Secure Communication Protocols for Vehicle-to-Vehicle Communication in Autonomous Vehicles

By Dr. Ekaterina Vybornova

Professor of Artificial Intelligence, ITMO University, Russia

1. Introduction

The evaluation findings show that the proposed autonomous communication system for vehicles is capable for vehicular communication. Through the use of encrypted signatures, the system can protect against attacks and guarantee a safe and genuine exchange of messages between two self-driving cars. [1]

Vehicle-to-Vehicle (V2V) communication is considered an essential technology for autonomous vehicles (AVs). It has demonstrated potential to enhance safety, improve the efficiency of vehicles on roads and reduce traffic congestion at the intersections. This technology has significantly impact the road transport industry. However, security attacks can happen in AVs when attackers disturb the communication system to attempt to get control of the vehicles and cause a range of issues including system instability, reducing the safety of the transportation system and disrupting the communications between vehicles. Therefore, the V2V communication system needs to have a suitably secure communication protocol that uses authentication and encryption methods to thwart eavesdropping and manipulating messages by an adversary .

1.1. Background and Motivation

Using blockchain to secure inter-vehicle communications can enhance the trust and safety among interconnected vehicles in the vehicular communication environment. The concept explores the potential for transmission security and enforces trust about the identity and location of the neighboring car [2]. Furthermore, the identities of communicating vehicles are shielded, rendering it nearly unattainable for an adversary to monitor the vehicles' interactions, all because of a hybrid secure-key agreement protocol that establishes protected, mutual secret keys based on physical layer attributes. This all rounds up into the blockchain

of physical security as trusted side channel TLS (SwElLS), incorporated into the visible light communication scheme + ultrasonic acoustics for safer inter-connected vehicles.

Security in communication systems is crucial, particularly for vehicle-to-vehicle (V2V) communication in autonomous vehicles, due to ever-increasing concerns over the vulnerability of electronic systems to cyber-attacks [3]. When designing secure communication techniques in V2V network, not only the communication medium to be employed, but also the protocol and the authentication mechanism play a significant role in the overall communication arrangement. The V2V industry is expected to grow by 300% in the next decade, attracting investments around $20 billion by the end of 2020, predicted to go up even more in autonomous vehicles [4]. To ensure authenticity and confidentiality in data transfer between vehicles, the proposed concept aims to take advantage of IP V2V in 6G network, I2V of vehicle-to-infrastructure (V2I) protocols in the 5G and IEEE 802.11p-based protocol dealing with V2V in connected vehicles.

1.2. Scope and Objectives

Different perspectives of the literature review taken are based on the security mechanisms implemented in physical, access, network, and the application layer. [1] introduced secure V2V communications to protect vehicle-to-vehicle communication from potential attackers by forming security clusters based on the vehicular secrecy capacity. The base station/cluster head calculates the secrecy capacity and broadcasts the cluster information. All member vehicles of the security cluster would identify the received security cluster information and executed the intra cluster handoff process to setup common secrecy key. Aware of vehicles located within the communication range of IoT devices can be protected from attackers in IoT environments.

The focus of this research is on developing a secure communication protocol for vehicle-to-vehicle communication in autonomous vehicles. A detailed literature review was conducted to obtain information on secure vehicular communications. [2] discussed a secure communication protocol for vehicle-to-vehicle communication through visible light with second channel acoustics for location and identity verification. It proposed a handshake protocol for the establishment of keys in TLS 1.2, and the existence of asynchronous error detection and non-reputation through attacks is also considered. [5] considered six security requirements, including availability, integrity, confidentiality, authentication, non-

repudiation, and traceability for vehicle ad-hoc network (VANET) communications after a detailed literature review.

2. Fundamentals of Vehicle-to-Vehicle Communication

Cars are increasingly equipped with advanced driver-assistance systems (ADAS) and automated driving capabilities. One of the strengths of V2V communication is to transfer information between Smart Cars belonging to different communication protocols, i.e., those belonging to the same V2X system or to different IoT systems such as device-to-device (D2D, or machine-to-machine M2M) and people-to-device (P2D) at any time. In case of necessary highway or urban traffic reorganization because of potential or real hazards or incidents, V2V communication is performing the negotiation of a common change of itinerary, speed or position of each Smart Car, proposing changes of lane, urban parking space, or length of works to all cars, including those having very different descriptions of the surroundings because of different vCAS versions, car generations, or even theoretical model year [6].

More and more devices and machines around us are interconnected, and among them, vehicles are generating considerable interest. Connected cars are often cited as an emblematic application of the internet of things (IoT) and contribute to the global discussion on the deployment and ethical aspects of autonomous and automated vehicles. The use of intelligent transportation systems is foreseen to lead to accident reductions by 35%. Considering that 93% of the causes of car crashes are due to human errors, the major part of these improvements is expected to result from a globally more reliable infrastructure and consistent vehicles performing better than the unconnected, semi-automated or manually driven ones. In Gauteng, South Africa alone, the financial cost of traffic congestion reached $793 million in 2011, providing strong motivations for improvements in transportation infrastructure V2V communication is expected to significantly decrease the rate of accidents, avoiding incidents related to prior known irrational behavior of the vehicle ahead or its driver.

2.1. Overview of V2V Communication Technologies

Nearly all vehicle manufacturer using Intra Vehicle Networking (IVN) and V2V/V1V communication for creating better distribution, interspatial communications, and collision avoidance. Automated vehicle manufacturers are adapting Intelligent Transportation System (ITS) communication standards for V2V communication [7]. Europe Smart Infrastructure (ITS-G5), Japan smart Infrastructure (C2X), and China smart infrastructure (C-V2X) are working

on V2X communication standards, for that multiple organizations are planning intelligent transportation systems (ITSs). Europe has ETSI-ITS-G5 and Automotive Industry Association (V2I-Vehicle to Infrastructure) communication as dedicated short-range communication (DSRC). China working on 0th generation (LTE-V) and 1th generation (PC5-V) vehicle communication standards.

In autonomous vehicles, monitoring the driver assistance systems or the entire environment of the vehicle is not enough to ensure safety and efficiency [8]. For automated driving, communication and driving behavior cooperation (CC) play a crucial role. Vehicle connectivity and communication, including V2V communication, is essential to enable efficient and realistic cooperative communication systems for V2V, V2X (Vehicle to Infrastructure) or V2X communication [3]. In particular, detailed observations and communications between vehicles are essential and preliminary for understanding complex traffic conditions, gaining information about traffic jam dynamics, road speeds or accident spread, dynamic jam-registering and avoiding effects, planning route, and proactive operation.

2.2. Key Components and Architecture

Vehicular communications are designed to support the exchange of information among all the entities and components that are installed in a vehicle. According to [9], vehicular networks (or Internet of Vehicles) enable various services such as traffic information, riding sharing, and electric vehicle (EV) authentication. Several federal agencies in the US have initiated projects to develop secure protocols for vehicular communication that are based on wireless communication like Dedicated Short Range Communications (DSRC) and cellular communication. In the existing DSRC protocol, Clear Algorithm 0 allows short-range communication between a vehicle-to-vehicle communication, while Clear Algorithm 1 is used for vehicle-to-infrastructure communication. In General, DSRC bases on public key infrastructure and wireless channel as the key generation and distribution infrastructure, respectively. This is a module that can be located onboard or off board, which corresponds to the security module in our architecture model for DS2 (DS-to-DS) and SD (Signal D). To protect the privacy and security of vehicle-to-everything communication, authentication schemes for vehicular networks are being researched. As earlier mentioned, vehicular networks are part of the Internet of Things, and security and privacy are the main challenges

in these networks. The main architectures proposed for enhancing the security of vehicular communication are based on the intelligent transport system. So, a secure internet of sensing things is defined as the security enhancement mechanism for an IoT-based vehicular communication system. Compare with the current vehicular communication standard, Long-Term Evolution (LTE) for V2V communication, the computer-based used unique smart message interface for data transfer between the car and the sensory device in 3GPP is a new standard through V2V communication system design to ensure that environmental sensing devices are aware of their respective information and queries, which is a replacement for the information and queries that are sent using V2V. Therefore, many mechanisms will be defined in this model for ensuring security, privacy, and availability @kindly send the data.

3. Security Challenges in V2V Communication

The security threats in V2V communications are manyfold, including attacks on the integrity of the communication, such as jamming and unauthorized messages, fake message injection, and privacy concerns due to contact tracking and location discovery through long-term observation and interference of the link reception. Thus, designing secure V2V communication protocols is crucial. [10]

Secure vehicle-to-everything (V2X) communication is crucial for future autonomous vehicles. A trust model for secure 5G-based V2X communication is designed, providing the two main players in a smart city, the vehicles (VSUs) and the road side units (RSUs), with the ability to assess the trustworthiness of each other [11]. [12]

3.1. Threats and Vulnerabilities

The developers, manufacturers, vehicle owners, and law enforcement personnel can leverage the mitigation approaches proposed. The contributions are two-fold: 1). We propose reinforcing the multi-factor authentication (MFA) leveraging a user's mobile device ownership to verify the identities, as suggested in the sharing group. 2). We comment the remote attestation is not always required. Additionally, the ego-vehicle is planned to keep a collection of shared secrets to authenticate other group members and verify the integrity and behaviors of the autonomous vehicle and machine-to-machine (M2M) interfaces [13]. However, appropriate material for the safe data sharing become additional challenge particularly when remnant time reduced after each clearance delay, since the ego-vehicle has to take the traffic situation into account. Thus, we provide insights into the relevance of the

shared secrets stored in the ego-vehicle considering the traffic situation and offer main ideas concerning the probable services that M2M communication, such as immediate accident clearance or proper accident site access, can deliver by sharing data between cooperative vehicles and infrastructure persuasion (IVIS) services.

In order to understand what type of secure communication protocols are most useful for autonomous vehicles (AVs), one has to first understand possible threats and vulnerabilities the vehicle has to deal with. The majority of security attacks can be categorized as ECU-targeted attacks, software-targeted attacks, or network-targeted attacks [10]. The ECU-targeted attacks are typically reverse engineering-based attacks, offline replay attacks, or Denial-of-Service (DoS) attacks. The traffic external interfaces that result from the compromised ECUs and have dynamic traffic will be described in an attacked model. The software targeted attacks mainly target the encryption, authentication, and permission verification mechanisms in most cases, while the network targeted attacks aim at the fact that messages acquired from the compromised external interfaces of the traffic will be sent to the directions with different numbers of hops, different outgoing buers, different link widths or channels in the physical electro-magnetic wave spectrum corresponding to the original traffic.

3.2. Authentication and Authorization Mechanisms

Most of the harmful security attacks happen at roadside terminals in VANET infrastructure. Therefore, RoutrTable contains only registered trusted Roadside Unit (R-SU) or MD-PC. The RoutrTable and identified solution could constitute one kind of the table in a tabular matrix with entries. StationaryVNE B As considered in A mode, the VIN is considered as a regular piece of information at the time of VIN transmission & reception. B mode is divided into two situations for the elimination feature. By default "all entries in EK (except one) in a certificate" are suspended in the first case, and the station's certificate is created certainly compiled in the list of the Federal-approved vehicle recognition attributes or unapproved and non-safe vehicles in the absence of the Club-vin VIN. Use a theory where the VIN is particularly stored in a distinct key storage unit to prevent the secured vehicles from being used by more than one authentication key. The software and hardware bright Room (Sha), Vehicular Tough Excel (VTE), Fuzzy way (IEEE1619554), Cough Guard Method (ISO 151184) are integrated with a high difficulty of the Corporation Certification Authority (EVCA) as well as the description descriptions in the cases of their security [4].

Transmission Control Protocol (TCP) and Internet Protocol (IP) and Hyper Text Transfer Protocol Secure (HTTPS) are some of the identification purposes of an autonomous vehicle. In the domain of V2V put forward the RESCUE MANET Authentication Protocol (RMAP) to use the temporal identifiers, and the proposed mechanism is considered stronger than the ones in the existing work [14]. The US Federal- Information Processing Standards (FIPS), which is termed as FIPS 1964 and FIPS 140-2/3, is used for the hardware encryption block model of the apex organizations. FIPS 140-2/3 is used for the encryption Organizational Security Level (OSL) 3/4 cryptographic modules to support secure communication requirements in selected numbers of hardware blocks inside an autonomous vehicle and at phase mitigation phase Data Link Layer (DLL) at communications wall becomes used by using the IPsec security protocol in a session key. IPsec is the family of the suite for the IP network and protocol for the Internet. The key exchange protocols of IPsec are used in Autonomous Vehicle-to-Autonomous Vehicle communications, which include Transport Layer Security (TLS) with a secure need for minimal overhead. In Table 11, the types of security mechanism overhead are taken improvement possible are conducted in each security mechanism and its limitations are proposed [15].

4. Existing Communication Protocols in V2V Systems

Vehicular communication is a prominent subclass of wireless ad hoc network communications, extracted from VANETs and is a subclass of Mobile ad hoc network (MANET). In addition, the reliability of the data communicated and latency also determine the adoption of the V2V communications. As a result, the cars or any other vehicles are made to communicate amongst them through V2V communications. As discussed in Section 3.1, there are quite a few promising security techniques to analyse in detail, in order to assess the security level they would offer in V2V communication [16]. With the latest discovery of The kernel Layered JN % is an latest, secured key exchange protocol witch guarantees sevral critical requirements including forward secrecy, traceability, traceable authenticity ,immunity to off-line dictionary attacks etc. KLJN seamlessly integrates a variety of protection mechanisms, with time-based message identity, geographic location, equipment edition, network communication policy, and re-key technique. The contrast security assessment outcomes among multiple protocol performances are elaborated with particular end to end and systemic protections.

V2V, V2I, and V2RSD communications enable vehicles to alert oncoming vehicles when a critical event occurs, help optimize traffic networks, and provide road service vehicle drivers with relevant information. As a result, the security of V2V communication is of considerable importance. VANET standards have been documented by the IEEE 802.11 working group, and both standardized and non-standardized layers have been widely reported in the literature. Lu et al. proposed SLA, an adaptive eavesdropping detection algorithm for V2V communication in vehicular networks based on IEEE 802.11p [17]. Moreover, a modified IEEE 802.11p MAC protocol for scalable V2V communications (also known as IEEE 802.11 s) was proposed by Rodríguez-Molina et al. However, advances in the applications of wireless communication technologies (as well as battery technology and embedded systems), an advancement in VLSI (Very Large Scale Integration), the development of sustainable motor vehicles, and the concomitant global movement toward autonomous vehicles for Intelligent Transport Systems have led to increasing attention on the security of connected vehicle technology.

4.1. IEEE 802.11p (DSRC)

Authors of [18] proposed a new usage priority of each group (RSUs, vehicles, and CAVs). In fact, by determining each vehicle's communication priority, all vehicles would share the DSRC links more efficiently. The main contribution of this paper is an adaptive communication protocol for RSUs, vehicles, and CAVs in vehicular networking where the environment is in high-density vehicular. The main idea behind this contribution is to enhance the vehicle's message priority in the sets of vehicle-to-vehicle messages, vehicle-to-roadside messages, and vehicle-to-CAV messages so that the higher danger level have higher priority in the set of the previous messages so that the probability of packet loss in the situation of packet collision, packet overhearing, and dark spot environment be minimized. Also, by using the proposed vehicular aggregation, the number of vehicles that successfully share the DSRC communication link can be increased.

[ref: 50717b73-6d4c-4e27-87b7-ed37a603a997, 8913ef40-105f-40f3-b280-3bcbc878f0c6] IEEE 802.11p, in the Dedicated Short-Range Communications (DSRC) frequency band (5.850 – 5.925 GHz), has been selected by standard agencies as the recommended communication standard for V2X applications [19]. However, this standard has several limitations including its low data rate, communication glitches in high density, dark space, fast changing topologies, and

high mobility environments. A helpful comparison between the aforementioned features is shown in Table 2. Many V2X communication protocols have been recently proposed in the literature to cope with such limitations of the IEEE 802.11p standard.

4.2. Cellular V2X (C-V2X)

C-V2X offers a solution for the safety reception problem concerning cornering and non-line-of-sight conditions, which cannot be solved by 4G and 4.5G DSRC standards because 5G frequency bands can bend around the road-barrier corner and thereby reach terminals behind corners and blocked Line-of- Sight (LOS) links. At drivetime, although numerous vehicles share categories of V2X information, the vehicles cani) track previously known (pre-existing hidden) other vehicles with time-consuming Channel State Information (CSI) based Channel Estimation-Equalization and Detection over time-varying CIR, ii) As new moving hidden terminals and time-varying CIR introduce uncertainty at transmitter and receiver, vehicles need to recursively learn the moving wireless channel parameters on the fly based on new CSI (Veh's Aur) based periodic Barely-Perfec t Recursive Least Squares (pBPLRS) method, iii) recurrently decode hybrid-CSI-based AER channels and iv) repeatedly predict estimator (also called outcome) 's status as Hidden at frame-level CSI merging and at symbol-level Result Merge and Latency-Maximizing Decision Making (RMLMDMAE) stages.

Studies on fifth-generation networks are enabling smart factories, the smart grid, the Smart "Village/City", civil infrastructures, smart transportation, autonomous vehicles, smart agriculture, and wind turbines, among others [20]. Consequently, increasing numbers of industries are becoming involved in telecommunications, requiring flexible, adaptable, cost-saving, low-latency, highly secure, private, efficient, and reliable networking systems. Autonomous vehicles are being used in smart, safe, clean, and efficient Future Urban Mobility (FUM), which is widely recognized across the world today as a key application requiring third-generation partnership project (3GPP) fifth-generation network technology (5G) communication system units (C-V2X). C-V2X is expected to provide a dominant part in C-V2X and Vehicle-to-Everything (V2X) industries given the significant cooperation between global mobile telecommunications system alliance (GMLC) and 3GPP and the compatibility, backward compatibility, and the full spectrum utilization needed for ensuring faster and seamless V2X communication [21].

5. Requirements for Secure V2V Communication Protocols

1. Privacy: Ensuring that vehicles' corresponding anonymous data is secure and cannot be traced. 2. Lightweight: Unlike V2I communication, a large number of calculations are required for evaluating the forwarding set, and as a result, extensive message encryption and decryption will be required. This will translate into a large computational overhead that will in the long run adversely affect battery life and operational overhead. 3. Safety: Security concerns extend beyond just integrity, authentication and confidentiality. The integrity of the messages received is important because subsequently decisions must be made based on the messages received. Authenticating other VAs should prevent any security issues like the Man-in-the-Middle attack. Confidentiality is concerned with preserving the sensitive data while being conveyed between the VAs [4]. With lightweight communicating security concerns can be diluted easily if a low amount of overhead and resource is required. To make the VANET system work smoothly, its operational characteristics must not be negatively affected by the security measures employed. 4. Fast and scalable: For robust stream processing, a very low level of latency should be maintained to enable success in the given context. All the VAs will maintain GPS data locally and as a result, quick decisions could be taken. This will also make the network robust in terms of taking quick corrective actions. Reducing this process to reduce latency with both human-driven and autonomous vehicles context is a challenging task. Since a vast amount of VAs could be communicated, the scheme should be scalable. The achievable throughput and latency are major performance metrics in VANET communication.

Communication in vehicular ad-hoc networks (VANETs) comes with its own set of challenges since, among other things, data emanating from the vehicles participating in these networks is vulnerable [22]. These systems must exchange various sensitive data in real time, and thus, the provi-sion of robust security for VANETs is essential. To address this issue, numerous secure communication protocols for V2V communication have been proposed in literature [23]. However, a secure V2V communication protocol suitable for autonomous vehicles must meet several critical requirements in order to function efficiently. Four of these important requirements are outlined below.

5.1. Privacy Preservation

Additionally, to realize secure movement for the operations of autonomous vehicles connected to the internet, the 5th Generation of mobile networks (5G) has not only

transformed the way of living and working but also drastically changed the living of individuals in terms of shaping additional privacy and safety security risks. As a result, satisfying the conflicting goals of internet security and privacy has become a key challenge. The vehicles exchanged significant security information as the autonomous vehicles needed secure privacy and safety from their related communications-based data. However, due to powerful attackers such as quantum computers, enhancing security in V2V has recently become challenging [1]. Therefore, this study is carried out to achieve an autonomous vehicle theoretical privacy architecture by defining a sustainable privacy analysis and energy-efficient secure communication standards for the future autonomous driving for whom the execution of the most organized testing sequence will be effectively controlled.

Security is a crucial aspect for implementing V2V communications in the communication system of autonomous vehicles. Security serves the main purpose for privacy preservation for wireless communication [ref: 7bd1daba-978d-4570-8ee6-cf9f5d264d37, 81982e0d-32ee-4a73-bf2c-d0f63fb7c62e]. To study the physical-layer secrecy analysis and design of the certificate authority based secure communication protocols, we consider a single-input single-output (SISO) vehicular communications system as shown in Figure 5. With the help of the random query process, the intrusion of quantum computers is allowed to restrict the most common security assumption. The discussion of secure movement is also discussed in the literature but there is no such work available which considers the specific security analysis of the communication system of autonomous vehicles especially affected by the quantum safe proposals with feasible privacy specifications, i.e., characteristic vehicular communication delay with flexible communication query model selection along with physical-layer secret key capacity as objectives. Furthermore, just in compliance with the uncorrelated Rayleigh fading channel, channel state information at the receiver (CSIR) has been used to predict the closed-form movable secrecy inferences of the system.

5.2. Data Integrity and Authenticity

Due to the sensitivity of CAV operations, collision prevention, tracking of traffic congestion through data collection, vehicle control, and maintenance of weather condition, researchers need to maintain the inherently resilient V2X communication system of vehicles [14]. For securing CAV communication, data integrity needs to be established in V2X communication, which is essential for assuring the receipt of legitimate information that has not been tampered

by other parties. With the ability to assure the authenticity of the data, the availability of V2X can be enhanced. PV2X (pseudo V2X), performed in a simulation environment, is recorded for Assuring Deterministic Authenticated Safety Environment Security (ADVITERS).

Encryption and key generation form the key subjects under discussion in the section. By implementing encryption software in communication between vehicles, the origin, integrity and freshness of the messages can be safeguarded [24]. Approaches for message integrity and authenticity verification use a hash algorithm, which is deployed at the transmitter side for creating a signature on plaintext and a verification method for detecting changes in transmitted data [25]. The HMAC (Hash-based Message Authentication Code) algorithm produces keys, which create a digest message for maintaining integrity; moreover, SHA-256 utilizes block cipher design along with encryption.

6. Proposed Secure Communication Protocols

In this section, several secure communication protocols are proposed, which are based on the authentication and key establishment mechanism. The communication protocol requires the user autonomy and with no need for the priori knowledge construction. Therefore, the information should be encrypted during the communication, i.e., establishing a secure and confidentiality communication process. Public key infrastructure (PKI) and bilinear pairing authentication mechanism have been exploited previously [26]. To optimize it for IoV AoVs, a LevCrypto algorithm is designed [27]. Later, a series of operations can be made so that the connection between the user of the AoV (input and direct user) and the communication between the AoVs and the SAP can be confidential. The SLCP uses the pairing protocol to implement the secure communication protocol. The improved protocol can maintain a high degree of confidentiality, resistance to direct and indirect communication between AoVs and SAP. And it can also achieve the perfect forward confidentiality and resistance to direct and indirect communication attacks. The weightings of different security attributes in the attribute set will evolve with changes in the situation. In this way, SLCP meets the requirements of IoV architecture and also adapts to the high intensity ad-hoc authentication mode formed by the characteristics of autonomous driving.Mobile communication technologies have made great strides over the past few years in terms of capability, performance and capacity, and now form a ubiquitous part of day-to-day life. Future generations of automotive communication systems are likely to include direct vehicle-to-vehicle (V2V) communication systems, possibly

supported by a central access point (CAP) as part of an intelligent transport system (ITS) infrastructure. However, all the protocols and algorithms are established in the IoV domain without the consideration of security and it is insecure communication for autonomous vehicles. The given schemes in the article have been established to build secure communication protocol for V2V communication inside IoV AoV. The threat model is established, which indicates the possible threat types in the autonomous driving, and the proposed IoV SSP, SLCP and MLCP schemes attempt to prevent aforementioned threats.

6.1. Hybrid Cryptographic Protocols

Efficient key management strategies are an important part of hybrid cryptographic protocols, as vehicular communication experiences high dynamics in mobility and node density. In, the researchers proposed a novel hybrid system for key agreement, which is a blend of the elliptic curve digital signature algorithm and the secure symmetric key encryption of lightweight block ciphers. The Curtail_Cy Ontana_LightAuth provides a hybrid cryptographic protocol with efficient communicated time and secured information and privacy [28].

Security is paramount in the world of autonomous vehicles, and the security of vehicular communication should be given particular attention. In addition to the security protocols described in [3.1], the role of hybrid cryptographic protocols has been crucial in achieving secure communication in autonomous vehicles. There are a few leading research works and articles that have dealt individually and categorically with cryptographic protocols. In fact, applying hybrid cryptographic protocols that combine the advantages of symmetric and asymmetric key algorithms have been observed to have low communication and computational overheads [29] In GURLP, the Merkle tree relies on symmetric key primitives called pseudorandom functions, and the signed pseudorandom functions are used for digital signature operations [2020.22225]. Secure key distribution by exchanging keys and a lower overhead parameter exchange between vehicles have been observed to have a significant effect on identity privacy [15].

6.2. Blockchain-based Solutions

Blockchains are mainly widely used to verify the integrity of transaction data in embedded systems, cellular telecommunications and vehicle-to-everything (V2X) communication [30]. A blockchain can store all transactions' hash as a block and a special block called a ledged can be appended to the blockchain at regular intervals that contains the hashes of all transactions.

Furthermore, a blockchain can provide a tamper-proof way of providing a distributed transaction ledger and achieve a consensus protocol. In the automotive field, two widely used blockchain consensus algorithms have been suggested, permission-less and permissioned blockchain algorithms.

Blockchain technology is one of the best candidates for developing intelligent and secure systems. Recent work has addressed the potential use of blockchain combined with IoT networks and networks formed by autonomous vehicles [31]. There are some existing efforts to use blockchain for blockchain based VANET with different aims [32] such as cryptographic vehicular networks, secure and privacy-preserving data sharing, efficient payment systems, privacy-preserving decentralized ride-hailing system, resilient blockchain-based authentication framework, secure message dissemination in blockchains, and incentive enforcement mechanisms. Additionally, possible challenges, which could limit the performance of blockchains when applied for VANETs, are discussed and solutions are proposed to address these challenges in this work.

7. Performance Evaluation and Comparison

In each communication protocol, we present a comparison of the network-stack profiles, general input/output, expected protocol behavior, differential protocol behavior, legitimate security service, security requirements with direct effect, positive impact security service relationship, and overall association with security service. Each protocol uses mostly 802.11p with slight modifications. Based on our evaluation, we conclude that the SAE J2735 standard communication protocol is fit for exchanging GPS and other position information between the vehicle antennas, but it has serious security vulnerabilities, which if exploited, can bring catastrophic crashes leading to fatalities. The situation can be improved using the ITU-T X.800 series or IEEE 1609 security standards; however, IEEE 1609 needs to be modified significantly in order to control denial-of-service, theft of service, and spoofing attacks, which can otherwise lead to crunched roads and an imbalanced traffic load ratio [1].

Vehicular communication with vehicles in close proximity is an essential component of intelligent transport systems (ITS). Communication protocols at the physical and data link layers need to be compatible. For safe and secure communication, a compromise needs to be maintained between data integrity, privacy, accountability, and real-time transmission. Each protocol must have support for vehicle traffic safety services (VTSS), applications in

automotive, cellular vehicular segments for intelligent traffic management, urban safety services, overtaking, road condition services, communication with roadside units (RSU) critical situation detection, and also timer resolutions for different applications [7].To solve these issues, this work presents a critical comparison of secure and efficient communication protocols operating at the data link layer of the ISO/OSI model.

7.1. Security Metrics and Criteria

1. Security Percentages. The performance of VANETs is estimated using security percentages, especially in terms of throughput, normal working time, and delay, which ultimately improve the packet delivery ratio of secure messages. Essentially, it measures the accuracy of the security schemes for preventing the intrusion or severe delay in transmitting secure packets through the network. Higher security percentages give better throughput, less latency, and optimum network capability. 2. Computational Complexity. This metric measures the efficiency of security schemes during message communication for preserving the cyber-physical system. It shows the low latency for message delivery, avoid congestion, enhances network stability, saves energy, and gives higher total throughput for broadcast and unicast communication [27]. Mostly, the Computation Complexity is a key criterion to estimate the security effectiveness of efficient vehicular communication over the VANETs. 3. Throughput and Traffic Flow. Due to security constraints, several existing routing protocols for VANETs have significant probability of extra delay in bi-directional and complex network architectures. It is important to estimate the extra packet delay to meet the privacy and security requirements of data transmission among vehicular population. A high message transmittal percentage is required from the roadside infrastructure to the vehicles and the security is optimized to ensure vehicle security. It gives insight to the route optimization and congestion avoidance of user vehicular input-output system. 4. Message Overhead. Message overhead is measured by the cost of managing the broadcast secure vehicle communication in the network. The effective vehicle communication for secure data movement over the network is measured through message overhead. It is a performance metric for authenticity and integrity of secure communication [5]. However, the overhead of message increases with the increasing number of instances. This provides computation of the additional parameters in measuring the overhead of secure packet traffic in the outsourced cloud model.

There are different methods of security schemes defined in the literature for the establishment of secure communication among vehicles in VANETs. The logical choice of a security algorithm depends upon the security metrics and criteria to achieve a secure communication in the distributed network [30]. The major classification of security metrics and criteria used to estimate the effectiveness of security schemes for VANETs are summarised as follows:

7.2. Case Studies and Simulation Results

Adversary attacks like maintaining road obstructions and curbing visibility includes environmental attacks and insider attacks whereas hiding road objects through passive and active attacks. Object smartly provide rogue coordination and evading road front devices authorities. Adversary first trick one or more RSUs and may forge a shadow (fake) image on the sensor data to hide the traffic obstacles that lead to a potential car accident. Our protocol detects this kind of forgery attack that adversarial abuse the tolerance limits of sensors and untrusterted node. The vehicle intelligently uses the technology named simulation and enables detection of the attack with approximation technique. It also securely performs a sensor verification with physical checking of the distance. Therefore, system detects vehicles which work as an authority may defect adversarial detection and unable to dodge when fairness of security nodes attack [33].

Security is a major concern for the continuous viability of autonomous and connected vehicle. Regular, hack resilient cryptographic security protocols are vital. There are many secure communication protocols available for V2X communications and they all have some unique properties that make them different from others. For example, IEEE 1609.2 standard is heavily used for VANET. Certificates for authentication are used in this protocol. These certificates are provided by certificate authority. The security goals include authentication by the CA (certificate authority) of the V2X certificate issued to the vehicle, and privacy with plausible deniability. The protocol is computationally secure, which ensures that secure V2X messages can be verified only by the senders themselves and can be convinced as genuine and correct V2X messages when verified by anyone else. Privacy respecting the anonymous communication of the vehicles and the drivers is the central requirement to protect the individual's private data in the already registered V2X security certificates [4].

8. Implementation and Deployment Considerations

Increasingly, traditional and countermeasure methods show limited abilities to safeguard the IoV systems. Challenges to these methods are relatively complex, there is a contradiction and confliction between the performance and security of networks, as well as the high energy consumption which is not suitable for resource-constrained devices [13]. Many improvements have been proposed, which make signals too complex for passive eavesdropping attacks. However, these methods are still facing challenges to provide strong security in IoV. Security is a crucial aspect of vehicular communications, public key scheme being the most commonly used approach. Other techniques such as group signature and symmetric authentication schemes are also used, but to a lesser extent. In this paper, we reviewed the V2X, I2X, and P2X communications and their applications. Our review hopefully illuminates the strength and weaknesses of existing communication technologies in the automotive industry, and assists in developing better future technologies.

One challenging aspect of implementing communication systems for cooperative driving in practice is testing the protocols and algorithms under real-world conditions [4]. Current IEEE 802.11p transponders are based on dedicated communication hardware and have interfaces to a vehicle's external bus system, the Controller Area Network (CAN). As a result, they usually do not have an operating system and the appropriate interfaces to directly run reinforcement learning strategies. On the communication level, most of the components have to guarantee the delivery of the sent 1-hop communication packet. WAICOM research and development activities are focused on vehicular network simulators, real-world vehicular deployments, and simulations of reinforcement learning strategies [6]. WAICOM team has worked on extending IEEE 802.11p with the 5G New Radio communication technology to demonstrate the ability to consider vehicle-to-vehicle connectivity for current and future cooperative driving use-cases.

8.1. Hardware and Software Requirements

2) Hardware Requirements The hardware requirements [5] specify the components, interfaces, and states of the hardware. Essentially, the output is the selection of electronic parts that meet the requirements for the implemented design. Here, the hardware requirements include the criteria for electronic parts that are used in the car. When evaluating vehicle components, it is important that vehicular communication systems are secure in order to help

prevent accidents or traffic congestion. For example, in V2V communication, vehicles communicate with each other in order to prevent and/or reduce the damage from accidents, such as rear-end or rotation accidents. In addition, V2V communication can minimize congestion during an emergency situation and contribute to improve traffic flow. In Vehicular Communication Systems, components consist of Vehicles, Roadside Devices (RSDs), and Certification Authorities (CAs). Vehicles are able to perform V2RSD communication, V2V communication, and Vehicle-to-Certification-Authority (V2CA) communication.

1) Automotive Requirements In terms of automotive requirements [3], the vehicle must be able to be transported, operated, and maintained. There are several requirements related to the safety, including the fact that the vehicle must be able to withstand a crash (up to a certain force) and be operable in a certain range of temperatures. The assessed design should not obstruct functions that are mandatory for roadworthy vehicles (e.g. environmental requirements like conditions for scratch resistance).

The requirements for the implemented design have been divided into two categories, namely, hardware and software. The hardware requirements include the criteria for electronic parts to be used in the car. The software requirements, on the other hand, define the capabilities of the software integration. The evaluation criteria are based on the automotive, hardware, and software industries. In particular, we consider the specific requirements of autonomous vehicles based on: emergency response system, real-time behavior, state of completeness, processor, and memory management [16].

8.2. Integration with Existing V2V Systems

The vehicles were equipped with two parallel eyes. The first one, the traditional one, is created in order to coexist with a number of different legacy-V2I systems, whereas the second single-source sender, together with single-source authentic-and- confict-conficted-as-well receiver, were connected with each other by using the Designated Verifier Signature (DVS) to reduce the transmissions over the inter-connections communication system [34]. A Tablet or Laptop can realize the inter-connections by using the binary long division with remainders. In other words, we do not need to build the infrastructure, as this will be able to do with the help of the Central Authentication Server from the HESH attributes space.

Currently, transportation infrastructure utilizes a completely separated vehicle-to-vehicle (V2V) communication system. Building an entirely new infrastructure to allow vehicles to

communicate with one another via V2V transmission may not be feasible, especially with autonomous vehicles gaining popularity on the road [6]. We propose the usage of an existing vehicle-to-infrastructure (V2I) communication system in our new divide-and-conquer secure V2V communication model [35] . The basic tenet consists of two devices, namely a weak and strong vehicle equipped with up-to-date legacy-V2I and CAV-V2V device, respectively. It is assumed that the legacy-V2I device may communicate tampered data to either vehicle. It is noteworthy to mention that the communication model may be expanded by considering a fleet of vehicles (more than two V2V devices).

9. Regulatory and Standardization Aspects

The rapid increase in the number of connected vehicles on the road means that the security of safety-critical applications becomes more crucial. The industry is promoting the standardization of automotive communication for automated driving. Nevertheless, V2X security remains a challenge as no standardized technique exists to guarantee the confidentiality and integrity of the transmitted data. In this article, we refer to specific V2X strategy within autonomous vehicles using the V2V communication as one of the key principle aspects in the field of vehicle safety relevant to the confidentiality and integrity of the transmitted data. However, completely secure communication protocols are not available for V2V scenarios but protected message data represent important requirements for highly secure V2V applications. Therefore, this article also focuses on the fundamental aspects necessary for generating secure communication protocols by using a standard integrated Public Key Infrastructure (PKI) having the goal to ensure data privacy and integrity in V2X communication within autonomous automobiles [36].

In recent years, the increase in vehicular networks has implications in telecommunication. Security is one of the major concerns in the field of vehicular networks, especially in the V2I communication mode. However, it is essential to address the security of V2V communication, i.e., where the vehicles are the communicating parties together with V2I. A literature review was conducted on V2V security in vehicular ad hoc networks to collect and provide authoritative sources using a systematic and scientific way to summarize current knowledge. A bibliographic database tool was used to search articles in journals and conference proceedings. Then, searches were executed by defined criteria to retrieve relevant papers. We have classified several types of attacks that threaten V2V communication, including attacks

targeting location, privacy, routing, trust, and security solutions, as well as evaluating these security solutions. The evaluation process includes simulation, testing, analysis, verification, and comparison of proposed security solutions [37]. A realistic view of the characteristics and limitations of V2V communication security is provided. The review would help researchers to get a clear view of authentic work conducted in the field of V2V communication security. The research contributions summarized in the paper provide opportunities for future research to work along the lines of integrating the proposed approaches of literature review to develop effective and potential security solutions for V2V communication security in VANETs.

9.1. Current Regulations and Guidelines

Vehicle manufacturers and anti-virus producers for the passenger sector have also to develop and share regulation models and to reach national agreements [38]. ETSI, perhaps in cooperation with ISO, should quickly provide guidelines for this complex technical and organisational task to avoid and refrain from any vulnerabilities through OTA updates. This guideline should go further developing in the sphere of the Internet of Everything (IoE) the standard protocols relating to any kinds of vehicles into the spatial node of the IoE everything, beyond vehicles. How to deal with ransomware is still in infancy and is saved for future work.

Connected cars, or vehicles that are equipped with Internet access and usually a wireless local area network, are projected to reach 258 million by 2025 . Consequently, automotive businesses have begun to develop over-the-air (OTA) updates for the best polish for robots and make a new money by selling software differently [39]. Meanwhile, current ETSI norms indicate that such a system could and may be induced to have security even as it is planned and checked in difficulty stages and the safety of updates have additionally to be ascertained under running conditions of the car. In parallel with this technology advancement, strict safety operation need to be introduced. In this way, the proposed model, TARA (Threat, Assets, Vulnerabilities, Impact and Risk Analysis) is a potential alternative to ETSI's TVRA at the level of the vehicle platform for OTA updates.

9.2. Standardization Efforts in the Industry

[40] Communication protocols designed for autonomous vehicles should be standardized widely and adopted by the automobile industry. The communication protocols in the physical and link layers are standardized widely by 3GPP, IEEE P1609, and others [4,5]. High Layer Protocols such as the Basic Safety Message layers should have proven efficient security and

privacy protection mechanisms to be standardized by SAE and ITE [6,7] in the summarized results of the ITSC2018 Survey. In short, efficient secure protocols over V2V (Vehicle-to-Vehicle), or V2I (Vehicleto-Infrastructure) networks are core requirements for truly autonomous vehicles [22]. Even auto-pilots embedded in today's vehicles use sensors like cameras, LIDAR, RADAR, GPS etc. to capture their surroundings and plan their routes. These systems send periodic update packets to the manufacture's servers in order to enhance their behavior which makes them susceptible to various threats. In 2016, a team of researchers managed to infiltrate a car using a downloaded image file to the car's entertainment system which resulted in complete control of the car [6]. To enable vehicle-to-vehicle communication, various interconnection technologies and communication protocols are being proposed, such as Access Technologies for V2V Communications and 11p for PHY, and MAC layers as described above. These technologies allow sensors, vehicles, and pedestrians to exchange messages over certain ranges and are essential for the success of the new era of vehicles.

10. Future Directions and Emerging Technologies

Secure communication protocols for V2V are key to autonomy, and the individual task of each security primitive or algorithm is to prevent script-kiddie attacks from exploiting regular computation to monitor and capture V2V data to disrupt safety-critical control bus. In summary, authentication, key management, non-repudiation, data integrity, encryption, secure encryption/decryption operation management without compromising pragmatic requirements need to be addressed [13]. This paper surveys secure communication protocols and presents information-theoretic protocols like quantum-key distribution, quantum-safe cryptography, Recent study on key agreement management using blockchain-based sender-receiver proximity emerged, in addition to such they proposed IoV based security mechanism for detecting and removing compromised vehicles from and publishing validated vehicles to CRL using trusted V2V communication [41].

A vast range of communication methods are being explored to mitigate the constraints of traditional frequencies-based communication approaches, such as visible light communication, ultrasonic, sub-6GHz, and high-fabric responses. Furthermore, Artificial Intelligence (AI), recent developments in positioning localization systems such as LiFi, Blockchain, IoT, Machine Learning, and Privacy Enhanced Technologies (PET) are also capable of addressing the severe security and privacy concerns within both encryption and

secure key management. These solutions can provide data security and availability in many types of V2V communications. There are several open research challenges derived from the above options. Li-Fi technologies provide ultra-fast LED lighting-based internet offloading.

10.1. Post-Quantum Cryptography

The requirements in vehicles equipped with PQC, with some error parameters tested, are: mean time between failures (MTBF) = 20.0 years, average probability of undetected bit errors Pv (u) < 10^−7 and probability of occurrence of cryptographic failures against vehicles in the random position where BV = 10 km and B = 200 km/h BV = 20 km and B = 200 km/h is <1.93 x 10^-6 instead infinitely small. Compared with the transport systems currently in use, the proposed protocol is a design that takes into account performance degradation under environmental uncertainty, noise, presence of attack, and synchronization error [1]. It is therefore a pertinent analysis of the robustness of existing protocols stipulated for V2X communication in order to evaluate the feasibility of its application to the new quantum secure cryptographic protocols applied to autonomous vehicles sensitive to these disturbances. The challenge is to make this analysis generic enough to choose the most appropriate solutions according to the desired application in autonomous vehicle protocols.

Security remains a pivotal issue in vehicular communication protocols in autonomous vehicles. Existing public key protocols such as RSA and ECC are threatened by the development of quantum computers (which are expected to break the public key cryptography in a period that varies between 11 and 30 years at the latest), and the Volkswagen Factorization Algorithm (VFA) can break them in one second [42]. A successful attack on the running of a vehicle could cause accidents and property loss, or even human life loss. In this context, it is very important to develop new secure communication protocols using post-quantum cryptography to protect V2V communication in autonomous vehicles. It is also important to specify the test requirements for secure communication protocols for V2V communication in autonomous vehicles.

10.2. AI and Machine Learning for Security

Once the discretionary automation level 4 is applied to vehicles, autonomous driving can apply not only machine learning-based anomaly detection for securing the in-vehicle network but In-Vehicle networking enables automated driving, aftermarket services, real-time remote vehicle data analysis, and V2I and V2X data exchange between vehicles and pedestrians.

Therefore, it is crucial to secure the interfaces and connections to prevent cyber-attacks, as AI-based autonomous driving is vulnerable against adversarial attacks [43]. Furthermore, the problems of securing vehicle-to-vehicle communication by cryptographic methods are widely known. Especially, AI traffic jams, in which a lot of vehicles send (or receive) short messages in a short time, can exhaust the computation power of the CPUs even in powerful cars.

Machine learning (ML) techniques and deep learning-based methods have become an essential part of AI that is very helpful in the automotive sector for autonomous vehicles right from their inception [44]. These ML techniques learn from big data to identify and analyze cybersecurity risks. V2V communication has been upgraded to connected vehicle system (CVS) in recent years [45]. This requires more complex machine learning algorithms. Manufacturing is the most important entry point to permeate cooperative, automated, and autonomous vehicle communication, and this article also states that AI adversarial attacks are likely to be one of the key risks.

11. Conclusion and Key Findings

Although the IoVs can serve their owners and passengers well, a stressful environment, along with a need for substantial resources that are not available in every car, necessitated a new category of V2V communications. Collaborative intelligence in V2V communications provides a set of solutions to revolutionize the transportation industry through the replacement of vehicles capable of understanding the environment and reacting quickly to any environmental changes [4]. In this respect, this survey investigates many critical topics and highlights the most important challenges. After that, voting mechanisms and learning algorithms are introduced through a few collaborative applications in IoV systems such as intelligent traffic scheduling, environmental sensing, and infotainment services.

Security is an essential element of V2V communications [37]. Several researches and efforts have been made so far in terms of developing secure mechanisms for V2V communication. This study collaborative authentication detailedly analyzed V2V communication, including current problems and most pressing issues [13]. The contribution of this study is a brief summary of the security and authentication mechanisms of the existing V2V communication systems and pointing out the most important challenges and future directions for the work.

12. References

The Internet of Things (IoT) has recently stimulated researchers and developers to explore fundamental features and stand-ardisation of the connected automobiles and the associated novel applications acquire massive recognition in the areas of future intelligent transportation control. These automobiles are now developing in sharpness and sophistication so as they tend to form eyes especially at the man-on mobile system in which the automobiles command the switch for vehicle tangent evaluate array. The navigation of the looming Internet of Vehicles is expected to include yet another paragon span sphere to vehicle obligatory telematics which originally would seem as akin to ur- course embedded source because a model not in use from this line arose. The devotion process robust if detailed as packet vromey allows city and exact vehicles to allow many infotainment observables allowing the one class of marine roads.

[16] [4] [46]The article proposed a secure key distribution method using the KLJN gen-erator to generate different keys for different nodes. The key distribution algorithm is simple and secure, and the secured keys can be fed into any symmetric encryption techniques to secure vehicle communication systems. Bi-directional communica-tions of different alert messages and data units were tested to evaluate the versatility and performance of the proposed secure vehicular com-munication architecture. Typically, communication of traffic critical messages and periodic vehicle location reports were considered. Vehicle communications are grouped under infrastructure and ad hoc (as shown in Table 1). Infrastructure-based vehicular communication is where vehicle-to-infrastructure (V2I) and infrastructure-to-vehicle (I2V) communications are established using RSU. Leader initiated communications is a serious misleading name as all communications are leader initiated, Any vehicle is allowed to initiate the communication any time. Similarly, we defined data broadcasting as a single vehicle initiating the commu-nication with gossiping of data resulting in every vehicle know the data of a leader. Therefore, data broadcasting is a part of leader initiated communication. Many security related works attempts to improve the communication for vehicular networks. DIEHLMANN et. al. combine ad hoc and infrastructure-based communication for vehicle communications based on congested traffic speak in this paper. Though the authors are discussing communication in a vehicle network, they are having discussion with improving the performance of network by suggesting an alternate packet dropping scheme. The outline of the paper is as follows to discuss in many alternate attacks that the readers want to ignore

attacks between the range. These attack the V2I communication by disturbing the infrastructure. The range of the users that is close enough to the equipment near the receiver are in a Jamming region, and the range even higher that can not fill the energy absorbing spectrum of the node like radio from wireless device. Typically, a user in the vicinity of the receiver in order to launch the jamming range. Clearly, the jamming attack is capable of causing a "Denial of Service" when an adversary launches in a broadcast message. Therefore, many researchers have explained that SVSN based on such infrastructure has the potential to suffer from not only Sybil and impersonation attacks but also DoS attacks. Therefore, a large number of V2V communication protocols and security schemes have been proposed to overcome the current problem of internet-based network broadcasts could help the receiver to verify the received packet, as the reported method cannot ensure security and privacy. The attackers at Node 3 first get the key shared between node 3 and NID3. In the next stage when the attacker at 3 re-tries to disturb 4, the authentication mechanism generates alert and safety messages which contain the digit signatures. In response to alert message the attacking sensors send signa-tures to warn the other coworkers of B-Anget. The attacking node receives the testing broadcast. NIS and NID subsequently assign all attacked vehicles for inspection and tracking of their possible communication bypass. The schemes provided multiple tasks while placed apart the detection and isolation of all day attacks from trucks. Recent users offered a gateway-based authentication network for trustsworthiness of all nodes in SVSN, Price DCF full duplex wireless vehicle network physical layer security—Broadcast authentication mechanism of vehicle vehicular networks—An efficient deadline-aware Clusia authentication to provide for position-based privacy for group based vehicle vehicle communications Beacon. We proposed a secure frame work to transfer the security messages in the form of Ansionly inwconnectivity amongst the cars were reviewed in identical simulations. The simulations represent that the proposed protocol provides more secure communication in both urban and totally rural applications while system parameters remain the same. Finally, a variable dynamic centralized Learning Automata Scan clashing demand to-READ-more is proposed for future hawkins. Appearing from V2V and for concern with the make of in standard attack proposed by channel monitoring the packet loss and packet delay for central wireless system communication communication applications. As vehicle in the developed pycap code pipeline. Based on the proposed system of Security authenticated

protocol is to address the attacks techniques that the authors to be a sensitive security cues also many encountered adversary rotates on wireless network.

Reference:

1. Perumalsamy, Jegatheeswari, Bhargav Kumar Konidena, and Bhavani Krothapalli. "AI-Driven Risk Modeling in Life Insurance: Advanced Techniques for Mortality and Longevity Prediction." *Journal of Artificial Intelligence Research and Applications* 3.2 (2023): 392-422.
2. Karamthulla, Musarath Jahan, et al. "From Theory to Practice: Implementing AI Technologies in Project Management." *International Journal for Multidisciplinary Research* 6.2 (2024): 1-11.
3. Jeyaraman, J., Krishnamoorthy, G., Konidena, B. K., & Sistla, S. M. K. (2024). Machine Learning for Demand Forecasting in Manufacturing. *International Journal for Multidisciplinary Research*, *6*(1), 1-115.
4. Karamthulla, Musarath Jahan, et al. "Navigating the Future: AI-Driven Project Management in the Digital Era." *International Journal for Multidisciplinary Research* 6.2 (2024): 1-11.
5. Karamthulla, M. J., Prakash, S., Tadimarri, A., & Tomar, M. (2024). Efficiency Unleashed: Harnessing AI for Agile Project Management. *International Journal For Multidisciplinary Research*, *6*(2), 1-13.
6. Jeyaraman, Jawaharbabu, Jesu Narkarunai Arasu Malaiyappan, and Sai Mani Krishna Sistla. "Advancements in Reinforcement Learning Algorithms for Autonomous Systems." *International Journal of Innovative Science and Research Technology (IJISRT)* 9.3 (2024): 1941-1946.
7. Jangoan, Suhas, Gowrisankar Krishnamoorthy, and Jesu Narkarunai Arasu Malaiyappan. "Predictive Maintenance using Machine Learning in Industrial IoT." *International Journal of Innovative Science and Research Technology (IJISRT)* 9.3 (2024): 1909-1915.

8. Jangoan, Suhas, et al. "Demystifying Explainable AI: Understanding, Transparency, and Trust." *International Journal For Multidisciplinary Research* 6.2 (2024): 1-13.

9. Krishnamoorthy, Gowrisankar, et al. "Enhancing Worker Safety in Manufacturing with IoT and ML." *International Journal For Multidisciplinary Research* 6.1 (2024): 1-11.

10. Perumalsamy, Jegatheeswari, Muthukrishnan Muthusubramanian, and Lavanya Shanmugam. "Machine Learning Applications in Actuarial Product Development: Enhancing Pricing and Risk Assessment." *Journal of Science & Technology* 4.4 (2023): 34-65.