TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Nathan Danzmann de Freitas 177780IVSB

AUTHENTICATION METHODS FOR INTERNET OF VEHICLES

Bachelor's thesis

Supervisor: Tauseef Ahmed

Ph.D

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Nathan Danzmann de Freitas 177780IVSB

SÕIDUKITE INTERNETI AUTENTIMISMEETODID

bakalaureusetöö

Juhendaja: Tauseef Ahmed

Ph.D

Tallinn 2018

Tallinn 2018

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Nathan Danzmann de Freitas

30.05.2020

Abstract

Many different methods of authentication for automated or autonomous vehicles have been proposed in the past few years with the advent of self-driving vehicles that are each time closer to reality and the development of the VANET proposal, or Vehicular Ad-hoc Network which is a decentralized and scalable network of vehicles communicating between each other and with a trusted authority for authorization, in this paper we aim to compare and analyse the most popular solutions that have been proposed, researched and implemented for authentication of autonomous vehicles, namely the widely used Conditional Privacy-Preserving Authentication which by itself have many iterations and different algorithms and we analyse the possibility of using the emerging Blockchain technology as a possible candidate with its potential of building decentralized and scalable network in the field of safe autonomous vehicles, with or without the cooperation of existing VANET and other infrastructure, which we will use to decide into what is the most proper solution for a future network of smart vehicles.

Annotatsioon

Sõidukite Interneti autentimismeetodid

Viimastel aastatel on pakutud välja palju erinevaid automatiseeritud või autonoomsete sõidukite autentimismeetodeid, mille käigus on välja tulnud isesõitvaid sõidukeid, mis on iga kord reaalsusele lähemal, ning välja on töötatud VANETi ettepanek või sõidukite ad hoc võrk, mis on detsentraliseeritud ja skaleeritav sõiduki võrk, mis suhtlevad omavahel ja autoriseerimiseks usaldusväärse autoriteediga, ja selle töö eesmärk on võrrelda ja analüüsida kõige populaarsemaid lahendusi, mis autonoomsete sõidukite autentimiseks on välja pakutud, uuritud ja rakendatud, nimelt laialt levinud Conditional Privaatsust säilitav autentimine, millel on palju iteratsioone ja erinevaid algoritme, ning analüüsime võimalust kasutada arenevat Blockchaini tehnoloogiat võimaliku kandidaadina turvaliste autonoomsete sõidukite detsentraliseeritud ja skaleeritava võrgu ehitamiseks.

See lõputöö on kirjutatud inglise keeles ja on 44 lehekülge pikk, sisaldades 7 peatükki, 6 joonist ja 1 tabel.

List of abbreviations and terms

CL-CPPA	Certificate-Less Conditional Privacy Preserving Authentication
CPPA	Conditional Privacy-Preserving Authentication
ID-CPPA	Identity-based Conditional Privacy Preserving Authentication
RSU	Road-side Unit
IoV	Internet of Vehicles
IoE	Internet of Everything
IoT	Internet of Things
PKA	Private-Key Authentication
MANET	Mobile Ad-Hoc Network
OBU	On-board unit
OTA	Over-the-air updates
POW	Proof-of-Work
RAISE	RSU-aided Message Authentication Scheme
RSU	Road-Side Unit
TA	Trusted Authority
VANET	Vehicular Ad-Hoc Network

Table of contents

List of figures

List of tables

Introduction

The current technological revolution impacts everything. Our desire for more intelligent and connected devices has created the Internet of Things is now all around us. The forecast of IoT connected devices will reach 64 billion by 2025, from 10 billion in 2018. It will create a world where every device communicates with one another.

Thus our cities become more connected, this in turn will allow connected vehicles to slowly transform into autonomous ones, but none of this will be possible without a new advanced network.

One of the most important concepts in such a feat is the Internet of Vehicles (IoV). An adaptation of IoT for vehicles, it allows vehicles to exchange information, efficiency but above all safety, with each other and also with infrastructures using Vehicular Ad Hoc Networks (VANETs).

The future of transportation relies on autonomous vehicles, whether it be self-driving personal vehicles (e.g. cars) or mass transit (e.g. buses, trains) and the prospect of a machine in full control of a vehicle that contains human lives is a matter that requires a very cautious development. The authentication system is the interface between such machines software and a human input on then, and as such, it poses many concerns in the data authenticity, integrity and privacy matters as only authorized individuals should have the possibility to access, update or directly control an AV software, especially in the context of IoV where the vehicles are constantly connected to the internet and subject to attacks.

We are here to look into all the technologies being envisioned, mostly accepted and emerging in the purpose of safely authenticating self-driving vehicles.

This thesis is written in English and is 44 pages long, including 7 chapters, 6 figures and 1 table.

1 Theory Background

1.1 Autonomous Vehicle

An autonomous vehicle, or a self-driving or assisted-self-driving vehicle is the definition of a vehicle that is capable of sensing its environment and moving safely with little or no human input.

Self-driving cars combine a variety of sensors to perceive their surroundings, such as radar, lidar, sonar, Global positioning system (GPS), odometry and inertial measurement units. Advanced control systems interpret sensory information to identify appropriate navigation paths, as well as obstacles and relevant signage [1].

1.1.1 Safety of autonomous vehicles

This paper deals with the authentication aspect of autonomous vehicles, and thus it is important to indicate the reason of such importance. The insertion of a vehicle into the digitally controlled world, where the aspects of guiding a vehicle at high speed are interconnected in a subsystem through the public domain of the internet means that failing to properly authenticate an autonomous vehicle can lead to very disastrous consequences, from damage to theft to the loss of life of the occupants of the vehicle [1], [2].

1.1.2 Communication of Automated vehicles

The application of an interconnected network of mobile vehicles communicating to each other is an important and often included part in the discussion and development of self-driving vehicles, as the inter-vehicle communication can immensely improve the predictions for driving and making decisions, as an information acquired by a certain vehicle over a blockage of way can, for example, alert countless other cars a great distance away so that they can adjust their route and decision making according to it [3], [4].

1.2 Internet of Things

The Internet of things (IoT) is an arrangement of interrelated processing gadgets, mechanical and computerized machines with exceptional identifiers (UIDs), and the capacity to move information over a system without expecting human-to-human or human-to-PC association [5].

The meaning of the IoT has developed because of the intermingling of different advancements, constant investigation, AI, wearable sensors, and installed frameworks. Customary fields of implanted frameworks, remote sensor systems, control frameworks, mechanization (counting home and building computerization), and others all add to empowering the Internet of things. In the buyer advertising, IoT innovation is generally synonymous with items relating to the idea of the "savvy home", covering gadgets and apparatuses, (for example, lighting installations, indoor regulators, home security frameworks and cameras, and other home machines), and can be controlled through gadgets related with that environment, for example, smartphones.

There are various genuine worries about threats in the development of IoT, particularly in the territories of protection and security, and thus, industry and legislative moves to address these worries have started.

Fundamentally there are 4 security objectives that the IoT system requires:

- **Data confidentiality:** unauthorized parties cannot have access to the transmitted and stored data.
- **Data integrity:** intentional and unintentional corruption of transmitted and stored data must be detected.
- **Non-repudiation:** the sender cannot deny having sent a given message.
- **Data availability:** the transmitted and stored data should be available to authorized parties even with the denial-of-service (DOS) attacks [6].

1.3 Internet of Everything

In straightforward terms: IoE is the clever association of individuals, procedure, information and things. The Internet of Everything (IoE) portrays an existence where billions of articles have sensors to recognize, gauge and evaluate their status; all associated over open or private systems utilizing standard and exclusive conventions [7].

Pillars of IoE:

- People: Connecting people.
- Data: Converting data into decision-valuable information.
- Process: Delivering the right information to the right person (or machine) at the right time.
- Things: Physical devices and objects connected to each other and the Internet for intelligent decision making with the use of valuable data; often called Internet of Things (IoT).

The IoT concept is the application of only the “Things” pillar of the IoE.

2 Problem Statement

The impact of the autonomous vehicles advancements into our everyday life is getting clearer and the future in which they are used regularly comes closer, yet there is no consensus on the technology and assurance of authentication systems to be used for autonomous vehicles that will drive and be guided by information that must not be compromised. Dozens of privacy-preserving authentication protocols exist, it is easy to cause confusion into the difference between them and why they should be used, which one has been deprecated due to possible attacks found, furthermore there is an ever growing presence of advocates of the use of new emerging blockchain technologies into being used to replace the current widely accepted IoV system of the ad-hoc network that also promises to be safe and practical, but many think that the implementation of a blockchain-based technology would require the complete re-structuring and re-imagining all aspects of IoV infrastructure, in this paper we will try to find out how that is truth and compare the solutions with a blockchain-based one that best fits the current VANET based infrastructure without requiring massive refactoring of the concept of a network of autonomous vehicles, if such research exists.

3 Related Works

The conditional preserving authentication algorithms are a group of secure encryption that guarantees anonymity amongst the users, and authenticate warning messages in VANETs, this kind of algorithm is specifically designed to act within this vehicular networks as they are made having in mind the utilization of the 3-system pillar of VANETs which is TA, RSU and OBU units and the specific communication between them [8]–[11].

Blockchain is a technology developed with the creation of digital currencies (including the first digital currency, Bitcoin) which composes of a growing list of record blocks, linked to each other using cryptography algorithms. Each block, or record, contains a cryptographic hash of the previous block, a timestamp, and transaction data [12]

4 Methodology

The purpose of this chapter is to explain in detail the research methods and the methodology implemented for this study.
This paper uses qualitative research strategies. For a better understanding of the underlying reasons, future models, current models, case studies, data and technologies a series of explorations of other dissertations, researches, journals and some sourced news and blog articles were used.
The paper aims to provide insights into the problem or helps to develop ideas or hypotheses for further potential research into what could be the future of autonomous vehicles communication infrastructure. Following steps were followed for developing a methodology framework for this paper:

- Explaining how VANET works into developing an Internet of Vehicles
- Deeply investigating the existing technologies, algorithms and methods of securing and authenticating automated vehicles in an Internet of Vehicles environment, namely the Conditional Privacy-Preserving Authentication algorithm.
- Investigating alternative technologies in the blockchain emerging domain and how they could theoretically be applied for development of internet of vehicles.
- Reporting the faults and limitations of the existing and emerging technologies.
- Documenting the reasons and motivations behind the integrations.
- Building a demonstration of how the authentication technology works in the current domain of VANET.

5 VANET and Internet of Vehicles

This chapter covers a brief background and overview of the Vehicular Ad-Hoc Network technology inception and application, the detailed workings of a VANET, its implementation and authentication procedure will be discussed in chapter 5.1.

5.1 The background of VANET: MANET

VANET is a creation that is derived from mobile ad-hoc networks, also called MANET, which is the spontaneous creation of wireless networks of mobile devices.

The network is called ad hoc because it needs no pre-existing infrastructure, such as routers, switches or access points. Instead, each node participates in routing by forwarding data for other nodes, each node is at the same time client and router, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use.

This theoretical concept of decentralized network is very old with early tests revolving around radio communication with “mobile radios” in cars in the early 1970’s and the idea has evolved with the advent of the internet and it’s growth. The concept of a mobile network of general purpose devices after the evolution of wifi, mobile networking such as 3G, 4G and 5G and other centralized network solutions coupled with several drawbacks of the MANET network means that this is no longer a practical solution for modern networking. But, if adapted, it can make a comeback in smart vehicle networks. [13]

5.2 Overview of VANET

Vehicle Ad-hoc Networks (VANETs) are created by applying the principles of MANETs to the domain of vehicles. VANETs, which are sometimes referred to as Intelligent Transportation Networks, were first mentioned and introduced in 2001 under "car-to-car ad-hoc mobile communication and networking" [13], where networks can be formed and information can be relayed among cars. It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and other roadside services. VANETs are a key part of the intelligent transportation systems (ITS) framework in the future [13], [14].

During the early 2000's VANET were seens as mere application and light modification of a MANET to the domain of intelligent vehicles, but they have since greatly developed and the idea matured into a complete domain of its own right.

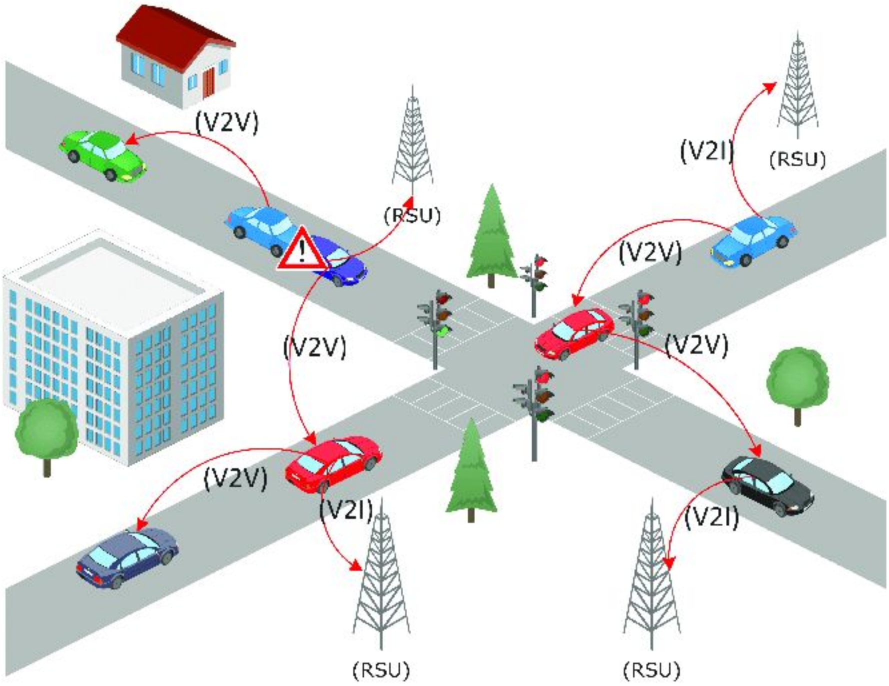

Fig 1. General implementation and communication of a VANET

Currently, as of 2020, the term VANET is, although not the same from the technical definition of it, synonymous with with the more broad term of inter-vehicle communication or IVC, even though the IVC area has a focus on the development, adaptation and use of Road-Side Units (RSUs) and cellular networks into the intelligent vehicle domain, VANET maintains the focus on the aspect of spontaneous networking. The confusion between the two terms are broadly accepted though, especially since both areas tend to be merging and the more colloquial pronunciation of VANET is easier to hear, learn and repeat[15].

5.2.1 Application of VANET

The integration of VANET into the working of the vehicle itself has many possible applications[15]:

- Digital braking: A mild and more easily applicable and imaginable application of VANET is in the creation of a electronic signal transmitted by a front vehicle in case of sudden braking that is transmitted into other vehicles following it, this signal can either be interpreted automatically by a completely self-driving vehicle that will make the immediate decision to follow the braking but also in a more "mild" and easily transitionable scenario, a signal that is shown to the driver so the driver himself make the follow-up braking decision.
- Platooning or road-train: An application that requires a full platoon of completely automated self-driving cars, a more distant application but it would allow vehicles to closely follow each other as their steering, acceleration and braking information is instantaneously communicated between each other. The biggest problem with the impossibility to follow up vehicles closely in the current situation is the delay in the response of a human driver to a situation that he cannot foresee.
- Road Information System: The RSUs present in the infrastructure, besides providing a middleman communication between the vehicle and a trusted authority for authentication, will provide a connection with conventional internet for real time information about blockages, weather,

traffic conditions and so on, with much more precision than currently in use so that the driver or the vehicle itself can take the correct decisions based upon absolutely real-time data.

- Advertisement: Another application that is related to the road information system previously mentioned is the possibility for road side units to provide real time information about gas stations, accomodations, markets and useful information for the driver/passenger himself or even promotion, discount and other advertisement related information, which could even generate a new branch and application of digital marketing.

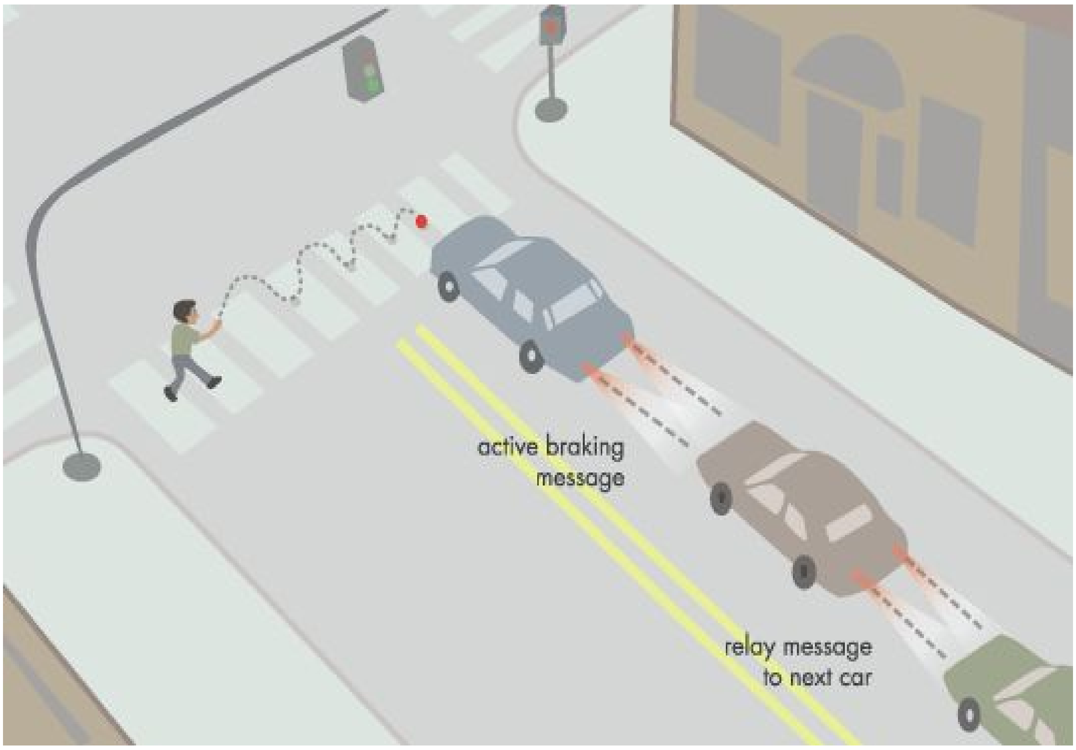

Fig 2. Application of an intelligent braking system in a VANET

5.2.2 How VANET works

There are three parts of VANET[14], [15]:

- Trusted Authority (TA)

- Road Side Unit (RSU)
- On Board Unit (OBU)

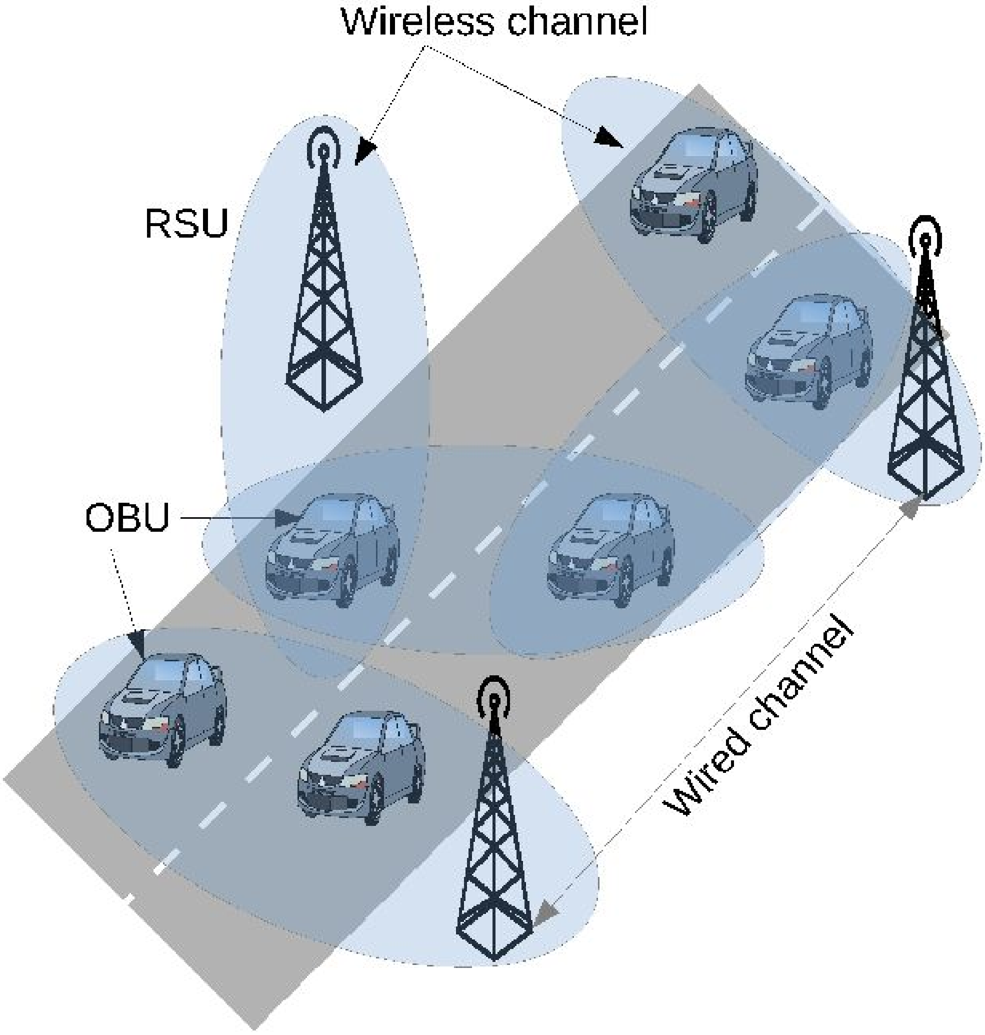

Fig 3. The structure of a VANET system with the mentioned three parts

5.2.3 Trusted Authority

The function of trusted authority is to generate system parameters and distribute the secret material, therefore the TA must have high computing power and storage capacity. Another function of TA is to do offline registration of RSU and OBUs.

5.2.4 Road-side Unit

The integrity and validity of the message is verified by the RSU and therefore high computing power and storage capacity is also necessary for RSU too. The messages are then sent to corresponding vehicles by notification messages.
The number of RSUs is less than OBUs logically, as one RSU can deal with countless OBUs, therefore the required infrastructured can be easily maintained at VANET, also taking into consideration the fact that much of this infrastructure may already exist in the form of 3G/4G towers and already implemented road-side technology that can be converted or added upon, use of mass-production can easily scale necessary roadside units that will mostly remain the same.

5.2.5 On-board Unit

Contrary to TA and RSU the computing power and storage capacity of OBU is smaller and is considered a semi trusted computing unit. Vehicle to vehicle communication took place in this section. The traffic related messages are issued and calculated through notification messages in the OBU.

5.2.6 Communication

The wireless channel is used to carry information among OBUs as well as OBU to RSU information, any kind of transmission system can be used for the RSUs, mostly through wired copper or fiber connections but also possible through wireless and satellite communications, especially for most remote and less densely-populated areas that the vehicle may go through.

5.3 Internet of Vehicles

The culmination of the technological revolution currently being developed in the domain of smart vehicles allied with the human desire of more intelligent and connected devices in all areas that keeps on growing year after year leads to the development of the “Internet of Vehicles” concept, which is a perfect implementation of VANET system [16].

The implementation of such intelligent connected devices into cities infrastructure will allow connected vehicles to slowly transform into autonomous ones, but none of this will be possible without a new advanced network.

In fact, the Internet of Vehicles is one of the drivers of IoT development itself. It allows vehicles to exchange information, efficiency and most importantly safety with others as well as with infrastructures using VANETs.

IoV is the evolution of that conventional VANET, which refers to the network of different entities, everything from vehicles to infrastructure, building, devices and even the pedestrian themselves sharing real-time communication among them.

The electronics used for that include infotainment systems, sensors, brakes, and GPS. There is a clear need for better communication and interconnectivity between vehicles. As they are turning into smart entities, cars are becoming an essential part of smart cities.

The IoV makes car sensor platforms, which absorb information from the environment, other vehicles and from the driver. All this for safer navigation, traffic management, and pollution control.

It is basically the application of the concept of decentralized VANET communication between vehicles to the communication between all interactable devices related directly or indirectly to the transportation/driving process of an autonomous vehicle[13], [16].

6 The security of VANET and autonomous vehicles

6.1 Access points of connected autonomous vehicles

It is important to start defining the parts of an automated vehicle in an Internet of Vehicles that are connected to the outside and most probable to be susceptible to attacks[14].

6.1.1 Controller Area Network (CAN)

The CAN is a bus that allows for communications between microcontrollers inside a vehicle without a need for a host computer. The bus is very simple and contains no direct support for secure communication[14].

6.1.2 On-Board Diagnostics (OBD) Interface.

OBD is an embedded computer system that allows technicians and the car manufacturer or service provider or vehicle owner to access the status of various subsystems in the vehicle, it is the entry point for the inner network of the vehicle. The OBD interface has a lack of authentication and inability to detect malicious code[14], [17].

6.1.3 Entertainment System.

In-vehicle Infotainment is the combination of hardware and software inside a vehicle which provides information and entertainment services to the driver and passengers, it is already an existent and widespread solution in many higher end cars in the market[4].

6.1.4 Over the Air (OTA) Update.

OTA Software upgrades are pushed from the original equipment manufacturer (OEM's) server to the remote vehicles. This model often lacks verification of the source and signature of the software going to be updated.

6.2 Challenges of securing self-driving vehicles:

Attacks against self-driving cars will inevitably have much bigger consequences than against normal cars. An attack against a car using information from computer systems to assist in guiding or fully guiding the vehicle, the passenger or driver has more reliance on the vehicle safety and security systems and will be less able to respond to an attack then on a normal car.

Currently the world is at race in developing automated vehicles and in this pace maintaining security controls of AVs is difficult as the products are tested and developed.

The development and creation of a safe authentication system for autonomous driving vehicles is a big challenge in the way that it must follow the highest level of security standard of a critical system as self-driving or assisted-self-driving vehicles are surely considered critical system due to their direct link to the safety of the person(s) and cargo aboard and on other vehicles around it.

The meeting of such criteria for a critical system security must be met with the possibility for it to be connected to the internet (as many critical systems follow a simpler no-connection and strict access control to make it more difficult if not impossible to be accessed by a non-authorized source) and also have the capacity to be easy enough to use that any user (driver) is able to register and login to the system safely without the knowledge of any of the major procedures happening.

At first glance, the problem of securing autonomous vehicles seems significantly harder than securing ordinary passenger vehicles. However, this is not necessarily the case[4], [14], [17].

Firstly, we explore possible scenarios of attack of authentication:

6.2.1 Remote Attacks:

These attacks are performed from remote distances and can affect the entire fleet of vehicles in a single attack. These kinds of attacks are considered as most impactful because they are performed from a large distance, they require little to no access to the vehicle itself, they are performed through means of acquiring access remotely through the internet. Some of the remote attacks that directly affect the AVs are:

- Base device attacks e.g. embedded entertainment system;
- Attack against listening service;
- Attack against a remote assistance style feature. For example Phantom Auto;
- Attack on AVs infrastructure.

Without physical access to the AVs the attacker can use exploitation techniques, security vulnerabilities and social engineering to have remote access to a Road Side Unit or the vehicle itself[4].

6.2.2 Short Distance Attacks:

In this type of attack the attackers exploit the AVs from a short distance range. These attacks are performed through direct access via means of bluetooth or wifi, in which the attacker is in close proximity to the vehicle. Some of these kind of attacks are:

- Attacks on the vehicles sensors (Jamming vehicle functions e.g. affecting vehicle perceiving environment functionality);
- Bluetooth and Wifi Attacks;
- Controlling the Tire Pressure Monitoring System (TPMS).

Due to availability of sensors and cameras in vehicles and widespread robust security technology in wifi connections, unless a major security flaw is unveiled or a short-range attack to infiltrate into an embedded system and perform a long-range attack later on, this type of attack can easily be perceived and is generally considered a weak attack[4].

6.2.3 Physical Access Attacks:

This is most commonly described closer to a tampering, modification, destruction or attack of any kind to equipment and devices in the vehicle itself or in the infrastructure that the vehicle uses.
These types of attacks require physical access to the automated vehicles. Injecting CAN messages to the CAN bus is one of the critical attacks in this category which can be implemented by plugging the device in CAN network and then reprogram an existing ECU to do something nefarious.
Of these examples, the hardest part for an attacker would be figuring out the internals of the autonomous vehicle, which would not be readily available to the attacker [4], [17].

6.2.4 Other Non-Critical Attacks:

Besides the above mentioned attacks which are focused on gaining control over critical-sensitive parts of the automated vehicle which command the movement of the vehicle and can end up in harm to the driver and passengers, other type of attacks that do not harm the occupants physically but must still be considered[4]:

6.2.4.1 Personal information theft

Attacks can use any of the above-mentioned methods and more to acquire personal information over any of the occupants inside the vehicle, especially if their personal information is registered into the vehicle embedded systems.

6.2.4.2 Fraud, vehicle theft

Attacks can use any of the above mentioned methods to either lock the user out of the vehicle and take control of it themselves for their own benefit (reprogramming and owning or selling), conducting blackmailing, social engineering or threats for monetary gains.

6.3 Optimism about securing automated vehicles

One advantage of the current self-driving vehicle is that it will be closely monitored. Automobile manufacturers do not typically track vehicles locations, speeds, or receive a constant stream of health updates and logs from their vehicles, but this is the case for self-driving cars. This can help spot problems before they are major issues. The other aspect of this level of control by a central authority is that if a problem is ever detected or a security violation occurs, it is possible to have all the vehicles return to their garage for inspection within a matter of minutes. Vehicles could even be immediately
(and safely) shut down remotely pending a critical security event.
Critical-systems like measures of fail safe procedures can also be (and most probably already are) implemented into automated vehicles, such as complete stop and disabling of the vehicle in case of any detected abnormality in the system or erratic behaviour, or integrated and segregated systems of sensors that are not connected to the outside world or even the subsystem of the vehicle but can bring the vehicle to a halt when detecting nearby collision probability or other anomalies based on analysis of outside environment [4], [18].

7 Authentication in Internet of Vehicles:

A self-organized network is organized by the internet of vehicles. Based on the roadside information the built in system warns drivers of potential accidents in advance. To improve the accuracy and safety of IoVs information can be possibly shared between these vehicles in real time, as has been previously discussed in more detail in section 3[19].

The attacker can easily steal the authentic data including the private data of vehicle users if effective security measurements are not provided. Data authenticity and integrity is vital in the internet of vehicles because without the authentic and secure system hackers can generate fake messages to misguide IoVs or human drivers to make wrong decisions on the roads. Therefore the key argument is that manufacturers should authenticate the IoVs before allowing it to join the network. A very simplified authentication scenario is shown in Fig.3

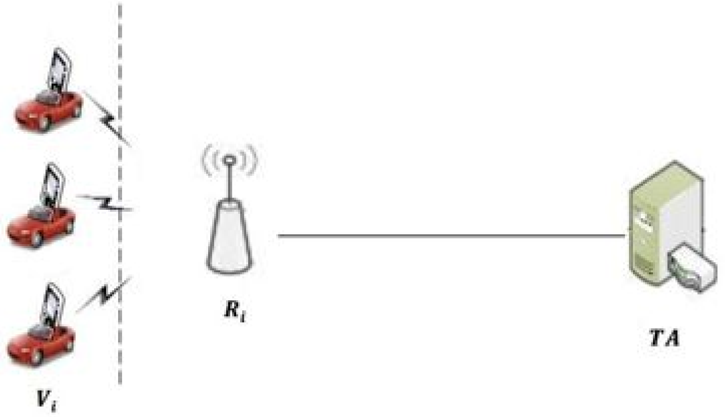

Fig 4. Typical authentication scenario of IoVs.

Recently, many authentication protocols for IoVs have been designed to protect the security of vehicles. One of the most widely used authentication protocols is

Conditional privacy-preserving authentication (CPPA) which is explained in the below sections[19].

7.1 CPPA (Conditional privacy-preserving authentication):

The Conditional Privacy preserving authentication is a type of system in which it is able to achieve message authentication and conditional privacy simultaneously, and is fully appropriate for solving the security and privacy issues in VANETs.

Several research works about privacy preserving authentication for VANETs have been proposed in recent years, which include public key infrastructure based (PKI-based) CPPA schemes, identity-based (ID-based) CPPA schemes from bilinear pairing, binary authentication tree and elliptic curve, and certificateless CPPA schemes [8], [10], [14], [19].

Extensive research has been made to design a framework with an objective of improving the efficiency of mutual authentication between vehicle and RSU. Since the location and identity of RSUs are fixed, RSU-to-vehicle authentication is easy and can be efficiently achieved by broadcasting signed messages from time to time. However, vehicle-to-RSU (V2R) authentication in many works needs the cooperation of TA. In some algorithms though [11], vehicle-to-RSU authentication in the CPPA framework does not require real-time interactions between RSUs and TA, but the TA maintains a dynamic list that contains sensitive information regarding authentication of vehicles, and every RSU must store the latest copy of this list in the background. This list enables RSUs to complete the anonymous authentication of vehicles by themselves, which reduces the workload of TA and promotes the efficiency of authentication [8], [14], [19].

As can be noticed, CPPA is a very broad range of different authentication algorithm implementations with dozens of known researches being done on the topic.

The assumptions in Conditional privacy-preserving authentication (CPPA) are as follows:

- TA will be completely trustworthy and none of the attacks will be compromised by TA;
- OBUs computing power and storage capacity are lower than RSU;
- The RSU storage capacity and computing power is less than TA but greater than OBU;
- The time in various parts of the entire VANET is synchronized;
- The authentication may use a concept of ideal Tamper-Proof Device (some researched have developed method that do not require such assumption [11]).

7.1.1 Different CPPA Algorithms:

Every recently developed CPPA authentication algorithms must conform to two principals from Internet of Things (IoT) development:

The first concern is the security of the IoV system. Wireless communication channels may be compromised and taken over by attackers, and therefore, data can be eavesdropped, modified, replayed, etc. Thus, researchers and implementers of IoV need to ensure that the system is sufficiently robust to withstand existing malicious attacks.

The other significant concerns are anonymity and traceability relating to the identity of the vehicle's owner/driver, the vehicle registration, origins and the computed route in which the vehicle is transiting on. If the vehicle's OBU transmits the identity of the vehicle's owner to other vehicles or RSUs without due protection, an adversary might trace the vehicle's routes via eavesdropping of the messages. There are potential real-world consequences of the leaked routes. Thus, the anonymity of the vehicle's owner is another significant property of IoV.

As previously mentioned, researchers have presented a number of conditional privacy-preserving authentication (CPPA) protocols, in order to achieve both of the above discussed properties in an IoV system [8]–[11], [18].

7.1.1.1 ID-based CPPA

One type of CPPA algorithm works on using ID-based cryptography. In this algorithm the overhead computation is reduced because the roadside unit (RSU) can authenticate the message in batch. To overcome vehicle revocation more time will be required for TA[19].

Another ID-based CPPA algorithm also supports batch authentication and is used to optimize the computation overheads. The drawback of this algorithm is that it does not guarantee the data integrity[10].

7.1.1.2 RAISE

Recently an algorithm was devised called RSU-aided Message Authentication Scheme or RAISE that can reduce the revocation process of vehicles and password modification for IoVs is more efficient than any other CPPA algorithm whilst preserving anonymity using k-anonymity technique [20]. The drawback of this algorithm is that it does not provide unlink ability and any attacker can associate owners of two messages by matching the vehicle registration time [21].

7.1.1.3 CL-CPPA

To address both privacy and security requirements in the internet of vehicles another algorithm is developed which is known as certificate-less CPPA (CL-CPPA) protocol. Using this protocol no certificates for tacking and verification are required for trusted authority (TA). The CL-CPPA protocol can prevent impersonation, modification and other attacks. The CL-CPPA protocol requires lower computation and communication costs as compared to other protocols[9].

7.1.2 How Conditional privacy-preserving authentication (CPPA) Work:

In this section it will be explained how the process of CPPA works using as an example a generic IBC (Identity-Based Cryptography) with Elliptic curve cryptography.

There are two main phases in Conditional privacy-preserving authentication (CPPA) i.e. offline registration and driving stage. Initialization of TA and registration of vehicles (OBUs) and RSUs are included in offline registration while mutual authentication, verification of messages, receiving of messages and release of traffic information come under the driving stage.
The main symbols used in offline registration and driving stage are depicted in Table 1 below;

Notation	Description
p, q	Two large prime numbers
E	An elliptic curve defined by $y^2 = x^3 + ax + b \bmod p$, as $b \in Fp$
G	An additive group which consists of all points on the elliptic curve E
IDr, TregRSU	The real identity associated with location and its corresponding registration time of RSU
IDv, TregOBU	The real identity and its corresponding registration time of vehicle
PKrsu, SKrsu	The public key and corresponding private key of RSU
Lrsu	The registration list of RSU that saved in TA
Lobu	The registration lists of vehicle that saved in TA
Lm	The message list that saved in RSU
h (·)	A secure hash function

Table 1. Notation for CPPA algorithm

7.1.2.1 Offline Registration:

System initialization is introduced in offline registration. OBU (vehicles) and RSU are registered in the manufacturing factory or during the annual inspection of the system. while identity distribution and management is the responsibility of the TA.

7.1.2.2 Initialization of TA

As mentioned in the earlier section that high computing power and greater storage capacity is the functionality of TA. All the operations and coordination of VANETs are controlled by TA. The TA is initialized in the following way; Two large prime numbers are chosen by TA, then an additive group G with the order q and its generator P is also selected. The P consists of which consists of all points on the elliptic curve E (the equation is mentioned in Table 1).
A random number s $\in Z * q$ as a master private key is selected by TA and then it computes, Ppub = s · P as the master public key.
A secure hash function h (·) is chosen by TA.
System parameters {p, q, a, b, P, Ppub, h} are broadcasted by TA periodicity.

7.1.2.3 RSU registration

According to location the identity IDr of RSU is selected by the TA, where then it computes KR = h (IDR||s), where TregRSU is the corresponding registration time. After that the registration time is saved by TA to the registration list LRSU and sends {KR, IDR} to RSU.

7.1.2.4 Registration of Vehicles:

The KV = h (IDV ||s) and ZV = KV $\oplus$ h (PW1||PW2) is calculated when the identity IDv and two passwords PW1 and PW2 are chosen by TA. The corresponding restoration time of OBU is TregOBU. If modification in passwords will be required then KV and ZV will be used. TA added TregOBU, IDV to registration list of Lobu, and then sends {IDV, PW1, PW2, ZV, Treg OBU} and {IDV , PW1, PW2} to OBU and the owner of the vehicle respectively.

7.1.2.5 Driving Stage:

The messages are broadcasted to all vehicles in range in this range periodically by RSU. A pseudo identity is generated by OBU whenever a vehicle enters into the range of RSU and it is that identity that is then sent to corresponding RSU. When a message from the vehicle is received and processed that pseudo identity is then sent to TA by RSU. The TA looks into the registration list based on timestamp and confirms the legal presence of OBU and RSU and then the message is returned back by TA to RSU. The returned message is then broadcasted by RSU after the process of computation and is received by the vehicle after confirming its legitimacy. By the time the vehicle receives the message TA, RSU and OBU should have completed the mutual authentication process. With the help of RSU, OBU can issue the traffic information after the authentication process.

7.1.1.6 Vehicle to vehicle communication:

Vehicle-to-vehicle communication is a critically important part of VANETs as many safety-related applications rely on single-hop beacon messages broadcast to neighboring vehicles.

High transmission rate and short latency characterized the vehicle to vehicle communication in the internet of vehicles. Useful information such as collision detection, emergency braking and condition tracking are broadcasted directly from vehicle to vehicle, this poses many challenges as it is possible to create Denial of Service attacks (DDoS) if a large number of broadcast beacons arrive in a short time, for example.

There has been research done on Prediction-Based Authentication (PBA) that allows for not only defending against computation-based DoS attacks, but also resist packet losses caused by high mobility of vehicles [22], [23].

7.2 Other Authentication methods for internet of vehicles:

It is good to speculate other emerging technologies in the field of a decentralized internet of vehicles.

One of the most relevant technologies that is on the rise as of writing of this paper is blockchain technology. This is an inherently decentralized and secure network of nodes communicating with each other.

In this section we will look for Blockchain-based authentication methods in IOVs.

7.2.1 The blockchain technology

Blockchain is a decentralized network of nodes (also called “records”) that allows users to store and transfer information and currency instantly in a safe and anonymous manner. The term blockchain then refers to how the data is stored in ”blocks” of information and then linked together in a permanent “chain.” As the new block is added to the chain it will be validated and “trusted” by both the previous and next blocks, making security very robust. There are several facets that make blockchain technology unique and valuable for many different types of business applications [17], [24], [25].
There are three basic parts to every blockchain;

- The record: This can be any type of information;
- The block: A bundle of different records;
- The chain: This contains all the blocks linked together.

7.2.2 Blockchain-based authentication:

The Blockchain technology works on the combination of many technologies including peer to peer technology, smart contract and incentive theory technology, asymmetric encryption technology and distributed ledger technology. The Bitcoin system is one of the underlying and most widely used models and examples of Blockchain technology. The Blockchain technology can be divided into three chains, the unique chain, co management chain and the contracted chain. Transparency, openness, traceability, encryption, untouchability and time series are some of the common characteristics of block chain technology. Degree if Decentralization, consensus, mechanism and trust mechanism are some of the common differences that lies in this technology. The block chain system consists of data layer, network layer, consensus layer, incentive layer, contract layer and application layer.

The block chain technology is suitable for complex traffic environments in the internet of vehicles where vehicles don't trust each other because of blockchain's characteristics of decentralization and distributed consensus. The attackers cannot temper the data if the protection of block chain technology is enabled. The same account information of the users can be maintained by multiple service providers jointly. Entire identity authentication on different servers is required by the user to maintain the account information on the ledger. This identity authentication can bring more efficiency. The vehicle itself provided the energy consumption in the block chain model unlike other internet of things (IOT). This can lead to a large amount of energy consumption on the block chain network [26].

7.2.3 Different blockchain solutions for IoV:

There are several different researches into the implementation of blockchain into Internet of Vehicles with widely varying consensus about operation, infrastructure, trust, centralization and authentication [17], [24], [26]–[28] which is probably one of the biggest hurdles and disadvantages of the technology in the realm of IoV (which will be discussed in more detail later on this paper). Some of the possible variations are, for example, the use of a public or private blockchain list, the latter of which is centralized and requires an overseeing entity to allow registration (which is more in line with the VANET system that we have looked into) and the former which is a decentralized system (which falls more in line with the dream of a fully decentralized system with guaranteed anonymity), this and several other differences brings us to decide on just finding the research more in line with the current view of VANET infrastructure [26] and use it from now on on the describing and comparing the work of blockchain-based solutions, and working and supposing a private-list blockchain system.

7.2.4 How Blockchain internet of Vehicle Works:

The block chain system for the internet of vehicles consists of three components: road side units (RSU), vehicles and cloud service providers. An orderly block of network is built among these three units of the system. Before transmitting and receiving broadcasting vehicles are required to submit their identity for registration with the road side unit (RSU). The relevant information of the vehicles are then encrypted and transmitted to the cloud service provider when RSU checks the validity of the concerned vehicle. In the next step it is the responsibility of the cloud service provider to write the relevant vehicle information into the trusted account book or not. After that the cloud service provider distributes these information to the rest of the road side according to consensus algorithms. The road side units then feedback this relevant information and unique identity of the vehicle to vehicle and thus the whole registration process is completed. When the above registration process is complete then the vehicles are permitted to transfer data and share broadcasting with the same registered vehicle only. The whole registration process is depicted in Fig 5

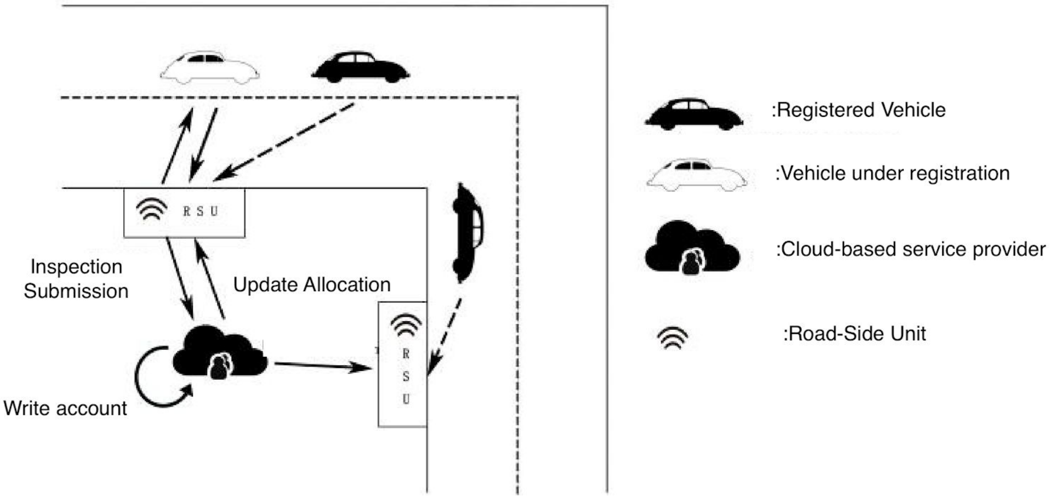

Fig 5: How Blockchain internet of Vehicle Works

7.2.5 How Blockchain authentication works in self-driving cars:

To build trust a standardized intelligent contract is needed because the environment of the internet of vehicle is full of mutual distrust. This standardized intelligent contract was first proposed by Nick Szabo in 1995. Well-structured architecture with smart contracts is now possible because of the development of Ethereum. Based on the Rayleigh consensus algorithm the new intelligent contract was designed to differentiate between blocking malicious nodes and joining new nodes from the root. The new intelligent contract is shown in Fig.6 [17].

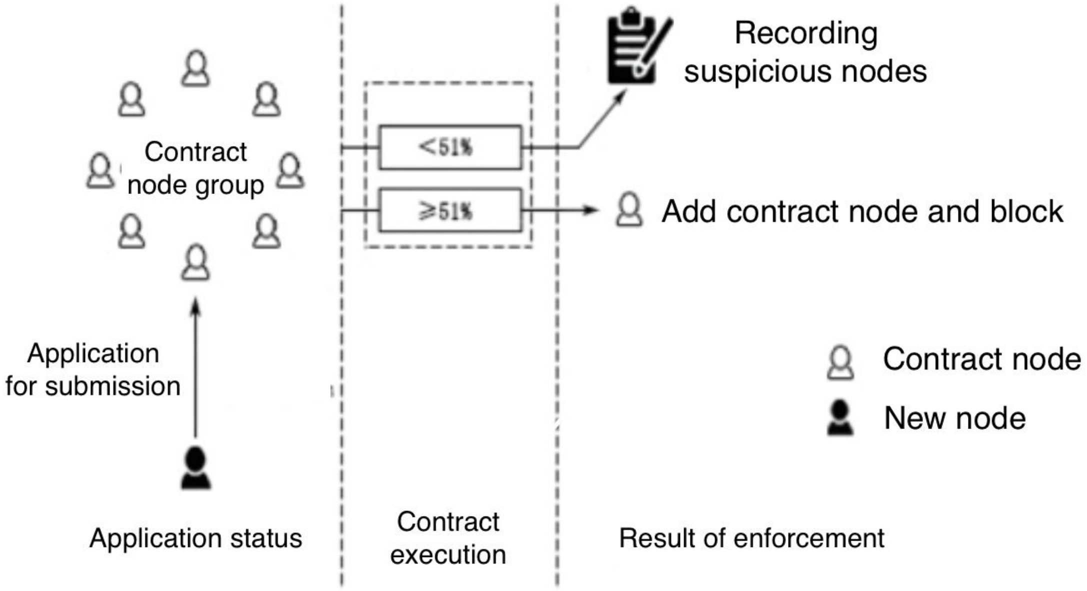

Fig 6: Block chain authentication in internet of vehicles:

In this block chain authentication algorithm it is guaranteed that the system does not begin to collapse from the root. Therefore the intelligent contract is implemented for vehicle manufacturers, cloud service providers and road side units (RSU) [24]. According to the blocks, the three components of block chain technology in IoV. The validated vehicles, road side units and cloud service providers form a node group in this intelligent contract. An application to the contract node group is submitted whenever a new node wants to apply to join the contract node group. The credit rating and credit record of current application nodes from the terminal database is retrieved when the application is received by the contract node group. The contract node group then decides whether to trust the new application node or not. The digital signature to the execution layer is submitted by the contract node if trust the new application node. In case the contract node denies to trust the new node no digital signature will be granted to that untrusted node. The new node is identified as a new contract node and is added to the block if more than 51% of digital signatures are collected. The node information is added to suspicious nodes and the new node application request is rejected if the number of digital signatures is less than 51%. These suspicious nodes are then broadcasted to the other blocks. When these suspicious nodes again send an application request to the contract node it will meet through more audits to meet the criteria of the new contract node.

The cost of authentication in block chain authentication increased with time as there are a lot of untrustworthy and unknown nodes in the authentication process. But on the other hand security of the system is maintained in a better way and trust among the system components is built using the block chain authentication in the internet of vehicles[24].

7.2.6 The challenges of Blockchain Authentication in self-driving vehicles

Besides the fact that this is an emerging technology that requires much more research into applications besides the current financial sector it dominates, we can find some drawbacks of the technology as it stands for implementation into IoV.

7.2.6.1 Storage and processing time

Data storage on blockchain comes with the extra effort of having to store and mine the blocks. Processing power is also an extremely important factor in the generation of the blocks, as the blockchains are based on the concept of PoW (Proof of Work) which defines the authenticity of a record. The embedded systems integrated into vehicles and authorities may have several resource usage constraints, implementing the CIA (Confidentiality, Integrity and Authentication) for vehicle embedded IoT devices can be a difficult task, especially as the application of the "Internet of Everything" philosophy in which the IoV is part of, inherently focuses on resource efficiency [29].

A variable that comes handy in these types of analyses is the block time, the time required to mine a block, (a set of records) and put it permanently in the blockchain. The usual time to mine a bitcoin block is around 10 minutes [30].

There should be incentives generated for the participating nodes for consensus generation, smart contracts can facilitate this transaction.

There has been studies done that work on which kind of technologies are better suited for using blockchain as its main philosophy [29]

The implementation of embedded systems into vehicles is not a big of a hassle however, as vehicles are not restricted by the size and weight constraint that many other IoE devices have to comply to, which is mentioned in the aforementioned research by Kurt Peker..

7.2.6.2 Scalability

Another major hassle in the adoption of blockchain-based technologies for IoV authentication is the scalability.

One of the major hurdles that is limiting the adoption of blockchain in the IoT sphere is the problem of scalability. The rate of transaction execution in the blockchain should facilitate the IoT system but due to the massive numbers of transactions and data exchange, current blockchains are unable to keep up with this. The biggest challenges in this integration are the scalability of ledger and rate of transaction execution in Blockchain. Also implementing blockchain peers into IoT devices can be a lot of resource input and more than the device can handle.

7.2.6.3 Infrastructure and implementations

The biggest hurdle of blockchain-based authentication is that the majority of research that exists into it does not take into consideration the current advancements of VANET as in the "traditional" infrastructure of IoV (Central Authority, Road-side assistance and on-board unit system) and they require the complete re-imagining and re-implementation of the entire structure of intelligent automated vehicles [17], [26]–[28], [31]

8 Comparison of authentication methods for Internet of Vehicles

After having an overview of different mature and researched CPPA authentication protocols and the emerging blockchain technology for authentication of automated vehicles in an IoV environment, we can discuss the differences, advantages and disadvantages of each.
Some blockchain research papers try to compare their technology to overall existing CPPA algorithms and even VANET itself [24], [28] but this paper is the first to truly compare VANET standard systems with Blockchain based systems.

8.1 Advantages and Disadvantages of CPPA authentication:

The summary of advantages regarding Conditional Privacy-Preserving Authentication algorithms.

Advantages:

- Identity privacy preservation: The real identity of vehicles cannot be obtained by the hackers when messages are shared by the vehicles. The real identity can only be identified by the TA in CPPA authentication;
- Traceability: malicious messages can provide the identity of the hackers and TA not only identifies the attacker but it also takes action against the malicious contents;
- Non-repudiation: The message sent by vehicle will be accepted if it is not malicious;
- Un-link ability: The message content of the vehicles cannot provide any relevant information of the same vehicles to the intruders;

- Resistant to continuous disruption: The CPPA authentication protocol in VANet is not only able to cease the continuous malicious behaviours but it also shows the real identity of attackers;
- Maturity: Arguably the most important advantage is the maturity of the research into the technology, which is very advanced with a big community dedicated to creating a specific algorithm for dealing with autonomous vehicle communications.

Disadvantages of CPPA:

- The drawback of this CPPA authentication in the internet of vehicles is that it does not guarantee the data integrity;
- Handling vehicle revocation requires more time;
- Many different algorithms that have to be standardized, they are mostly not compatible with each other, in a wider network, one must be chosen and set as standard.

8.2 Advantages and Disadvantages of Blockchain authentication:

The summary of advantages and disadvantages in blockchain authentication algorithms.

Advantages:

- The identity authentication problem between the vehicles, cloud servers and road side units can be solved by the Blockchain authentication technology in IoVs;
- The new block chain authentication mechanism has also allowed the management of the user accounts, thus enabling the user for multiple login to the same account;
- The identity information of the vehicle is encrypted by this authentication technology which will help in preventing the leakage of user information;

- New key mechanism is developed in block chain authentication which has further improved the security of the internet of vehicles;
- Data related to privacy can only be shared on demand;
- Private data of users such as location information of the users are private and confidential.

Disadvantages:

- The cost of authentication in block chain authentication increases with time as there are a lot of untrustworthy and unknown nodes in the authentication process;
- Multiple keys are owned for communication with users which are variable in the lifetime of vehicles;
- The data must be downloaded from the service cloud providers by connected vehicles which incurs packet overhead and delay in the overlay;
- High processing power and storage required in the system;
- Scalability;
- Very early stage technology with a wide range of widely diverging and changing methods of implementing IoV infrastructure, high cost of research and implementation.

9 Demo application

It is good to speculate over emerging technologies to be implemented in a future Internet of Vehicles network, but VANET is currently the most mature and verifiable system that could make up an internet of automated vehicles in the future. Following this assumption, an application has been developed that demonstrates the authentication process for generating a registration of a new vehicle from a trusted authority, and the process of login to the vehicle by a user which the registration was generated to.

The choice of language was python due to the easiness of not just implementing a complex authentication algorithm but the much better readability of said algorithm for someone who wishes to navigate the code to understand the operations in detail. It is a console application with no graphic interface, as it has been deemed not necessary for a demonstration of an authentication algorithm.

The code for this demo application can be accessed by cloning the repository marked in **Appendix 1**

The algorithm follows the ID-based Conditional Privacy-Preserving Authentication algorithm due to being easy to implement and explain.

The program executes the following instructions in sequence:

9.1 Input for registration

Receives a chosen Vehicle user for registration to be saved for later use, an ID that is a number used to identify the specified vehicle. Random prime numbers for s, p and g are chosen.

9.2 Generating hash function

At this point, password and random number are concatenated, the hash object is generated by using python's built-in property *hash()* with the concatenated result called *hash_find*, same is applied to the vehicle ID created in the previous step. Both hashes are concatenated, private key for TA is chosen and public key is calculated with the random created primes, both are hashed.
Ni is determined by taking the XOR operation with the *hash_find* and the hash generated with the keys and vehicle id.
This data is then “issued” to the smart-id used for authentication.

9.3 User login process

In this phase the user enters the smart card into the vehicle and enters the ID, Password and Random No. The Smart card computes the Ai (Authentication Information) and matches it with the stored Ai (Authentication Information).

9.4 Data authentication process

For each time a vehicular user Vi wants to connect to the TA through a nearby RSU Rx , it executes the following steps to obtain a session key.

9.4.1 Vehicle retrieving public key from smart card

Vi retrieves the K and Y from the smart card a generates the random integer Alpha (a) and computes attributes with time T.

Hashing the car ID inputted by user (smart card), performing *Di = ga mod p*

```
hash_IDVs = IDV ^ s
hash_k = hash(hash_IDVs)
```

Calculating *alpha a*

```
rand_int = randint(0, 100)
```

Vehicle calculating attributes

```
Di_modless = g ** rand_int
Di = Di_modless % p
Ei_modless = int(y) ** rand_int
Ei = Ei_modless % p
hash_Ei = hash(Ei)
AIDi = int(IDV) ^ int(hash_Ei)
k_ll_Ei = str(hash_k) + str(Ei)
hash_DIDV = hash(k_ll_Ei)
concat_CVi = str(AIDi) + str(hash_DIDV) + str(Ei)
hash_concat_CVi = hash(concat_CVi)
```

9.4.2 Processing at the Trusted Authority

Subsequently *Vi* (vehicle) also sent the above detail to the RSU. (RSU = *Rx*)
When Rx receives the login message from a vehicle, it drops the message if time *T* in the login message expires. Otherwise, it appends its ID *IDRx* to the message and relays it to the TA.
Now the message reached the TA and it will validate the login message.
TA will validate following things:
Ei-star, K-star,CVi-star.
Performing: *Ei-star = DiX mod p*

*Ei_stars = (Di) ** x*

Ei_star = Ei_stars % p

Performing *K-star = hash(AIDi XOR hash(Ei-star) XOR s)*

hash_Ei_star = hash(Ei_star)

K_star = hash(AIDi ^ hash_Ei_star ^ s)

Performing *CVi-Star = hash(AIDi || DIDV ||Ei_star)*

CVi_star = hash(str(AIDi) + str(hash_DIDV) + str(Ei_star))

Now by matching *CVi-Star* and *hash_concat_CVi,* if they are the same, then authentication is successful with the Trusted Authority.

TA will then generate random number *B = beta*

rand_beta = randint(100, 200)

It uses it to compute: Gi, Ks, Ci

Performing Gi = gB mod p:

*gbeta = g ** rand_beta*

Gi = gbeta % p

Performing *Ks = hash1(DiB mod p),* this is session key

*Di_beta = Di ** rand_beta*

Ks = hash(Di_beta % p)

Performing *Ci = hash1(DiB mod p || Ei_star || K_star)*

Di_beta_mod_p = Di_beta % p

Ci = hash(str(Di_beta_mod_p) + str(Ei_star) + str(K_star))

It sends fAIDi;Ci;Gig to *Rx* and the RSUs near *Rx* through a secure channel. *Rx* and these RSUs broadcast the same message on air. The messages are also sent to the nearby RSU to prevent *Vi* moving away from Rx.

9.4.3 Vehicle computing attributes

Performing *Ci_stars =hash1(Gia mod p || Ei || K)*

*Gi_alpha = Gi ** rand_int # Gi and Alpha*

Gi_mod_p = Gi_alpha % p

Ci_star = hash(str(Gi_mod_p) + str(Ei) + str(hash_k))

Performing *KS_stars = hash1(Gia mod p)*

KS_star = hash(Gi_mod_p)

It will accept the protocol and successfully log in if *Ci_star* = *Ci* using KS as the session key.

Summary

We live in a world thriving for ever more integration and connection between things and people, the internet has changed our perception of the world and how things work through the ever more present implementation of Internet of Everything (IoE), these advancements will inevitably reach the transportation sector, with the advent of automated vehicles, this seems like the perfect scenario to have a fully integrated and connected network of vehicles communicating to each other and to infrastructure and from them on, to everything. Unfortunately the very same risks and drawbacks that affect the IoE apply to the automated vehicle integration, with the added risk that this is a critical system that can cause far greater damage, leading up to the loss of life. Having a safe authentication protocol for these cases is one of the most important aspects for implementing a Vehicular Ad-Hoc Network (VANET). Based on the data acquired from this paper we can assume that VANET is the most sophisticated and complete form of infrastructure in the development of Autonomous vehicles communications infrastructure. The development of implementing emerging blockchain technologies is a field of interesting research that can greatly benefit the development of an Internet of Vehicles, especially when added the financial benefits of blockchain in the integration of payment and trust-based blockchain list systems.

As far as the authentication is concerned, the current CL-CPPA and ID-CPPA authentication techniques are provably efficient and secure, greatly improving upon previous iterations of privacy-preserving algorithms and are deemed at the same time secure and efficient for a critical system.

The application of one of the aforementioned CPPA algorithms into a VANET is the best course for the development of Internet of Vehicles, and a possible topic for future research can be the benefits and advantages of applying features of blockchain-based solutions into the mature VANET system, instead of redesigning it from scratch.

References

[1] A. Taeihagh and H. S. M. Lim, “Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks,” *Transp. Rev.*, vol. 39, no. 1, pp. 103–128, Jan. 2019.

[2] J. Dokic, G. Meyer, and B. Müller, “European Roadmap Smart Systems for Automated Driving (No. 1.2).” EPoSS. http://www. smart-systems-integration. org/public/documents/publications, 2015.

[3] H. S. M. Lim and A. Taeihagh, “Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications,” *Energies*, vol. 11, no. 5, p. 1062, Apr. 2018, Accessed: Apr. 30, 2020. [Online].

[4] C. Miller and C. Valasek, “Securing self-driving cars (one company at a time),” in *presented at Black Hat*, 2018, [Online]. Available: http://illmatics.com/securing_self_driving_cars.pdf.

[5] M. Rouse and Others, “Internet of things (IoT),” *IoT Agenda*, 2016.

[6] S. Supriya and S. Padaki, “Data Security and Privacy Challenges in Adopting Solutions for IOT,” 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)*, Dec. 2016, pp. 410–415.

[7] J. L. Holland and S. Lee, “Internet of Everything (IoE),” *Harnessing the Internet of Everything (IoE) for Accelerated Innovation Opportunities*. pp. 215–245, 2019, doi: 10.4018/978-1-5225-7332-6.ch010.

[8] J. Li *et al.*, “EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *Vehicular Communications*, vol. 13, pp. 104–113, Jul. 2018.

[9] J. Li, Y. Ji, K. R. Choo, and D. Hogrefe, “CL-CPPA: Certificate-Less Conditional Privacy-Preserving Authentication Protocol for the Internet of Vehicles,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10332–10343, Dec. 2019.

[10] D. He, S. Zeadally, B. Xu, and X. Huang, “An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[11] B. Wang, Y. Wang, and R. Chen, “A Practical Authentication Framework for VANETs,” *Security and Communication Networks*, vol. 2019, May 2019, doi: 10.1155/2019/4752612.

[12] M. van Rijmenam and P. Ryan, “What is the Blockchain?,” *Blockchain*. pp. 12–39, 2018, doi: 10.4324/9780429457715-2.

[13] C. K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*. Pearson Education, 2001.

[14] Sheikh, Sheikh, Liang, and Wang, “A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs),” *Sensors*, vol. 19, no. 16. p. 3589, 2019, doi: 10.3390/s19163589.

[15] C. Sommer and F. Dressler, *Vehicular Networking*. Cambridge University Press, 2015.

[16] P. Newman, “THE INTERNET OF THINGS 2020: Here’s what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue,” *Business Insider*, Business Insider, Mar. 06, 2020.

[17] R. Ramaguru, M. Sindhu, and M. Sethumadhavan, “Blockchain for the Internet of Vehicles,” *Communications in Computer and Information Science*. pp. 412–423, 2019, doi: 10.1007/978-981-13-9939-8_37.

[18] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *Int. J. Inf. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[19] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, “Conditional Privacy-Preserving Authentication Using Registration List in Vehicular Ad Hoc Networks,” *IEEE Access*, vol. 6, pp. 2241–2250, 2018.

[20] V. Khanaa, Dean-Information., Bharath University, R. Udayakumar, A. Prof., and IT. Bharath University, “Protecting Privacy When Disclosing Information: K Anonymity and its Enforcement Through Suppression,” *International Journal of Business Intelligents*, vol. 001, no. 002. pp. 28–31, 2012, doi: 10.20894/ijbi.105.001.002.001.

[21] C. Zhang, X. Lin, R. Lu, and P. -. Ho, “RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks,” in *2008 IEEE International Conference on Communications*, May 2008, pp. 1451–1457.

[22] M. Lalli and G. S. Graphy, “Prediction based dual authentication model for VANET,” in *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, Jul. 2017, pp. 693–699.

[23] C. Lyu, Y. DawuGu, and P. B. A. PrasantMohapatra, “Prediction-based Authentication for Vehicle-to-Vehicle Communications IEEE Transactions on Dependable and Secure Computing.” 2015.

[24] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “BlockChain: A Distributed Solution to Automotive Security and Privacy,” *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[25] T. Economist, “The great chain of being sure about things,” *The Economist. Accedido desde http://www. economist. com*, 2015, [Online]. Available: https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

[26] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, “An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology,” *IEEE Access*, vol. 7, pp. 45061–45072, 2019.

[27] T. Jiang, H. Fang, and H. Wang, “Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019.

[28] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, “Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[29] Y. Kurt Peker, X. Rodriguez, J. Ericsson, S. J. Lee, and A. J. Perez, “A Cost Analysis of Internet of Things Sensor Data Storage on Blockchain via Smart Contracts,” *Electronics*, vol. 9, no. 2, p. 244, Feb. 2020, Accessed: Apr. 30, 2020. [Online].

[30] A. F. Zorzo, H. C. Nunes, R. C. Lunardi, R. A. Michelin, and S. S. Kanhere, “Dependable IoT Using Blockchain-Based Technology,” in *2018 Eighth Latin-American Symposium on Dependable Computing (LADC)*, Oct. 2018, pp. 1–9.

[31] L. Zhang *et al.*, “Blockchain based secure data sharing system for Internet of vehicles: A position paper,” *Vehicular Communications*, vol. 16, pp. 85–93, Apr. 2019.

Appendix 1

Demo application source code can be found at:

https://github.com/Danzmann/iov_authentication_simulation

The application can be cloned into any machine capable of running python then, on Linux and Mac (tested platforms) run on terminal in the location of file:

```
python3 iov_simulation.py
```