Article

Performance Analysis of Blockchain-Enabled Security and Privacy Algorithms in Connected and Autonomous Vehicles: A Comprehensive Review

Rabia Khan[1], Amjad Mehmood[1,2*], Carsten Maple[2], Ghulam Abbas[3], Kevin Curran[4]

1 Institute of Computing, Kohat University of Science & Technology, Kohat; rabia82@gmail.com
2 Secure Cyber Systems Research Group (CSCRG), WMG, University of Warwick, Coventry, UK,dramjad.mehmood@warwick.ac.uk, cm@warwick.ac.uk, gregory.epiphaniou@warwick.ac.uk
3 Department of Information Technology , Hazara University, Pakistan, abbasfacho@gmail.com
4 School of Computing, Engineering & Intelligent Systems, Ulster University, Londonderry, UK. Kj.curran@ulster.ac.uk
* Correspondence: dramjad.mehmood@ieee.org

Abstract: Strategic investment(s) in vehicle automation technologies led to the rapid development of technology that revolutionalised transport services and reduced fatalities on a scale never seen before. Technological advancements and their integration in Connected Autonomous Vehicles (CAV) increased uptake and adoption and pushed strongly for the development of highly supportive legal and regulatory and testing environments. However, systemic threats to the security and privacy of technologies and lack of data transparency have created a dynamic threat landscape within which the establishment and verification of security and privacy requirements proved to be an arduous task . In CAV,security and privacy issues can affect the overall resilience of these systems and hinder the safety of the passengers. Existing research efforts have been placed to investigate the security issues in CAVs and propose solutions across the whole spectrum of cyber resilience. This paper examines the state-of-the-art security and privacy solutions for CAV and investigates their integration challenges, drawbacks and efficiencies by coupling them with distributed technologies such as Blockchain. This survey paper has highlighted the strengths and drawbacks of the security and privacy measures proposed in the published literature based on Blockchain technology. It has also listed different cyber attacks being investigated while designing security and privacy mechanism for CAVs.

Keywords: Cyber-Physical System, Connected and Autonomous Vehicles, Blockchain Technology, Security, Privacy

Citation:
. *Appl. Sci.* **2021**, *11*, x. https://doi.org/10.3390/xxxxx

Academic Editor: FirstnameLastname

Received: date
Accepted: date
Published: date

1. Introduction

Enormous advancement and expansion in information technology have brought a revolutionary impact in every aspect of life. The growth and deployment of different Cyber-Physical Systems (CPS) are the representative examples of the information technology revolution. CPS is the combination of different physical and cyber elements to emulate the capabilities of an embedded system [1]. Physical elements comprise anything in the physical world, such as natural events (flood, earthquake, etc.), vehicles, sensors, actuators, grids, buildings, etc., while the cyber elements comprise communication and computing devices. CPS has been deployed in various domains such as transportation systems, household appliances, electricity and gas distribution grids, healthcare systems and many more. The objective of CPS is to monitor the behaviour of physical elements and generate appropriate actions to ensure the smooth funtionings of all the CPS components [2].

The increased demand for installing and deploying embedded systems (smart grids, autonomous automobile systems, industrial control systems) in managing and handling complex tasks is becoming more prone to cyber-attacks due to the increased attack surface and increased adversarial motivations. The complexity of CPS interactions expands the attack types from cyber-to-cyber to cyber-kinetic and increase the complexity and level of resources required in detection and mitigationprocesses [3]. A CPS is not capable to handle every type of security threat which further raises the security and privacy concerns during their deployment and operation. The heterogeneous nature of CPS components complicates the communication processes , rendering existing threat models inadequate to capturing all interactions that give rise to the different adversarial scenarios[3]. Since all the physical components are integrated, it is challenging to examine and identify every component for any possible attack as adversaries can attack both the physical elements and the communication mechanisms. Although current research on security and privacy for CPS is gaining traction, existing controls for CPS are static and seem to lack the holistic defence requirements needed in these modern cyber infrastructures [3].

Though different security and privacy solutions have been proposed in the public literature, this paper emphasises security and privacy mechanisms using Blockchain technology for connected and autonomous vehicles (CAVs) and consider the published research from 2016 -2020. It also covers the challenges posed by different threats in response to security measures, their attack matrix, and respective mathematical models in order to analyse their performance.

1.1. Applications

CPS represents a new generation for the digital world. It finds its future in almost every domain of life. Some of the practical impact of CPs on life as mentioned here. Underground Wireless Sensor Network is launched to garner the benefits of CPS for precision agriculture [4]. Smart Pest Control using CPS has been proposed to control and monitor the rats in the agricultural fields [5]. Using CPS and agents, a controlling mechanism has been proposed to ensure agricultural proactivity versus the market and environmental changes [6]. Healthcare is the sector in particular where benefits of CPS have been withdrawn at large. A cyber-physical management system has been introduced to support surgeons in operating rooms [7]. A generic framework for related medical services and devices has been proposed to assist patients to remain in connection with their doctors in case of any emergency and continuous monitoring [8]. CPS has been utilised in smart learning environments. A Smart University Laboratory environment has been constructed using CPS, including the mechanisms for statistical analysis, communication, and habit-based control [9]. Energy supply has always been a challenge. Energy Management Framework (EMF) has been proposed to integrate CPS for collecting real-time power consumption and demand status from autonomous electric vehicles and the charging stations within the smart grid [10]. CPS can also be used to control and monitor the traffic system by installing many advanced information management systems and electronic devices to the traffic system, which can improve the safety level and improve the operational efficiency [11]. Process control CPS is the first step to provide autonomous control on the production process through control loops. The application of CPS is applied in industrial 4.0 to enhance process control generating smart industry [12].

1.2. Motivations

CAV is the need of future. Being part of intelligent transportantion, security, privacy and reliability are the major challenges being faced in CAVs. Motivations to write this survey paper are:

i. To highlight the security and privacy issues in the connected vehicles
ii. To highlight the security and privacy measures based on Blockchain for the CAVs

Though numerous security measures such as encryption, trust management, key management, authentication techniques, software-based solutions, and network solutions have been intensively studied and analysed, but here the focus will be on the security and privacy measures based on Blockchain.

1.3. Contributions

Several surveys have been conducted to highlight the security and privacy issues and controlsin CPS. Since the main focus of this paper is connected vehicles,the published literature for security and privacy for connected vehicles is considered. It has been observed that existing literature on security and privacy of CAV discusses security measures in generals. The existing literature generalise the security and privacy mechanisms by highlighting the pros and cons of different measures. As such, authors in [13] studygenericsecurity and privacy attacks on CAV and highlights the mitigation controls generically.A different aspect of CAV and their associated threats and available security measures have been studied and highlighted the knowledge gap for future research directions [14]. Individual contributions towards security and privacy issues of connected vehicles are provided in the published literature.

The contributions of this paper are:

i. A state-of-the-art and in-depth analysis and comparison of the existing and emerging security and privacy attacks and vulnerabilities on CAV
ii. A comparison of the Blockchain technology as a security mechanism against the attacks identified in the published literature
iii. Detailed analysis of the future directions being promised by Blockchain technologyasadefence mechanism.

The rest of the paper is organised as follows: Section 2 presents the background highlighting a general architecture of CPS. Connected and Autonomous Vehicles (CAVs) are discussed in detail as an application of CPS in section 3. Section 4 highlights the Security requirements for CAVs, focusing on the attacks and vulnerabilities analysed. Literature on security and privacy solutions using Blockchain technology is discussed in-depth in section 5. Discussion on the literature and future research direction is provided in section 6. Finally, section 7 concludes the paper by summarising our main findings. The distrubution of the paper is also as shown in the follwong table for ease to understand the contents of the paper.

1. Introduction	a. Application
	b. Motivations
	c. Contribution
2. Background	
3. Connected and autonomous vehicle-application of CPS	a. Wireless communication
	b. Engine control unit
	c. Censor and cameras
4. CAVs security and privacy	
5. Security and privacy solution using blockchain	
6. Findings	
7. Conclusion	

2. Background

In general, CPS has been designed to consist of two elements on which all researchers agree, i.e., physical elements and cyber elements. Physical layers consist of natural and man-made physical elements, while the cyber layer is comprised of communication and computing devices. The main task of the physical layer is to capture the sensed data and perform cyber layer operations/commands while the cyber layer analyses and processes physical layers data and accordingly generates appropriate commands/operations [15]. Multiple layered architectures have been proposed in the literature [15-18]. In general, a three-layered architecture can be considered, consisting of perception/ hardware/physical layer, transmission/communication/network layer, and application/services layer [19]. Figure 1 shows the three-layered architecture of CPS.

The first layer is the hardware layer, also known as the sensor layer [19]. This layer is characterised by the hardware devices that include detectors, sensors, actuators, GPS, home appliances, cameras, RFID, intelligent scanners and many more that can sense and collect data he second layer is the network layer, also known as the transmission layer.The major role of this layer is to facilitate the communication between the hardware and the application layer. The third layer is the application layer that processes the data received from the network layer and generates appropriate commands to be executed by the devices in the physical layers [20].

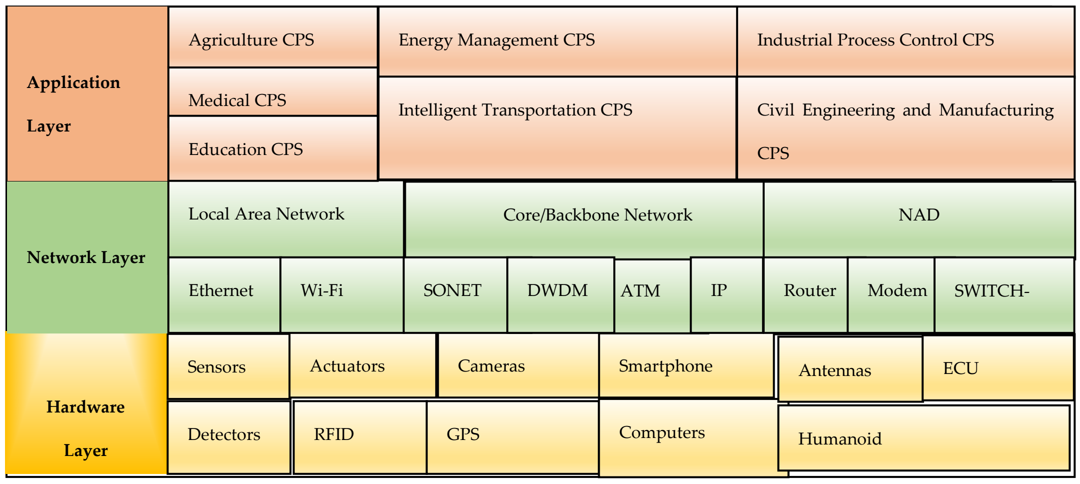

Figure 1: Three Layered Architecture of CPS

3.Connected and Autonomous Vehicles-An Application of CPS

With the arrival of intelligent transport systems, transportation will become safer and energy-efficient [21]. Connected and Autonomous Vehicles (CAVs) is the most significant technology within the transportation system [22]. CAVs use different devices such as cameras as sensors, lidar and radar to perceive the surroundings [23]. The driving control within CAVs is regulated by one of the six levels of automation ranging from 0-5 [24]. Table 1 shows the six levels of automation. The exact architecture of CAV is under study; however, numerous reference architectures have been proposed in the literature [25-27]. The general components that collectively form integral elements of CAVs are as follows:

3.1. Wireless Communication

CAVs need to be equipped with different antennas in order to be capable of communicating using wireless protocols. In vehicle-to-vehicle (V-V) communications, a different set of communication technologies are utilised by both the driver and underlined roadside infrastructure. There are three major communication categories within CAVs as found in the literature [28]: Vehicle-to-Vehicles (V-V), Vehicle-to-Infrastructure (V2I) and the cloud. V-V Communication ensures that different CAVs communicate in more or less peer-to-peer style and uses IEEE 802.11 protocol for it [28]. V2I provides communication with the electronic devices that are monitoring and controlling the surroundings [29]. V2I communication also includes internal communication among different components of a CAV.

3.2. Engine Control Unit (ECU)

Internal communication among different components of CAV is also required. The internal communication system connects different components to implement different functions [26]. Modern vehicles use ECU to control the functionality of the vehicles. The acquisition, processing, and control of the electronic signals [28] is done through Controller Area Network (CAN)buses and and FlexRay [30] to ensure distributed real-time control [28],

3.3. Sensors and Cameras

CAVs are equipped with sensors and cameras to detect, collect information from the surroundings, categorise them in some predetermined criteria, and make predictions related to vehicle activity accordingly [28]. Sensors to measure inertial units, engine control, tyre pressure monitoring system (TPMS), light detecting and ranging (LiDAR), GPS, cameras and infrared systems[28] are common examples.

The connection mechanisms within CAVs support communication between infrastructure and vehicles in order to share data such as speed, position etc. [31]. In return, every connectivity function supports automation that transforms the role of driver from driver to monitor by reassigning the functions to a vehicle that were previously performed by human actor [28]. This automation is achieved using sensor technology to surveying the surroundings with pre-determined or learned knowledge to perform/plan vehicle activity [32].

Table 1. Six Levels of Vehicle

Title 1	Title 2	Title 3
0	Human/Manual driving	Manually controlled vehicles.
1	Driver Assistance	Single automated system for driver assistance such as cruise control while other aspects of driving are controlled by humans such as braking and steering.
2	Partial Driving Automation	A vehicle can control accelerating and steering, but the driver has to sit at a driving seat and take control of the vehicle.
3	Conditional Driving Automation	Hence, vehicles have environmental detection capability to make informed decisions, such as accelerating past a slow vehicle, but a human driver is still required. The driver needs to remain alert and take control of the vehicle if it is not able to perform the task.
4	High Driving Automation	Vehicles can drive in self-driving mode but within a limited area, and humans still can manually drive them.
5	Full Driving Automation	Vehicles are driverless. They do nothave a brake, accelerate and steering wheel and hence are known as fully automated.

4. CAVs Security and Privacy

CAVs are going to become a reality in the coming future, and there has been an increasing number of research studies being conducted on the behaviour and security of the CAVs. It is quite acceptable that with the arrival or invention of any new technology, there are potential threats and vulnerabilities attached to it, and the same goes for CAVs. A certain amount of hesitation from the public has also been observed to accept the notion of self-driving cars after few accident reports in Arizona and California in the United States [33-34]. Due to these accident reports and cyberattacks on inter as well as intra-vehicular communications, the security and privacy of passengers havebecome an important area of research [35].

5. Security and Privacy Solutions using Blockchain Technology

With the appearance of fully automated vehicles and the intellectualisation of vehicles, it is evident that society in general and vehicles, in particular, will face new challenges and threats [36]. There would be development in repair, maintenance methods besides devising new technologies for logistics [37] besides ensuring new methods and technologies to ensure safety and privacy of CAVs.Blockchain is a secure technology to store users' private information. Blockchain is a reliable distributed ledger to store transactions, and most commonly, it has been used in bitcoin transactions [37]. Blockchain is the chain of data blocks, the more the volume of data is growing, the moreblocks are being added to the chain. The blocks are written to the Blockchain in linear-sequential chronological order [37]. Every node is characterised as a computer within the blockchain network used by a client who checks and transfers the transactions [37]. So every node stores the copy of the Blockchain and is automatically downloaded when some miner joins the network.

Though researchers have played their role in integrating blockchain technology in different areas within Internet-of-Things (IoT), minimal research has been observed in literature when blockchain Blockchain provides security and privacy CAVs. This section highlights the contribution of literature towards providing security and privacy for CAVs using Blockchain. Every IoT device providing information about vehicles registers itself on the blockchain network, and information about vehicles is also stored on the Blockchain network [60]. Blockchain is used to track vehicles' actions by sending parameters of the current state of every vehicle using signals of neighbouring vehicles [36]. Novel automotive security architecture based on Blockchain has been proposed by using changeable private keys [38]. An open platform for the exchange of messages has been proposed between driver and service provider using Blockchain [39].

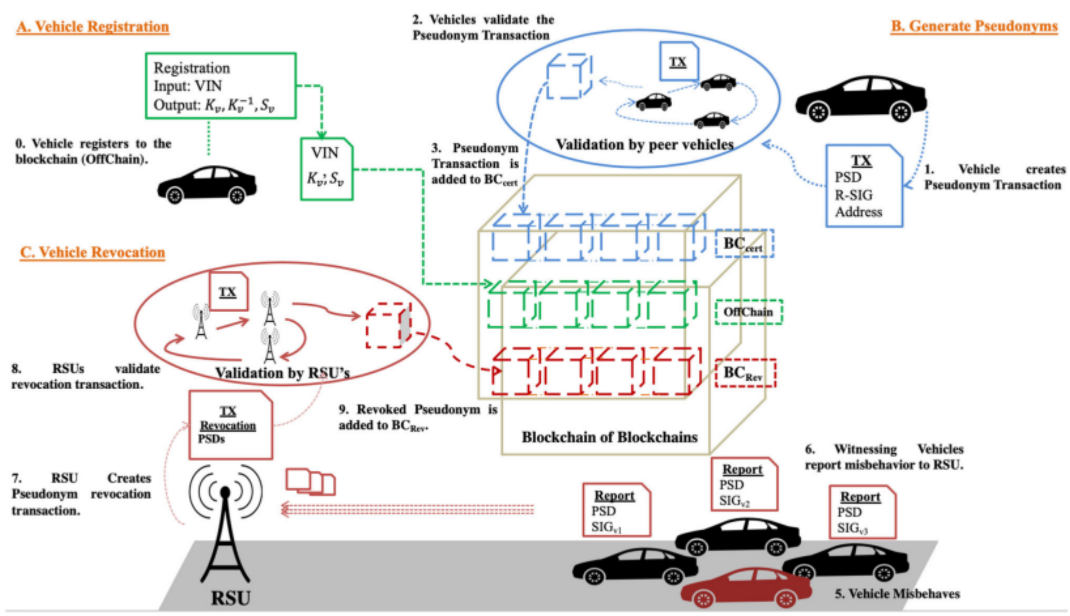

Figure 1. Blockchain-Based Pseudonym Management as proposed in [41]

Pseudonym generation has been an issue in Public Key Infrastructure (PKI), and vehicular networks rely on PKI. Pseudonyms are used by vehicles to sign their messages that ensure the message's integrity and help in the authentication of the sender. The pseudonym generation technique has been introduced by [41] stored in Blockchain to ensure privacy and maintain the vehicular network's security. Figure 1 shows the complete mechanism of the proposed system. The proposed system utilisesthreedifferent Blockchains, a decentralised mechanism of self pseudonym generation by vehicles instead of relying on centralised Certificate Issuing Authority (CA) and uses ring signature algorithm for vehicle certification. The proposed system is successful in providing security and ensuring privacy within the vehicular network as it has been assessed against the traditional VPKI for the probability of occurrence of different types of attack vectors using the following mathematical model:

$$Po = w(U(x) + U(y) + U(z))$$

$$U(f) = Cf / f, \text{ where } Cf = 0.2.$$

The proposed architecture successfully ensures secuirty and privacy through Blockchain. But the cost to implement the above architecture is expensive as opposed to traditional CA. Ring

Signature Algorithm is quite time consuming In a situation where vehicles are increasing rapidly requiring quick request/transaction processing, relying on ring signatures may be quite expensive and risky. Though vehicles have been given the flexibility of generating their own pseudonyms as opposed to VPKI where pseudonyms were used to be generated by CA still, vehicles need to rely on some centralised body to register themselvesand to get a secret key, so the proposed system is not totally decentralised. Since the secret key is being generated by some registration body that also means one point failure if the registration body goes compromised, the secret key of any vehicle can be either hacked or changed, which will ultimately change the one-time address of the sender that has been calculated in the proposed system by *H* (*Kv*, *Sv*, *htx*), where H is the Hash function taking parameters K_v (public key of the vehicle), S_v (secret key of the vehicle) and h_{tx} (hash of transaction). This makes it difficult for the vehicle to get certified by neighbouring vehicles and hence become part of the architecture.

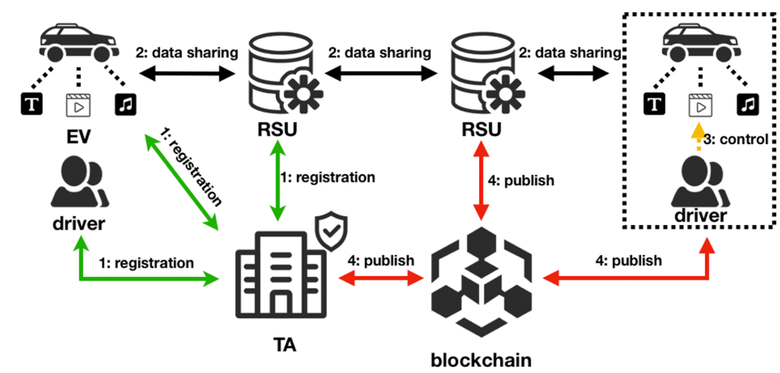

Figure 2: System Architecture for Blockchain-Based Multimedia Data sharing in VSNs as Proposed in [42]

Vehicles can develop social relationships within vehicular networks, also known as Vehicular Social Networks (VSNs). VSNs bring security challenges when vehicles try to send/receive multimedia data. It may be possible that the privacy of vehicles and users get leaked, and attackers may analyse their communication habits besides tampering with the multimedia data. A privacy-preserving scheme has been proposed in [42] which is based on Blockchain for multimedia sharing within VSNs. The proposed system used cryptographical primitives such as pseudonyms to hide the identities of vehicles, users and RSUs. Trusted Authority has been used by [42] to verify the user, vehicle and Road Side Unit (RSU). TA authority uses pseudo-random function F to generate unique identities of users and RSUs, key generation algorithms to generate keys (public and private keys) for the users and the RSUs and generates hash chain H for both users and RSUs for authentication purposes. RSUs uses a signature algorithm to sign the transaction and a verification algorithm to verify the messages sent by users. TA stores the user, vehicle and RSU information on Blockchain along with a time stamp duly signed by TA as a transaction. The multimedia data sharing can be either peer-to-peer or broadcasting to the network. For sending peer-to-peer multimedia data, the user gets authenticated to RSU by sending its hash value verified by RSU by retrieving hash associated with the user from the Blockchain. After a connection is established between user and RSU, the user then sends multimedia data to RSU, which is in the format of {*m*, *uIDs*, *uIDr*, *hm*, *σs* } where m represents a message, uID_s represents sender id, uID_r represents receiver id, *hm* represents a hash of the multimedia message, and *σs* represents a signature of a user over message within defined time stamp. RSU calculates the hash of the message to verify if the received multimedia data has not been tempered and obtains the user's public key from blockchain Blockchain to verify the signature to ensure itis a valid sender. RSU stores this information as a transaction on blockchain and the format of the data sharing transaction is *(uIDs ||uIDr ||type||hm||σs ||t)||SignRSUi)* duly signed by RSU. Here type shows either the data sharing is peer-to-peer or broadcasting to the whole network, so if it is peer-to-peer data sharing, the type is set to 0. RSU then sends {*m*, *uIDs*, *uIDr*, *hm*,

σs } to receiver. Similar activity is performed when data is intended to be broadcasted in which the type is set to 1.

The proposed system [42] claims to help in privacy protection, reliability and integrity of the messages, traceability of the malicious user. The proposed system has been evaluated for experimental results, and it has been observed that the proposed system assumes the trustworthiness of TA, which is highly risky in a situation where almost every entity can be under attack. That means if the proposed system verifies the integrity of users, vehicles, and multimedia data, it must have to verify TA's integrity and authenticity. If the TA is under attack, all the data stored on it and the transactions it creates can become malicious, which can spoil the whole blockchain network. It has also been observed from the simulated results of the study that the user, vehicle and RSU initialisation is taking quite a lot of computational cost in terms of time, and the time goes on increasing if the number of users and vehicles are getting added to the network. Secondly, the multimedia data transferred from user to RSU is again quite costly, whichrequires a high computational cost on the part of RSU by running signature and verification algorithms which seem to be time-consuming. The overall delay in information processing at different stages of the proposed system can be a bottleneck in the realisation of the system. The paper does notprovide any comparative study that can prove its effectiveness against any known attack vector compared to the current system to validate its effectiveness in multimedia data sharing within VSNs.

The traditional architecture of VANET heavily relies on centralised trusted authorises for managing vehicular information, while data processing is also done on centralised servers. The centralised entities are not completely credible, as if once attacked, it can bring severe security and privacy threats. A novel decentralised Blockchain-based VANET architecture has been proposed in [43] that successfully tackles distrust among users, vehicles and RSUs and centralisation in VANET. For protecting identity and location privacy, the proposed architecture introduced dynamic threshold encryption and k-anonymity unity. The architecture of the proposed system is shown in figure 3.

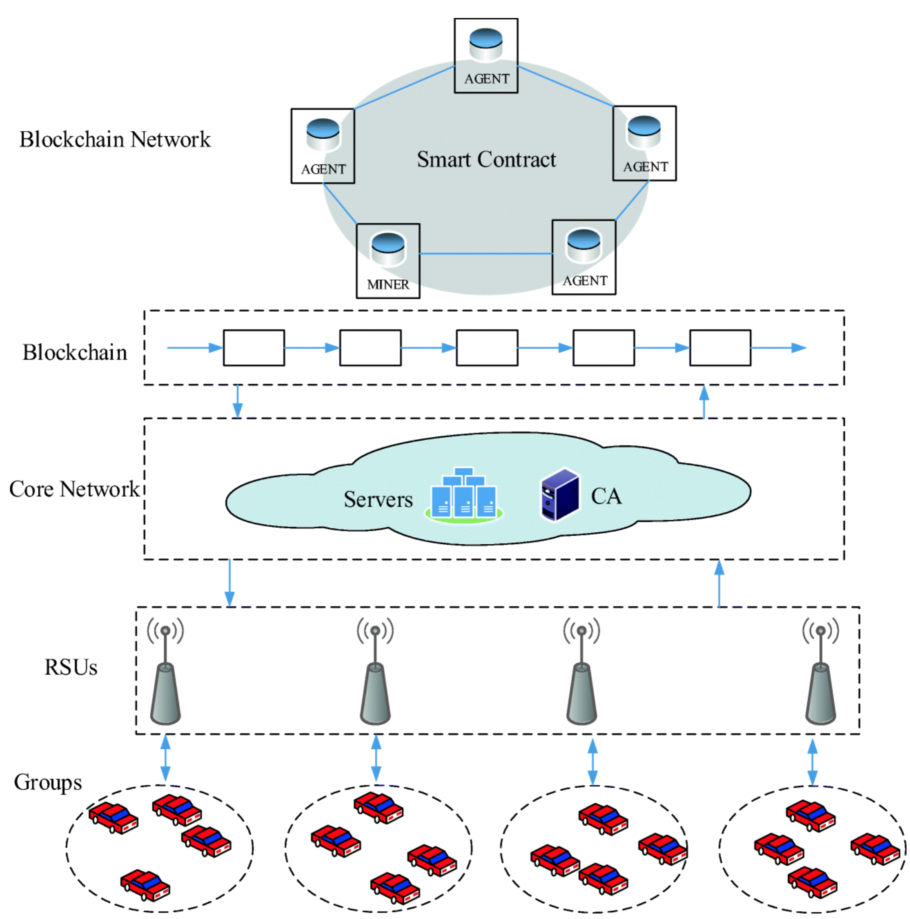

Figure 3: Decentralised Architecture and Interaction as proposed in [43]

The proposed system uses dynamic threshold encryption and k-anonymity unity to achieve identity and location privacy protection. The vehicle needs to construct the m-1 degree polynomial using formula: $f(x) = s+a1x+ a_2x^2 +\ldots+ a_ix^i +\ldots+ a_{m-1}\, x^{m-1}$; $a_i \in GF(q)$ and calculates sub-secrets in form (m, r) that shows m sub-secrets of r vehicles. The threshold is kept on updating ata specified time so that no attacker at any point intime can collect m secrets to identifying a vehicle. For location privacy, k-anonymity unit algorithm in which a vehicle uploads its SBM with k-1 other vehicles' SBMs. In order to preventall vehicles in a group to upload the same message, the k-anonymity unit algorithm has been modified to take two indicators to ensure the effectiveness of the unit algorithm. One of the two indicators is Connectivity∆ which develops an undirected graph between vehicles in a group;the connectivity can be measured by $\Delta = num.(V)/n \geq k/n$. The second indicator is Average Distance D. For location privacy;the k-anonymity unit will not be valid if the vehicles in a group are in the same location or adjacent. So the larger the average distance would be among vehicles in a unit, the better can be the effect of the location privacy k-anonymity unit. The proposed system has been evaluated against centralised and distributed architectures proving effective against them in terms of identity privacy with the use of m sub-identities within a limited time while the use of k-anonymity unit ensures location protection. The proposed system claims that no two vehicles in a group can have the same location. Neither can be adjacent, as the more the distance between the vehicles is, the harder it is to identify the exact location of a specific vehicle within a group. After analysing the proposed system, it has been observed that k-anonymity unit algorithm though is effective in hiding the identities of vehicles by generating m sub-identities of a single-vehicle but again, it is hard to compute sub-identities using m-1 polynomial through dynamic threshold encryption. With the increasing number of vehicles joining VANET, it is going to put the burden on low powered user devices to compute sub-identities. This can overall increase the processing time of the proposed system besides delays in transaction creation, and SBM processing since an SBM consists of messages from multiple vehicles and responding to different vehicles in a specified amount of time can add to the processing time of the proposed system. Appendix Table A2 shows a detailed analysis of the literature on the security and privacy of CAVs using Blockchain.

6. Findings

Cyberspace is an open platform for attackers, increasing the type and amount of cyber-attacks, which reduces the surveillance of security measures. Countless -attacks are initiated within no time, further reducing the security and privacy measures already in place. Since the expansion of CPS is inevitable because CPS applications in different domains are evident, reliance on CPS is undeniable. But the more free data movement is ensured, the more threat penetrating the CPS for data travel, data storage, individuals holding data, and even complete organizations organisations may come under severe cyber threats. With the invention of the Internet, there have been tremendous efforts in providing and scaling the security and privacy measures to the data. Wireless sensor networks had made the communication more rapid along with introducing more attack vectors on the data, the communication mechanism and the devices responsible for the transmission/receiving of data. Traditional security and privacy measures provided for the protection of data and communication mechanisms are mainly developed against the attacks introduced due to the wireless sensor networks. After studying the literature, it has been observed that the majority of the security and privacy measures rely heavily on techniques proposed for the wireless sensor networks. They are not as effective as they should be since CPS is widening the stage for the cyberattacks, and accordingly attack vector is getting broadened. Traditional security and privacy measures become less effective and least efficient in handling attack vectors posed by the CPS. Hence, it is important to put forth efforts in formulating defence strategies that can effectively manage cyber attacks when it comes to CPS.

The applications of CPS in different domains have been discussed in this paper. It is quite evident that CPS is providing numerous benefits, especially within the medical domain, making it more helpful for medical practitioners to supervise the medical conditions of patients. The more benefits can be imparted from the CPS, the more strong security and privacy measures need to be in place to prevent data loss, life loss, data communication deterioration and data storage sabotage. New attack vectors posed by CPS require new and more strong security measures to handle them, and reliance on traditional security and privacy measures need to be reduced. This survey paper targets one application of CPS, which is connected and autonomous vehicles and investigated the security and privacy measures proposed in the literature for them. After analysing the literature, most of the literature on security and privacy for the CAVs still relies on traditional security and privacy measures, which were mainly proposed for the wireless sensor networks. Still, the focus of this survey is Blockchain technology being a new and promising technology to provide security and privacy for the CAVs. So it investigated the literature to analyse the use of Blockchain for providing security and privacy for the CAVs. In that case, traditional encryption techniques are also more prevalent.

The main intention of this survey was to give an overview of the recent trends in security and privacy for CAVs using Blockchain technology and perform their performance evaluation in terms of the shortcomings in the proposed mechanisms. This survey also presented the different types of attacks and vulnerabilities for the security and privacy of CAVs. It is further encouraged that the research for security and privacy of CAVs using Blockchain should be further investigated in order to develop simpler, lightweight and scalable algorithms, and the simulation tools supporting those algorithms should be available free.

Driverless cars are the next generation invention, and they are highly vulnerable to security attacks. In fact, they present an open platform for cyber-attacks of different types, as presented in this survey paper. The more advances in the CAVs technology will happen, the more cyber attacks will be observed hence widening the scale for the attack vector. Though traditional security and privacy measures such as authentication, trust management, encryption and others are available solutions, they focus more on a centralised mechanism to provide security and may not effectively address the heterogeneity of the devices within CAVs. So new technologies and techniques need to be modularised, such as Blockchain,which has proven positive impacts in the virtual banking and e-commerce sector. The research on Blockchain regarding security and privacy for CAVs is yet in the infancy stage, and not many contributions are identified in the literature. Though Blockchain has been investigated to be used as a means for communication,and sharing of information over IoT and CPS for CAVs, the efforts are still required. It is time to harness the benefits of Blockchain for the security and privacy of CAVs, but it is encouraging to notice that research is being directed towards exploring new technologies in this direction.

The findings from this survey indicate that though Blockchain is a new technology for providing decentralised security and privacy mechanism for CAVs. However,the algorithms formulated over Blockchain are still old and heavy-weight,consuminga lot of computational power. It is also interesting to mention here that computational work has not been provided, which can help assess the computational speed of the proposed mechanism and help researchers improve on them in the future.

7. Conclusion

In this paper, we exhaustively investigated the current research trends in security and privacy of CAVs during 2016-2020 using Blockchain.The paper also investigated attack vectors and vulnerabilities for CAVs. This paper only analysed Blockchain as the main security and privacy mechanisms. It is further added that Blockchain provides a decentralised data storage mechanism researchers have used that for record-keeping in different studies. But it is equally important here to mention that Blockchain has not been relied upon independently as a sole secure means of communication. The majority of the literature we investigated during this survey has shown to be heavily dependent on traditional security measures such as trusted third party authorities, pseudonym and key generation algorithms that still bring inefficiencies and delays in providing timely secure communication. The need is to move away from the traditional security and trusted third party techniques and deploy new security algorithms over Blockchain,which are lightweight in their performance and efficient enough to ensure secure communication.

Though Blockchain technology is also considered a means of providing security and privacy within CAVs as observed in the literature, it is not investigated independently as standalone security and privacy parameter. Traditional encryption algorithms are being run on Blockchain, which further multiplies the computational energy consumed by the Blockchain network and ultimately, the solution may not be as effective as it should be. Traditional encryption algorithms are quite heavy-weight, which requires heavy computational energy and takes a lot of time in calculating the results. Suppose traditional algorithms are tied up with Blockchain. In that case, it will maximise the computational energy and time required to generate the results as Blockchain itself utilises quite a lot of energy in mining and authenticating data on blocks. It is suggested that future security and privacy measures for CAVs be designed around new encryption techniques over Blockchain, which is light enough to reduce the overall computational energy and time consumed. By doing so, the new world of CPS will be ready to face new challenges and threats posed due to cyber attacks.

The need is to harvest the Blockchain technology eliminating or reducing the bottlenecks which it brings along, such as the heavy computational energy required for calculating results. The future is connected and autonomous vehicles requiring tight security and privacy measures in place, which cannot be achieved using traditional security techniques alone. Therefore, we need a bit strong – perhaps more effort have to be placed on further examining the efficacy of decentralised security operations facilitated by Blockchain and design innovative security and privacy algorithms that are smart enough to cater for the needs and demands of CAVs. The world is going to witness fully autonomous vehicles very soon, and with this realisation, we need to be also ready for new attack vectors to pave their way through cyber attacks. Broadening the scale of action for new security and privacy measures can help highlight indicators, targetting, manage, handle, and mitigate the novel cyberattack vectors weaponising CAVs.

References

[1] N. Kim, S. Rathore, J. Ryu, J. Park and J. Park, "A Survey on Cyber Physical System Security for IoT: Issues, Challenges, Threats, Solutions", *Journal of Information Processing Systems*, 2018, vol. 14, no. 6, pp. 1361-1384, Available: https://doi.org/10.3745/JIPS.03.0105. [Accessed 17 August 2020].

[2] Mackintosh, M.; Epiphaniou, G.; Al-Khateeb, H.; Burnham, K.; Pillai, P.; Hammoudeh, M. Preliminaries of Orthogonal Layered Defence Using Functional and Assurance Controls in Industrial Control Systems. *J. Sens. Actuator Netw.* **2019**, *8*, 14. https://doi.org/10.3390/jsan8010014

[3] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET", *IEEE Journal on Selected Areas in Communications*, 2007, vol. 25, no. 8, pp. 1569-1589, Available: 10.1109/jsac.2007.071007.

[4] M. Mohamad Noor and W. Hassan, "Current research on Internet of Things (IoT) security: A survey", *Computer Networks*, 2019, vol. 148, pp. 283-294, Available: 10.1016/j.comnet.2018.11.025.

[5] A. Silva and M. Vuran, "(CPS)^2: integration of center pivot systems with wireless underground sensor networks for autonomous precision agriculture", in *1st ACM/IEEE International Conference on Cyber-Physical Systems*, Stockholm, 2010, pp. 79-88.

[6] F. Mehdipour, "Smart Field Monitoring: An Application of Cyber-Physical Systems in Agriculture", in *2014 IIAI 3rd International Conference on Advanced Applied Informatics*, Kitakyushu, Japan, 2014, pp. 181-184.

[7] S. Caramihai and I. Dumitrache, "Agricultural Enterprise as a Complex System: A Cyber Physical Systems Approach", in *20th International Conference on Control Systems and Computer Science*, Bucharest, Romania, 2015, pp. 659-664.

[8] Y. Li, M. Jacob, G. Akingba and J. Wachs, "A Cyber-Physical Management System for Delivering and Monitoring Surgical Instruments in the OR", *Surgical Innovation*, 2012, vol. 20, no. 4, pp. 377-384, Available: 10.1177/1553350612459109.

[9] D. Dogaru and I. Dumitrache, "Cyber-physical systems in healthcare networks", in *E-Health and Bioengineering Conference (EHB)*, Iasi, Romania, 2015, pp. 1-4.

[10] C. Lei, H. Liang and K. Man, "Building a smart laboratory environment at a university via a cyber-physical system", in *Proceedings of 2013 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*, Bali, Indonesia, 2013, pp. 243-247.

[11] J. Wan, H. Yan, D. Li, K. Zhou and L. Zeng, "Cyber-Physical Systems for Optimal Energy Management Scheme of Autonomous Electric Vehicle", *The Computer Journal*, 2013, vol. 56, no. 8, pp. 947-956, Available: 10.1093/comjnl/bxt043.

[12] S. Jianjun, W. Xu, G. Jizhen and C. Yangzhou, "The Analysis of Traffic Control Cyber-physical Systems", *Procedia - Social and Behavioral Sciences*, 2013, vol. 96, pp. 2487-2496, Available: 10.1016/j.sbspro.2013.08.278.

[13] H. Singh, "Big data, industry 4.0 and cyber-physical systems integration: A smart industry context", *Materials Today: Proceedings*, 2020. Available: 10.1016/j.matpr.2020.07.170.

[14] M. Dibaei et al., "Attacks and defences on intelligent connected vehicles: a survey", *Digital Communications and Networks*, 2020. Available: 10.1016/j.dcan.2020.04.007.

[15] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges", *IEEE Transactions on Intelligent Transportation Systems*, 2017, vol. 18, no. 11, pp. 2898-2915, Available: 10.1109/tits.2017.2665968.

[16] T. Lu, J. Lin, L. Zhao, Y. Li and Y. Peng, "A Security Architecture in Cyber-Physical Systems: Security Theories, Analysis, Simulation and Application Fields", *International Journal of Security and Its Applications*, 2015, vol. 9, no. 7, pp. 1-16, Available: 10.14257/ijsia.2015.9.7.01.

[17] R. Khan, S. Khan and R. Zaheer, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges", in *10th International Conference on Frontiers of Information Technology*, Islamabad, Pakistan, 2012, pp. 257-260.

[18] M. Noor and W. Hassan, "Current research on Internet of Things (IoT) security: A survey", *Computer Networks*, 2019, vol. 148, pp. 283-294, [Accessed 20 August 2020].

[19] M. Aly, F. Khomh, M. Haoues, A. Quintero and S. Yacout, "Enforcing security in Internet of Things frameworks: A Systematic Literature Review", *Internet of Things*, 2019, vol. 6, p. 100050, Available: 10.1016/j.iot.2019.100050.

[20] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures", in *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015, pp. 336-341.

[21] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo and F. Xie, "Cyber-physical System Risk Assessment", in *Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Beijing, China, 2013, pp. 442-447.

[22] R. Krueger, T. Rashidi and J. Rose, "Preferences for shared autonomous vehicles", *Transportation Research Part C: Emerging Technologies*, 2016, vol. 69, pp. 343-355, Available: 10.1016/j.trc.2016.06.015.

[23] P. Bansal and K. Kockelman, "Are we ready to embrace connected and self-driving vehicles? A case study of Texans", *Transportation*, 2016, vol. 45, no. 2, pp. 641-675, Available: 10.1007/s11116-016-9745-z.

[24] J. Guanetti, Y. Kim and F. Borrelli, "Control of connected and automated vehicles: State of the art and future challenges", *Annual Reviews in Control*, 2018, vol. 45, pp. 18-40, Available: 10.1016/j.arcontrol.2018.04.011.

[25] D. Elliott, W. Keen and L. Miao, "Recent advances in connected and automated vehicles", *Journal of Traffic and Transportation Engineering (English Edition)*, 2019, vol. 6, no. 2, pp. 109-131, Available: 10.1016/j.jtte.2018.09.005.

[26] F. Munir, S. Azam, M. Hussain, A. Sheri and M. Jeon, "Autonomous Vehicle: The Architecture Aspect of Self Driving Car", in *2018 International Conference on Sensors, Signal and Image Processing (SSIP 2018)*, Prague Czech Republic, 2018, pp. 1-5.

[27] C. Maple, M. Bradbury, A. Le and K. Ghirardello, "A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis", *Applied Sciences*, 2019, vol. 9, no. 23, p. 5101, Available: 10.3390/app9235101.

[28] M. Lio, A. Plebe, D. Bortoluzzi, G. Papini and R. Don`a, "Autonomous Vehicle Architecture Inspired by the Neurocognition of Human Driving", in *4th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2018)*, Funchal, Madeira, Portugal, 2018, pp. 507-513.

[29] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges", *IEEE Transactions on Intelligent Transportation Systems*, 2017, vol. 18, no. 11, pp. 2898-2915, Available: 10.1109/tits.2017.2665968.

[30] C. Liu and F. Luo, "FlexRay Protocol Controller Conformance Test Implementation", *International Journal of Computer and Electrical Engineering*, 2016, vol. 8, no. 3, pp. 250-258, Available: 10.17706/ijcee.2016.8.3.250-258.

[31] S. Banerjee and D. Harekal, "Vehicle Control in Vehicle to Infrastructure (V2I) Environment", *International Journal of Computer Applications*, 2017, vol. 164, no. 8, pp. 25-30, Available: 10.5120/ijca2017913714.

[32] N. Lu, N. Cheng, N. Zhang, X. Shen and J. Mark, "Connected Vehicles: Solutions and Challenges", *IEEE Internet of Things Journal*, 2014, vol. 1, no. 4, pp. 289-299, Available: 10.1109/jiot.2014.2327587.

[33] L. Jing, "Research on Autonomous Capability Evaluation of Unmanned Ground Vehicles", *Science Discovery*, 2016, vol. 4, no. 1, p. 12, Available: 10.11648/j.sd.20160401.13.

[34] J. Stewart, "Tesla's Self-Driving Autopilot Involved in Another Deadly Crash", *Wired*, 2020. [Online]. Available: https://www.wired.com/story/tesla-autopilot-self-driving-crash-california/. [Accessed: 22- Aug- 2020].

[35] A. Davies, "The Unavoidable Folly of Making Humans Train Self-Driving Cars", *Wired*, 2020. [Online]. Available: https://www.wired.com/story/uber-crash-arizona-human-train-self-driving-cars/. [Accessed: 22- Aug- 2020].

[36] M. Dibaei et al., "Attacks and defences on intelligent connected vehicles: a survey", *Digital Communications and Networks*, 2020. Available: 10.1016/j.dcan.2020.04.007.

[37] S. Narbayeva, T. Bakibayev, K. Abeshev, I. Makarova, K. Shubenkova and A. Pashkevich, "Blockchain Technology on the Way of Autonomous Vehicles Development", *Transportation Research Procedia*, 202, vol. 44, pp. 168-175, Available: 10.1016/j.trpro.2020.02.024.

[38] O. Stopka, "Approach technique of specifying a proper autonomous cart type for its service in the logistics center", *The Archives of Automotive Engineering – Archiwum Motoryzacji*, 2019, vol. 84, no. 2, pp. 23-31, Available: 10.14669/AM.VOL84.ART2. [Accessed 23 August 2020].

[39] A. Dorri, M. Steger, S. Kanhere and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", *IEEE Communications Magazine*, 2017, vol. 55, no. 12, pp. 119-125, Available: 10.1109/mcom.2017.1700879.

[40] C. Kaiser et al., "Towards a Privacy-Preserving Way of Vehicle Data Sharing – A Case for Blockchain Technology?", in *Advanced Microsystems for Automotive Applications 2018 Smart Systems for Clean, Safe and Shared Road Vehicles*, Switzerland: Springer, 2018, pp. 111-122.

[41] L. Benarous, B. Kadri and A. Bouridane, "Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Networks", *Arabian Journal for Science and Engineering*, 2020, vol. 45, no. 8, pp. 6033-6049, Available: 10.1007/s13369-020-04448-z.

[42] K. Shi, L. Zhu, C. Zhang, L. Xu and F. Gao, "Blockchain-based multimedia sharing in vehicular social networks with privacy protection", *Multimedia Tools and Applications*, 2020, vol. 79, no. 11-12, pp. 8085-8105, Available: 10.1007/s11042-019-08284-8.

[43] H. Li, L. Pei, D. Liao, G. Sun and D. Xu, "Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET", *Peer-to-Peer Networking and Applications*, 2019, vol. 12, no. 5, pp. 1178-1193, Available: 10.1007/s12083-019-00786-4.

[44] A. Davies, "The Unavoidable Folly of Making Humans Train Self-Driving Cars", *Wired*, 2020. [Online]. Available: https://www.wired.com/story/uber-crash-arizona-human-train-self-driving-cars/. [Accessed: 22- Aug- 2020].

[45] M. Dibaei et al., "Attacks and defences on intelligent connected vehicles: a survey", *Digital Communications and Networks*, 2020. Available: 10.1016/j.dcan.2020.04.007.

[46] R. Currie, "The CAN Bus: Basic Manipulation of a Modern Automobile through CAN Bus Reverse Engineering", SANS Institute, North Bethesda, MD, USA, 2017.

[47] L. Wang and J. Kangasharju, "Measuring large-scale distributed systems: case of BitTorrent Mainline DHT", in *IEEE P2P 2013 Proceedings*, Trento, Italy, 2013, pp. 1-10.

[48] O. Puñal, A. Aguiar and J. Gross, "In VANETs We Trust? Characterising RF Jamming in Vehicular Networks", in *Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications, (VANET '12)*, Low Wood Bay, Lake District, UK, 2012, pp. 83-92.

[50] J. Tobin, C. Thorpe and L. Murphy, "An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks", in *IEEE 85th Vehicular Technology Conference (VTC Spring)*, Sydney, NSW, Australia, 2017, pp. 1-6

[51] S. Mitra, B. Jana and J. Poray, "A novel scheme to detect and remove black hole attack in cognitive radio vehicular ad hoc networks (CR-VANETs)", in *International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, Kolkata, India, 2016, pp. 1-5.

[52] S. Raj, D. Midhunchakkaravarthy and D. Bhattacharyya, "Security Issues and Various Attacks in Wireless Sensor Network: A Survey", *International Journal of Security and Its Applications*, 2019, vol. 13, no. 3, pp. 9-16, Available: 10.33832/ijsia.2019.13.3.02.

[53] P. Syverson, "A taxonomy of replay attacks [cryptographic protocols]", in *Proceedings The Computer Security Foundations Workshop VII*, Franconia, NH, USA, USA, 1994, pp. 187-191.
[54] P. Wang, X. Wu and X. He, "Modeling and analysing cyberattack effects on connected automated vehicular platoons", *Transportation Research Part C: Emerging Technologies*, 2020, vol. 115, p. 102625, Available: 10.1016/j.trc.2020.102625.
[55] M. Rahbari and M. Jabreil Jamali, "Efficient Detection of Sybil attack Based on Cryptography in Vanet", *International Journal of Network Security & Its Applications*, 2011, vol. 3, no. 6, pp. 185-195, Available: 10.5121/ijnsa.2011.3614.
[56] A. Singh and A. Jain, "Study of Cyber Attacks on Cyber-Physical System", in *3rd International Conference on Advances in Internet of Things and Connected Technologies (ICIoTCT) 2018*, Jaipur, India, 2018, pp. 686-690.
[57] J. Cui, L. Liew, G. Sabaliauskaite and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles", *Ad Hoc Networks*,2019, vol. 90, p. 101823, Available: 10.1016/j.adhoc.2018.12.006.
[58] S. Narbayeva, T. Bakibayev, K. Abeshev, I. Makarova, K. Shubenkova and A. Pashkevich, "Blockchain Technology on the Way of Autonomous Vehicles Development", *Transportation Research Procedia*, 202, vol. 44, pp. 168-175, Available: 10.1016/j.trpro.2020.02.024.
[60] Rathee, Sharma, Iqbal, Aloqaily, Jaglan and Kumar, "A Blockchain Framework for Securing Connected and Autonomous Vehicles", *Sensors*, 2019, vol. 19, no. 14, p. 3165, Available: 10.3390/s19143165.
[61] A. Dorri, M. Steger, S. Kanhere and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", *IEEE Communications Magazine*, 2017, vol. 55, no. 12, pp. 119-125, Available: 10.1109/mcom.2017.1700879.
[62] C. Kaiser et al., "Towards a Privacy-Preserving Way of Vehicle Data Sharing – A Case for Blockchain Technology?", in *Advanced Microsystems for Automotive Applications 2018 Smart Systems for Clean, Safe and Shared Road Vehicles*, Switzerland: Springer, 2018, pp. 111-122.
[63] M. Salem, M. Mohammed and A. Rodan, "Security Approach for In-Vehicle Networking Using Blockchain Technology", in *Advances in Internet, Data and Web Technologies. EIDWT 2019. Lecture Notes on Data Engineering and Communications Technologies*, 29th ed., Barolli L., Xhafa F., Khan Z. and Odhabi H., Ed. Springer, 2019, pp. 504-515.
[64] K. Lei et al., "Blockchain-Based Cache Poisoning Security Protection and Privacy-Aware Access Control in NDN Vehicular Edge Computing Networks", *Journal of Grid Computing*, 2020, vol. 18, no. 4, pp. 593-613, Available: 10.1007/s10723-020-09531-1.
[65] K. Shi, L. Zhu, C. Zhang, L. Xu and F. Gao, "Blockchain-based multimedia sharing in vehicular social networks with privacy protection", *Multimedia Tools and Applications*, 2020, vol. 79, no. 11-12, pp. 8085-8105, Available: 10.1007/s11042-019-08284-8.
[66] L. Benarous, B. Kadri and A. Bouridane, "Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Networks", *Arabian Journal for Science and Engineering*, 2020, vol. 45, no. 8, pp. 6033-6049, Available: 10.1007/s13369-020-04448-z.
[67] H. Li, L. Pei, D. Liao, G. Sun and D. Xu, "Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET", *Peer-to-Peer Networking and Applications*, 2019, vol. 12, no. 5, pp. 1178-1193, Available: 10.1007/s12083-019-00786-4.
[68]. Abbas, G., Mehmood, A., Carsten, M., Epiphaniou, G. and Lloret, J., 2022. Safety, Security and Privacy in Machine Learning Based Internet of Things. Journal of Sensor and Actuator Networks, 11(3), p.38.
[69]. Hassan, Z., Mehmood, A., Maple, C., Khan, M.A. and Aldegheishem, A., 2020. Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles. IEEE Access, 8, pp.199618-199628.
[70]. Khan, K., Mehmood, A., Khan, S., Khan, M.A., Iqbal, Z. and Mashwani, W.K., 2020. A survey on intrusion detection and prevention in wireless ad-hoc networks. Journal of Systems Architecture, 105, p.101701.

Appendix

Table A1: List Showing Attack Vector and Objectives

Ref.	Attack Category	Attack Name	Objectives
[26][49]	Wireless Communication	• EaVes Drop • MiTM intercept • Location, identity theft • Relay attacks	Compromise the devices that forward packets and the mechanism packets are forwarded
[44][45][48]	DoS Attacks	• DDoS • Targeting Harware Security Module (HSM) • Radio Jamming • Targeting V2X Communication • Flooding	Overloading host with huge amount of information to comprise its data processing, receiving and transmitting capability
[26][46]	Attacks on Ports	• Damaging CAN bus • Electrical damages	To gain access to internal CAN bus

		• Installing malicious software	
[45][50][51]	Black-hole Attacks	• Packets dropping • Grey-hole Attacks	Dropping packets between vehicle and infrastructure to hinder Communication
[26][52]	Attacks on Sensors	• Spoofing • Relaying • Delay • Blind • Jamming • Tamper • Node outage • Eavesdropping • DoS	Causing vehicle to take incorrect decision
[45][53]	Replay Attacks	• Man-in-the-Middle • Delayed • Repeated • Denning-Saco	Delaying or repeating of valid transmitted data
[45][54]	Impersonation Attacks	• Masquerade	Misleading other vehicles as legitimate member to send malicious information to target vehicles
[45][47][54][55]	Sybil Attacks	• Spoofing	Forging multiple identities to mislead vehicles and to create system chaos
[45][56]	Malware Attacks	• Phishing • Bluejacking • Bots • Pharming	Causing harm to host
[45][57]	Timing & Falsified Attacks		Delaying Transmission of packets and sending false information about surroundings

TableA2: Current Research on Security and Privacy of CAVs using Blockchain

Ref	Types of Attacks being Handled	Security Objective	Advantages	Disadvantage	Simulator/ computation/analysis tools
[60]	• Jamming • Falsification Attack • Impersonation Attacks • Man-in-the-Middle Attack	Secure Communication	Provides security of riders and drivers by constantly monitoring the sensors	Huge number of vehicles increases the computational complexity	NS2
[58]	• Traffic offences • Accidents • Impersonation Attacks	Secure Communication	ECDSA algorithm is used which is fastest cryptographic algorithm	• Size of encrypted messages increase by ECDSA • ECDSA is more complex and difficult to implement hence implementation errors may increase which may reduce the security feature of the algorithm	Exonum
[61]	• Linking Attacks • Malware • Falsified Attacks • DDoS	Secure Communication	• Optimisedfor large scale low resource networks • Distributed trust algorithm to reduce the processing time connected with every validating blocks	• A vehicle may have numerous changeable private keys during its lifetime increasing burden on relay nodes • Asymmetric encryption is used which is slower and time consuming technique	Not Available

[62]	• Impersonation Attacks • Falsified Attacks • Attacks on Ports	Secure Communication	vehicle may not need to share entire dataset	• Complete privacy is not guaranteed	Not Available
[63]	• Attack on internal communication (in-vehicular communication)	Secure Communication and data protection between ECUs	• Reducing processing time • Authentication	• Centralisedblockchain network	NXP Microcontroller
[64]	• Content poisoning attacks on packets to isolate user's access to authentic content	Avoiding unauthorised access to the copes of content cached on intermediate nodes	• Delegate Consensus Algorithm • Protection of data packets	• Traditional Symmetric encryption takes time in processing/verification of two keys	ndnSIM Platform, NS-3, Corei5-6500, 3.2GHz & 8GB RAM
[65]	• Attack on multimedia	Privacy preserving	• Blockchain to ensure reliable data source and keep attackers from tempering multimedia data	• Rely on Trusted Authority (TA) for identity registration & key distribution for Electric Vehicle, user and RSU • Assumption TA is trustworthy	MacBook Pro, 2.3GHz, Corei5 processor & 8GB 2133MHz LPDDR3 Memory
[66, 68]	• Random packets injection • Impersonation attacks • DDoS	Secure communication, preserving privacy	• DecentralisedKPI using Blockchain • Self Pseudonyms generation by vehicles	• Public and private key generation/verification techniques are time consuming • Conditional privacy	Not Available
[67-70]	• Impersonation attacks • Sybil attacks	Identity and Location Privacy	• Decentralisedarchitecture using Consortium Blockchain • No reliance on Centralized Authority (CA) • Multiple sub-identities for vehicles	• K-Anonymity Unit is NP hard • Processing time enhances if more vehicles are added to VANET	OPNET & Ethereum