yu, F.R., Wang, Y., Ning, B., Tang, T.: Big data analytics in intelligent transportation systems: A survey. IEEE Transactions on Intelligent Transportation Systems **20**(1), 383–398 (2018)

[43] Zualkernan, I.A., Aloul, F., Al Qasimi, S., AlShamsi, A., Al Marashda, M., Ahli, A.: Digimesh-based social internet of vehicles (siov) for driver safety. In: 2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI). pp. 1–5. IEEE (2018)

Appendices

A Search Process

For this thesis search process, digital libraries such as IEEE Xplore,Springer, Science Direct were used. The search queries included ("Autonomous vehicles" OR "connected vehicles" OR "IoT") AND ("privacy" AND "privacy leakage") AND (BPMN OR PE-BPMN OR SPBAC), ("Privacy Enhancing Techniques" AND "Attribute Based Encryption").

A.1 Paper selection

The papers selected were subjected to initial filtering by reading through the abstract and a quick scan of the entire article to ascertain the relevance to my research work. To select our papers that are more in line with our research, the following filters were used;

1. **Filter 1:** All research papers, journals, conference proceedings etc. were subjected to initial filtering of inclusion/exclusion (see Table18). Table17 presents the result of applying the inclusion/exclusion criteria resulting in a total of 49 results.

2. **Filter 2:** After undergoing the first filter process, the selected papers were screened by Kitchenham quality guidelines with the following questions:

1. Does the research paper cover the scope of work?

2. Does the research paper describe privacy issues as related to internet of vehicles and does it identify possible mitigation to the mentioned issues?

3. Does the paper provide information of privacy enhancing technologies as identified in our paper?

The answers to above questions are scored as follows: 1 = Fully satisfied, 0.5 = Partially satisfied, 0 = Not satisfied. The outcome of the

A.2 Selected search sources for literature review

Sources	IEEE	Science Direct	Springer	Other sources
Filter 1	43	6	7	23
Filter 2	27	2	3	11

Table 17. Selected Sources for Literature Study

A.3 Inclusion/Exclusion Criteria

Table18 shows the inclusion and exclusion criteria for this thesis paper.

Inclusion	Exclusion
Research papers that are in the scope of IoV, ITS, Autonomous vehicles and hyper-connected vehicles .	Research papers that are not in scope of IoV, ITS, Autonomous vehicles and hyper-connected vehicles
Research papers that covers the scope of PE-BPMN,and BPMN modelling techniques.	Research paper that are in scope of other modelling techniques aside PE-BPMN and BPMN.
Research paper that are from digital libraries, blogs.	Masters thesis of students.
Research papers in scope of PETs such as encryption, attributes based	Research papers that are in scope of other protection techniques aside the mentioned ones
Research papers in scope of privacy and security	Research papers in scope of only security

Table 18. Inclusion/Exclusion Criteria

B AVP Scenario

This subsection provides more information on our learning model (AVP) scenario.

B.1 Phase 1:Register with Parking Service Provider (PSP)

The privacyless models shows the registration process for the Automated Valet Parking. In this scenario we have two system entities Autonomous Vehicle (user device) and Parking Service Provider (PSP), involved in the process and communication flow.The scenario description for B.1 can be illustrated in Figure11 is follows;

1. The user with his smart device (e.g smart phone) registers his personal data (name, email, phone, vehicle plate number) with the PSP to get a parking service credential.

2. The PSP receives the user's data for registration and generates a parking service credential based on the user data.

3. The parking service credential generated by the PSP is then sent to the user's device. The parking service credential would serve as a login authentication entity for the user when he intends to use the PSP service. The PSP updates it's credential storage (PSP credential storage).

Figures 11, 12, and 13 shows the privacyless AVP scenario.

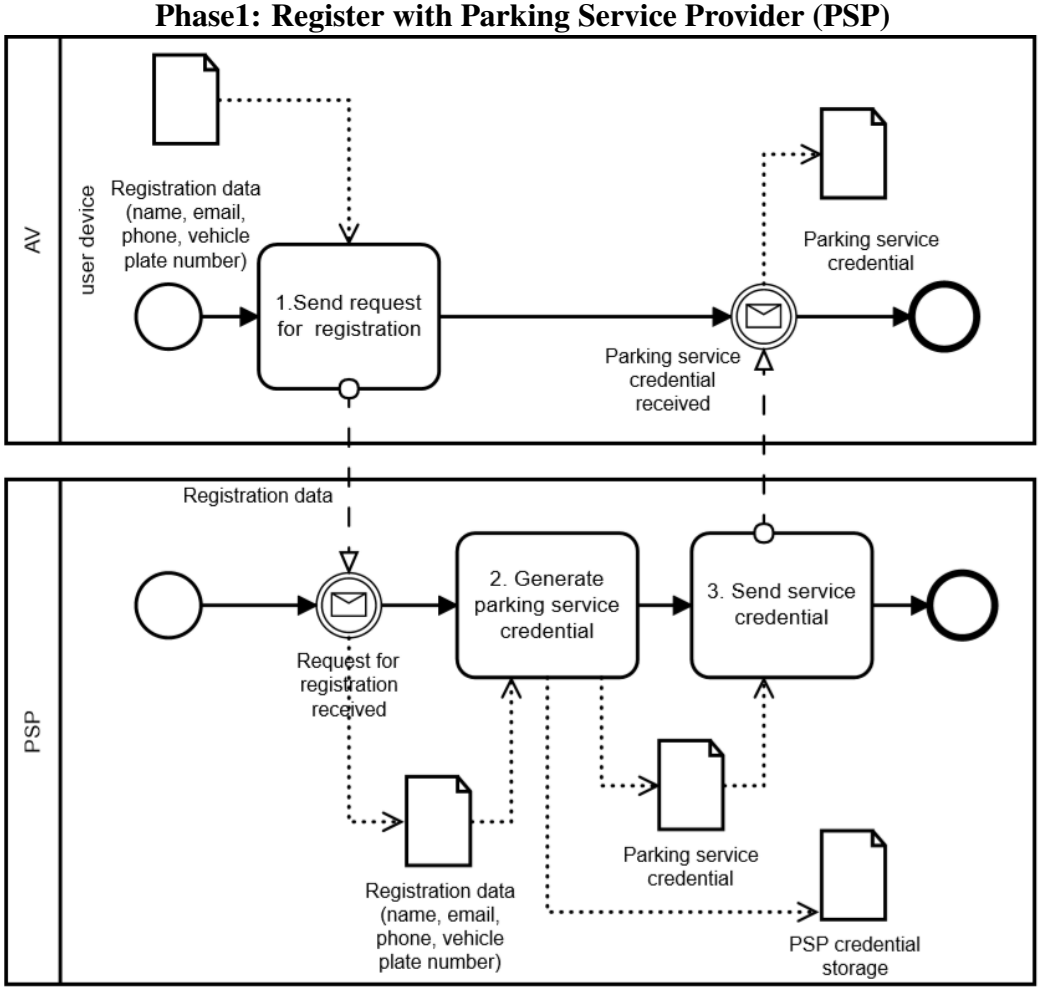

Figure 11. Privacyless Model Automated Valet Parking

B.2 Phase 2:Getting Parking Permit From Parking Lot Terminal(PLT)

In this AVP scenario, there are 3 system entities involved (AV, PSP and PLT). This scenario shows how the information/data collected in the first scenario is being used by the three system entities to generate the parking permit. The scenario description for B.2 can be illustrated in Figure12 is follows;

4. The user uses his parking service credential to login to the PSP.

5. The PSP receives the parking service credential and checks the authenticity

of the parking service credential from the PSP credential storage.

6. After the check, the PSP sends login notification to the user's device.

7. The user receives the login notification from the PSP. If the notification is positive the user can go ahead to request parking service with his location (where he intends to go). If the login notification is negative, the user is taken back to the login page.

8. When the user makes a parking request, the PSP receives the request and checks with the parking lot terminal (PLT) around the location where the user intends to go for parking availability.

9. The PLT receives the request and checks for available parking space in the PLT parking space storage.

10. The PLT sends notification about the parking space availability to the PSP.

11. The PSP receives the notification about parking space availability. If there is an available parking space (YES), the PSP generates the parking reservation (which contains the Location, vehicle plate number) on behalf of the user. If there is no available parking space the PSP checks with the PLT later to see if any space opened up.

12. The PSP sends the parking reservation (which contains the Location, vehicle plate number) generated to the PLT.

13. The PLT receives the parking reservation from the PSP and generates a parking permit (which contains PLT name, parking space reserved for the user and vehicle plate number). The parking permit allows the user into the PLT.

14. The PLT sends the parking permit to the PSP and also stores the parking permit in it's PLT parking permit storage.

15. The PSP receives the parking permit and sends it the user's device. The user device receives the parking permit.

Phase2: Getting Parking Permit From Parking Lot Terminal(PLT)

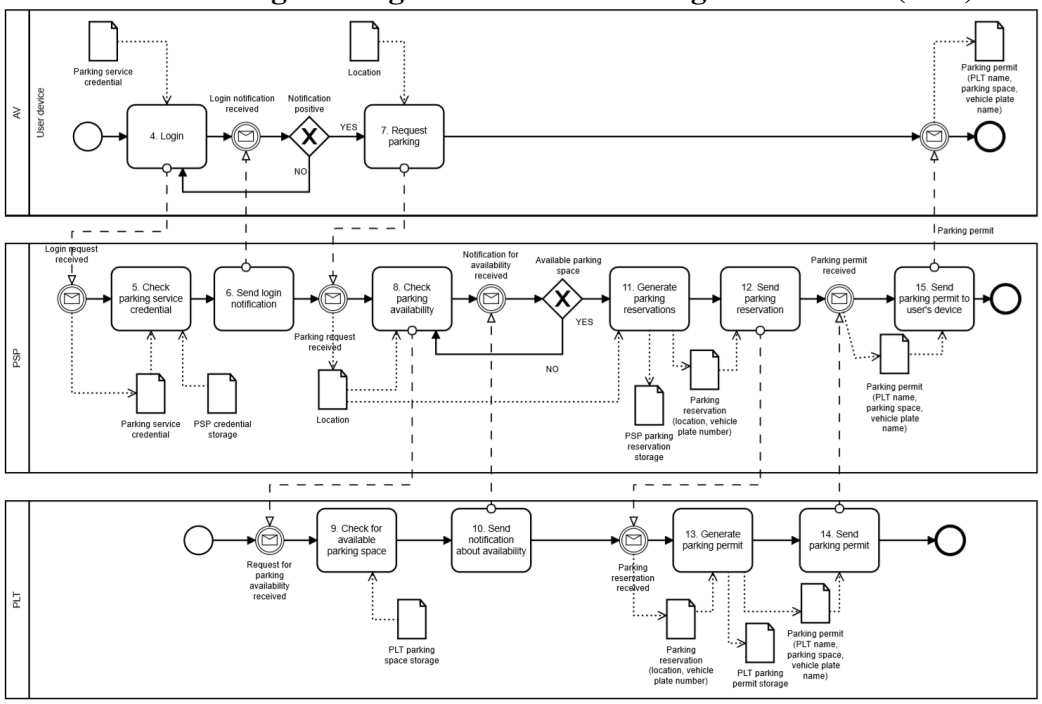

Figure 12. Privacyless Model: Automated Valet Parking

B.3 Phase 3 Scenario Description: Using the Parking permit

In this scenario, we would see how the AV uses the parking permit to get into the PLT and we would see how the PLT uses the AV attributes to allow entrance into the PLT. When the user receives the parking permit, he navigates to the designated PLT as on the parking permit and leaves the AV at the drop off point. Once at the drop off, the user. The scenario description for B.3 can be illustrated in Figure13 as follows:

16. Activates the AV automatic parking.
17. The on board unit (OBU) receives the signal from the user's device and navigates to the PLT.
18. When the AV gets to the PLT, he requests entrance using his parking permit.
19. The PLT receives the entrance request (parking permit) and checks it from the PLT parking permit storage.

20. If the parking permit is valid, the vehicle is allowed to enter.

21. If the parking permit is not valid, it stops the vehicle from entering.

22. The PLT sends entrance notification to the on board unit. If entrance is granted, the AV navigates to the reserved parking space.

23. If entrance is not granted, the AV notifies the user about the invalid parking permit.

Phase3: Using the Parking Permit

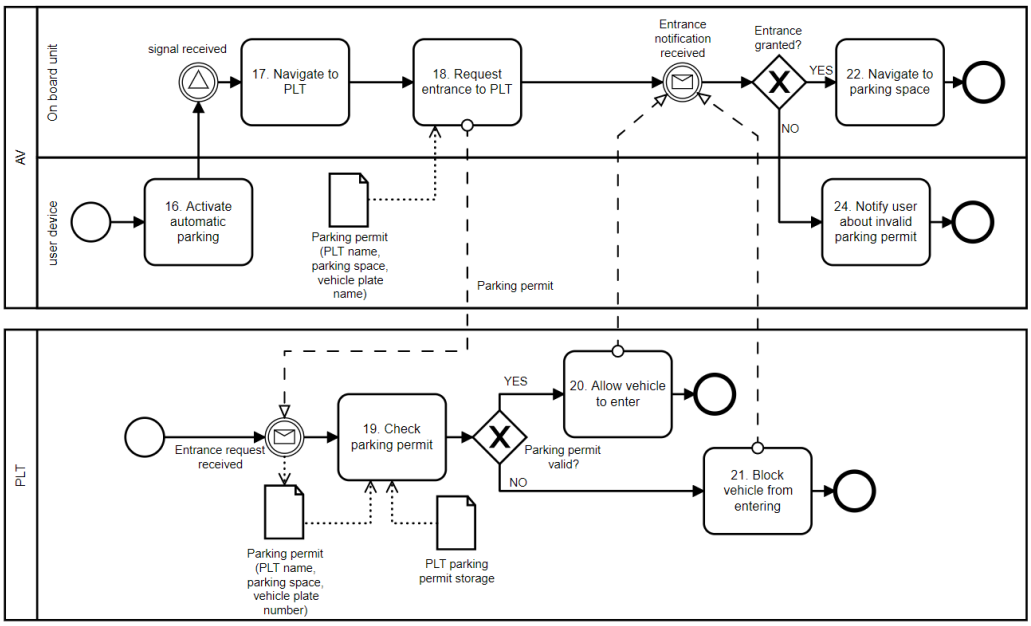

Figure 13. Privacyless Model: Automated Valet Parking

B.4 Phase 1: Register with Parking Service Provider (PSP)

In this phase, the encryption process begins with the user encrypting his data and sending the encrypted data the PSP. The scenario description in B.4 can be illustrated in Figure 14.

1. The user encrypts ($PKEncryption$) his personal data (name, email, phone, vehicle plate number) with his secret key for registration with the PSP. The result of this process is an Encrypted Registration Data.

2. The user sends the encrypted registration data to the PSP.

3. The PSP receives the encrypted registration data and generates an encrypted parking service credential based on the encrypted registration data ($PKComputation$) and stores it in the PSP credential storage which is also encrypted.

4. The encrypted parking service credential generated by the PSP is then sent to the user's device.

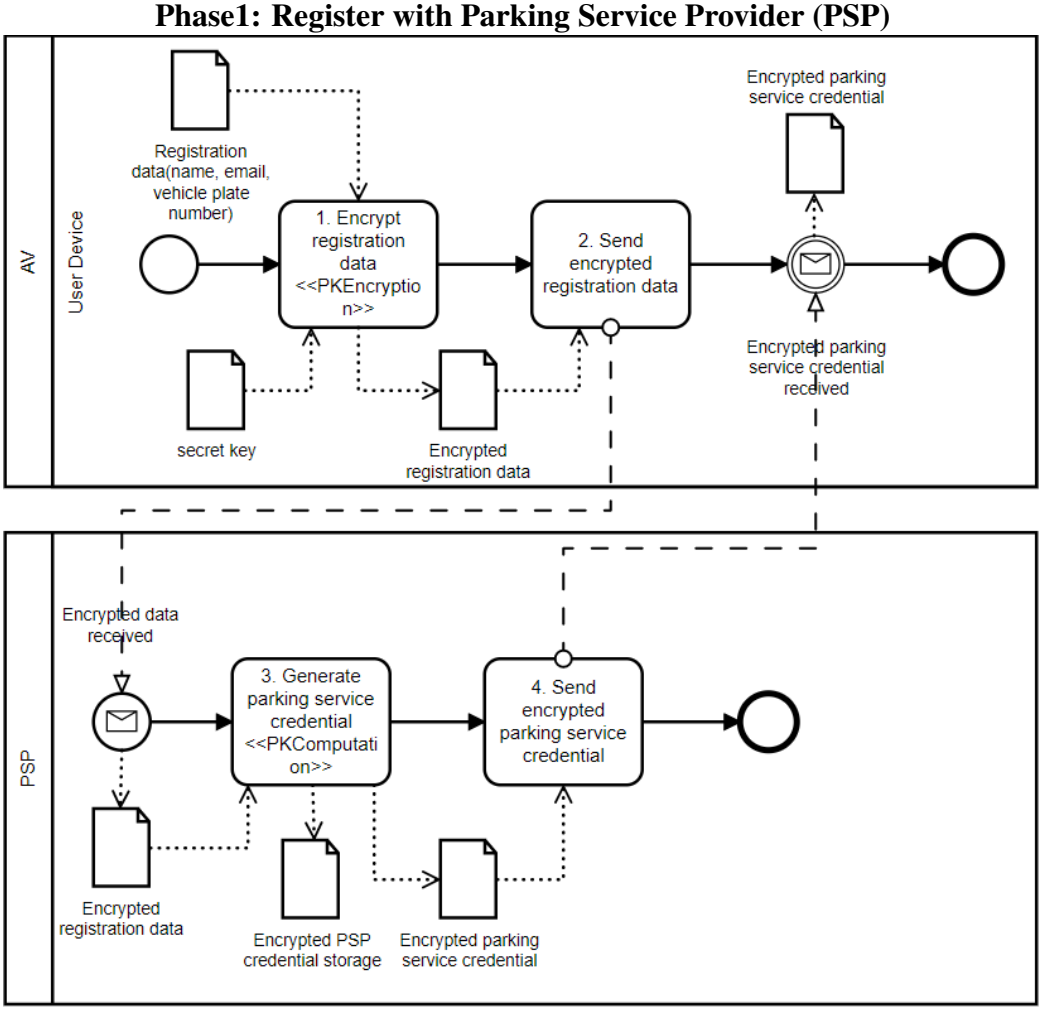

Figure 14. Privacy Enhanced Model for AVP: Encryption

B.5 Phase 2: Getting Parking Permit From Parking Lot Terminal (PLT)

The scenario descriptions in B.5 can be illustrated in Figure 15.

5. The user uses his encrypted parking service credential to login to the PSP.
6. The PSP receives this request and checks the user encrypted parking service credential from the PSP credential storage (encrypted).
7. The PSP sends the login notification to the user's device.

8. If the login notification is positive (yes), the user generates a parking request with his location (where he intends to go). If the notification is not positive (NO), the user is sent back to the login page.

9. The user encrypts ($PKEncryption$) his parking request which contains his location with his public key. The result of this is Encrypted parking request(location).

10. The user sends the Encrypted parking request(location) to the PSP.

11. The PSP receives the parking request and checks for available parking space in the PSP.

12. The PLT receives the parking availability request and checks for an available parking space from the PLT parking space storage.

13. The PLT sends notification about availability to the PSP.

14. The PSP receives the notification about the available parking space. If there is an available parking space (yes), the PSP generates a parking reservation with the Encrypted parking request(location) to produce Encrypted parking reservation and stores it in the PSP parking reservation storage (encrypted). If there is no available parking space the PSP checks with the PLT again much later.

15. The PSP sends the encrypted parking reservation to the PLT.

16. The PLT receives the encrypted parking reservation, generates the encrypted parking permit and stores it in the PLT parking permit storage (encrypted).

17. The PLT sends the encrypted parking permit to the PSP.

18. The PSP receives the encrypted parking permit and sends it to the user.

19. The user receives the encrypted parking permit and decrypts it with his private key to produce the Parking permit (PLT name, parking space, vehicle plate number).

Phase 2:Getting Parking Permit From Parking Lot Terminal(PLT)

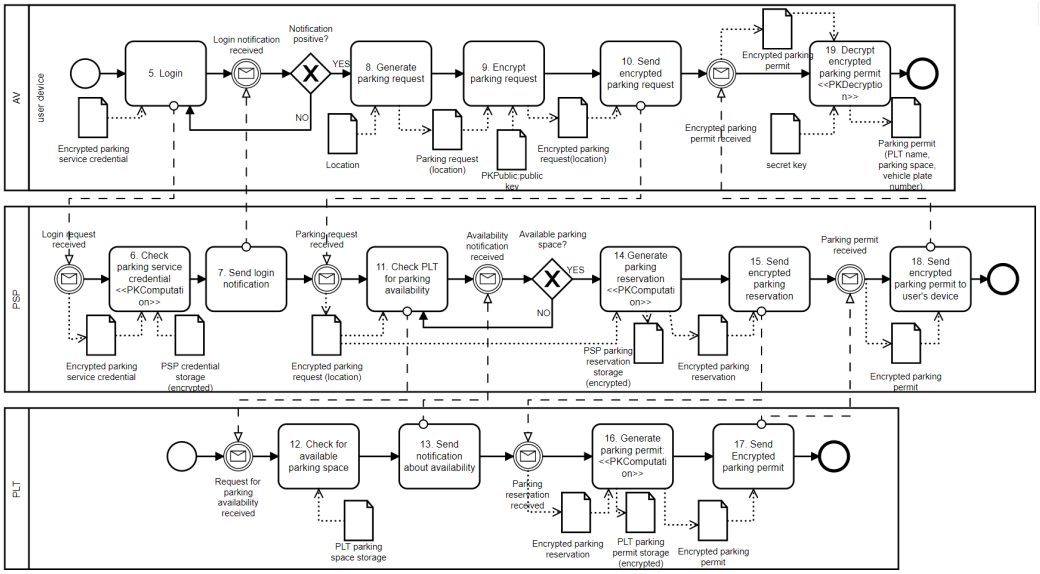

Figure 15. Privacy Enhanced Model for AVP: Encryption

B.6 Phase 3: Using the Parking permit

When the user receives the parking permit, he navigates to the designated PLT as on the parking permit and leaves the AV at the drop off point. The scenario descriptions in B.6 can be illustrated in Figure 16

20. The user activates the automatic parking from his device.
21. The OBU receives the signal and navigates to the PLT.
22. The OBU requests entrance to the PLT with the encrypted parking permit.
23. The PLT receives the entrance request with the encrypted parking permit and checks the encrypted parking permit ($PKComputation$) from the PLT parking permit storage(encrypted).
24. If the parking permit is valid, the PLT allows the vehicle in.
25. If the parking permit is not valid, the PLT blocks the vehicle from entering.
26. The PLT sends entrance notification to the OBU. If the entrance notification is positive, the AV navigates to it's designated parking space.

27. If the notification is negative, the user is notified about invalid parking permit.

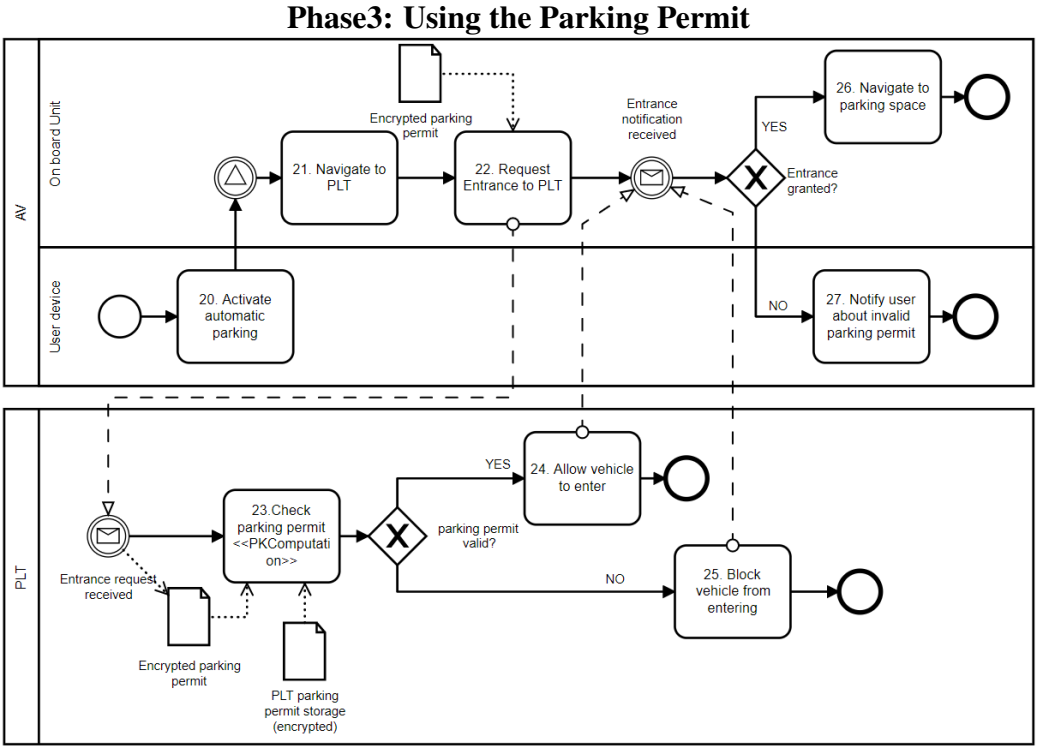

Figure 16. Privacy Enhanced Model for AVP: Encryption

B.7 ABC Phase 1:Register with Issuer

In this phase, the user request for credential enrollment with the issuer. The issuer-signed credential provides a form validation for the user based on the attributes provided by the user. The scenario description in B.7 can be illustrated in Figure 17

1. The user request for credential enrollment from issuer. The enrollment data contains name, phone number, email,vehicle plate number.

2. The issuer receives the enrollment data and generates a issuer-signed credential for the user containing the user's enrollment data (name, phone number, email,vehicle plate number) and the issuer's signature.

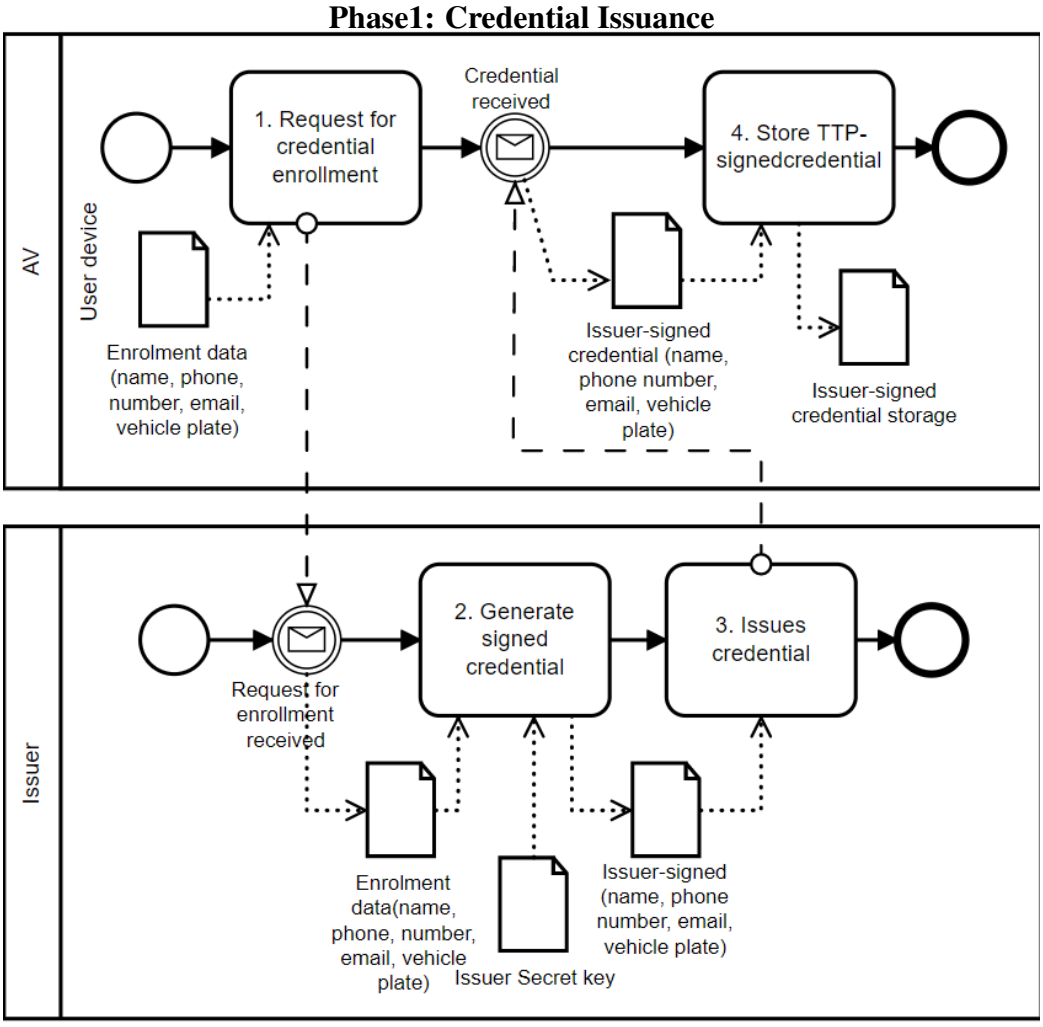

Figure 17. Privacy Enhanced Model for AVP

3. The issuer issues the signed credential to the user.
4. The user stores the issuer-signed credential.

B.8 Phase 2:Registering with The PSP

The user presents the credential to the PSP for registration. The scenario description in B.8 is illustrated in Figure 18

5. The user request registration with the PSP and uses the credentials for registration (email and vehicle plate number).

6. The PSP generates the parking service credential with the user's credential and also verifies the credential with the issuer public key.

7. The PSP sends the PSP-signed parking service credential to the user.

Phase2: Register with Parking Service Provider (PSP)

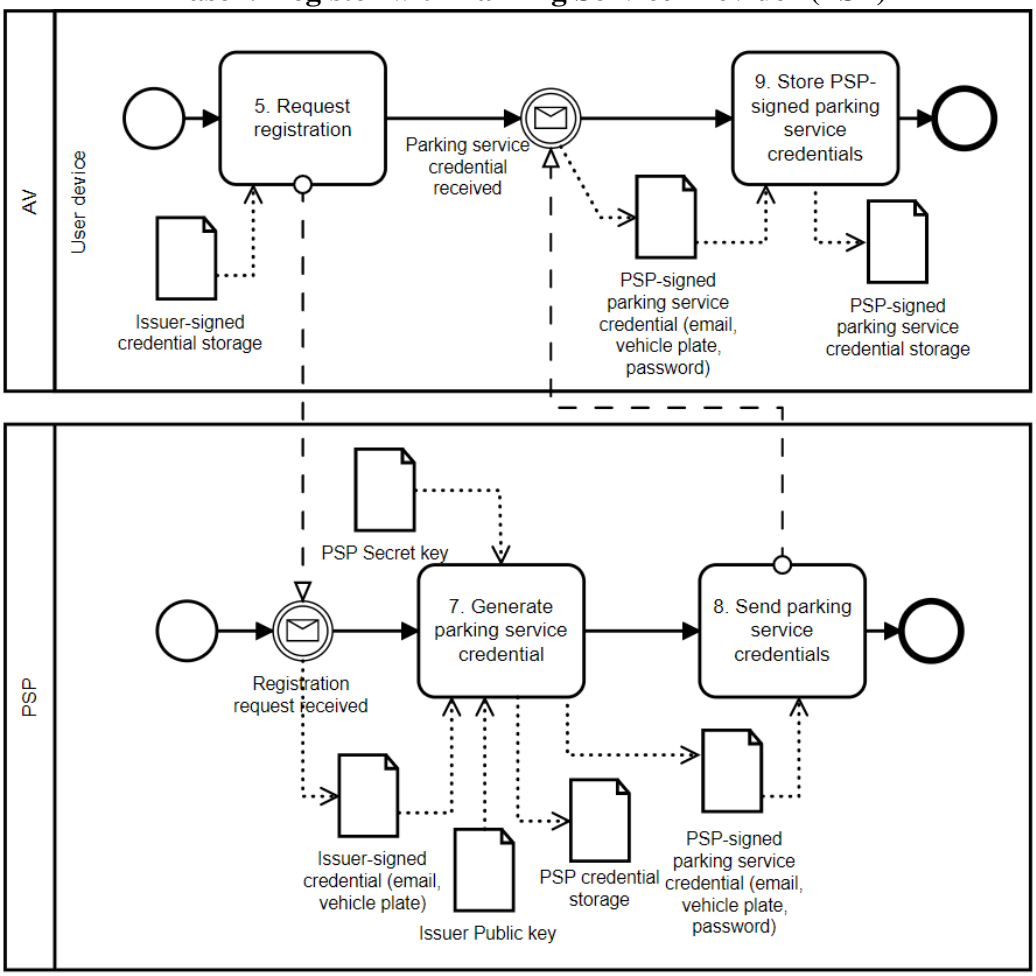

Figure 18. Privacy Enhanced Model for AVP:ABC

B.9 Phase 3:Checking Availability Getting Parking Permit

The PSP and PLT communicate with each other to provide the user with a parking permit. The scenario description in B.9 is illustrated in Figure 19

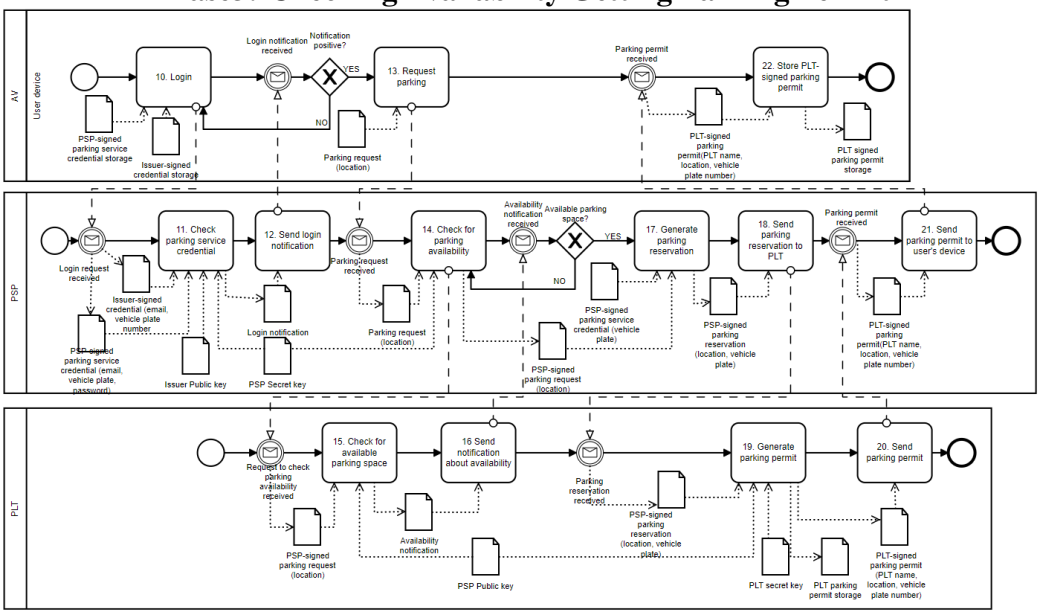

Figure 19. Privacy Enhanced Model for AVP:ABC

8. The user login to the PSP with his PSP-signed parking service credential(email, vehicle plate number and password) and his issuer-signed credential (email, vehicle plate number).

9. The PSP receives the parking service credential with the issuer public key and PSP secret key.

10. The PSP sends login notification to the user device.

11. The user receives login notification. If the notification is positive, the user request for parking service from the PSP. If the notification is negative, he is asked to login again.

12. The PSP receives the parking request (which contains the destination location of the user) and checks for parking availability with the PLT using the PSP secret key.

13. The PLT receives the PSP-signed parking request and checks for available parking space from the PLT parking space storage.

14. The PLT sends notification about availability to the PSP.

15. The PSP receives the notification about availability. If the notification is positive, the PSP generates a PSP-signed parking reservation from the PSP-signed parking service credential. If the notification is negative the PSP checks back for availability after some time.

16. The PSP sends the PSP-signed parking reservation to the PLT. The parking reservation contains the Location and Vehicle plate number.

17. The PLT receives the PSP-signed parking reservation and generates the PLT-signed parking permit with the PLT secret key. The parking permit consist of the PLT name, Location, Vehicle plate number and PLT signature.The PLT stores the parking permit in the parking permit storage.

18. The PLT sends the PLT-signed parking permit to the PSP.

19. The PSP sends the PLT-signed parking permit to the user device.

20. The user stores the PLT-signed parking permit in the PLT-signed parking permit storage.

B.10 Phase 4:Checking Availability Getting Parking Permit

In this phase, the parking permit is used to gain entrance into the PLT.The scenario description in B.10 is illustrated in Figure 20

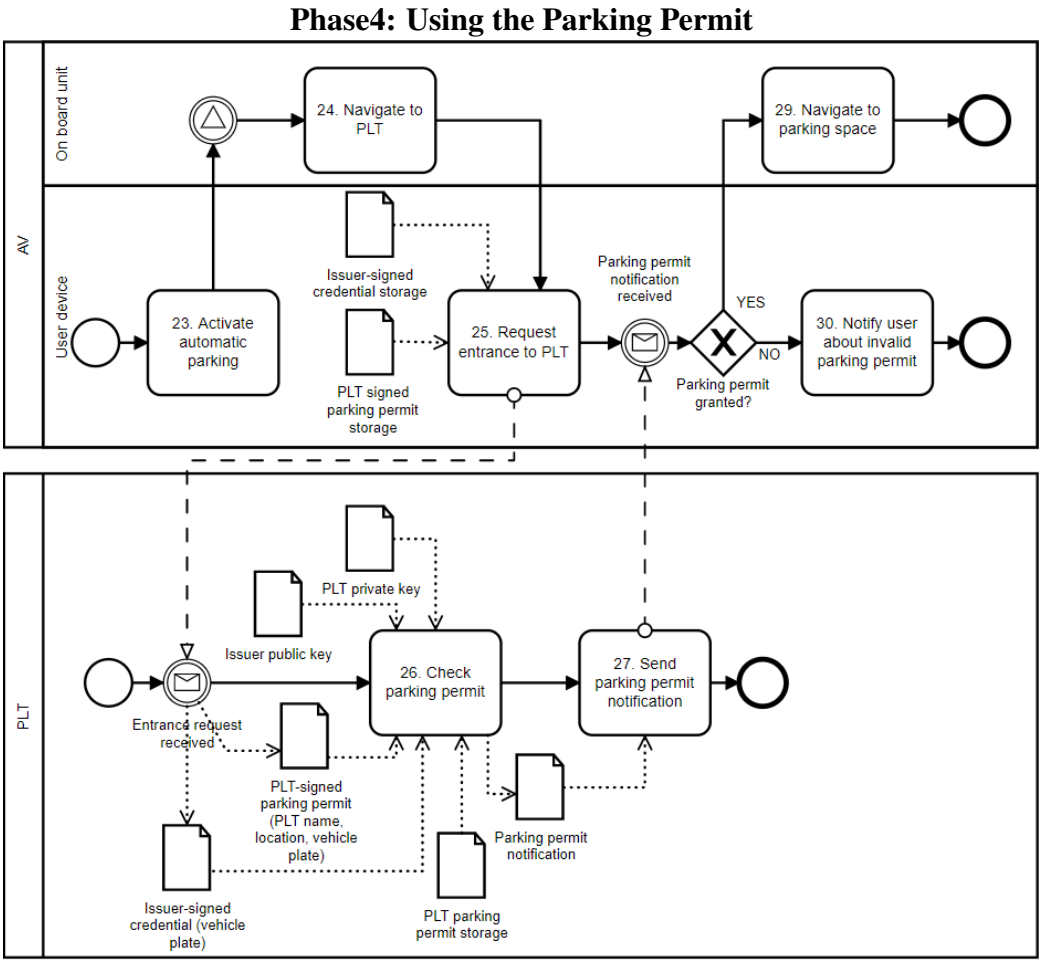

Figure 20. Privacy Enhanced Model for AVP:ABC

21. The user activates the automatic parking with his device.
22. The OBU receives the signal and navigates to the PLT.
23. The OBU request entrance to the PLT with the PLT-signed parking permit and the issuer-signed parking permit storage.

24. The PLT receives this request and checks the parking permit from the PLT parking permit storage and also with the PLT private key.

25. The PLT sends parking permit notification.

26. The user receives the parking permit notification. If the user parking permit is not granted, the PLT notifies the user about invalid parking.

27. If the parking permit is granted the user navigates to the parking space.

C Car Sharing Scenario

This subsection provides more information on our validation model (car sharing) scenario.

C.1 Privacyless Phase1: Registration with CSP

In Figure21, the following communication process takes place as the user registers with the Car Sharing Provider (CSP):

1. The user sends a registration request to the car service provider with his name,email and phone number.
2. The car service provider receives this request and generates login details.The login details contain the email and password.
3. The car service provider sends the login details to the user.

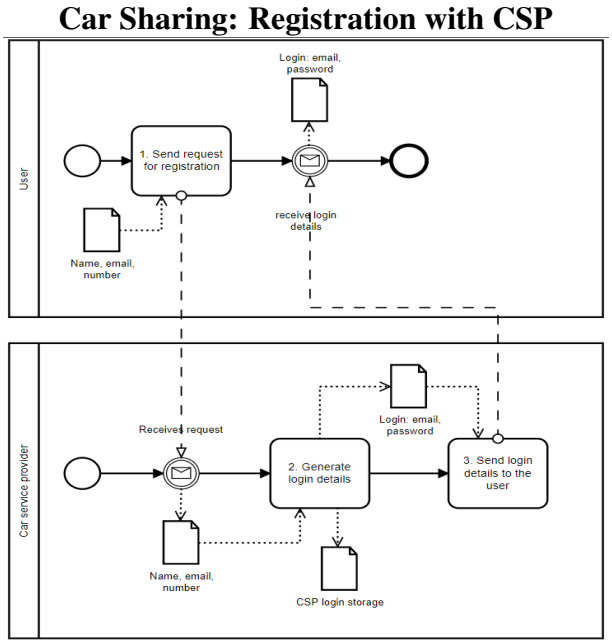

Figure 21. Privacyless Model: Car Sharing phase 1

C.2 Phase 2: Document Collection and Vehicle Search

In Figure22, the following process takes place with the user and CSP:

4. The user receives the login details and uses it to login to the CSP.
5. The PSP receives the login and checks the login details from the CSP login storage.
6. The PSP sends login to the user.
7. If the login notification is positive (YES), the user goes ahead to request for car sharing service, else (NO) the user is taken back to the login page.
8. The CSP receives the car sharing request and ask the user to upload documents (driver's license and credit card details).
9. The user receives the document request and uploads the required document (driver's license and credit card details) to the CSP.
10. The CSP receives the document and stores the document in the CSP credit card storage and CSP driver's license storage.
11. The CSP request for user's current location.
12. The user receives the request and sends current location to the CSP.
13. The CSP receives the user's current location and searches for the nearest vehicle based on the user's current location.
14. The CSP sends notification details about the nearest vehicle to the user. Details includes vehicle plate number,location and an access token to access the vehicle.

C.3 Phase 3: After the Trip

In Figure23, the following process takes place after the user's trip with the car:

15. The user notifies the car sharing provider about the end of his trip. The trip document contains the duration of the trip and the location of the car.
16. The CSP receives the notification and compute payment based on trip details to get the amount the user would pay.

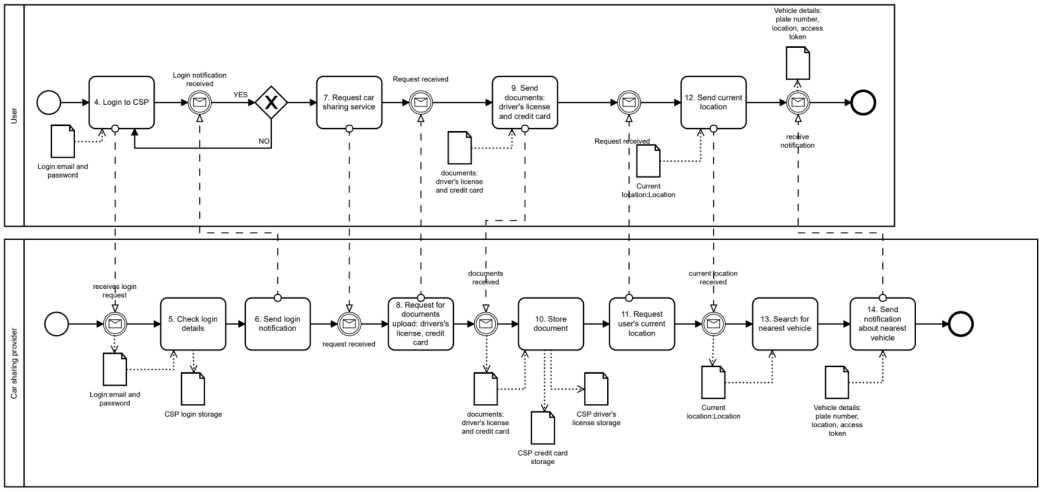

Figure 22. Privacyless Model: Car Sharing (Document Collection and Vehicle Search)

17. The CSP retrieves the user's credit card details from the CSP credit card storage. The credit card contains the bank name, card number and user's name.

18. The CSP charges the amount from the user's credit card.

19. The CSP notifies the user about the charges amount in form of a payment transaction document which contains the Bank name, amount, user's name and card number.

20. The CSP sends the payment transaction document to the user's bank.

21. The user's bank receives the payment transaction document and start processing the payment.

22. Once the payment process is done, the CSP is notified about the payment in form of a credit transaction (Amount and user's details).

23. The bank also notifies the user about the payment in form of a debit transaction in form of a debit transaction (Amount, CSP details).

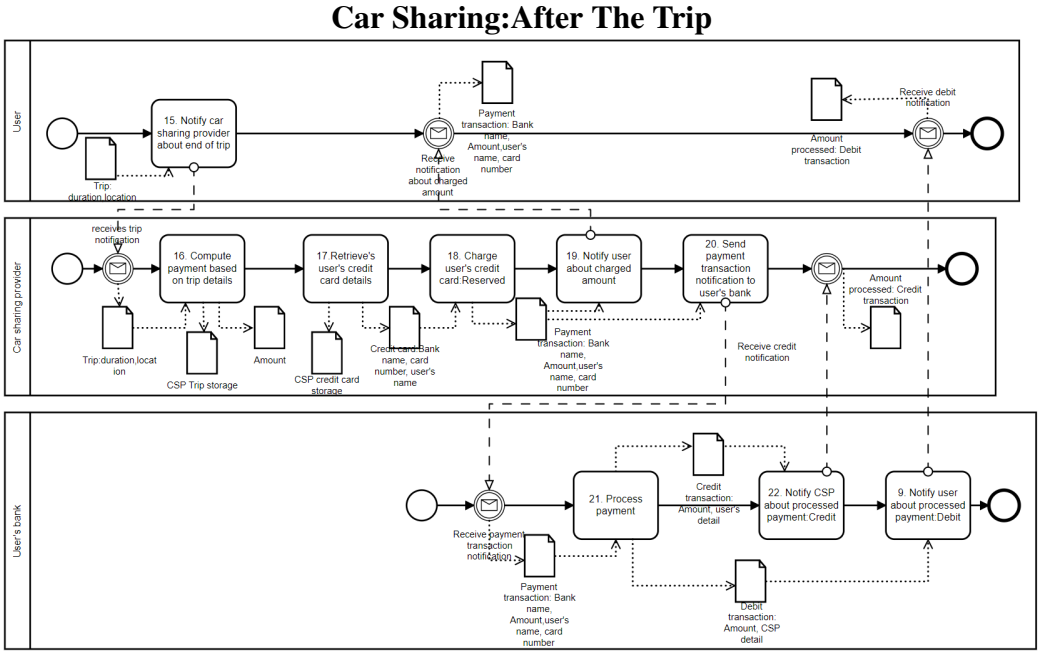

Figure 23. Privacyless Model: Car Sharing (After Trip)

C.4 Phase 1: Credential Enrollment

In the Figure24, the following process takes place:

1. The user request for credential enrollment with his (Name, email,driver's license,phone number and credit card) with the issuer.
2. The issuer receives the enrollment data from the user(Name, email,driver's license,phone number and credit card) and generates a issuer-signed credential for the user with the issuer secret key.
3. The issuer issues the signed credential to the user.
4. The user receives the issuer-signed credential and stores it in the issuer-signed credential storage.

C.5 Phase 2: Registration with CSP

In Figure25, the following process takes place:

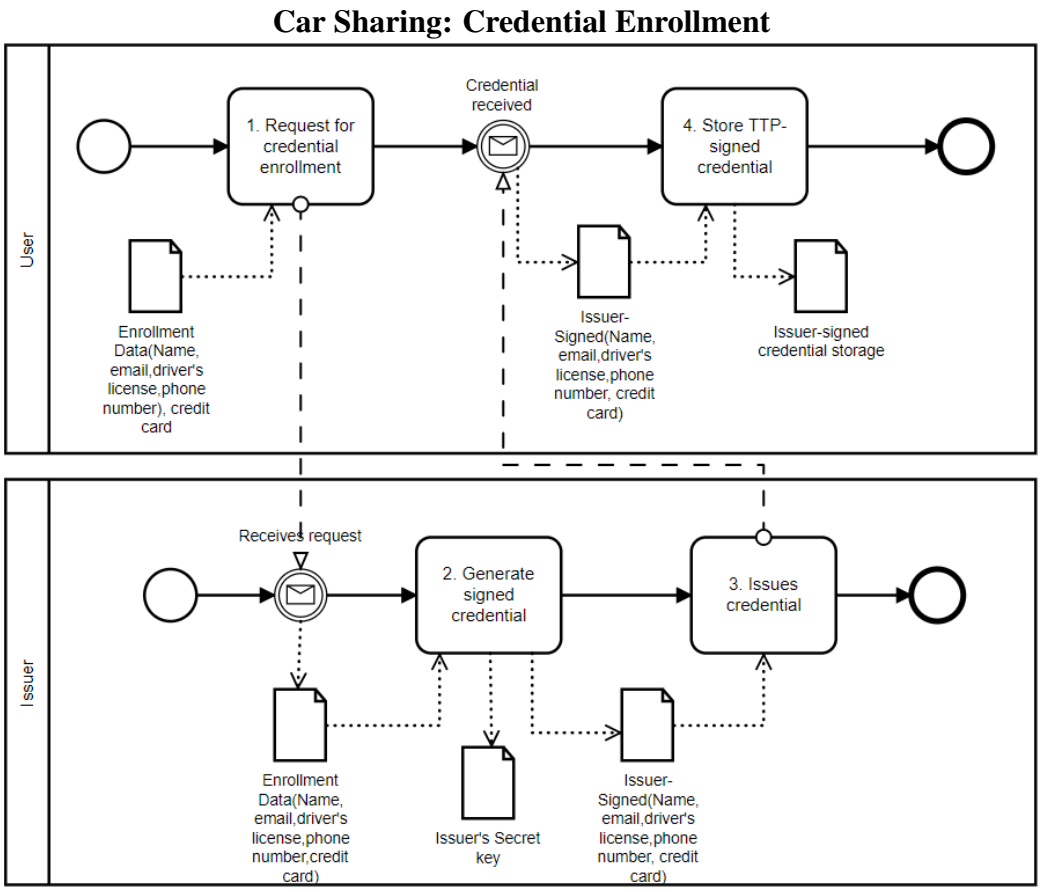

Figure 24. Privacy Enhanced Model: Car Sharing

5. The user generates a presentation token from the issuer-signed credential.
6. The user request for registration with the CSP, he presents the presentation token to the CSP.
7. The CSP receives the registration request(presentation token), verify the login of the user using the issuer public key and generates a CSP-signed login using the CSP secret key.
8. The CSP sends the signed login details to the user.
9. The user stores the CSP-signed login in the CSP-signed login storage.

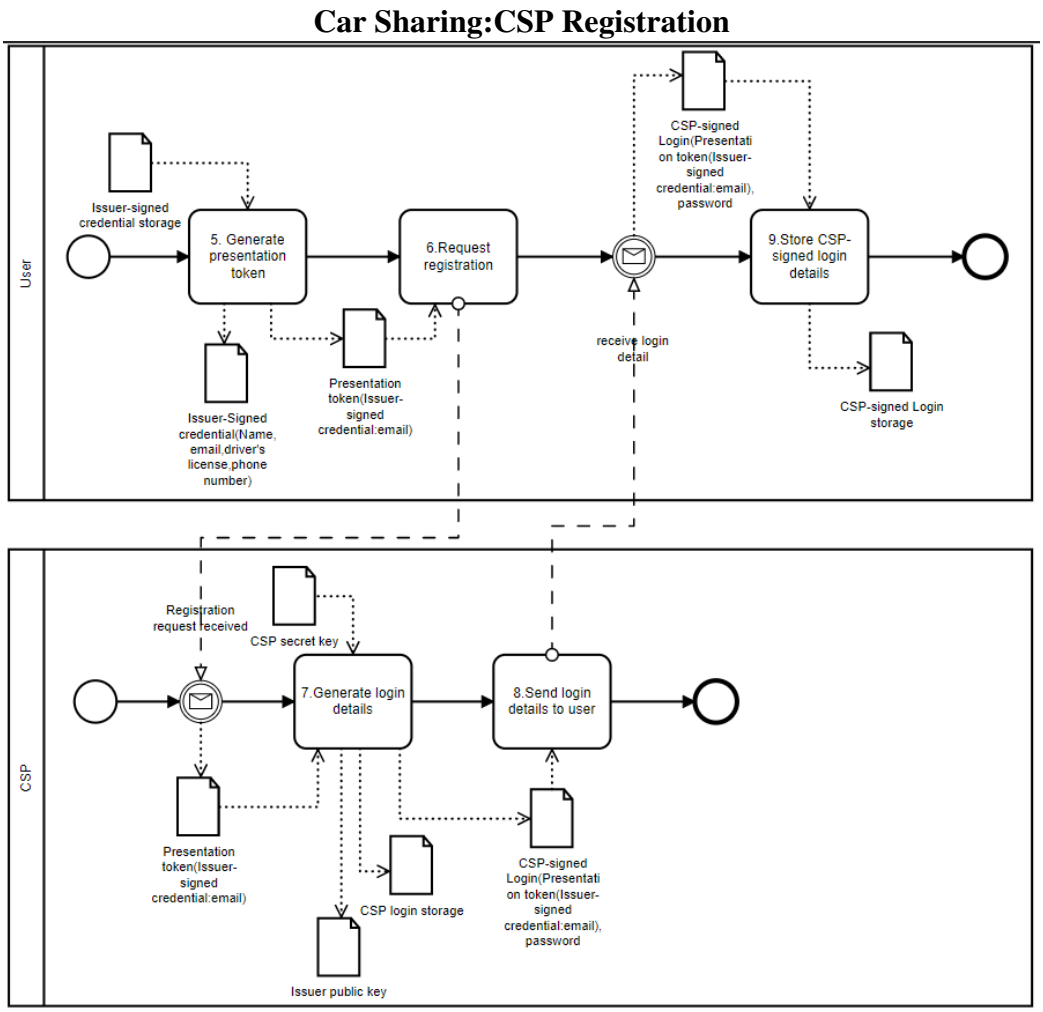

Figure 25. Privacy Enhanced Model: Car Sharing

C.6 Phase 3: Document Collection and Vehicle Search

In Figure26, the following process takes place:

10. The user logs in to the CSP using his CSP-signed login.
11. The CSP receives the login details and verifies the login detail with the issuer public key and CSP secret key.
12. The CSP sends the user a login notification.

Car Sharing:Document Collection and Vehicle Search

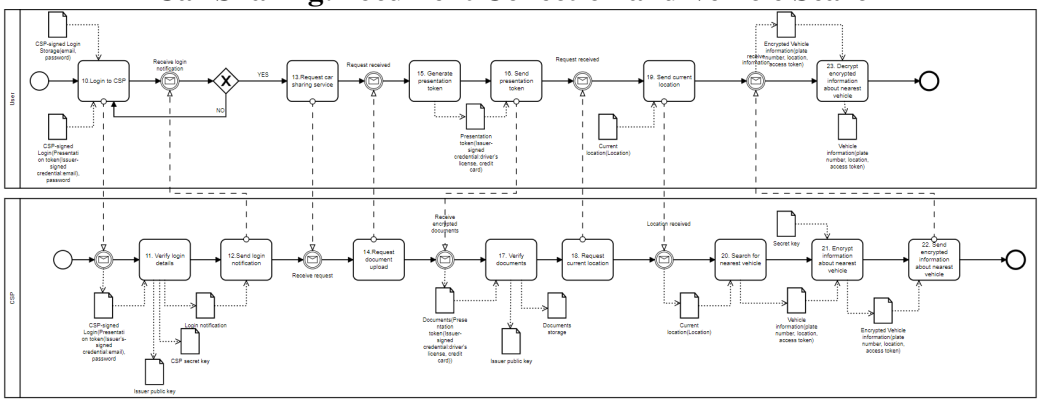

Figure 26. Privacy Enhanced Model: Car Sharing

13. If the login notification is positive the user requests for a car sharing service, else he is taken back to the login page if the login notification is negative.

14. The car sharing provider receives the user's request and requests for documents upload (driver's license and credit card) from the user.

15. The user generates another presentation token for the document upload. This contains some attributes from the credential such as his driver's license and credit card.

16. The user sends the presentation to the CSP.

17. The CSP verifies the document using the issuer's public key and stores the document in the document storage.

18. The CSP requests for the user's current location.

19. The user receives the request and sends the current location to the CSP.

20. The CSP receives the user's current location and searches for the closest vehicle around based on the user's current location.

21. The CSP finds a vehicle, compile the information and encrypts the vehicle information using it's public key. The information contains plate number, location, access token to enable the user identify the vehicle.

22. The CSP sends the encrypted vehicle information to the user.

23. The user decrypts the vehicle information using his private key to get the original vehicle information (plate number, location, access token).

C.7 Phase 4: After Trip

In Figure27, the following process takes place:

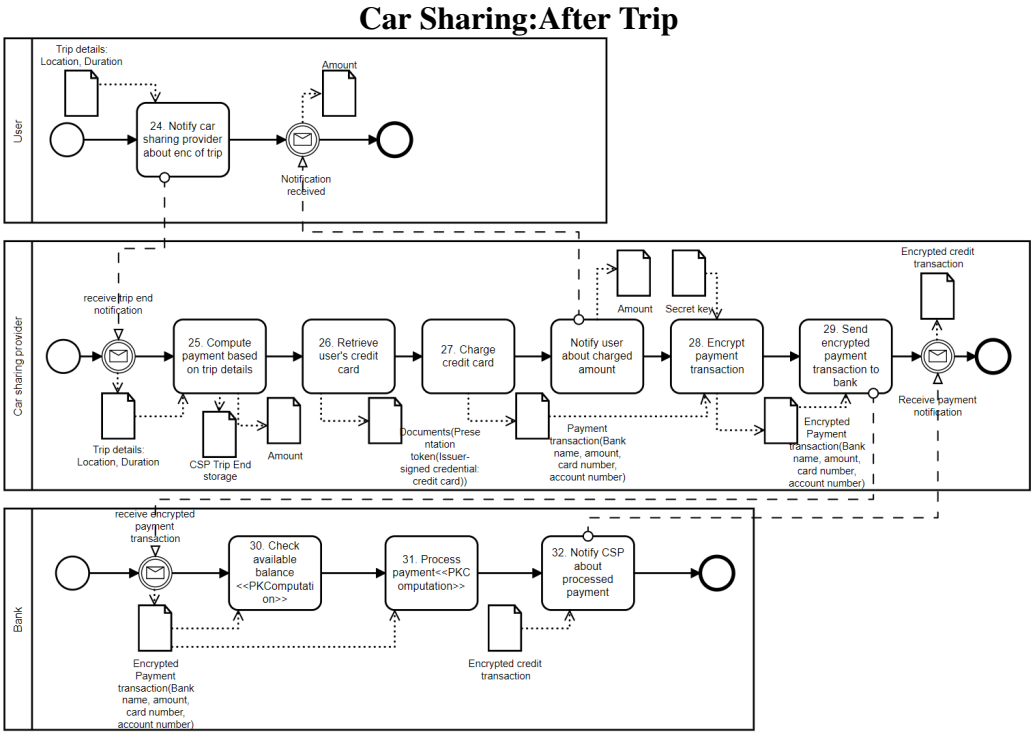

Figure 27. Privacy Enhanced Model: Car Sharing

24. The user notifies the CSP about the end of trip and sends the trip details (Duration) to the CSP.

25. The CSP receives the notification and computes payment amount based on the trip details (duration).

26. The CSP retrieve's the user's credit card details from the document storage.

27. The CSP charge the amount to the user's encrypted credit card and produces a payment transaction detail(Bank name, Amount, user's name, card number).

28. The CSP encrypts payment transaction details with it's public key.
29. The CSP sends the encrypted payment transaction to the user to notify user about the charged amount.
30. The CSP sends encrypted payment transaction to the user's banks.
31. The bank receives the encrypted payment transaction and processes payment.
32. The bank notifies the CSP about processed payment as a credit transaction with the encrypted debit transaction.
33. The bank notifies the user about processed payment as an encrypted debit transaction.

D License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Nwaokolo Anita Onyinye,**

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1 reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2 make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright of my thesis

   "A Comparison of Privacy Enhancing Technologies in Internet of Vehicle Systems"

   supervised by Raimundas Matulevičius, PhD and Abasi-amefon Obot Affia, Msc

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

   Tartu, 15.05.2020