ISSN: 2959-6386 (Online), Volume 2, Issue 2

Journal of Knowledge Learning and Science Technology

Journal homepage: https://jklst.org/index.php/home

Enhancing Data Security in Autonomous Vehicle Communication Networks

Monish Katari[1], Musarath Jahan Karamthulla[2], Munivel Devan[3]

[1]Marvell Semiconductor Inc, USA

[2]TransUnion, USA

[3]Fidelity Investments, USA

Abstract

In today's driving landscape, in-vehicle communication has become a cornerstone, facilitated by the proliferation of sensor-centric communication and computing devices within vehicles. These systems serve various functions such as vehicle monitoring, reducing physical wiring, and enhancing driving efficiency. However, the existing literature on cybersecurity for in-vehicle communication systems lacks dedicated solutions to mitigate in-vehicle cyber risks effectively. Current approaches primarily rely on protocol-specific security techniques, lacking a comprehensive security framework for in-vehicle communication. This paper critically examines the literature on cybersecurity for in-vehicle communication, focusing on technical architecture, methodologies, challenges, and potential solutions.

The paper presents an in-depth analysis of in-vehicle communication network architecture, outlining key components, interfaces, and associated technologies. Protocols utilized in in-vehicle communication are classified based on their characteristics and usage types. Furthermore, security solutions for in-vehicle communication are critically reviewed, encompassing machine learning, cryptography, and port-centric techniques. A multi-layer secure framework is proposed as a protocol and use case-independent solution

for in-vehicle communication security.Lastly, the paper identifies open challenges and outlines future research directions for enhancing cybersecurity in in-vehicle communication.

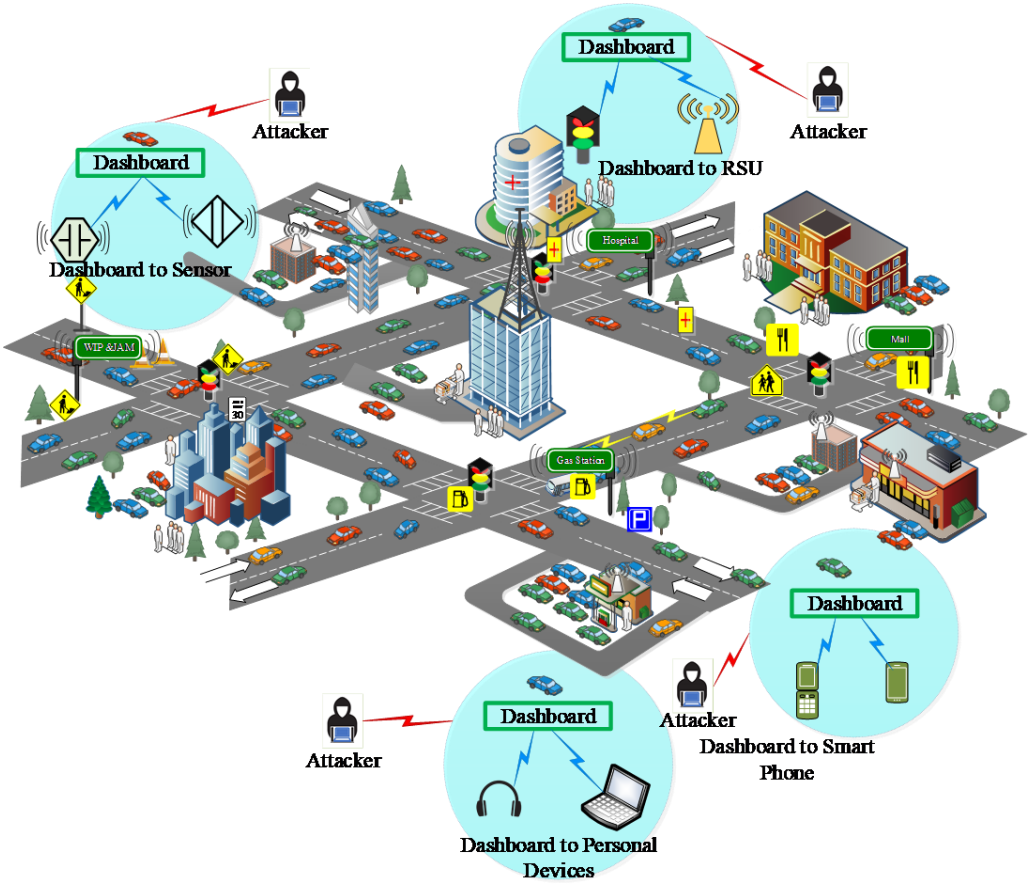
Keywords: machine learning; cryptography; cyber-attacks; cybersecurity; intrusion detection system; smart intelligent vehicles; in-vehicle network; controller area network (CAN)

Article Information:
Article history: Received: 01/10/2023 Accepted:15/10/2023 Online: 30/10/2023 Published: 30/10/2023
DOI: https://doi.org/10.60087/jklst.vol2.n3.p521

[i] ***Correspondence author:*** **Monish Katari**

Introduction

The contemporary landscape is witnessing remarkable advancements in in-vehicle automotive technologies, marking a transition to modern intelligent vehicles that can be deemed as cyber-physical systems. These vehicles exhibit exceptional capabilities to interface with external infrastructures [1]. Unlike traditional mechanical systems, modern intelligent vehicles feature integrated architectures comprising millions of lines of intricate code, facilitating the dissemination of real-time information to vehicle occupants. Advancements in in-vehicle communication technologies have paved the way for more sophisticated in-vehicle dashboard-centric communications, facilitating interactions with smartphones, sensors, earphones, laptops, and roadside units (see Figure 1). However, the proliferation of embedded hardware for in-vehicle short-range communications underscores the pressing need to address cybersecurity risks [2]. Notably, there has been a noticeable surge in research endeavors focused on devising secure in-vehicle network architectures. This surge has spurred the development of new protocols and smart applications [3]. Given the dynamic nature of automotive industries, there exists an urgent necessity for the development of efficient protocols that align with prevailing trends and technologies [4]. Figure 1 illustrates various in-vehicle communication security scenarios, highlighting associated security threats.



Modern intelligent vehicles rely on electronic control units (ECUs) interconnected via serial buses to deliver advanced in-vehicle functionality [5]. The Controller Area Network (CAN) protocol facilitates efficient communication among these modules in modern intelligent vehicles. While these vehicles boast smart connectivity and computerization, offering enhanced road safety and improved customer experience, they also expose vulnerabilities that hackers can exploit to compromise vehicle functionalities [6].

Existing in-vehicle network protocols suffer from various vulnerabilities, such as ID-based arbitration mechanisms and the absence of message authentication and encryption [7]. These vulnerabilities pose significant risks to both life and property on the road, highlighting the urgent need for enhanced cybersecurity measures in modern intelligent vehicles. The rapid advancements in technology for smart intelligent and self-driving vehicles have revolutionized the automotive industry, leading to increased connectivity and development of communication channels. However, these

advancements have also brought forth new challenges, particularly concerning the security and privacy of data [8]. The safety of individuals is at stake due to these cybersecurity vulnerabilities, given that modern connected vehicles share critical safety-related information with nearby vehicles and infrastructure in real-time [9].

Artificial Intelligence (AI) and Machine Learning (ML) techniques have emerged as promising solutions for addressing various challenges in the in-vehicle domain [12]. Notably, these techniques have proven effective in addressing security issues within in-vehicle networks [13, 14]. With modern intelligent vehicle networks relying heavily on wireless communication and increased connectivity, they are vulnerable to a wide array of attacks [15]. Consequently, researchers have leveraged machine learning techniques to develop security frameworks capable of identifying potential attacks and mitigating security-related issues in vehicular networks [16]. While cryptographic approaches have traditionally been used to address security issues in in-vehicle networks, their limitations in validating transferred values accurately have prompted exploration of alternative approaches [17].

In this paper, we conduct a critical survey of in-vehicle communication, addressing the following research questions:

- What are the main components of in-vehicle networks?
- Why is there a need to secure the in-vehicle network environment?
- What are the main approaches for securing in-vehicle networks?
- What challenges exist in securing in-vehicle networks?
- What are the future research directions in in-vehicle cybernetics?

We begin by identifying four major categories of attacks on in-vehicle systems and explore available defenses against these attacks, focusing on machine learning and cryptography-based approaches. We then present a multi-layered in-vehicle security framework and discuss open research challenges and future directions for preventing attacks on in-vehicle network systems. Our systematic survey serves as a foundation for understanding in-vehicle network attacks and security solutions based on machine learning and cryptography techniques, providing valuable insights for stakeholders at various levels.

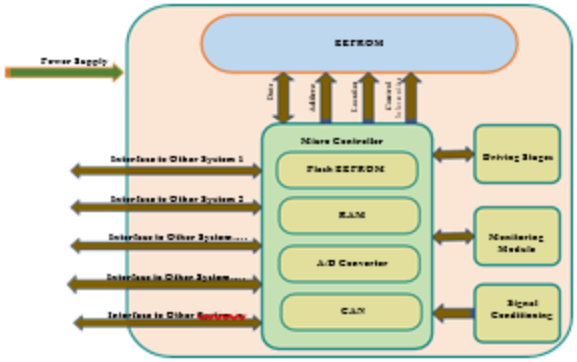
The paper is organized as follows: Section 2 presents the architecture and components of in-vehicle communication systems. Section 3 provides a brief overview of in-vehicle automotive protocols. Section 4 outlines the broad classification of attacks on in-vehicle communication systems. In Section 5, we conduct a comprehensive survey of security solutions for in-vehicle networks against malicious threats. Section 6 proposes a multi-layered in-vehicle security framework. Section 7 discusses open challenges and future research directions, followed by conclusions in Section 8.

Architecture and Components of In-Vehicle Systems

In-vehicle networks (IVNs) represent a burgeoning research domain within modern vehicular networks. The architecture of in-vehicle networks comprises several key components, including the Sensor Domain, which encompasses high-precision sensors, as well as the Chassis Domain, Infotainment Domain, Telematics Domain, and Powertrain Domain. These components facilitate crucial communication within the in-vehicle network, relying on protocols such as Ethernet, FlexRay, and Controller Area Network (CAN) [20]. The increasing connectivity among transportation systems, driven by technologies like V2X communications, has expanded the potential attack surface, allowing attackers to infiltrate the in-vehicle network.

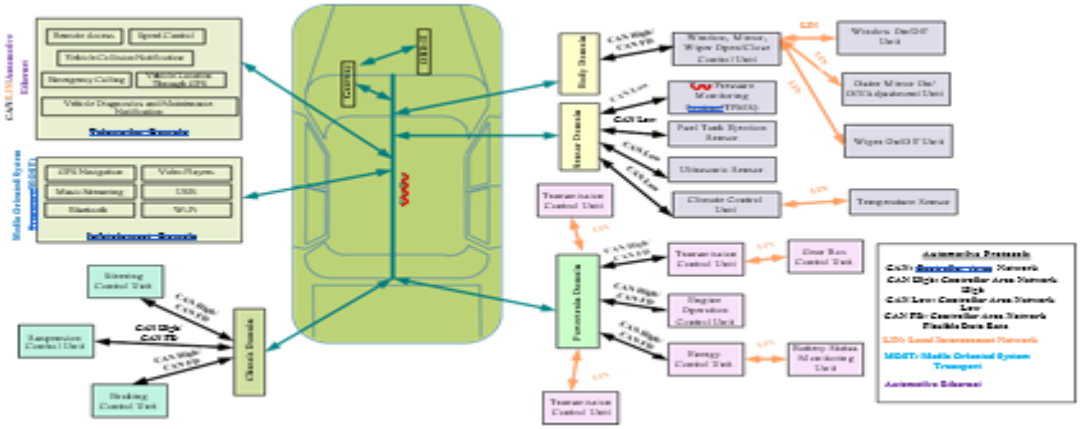
Internal Configuration of Electronic Control Units

The exchange of critical information occurs among various electronic control units (ECUs) installed within the vehicle. As the number of ECUs grows in advanced modern vehicles, so too does the complexity of in-vehicle networks. Each component within the vehicle has unique requirements in terms of bandwidth and latency, leading to increased complexity. The proliferation of ECUs in modern intelligent vehicles aims to provide a wide array of functionalities, including safety, security, and convenience. Consequently, numerous in-vehicle protocols have been developed to facilitate the interconnection of these ECUs, with ongoing research focused on enhancing their features. Moreover, ECUs are often connected to multiple bus networks to accommodate their diverse functionalities, which include vehicle control and monitoring [21]. Figure 2 illustrates the detailed internal configuration of an ECU.



2.2. In-Vehicle Network Architecture

In-vehicle networks, also referred to as internal communication networks, serve the crucial role of interconnecting diverse components within modern intelligent vehicles. These components include ECUs, gateways, sensors, and actuators, among others, which are considered the main core elements within modern intelligent vehicles. Furthermore, modern intelligent vehicles encompass various units, including the Telematics Domain, Infotainment Domain, Chassis Domain, Powertrain Domain, Body Domain, and Sensor Domain. Sensors provide inputs to these electronic units for further computation [19]. Figure 3 illustrates the general architecture of the in-vehicle network.



It is evident that miniature sensors play a crucial role in modern intelligent vehicles, serving as their backbone. These sensors possess the capability to promptly detect and report various issues for resolution, such as service requirements or component faults. They monitor a wide array of critical events, including vehicle speed, fuel levels, temperature, crankshaft rotation speed, tire pressure, exhaust gas oxygen ratio, engine air density, and more. Consequently, these

sensors must meet stringent standards, encompassing precision, resolution, sensitivity, accuracy, low power consumption, and minimal noise. By observing and reporting these events, sensors facilitate the early detection of problems, thus preventing potential vehicle damage. Autonomous vehicles are equipped with diverse types of sensors, including electric, mechanical, optical, sound, image, and light sensors, among others.

The classification of in-vehicle network architecture can be delineated into three distinct types. Firstly, there is the distributed electrical and electronics (E/E) architecture, characterized by the presence of a central gateway. Secondly, we have the domain-centralized electricals and electronics (E/E) architecture, wherein multiple operational domains are linked via a central gateway. Lastly, there is the future E/E architecture or zonal architecture, which features a centralized high-performance computing unit (HPCU), aimed at simplifying the complexities inherent in the former two architectures. Figure 4 illustrates the distributed electrical and electronics (E/E) architecture.

In the distributed E/E architecture, the primary components include function-specific ECUs in conjunction with a central gateway. Interconnection is facilitated through the controller area network (CAN) bus. The central gateway fosters robust collaboration among the ECUs, enabling the efficient execution of complex functions such as cross-functional connections and adaptive cruise control within this architecture.

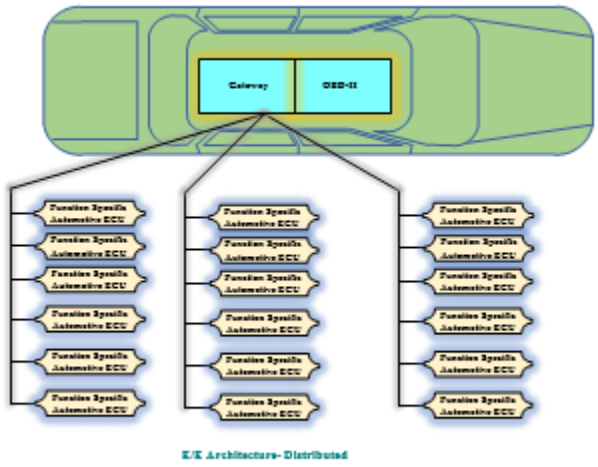


Figure 4. E/E Architecture-Distributed.

The primary drawback of the electrical and electronics (E/E) type in-vehicle network architecture is the heightened communication overhead resulting from the communication between different ECUs via a central gateway. To address this limitation, an alternative architecture was developed based on functional domains. In this architecture, various functional or operational domains are interconnected through a central gateway. Notably, the communication load on the central gateway is significantly alleviated, as the majority of communication occurs within these operational or functional domains themselves. Moreover, this architecture boasts scalable capabilities, as additional functional domains can be seamlessly incorporated.

In this architecture, the central gateway remains pivotal. Noteworthy features include the utilization of function-specific automotive ECUs and domain-specific ECUs. Function-specific automotive ECUs are connected to domain-specific ECUs via CAN bus and Ethernet connections. This architecture demonstrates enhanced efficiency in handling stringent complex functions, particularly through the consolidation of functions. Over time, domain-centralized architecture has evolved to accommodate the demands of autonomous driving features, necessitating a multitude of sensors and actuators, which in turn leads to higher data processing and bandwidth requirements, resulting in increased architectural complexity in such scenarios. Figure 5 illustrates the domain-centralized E/E architecture.

The third type of in-vehicle architecture, known as futuristic or zonal architecture, embodies advanced smart vehicle functionalities and technologies, coupled with a significant reduction in weight and cost. Key components of this architecture include function-specific automotive ECUs, HPCU, and zonal ECUs. In this paradigm, the HPCU serves as the central controller responsible for processing data received from various zones of the vehicle. Data transfer between zones occurs through the HPCU, which functions as a central gateway. To meet the high bandwidth and speed requirements for data transmission within the vehicle network, Ethernet connections are employed for ECU and HPCU connectivity. A distinctive feature of this futuristic architecture is its support for virtual domains. Two key functionalities of the HPCU include transferring embedded functions to the cloud and facilitating software update/download support over the air (OTA). Figure 6 depicts the zonal architecture.

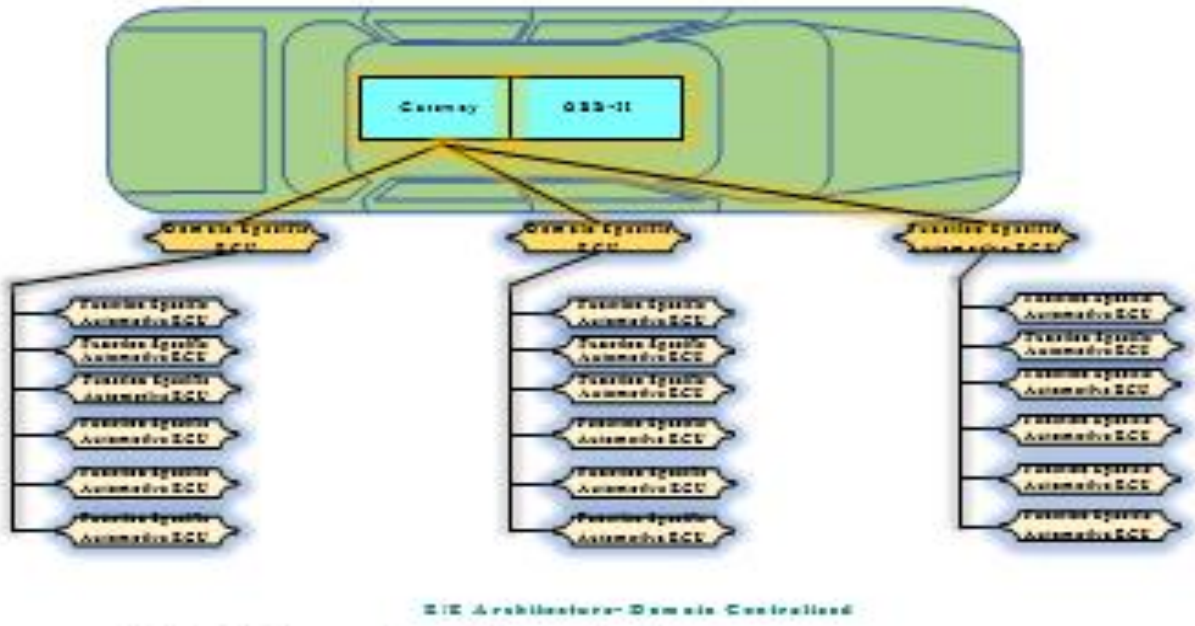


Figure 5. E/E Architecture-Domain Centralized.

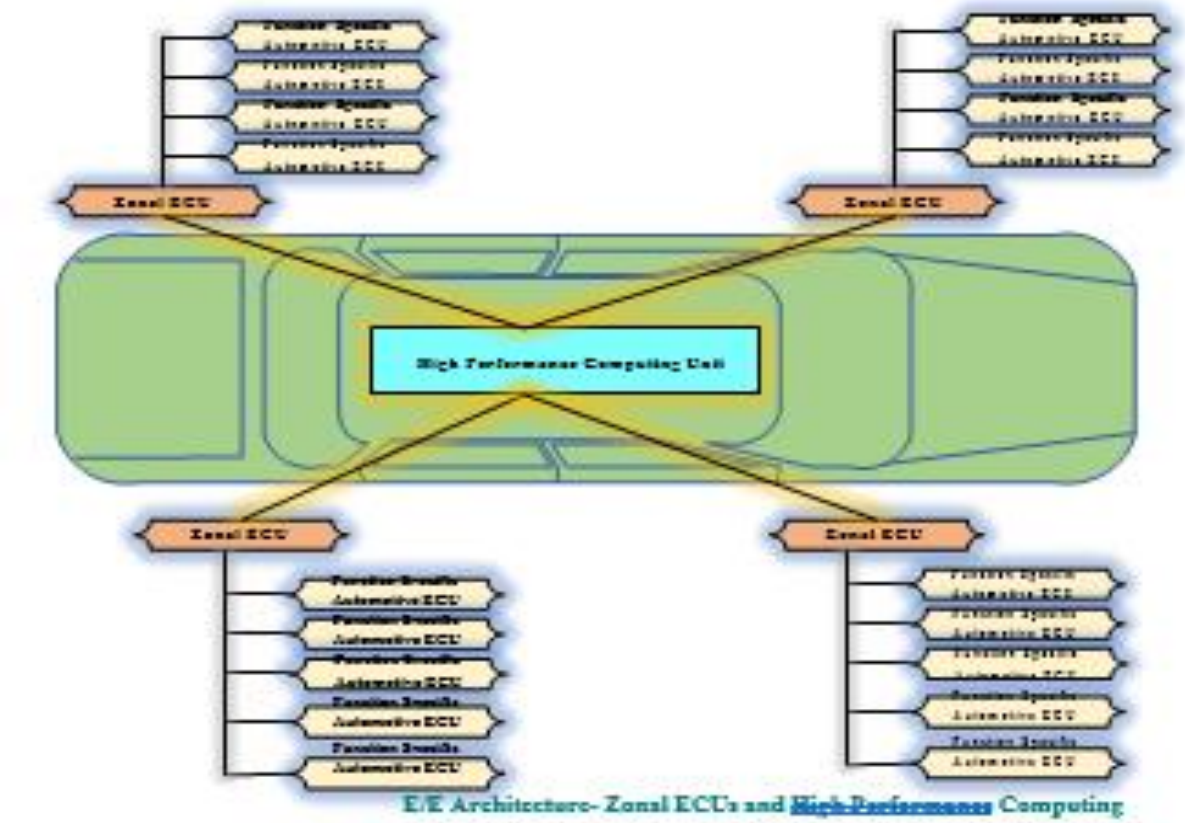


Figure 6. E/E Architecture-Zonal ECU and High-Performance Computing.

The automotive sector is poised for significant opportunities with the integration of consumer electronics technology and information technology into the automotive industry. However, this transformation requires substantial adaptation. In the current landscape, we witness rapid changes in automotive electronics architecture.

Classification and Characteristics of In-Vehicle Automotive Protocols

In advanced vehicles, including electric, hybrid, and driverless models, the exchange of stringent real-time information among different modules is crucial for smooth vehicle operation. This need is met through the rapid development of various applications of the Controller Area Network (CAN). Additionally, other heterogeneous and complex architectures of in-vehicle networks include protocols such as Media-Oriented Systems Transport (MOST), FlexRay, Local Interconnect Networks (LIN), and Automotive Ethernet (AE). Table 1 provides a classification of protocols for in-vehicle network communications.

Controller Area Network (CAN)

The CAN protocol is predominantly used for in-vehicle communications. CAN packets are transmitted between multiple Electronic Control Units (ECUs) via interconnected buses. This protocol employs a broadcast communications mechanism and offers advantages such as simplicity, low network complexity, and reduced wiring costs. However, CAN lacks real-time performance capabilities, which is critical for security-sensitive applications. Additionally, the protocol lacks authentication mechanisms and encryption, making it vulnerable to security challenges. Moreover, CAN has bandwidth limitations, which may not meet the requirements of rapidly advancing automotive applications.

Local Interconnect Network (LIN)

LIN is a single-wire network used for connecting sensors and actuators. While LIN is cost-effective, it lacks the reliability of CAN and is unsuitable for time-critical applications. LIN utilizes parity bits and checksums to detect incorrect messages in the network.

FlexRay Protocol

FlexRay protocol employs two parallel channels for synchronous and asynchronous data transmission. It is suitable for time-critical applications and offers reliability and fault tolerance features. However, the implementation cost of FlexRay is high. FlexRay addresses logical errors using checksums and redundancy mechanisms.

Media-Oriented Systems Transport (MOST)

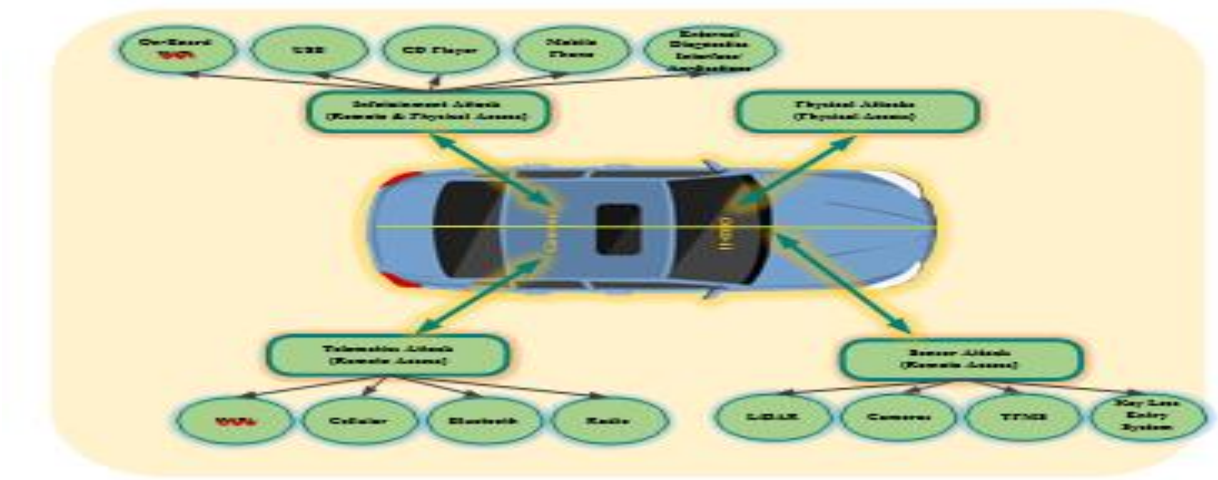
MOST protocol, developed for digital bus systems, supports synchronous and asynchronous data transmission modes. It also supports GPS applications and radio functionality. While MOST satisfies infotainment requirements, it may struggle to meet bandwidth demands under increased load.

Automotive Ethernet

Automotive Ethernet is a physical layer standard in the automotive domain, offering capabilities for advanced applications such as advanced driver assistance systems. It reduces wiring costs and supports switched network technology.

Classification of Attacks on In-Vehicle Network System for Possible Entry Points

This paper identifies four major categories of attacks on in-vehicle systems: sensor-initiated, infotainment-initiated, telematics-initiated, and direct interface-initiated attacks. Attackers leverage two main attack vectors—wireless access and physical access—to exploit internal vehicle networks. These attacks target ECUs via software bugs, remote key access, and other vulnerabilities. Research is ongoing to develop advanced security frameworks to address these security issues, particularly concerning wireless network exploitation of the in-vehicle bus system.



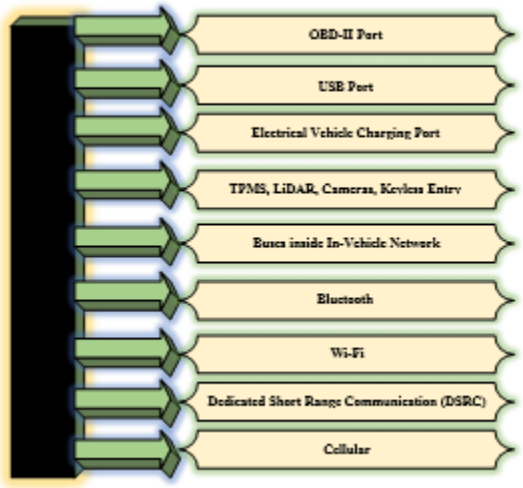
Entry Points to Smart Vehicles

As automotive technologies continue to advance rapidly, smart intelligent vehicles offer a plethora of features. However, no security mechanism is entirely foolproof against evolving security threats. With the evolution of technology, hackers are employing advanced techniques to exploit vulnerabilities in smart vehicles. Several entry points to smart vehicles are identified, as listed in Figure 8.

OBD-II Port

The On-Board Diagnostics II (OBD-II) port is utilized for monitoring various vehicle parameters such as emissions, speed, and mileage. Unfortunately, OBD-II ports are often considered the weakest link in vehicle security. Attackers can easily collect diagnostic data through this port, enabling access to the in-vehicle network and deployment of malicious programs. Two types of attacks are possible on the OBD-II port:

1. In-Vehicle Network Access Attack: Attackers may exploit the OBD-II port to install malicious devices within the in-vehicle network, with the primary aim of gaining physical access to the vehicle's systems.
2. Dongle Exploitation Attack: Dongles inserted into OBD-II ports can be remotely manipulated and decrypted by attackers, posing a significant security risk.



USB and Charging Ports

The utilization of USB ports in vehicles presents severe security threats. These threats include reprogramming of the controller processor, installation of various types of malicious codes, tampering with network cards, and altering operating system functionalities. Malicious codes contained within USB pen drives or CDs can be used to compromise the infotainment system, providing hackers with control over critical vehicle systems such as braking and engine control. Electric Vehicles (EVs) are vulnerable to attacks via charging infrastructure during the charging process. Additionally, smart grids may be targeted by attackers utilizing the charging system.

Tire Pressure Monitoring System (TPMS), LiDAR, and Keyless Entry Ports

Attackers can exploit the Tire Pressure Monitoring System (TPMS) for eavesdropping attacks to gain access to the vehicle network and conduct malicious activities. LiDAR and cameras introduce vulnerabilities to signal jamming attacks. Keyless entry systems are susceptible to interception attacks, where hackers intercept signals for capture and redirection. Current mechanisms lack adequate protection against radio signals, leaving vehicle keys vulnerable to interception by hackers.

Bus Network Ports

The Controller Area Network (CAN) lacks a communication protection mechanism, making it susceptible to attacks. Since CAN operates on a broadcast nature, every node in the network receives the transmitted frame without

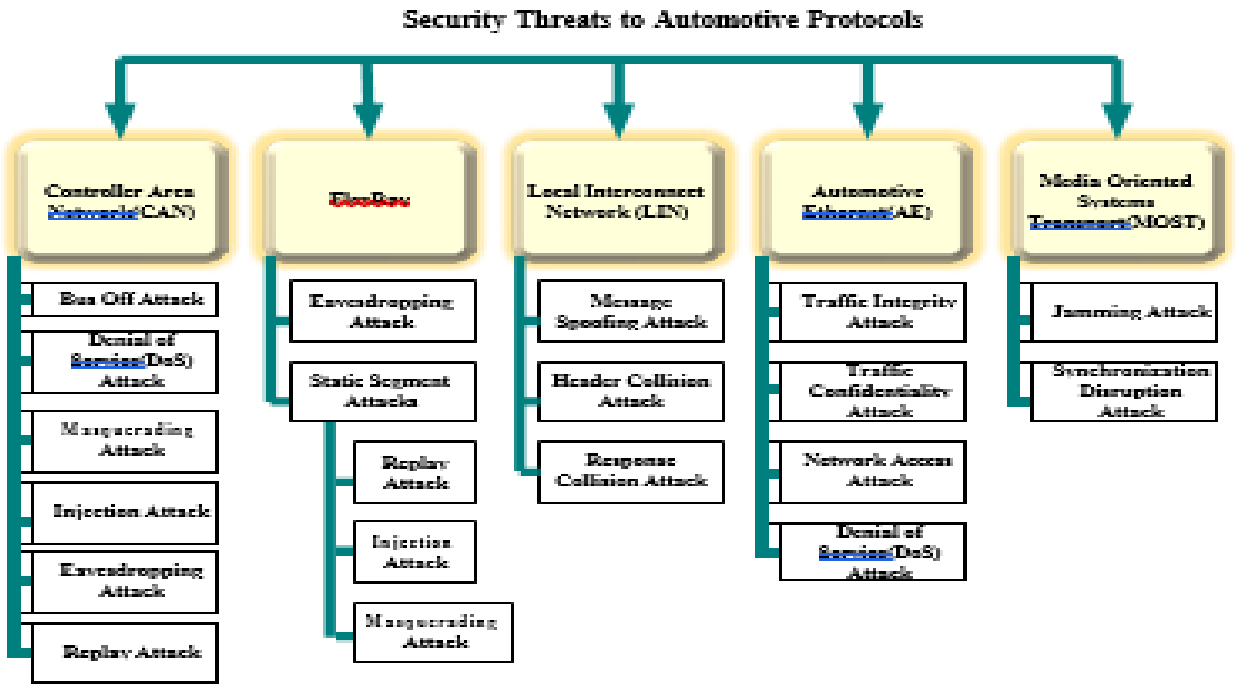
authentication or encryption. This vulnerability allows for the theft or manipulation of confidential data. Attackers can send fake frames to nodes, causing unintended behavior in the vehicle.

Vehicular Communication Ports

Smart vehicles equipped with Bluetooth and Wi-Fi are vulnerable to various attacks. Bluetooth connections can be exploited by hackers to gain full access to vehicle systems and perform malicious activities. Wi-Fi connections to roadside hotspots may expose vehicles to threats due to outdated security mechanisms. Dedicated Short-Range Communication (DSRC) and cellular technologies introduce additional vulnerabilities, allowing attackers to access vehicles for malicious purposes.

Corrective Mechanisms to Port Threats

Threats associated with OBD-II ports can be addressed by implementing a framework for tracking frame injection originating from these ports and by securing firmware updates through encryption and message signing. USB port threats can be mitigated by developing a standard USB security framework to prevent malware and viruses from accessing restricted security areas. Electric vehicle charging port vulnerabilities can be addressed through secure firmware updates, cryptographic signatures, and authentication schemes. The Open Charging Point Protocol (OCPP) has been developed to secure charging systems in the smart grid infrastructure.



CAN-Centric Security Threats

Research has identified six types of attacks on CAN bus systems: bus-off attacks, denial of service (DoS), masquerading, injection, eavesdropping, and replay attacks. Masquerading attacks occur when attackers gain knowledge of CAN frames, which are typically unencrypted and lack message authentication support. Eavesdropping attacks involve attackers intercepting broadcasted vehicular CAN messages to gain entry into in-vehicle networks. Injection attacks occur when attackers establish a connection with in-vehicle systems through OBD-II ports to compromise ECUs. Replay attacks involve attackers hindering the vehicle's real-time operation by continuously resending legitimate frames. Bus-off attacks involve attackers constantly sending bits in the identification field and other fields, disrupting normal processing. DoS attacks occur when attackers deliver CAN packets with high priority, blocking valid packets of low priority and potentially taking control of the vehicle. The primary guideline to guard against these attacks is to use encryption and authentication for exchanged messages between ECUs.

Survey of Security Solutions Based on Machine Learning Algorithms

In the realm of wireless networks, machine learning (ML) approaches are regarded as a promising solution for addressing security issues. Researchers are proposing ML-based solutions to tackle vehicle security concerns due to

their ability to make optimal predictions about various types of attacks. ML approaches offer significant advantages over other methods, particularly in achieving accurate attack predictions. Machine learning models, as illustrated in Figure 10, are employed in intrusion detection systems for in-vehicle networks.

Song et al. developed an efficient intrusion detection framework for in-vehicle networks, leveraging time intervals-based analysis of CAN messages to detect message injection attacks. Kang et al. designed a deep neural network-based intrusion detection framework that extracts feature vectors from in-vehicle network packets and trains a DNN model to discriminate between attack and normal packets, achieving improved detection accuracy. Ghaleb et al. proposed an ML-based model for misbehavior detection, updating features regularly to represent misbehavior and utilizing historical data for training a misbehavior classifier based on feedforward and backpropagation techniques. Jagielski et al. analyzed attacks targeting adaptive cruise control and local sensors using machine learning and physical-based constraints, highlighting the impact on safety, comfort, and efficiency. Seo et al. developed an intrusion detection system for in-vehicle networks using a deep learning approach that only utilizes normal data to detect unknown attacks. Ferdowsi et al. designed a deep reinforcement learning-based system to enhance the robustness of dynamics control for autonomous vehicles against cyber-physical attacks, utilizing a game-theoretic environment for analyzing vehicle reactions to attacks.

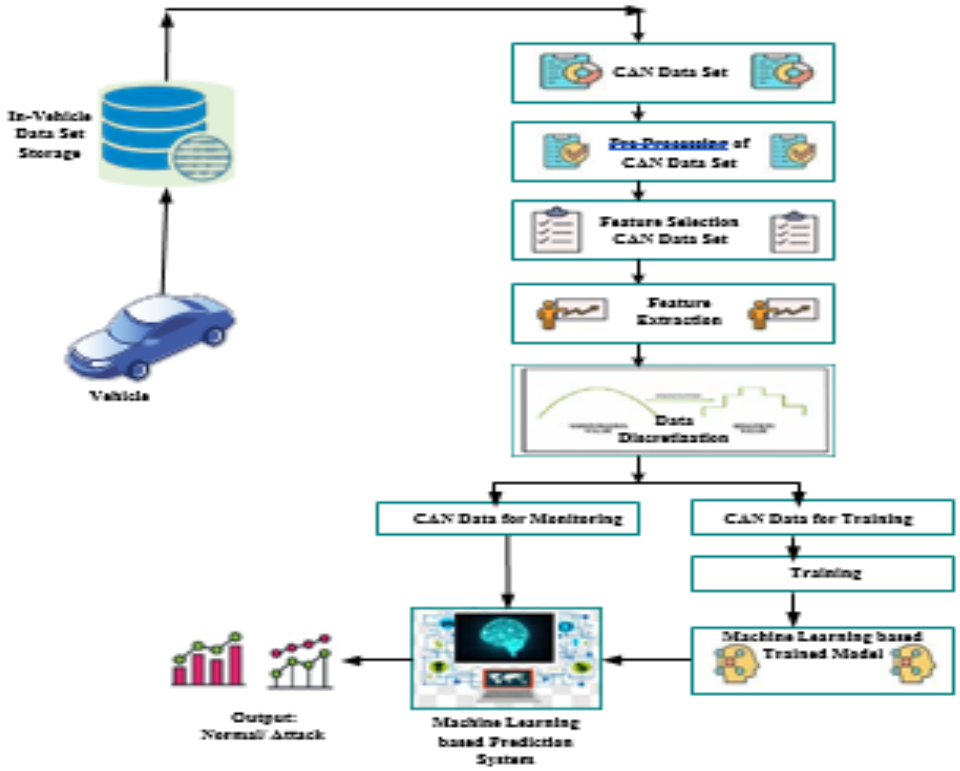


Figure 10. General Flow Diagram reflecting series of steps for intrusion detection using machine learning model.

Zhu et al. developed an efficient intrusion detection framework utilizing distributed long short-term memory (LSTM), which reduces complexity by utilizing binary CAN messages without revealing message semantics. This multidimensional framework considers both data and time dimensions for detection based on LSTM, achieving high accuracy in detection. Eziama et al. conducted a comparative analysis of five machine learning approaches, including K-Nearest Neighbor, Linear and Radial Support Vector Machine, Decision Tree-based models, Naive Bayes, and Random Forest. Their recommendation system utilizes different communication nodes to distinguish between honest and malicious data, with trust computation measures such as Recall, Precision, and Receiver Operating Characteristics (ROCs).

Sherazi et al. proposed an Intrusion Detection framework utilizing Q-learning and fuzzy logic specifically to counter Distributed Denial of Service attacks, demonstrating effective defense against such attacks. Khanapuri et al. designed a security framework using convolutional neural network (CNN) and deep neural network (DNN), training on noisy sensor data from various smart vehicle sensors to detect attacks. Song et al. developed a deep CNN-based intrusion

detection framework for protecting the CAN bus, achieving high detection performance with reduced complexity. Xiao et al. proposed a lightweight security framework comprising two individual frameworks: the simplified attention (SIMATT) framework based on machine learning and the security control unit (SECCU) framework, significantly reducing computational cost.

Guo et al. proposed a security framework consisting of a context-aware trust management model and a reinforcement learning model to evaluate message trustworthiness and select appropriate evaluation strategies, ensuring high precision in evaluated results. Katragadda et al. designed a sequence mining methodology for detecting low-rate injection attacks in CAN, measuring efficacy under various attack characteristics. Rasheed et al. proposed a deep reinforcement learning-based framework for maximizing control robustness in autonomous vehicles against sensor manipulation attacks. Lin et al. developed an effective intrusion detection framework utilizing deep learning for three specified attacks on CAN traffic, demonstrating outstanding performance.

Hossain et al. proposed an Intrusion Detection framework utilizing Long Short-Term Memory to protect against CAN bus attacks, training on attack-free normal data and attack data injected into the CAR. Angelo et al. proposed an intrusion detection framework utilizing two algorithms: one for learning traffic data behavior and the other for real-time classification, providing early alerts for malicious messages. Table 2 summarizes these in-vehicle security solutions based on machine learning algorithms.

In summary, machine learning approaches are prominent for detecting and predicting various types of attacks on in-vehicle networks. Their effectiveness depends on factors such as preprocessing methodologies for raw CAN data and the distinction between supervised and unsupervised learning approaches. While supervised learning can be time-consuming due to labeling and classification, unsupervised learning can effectively identify patterns and anomalies in CAN traffic.

Conclusion

The development of modern smart vehicles is a result of the integration of communication technologies and advanced computing into the automotive industry. Initially, automotive protocols were designed without considering security threats, but the current landscape demands advanced security measures to counter malicious attacks. These security

schemes leverage various technology environments, including cryptography techniques and machine learning algorithms. Numerous research articles have explored cryptography and machine learning algorithms to design security frameworks, with ongoing research focused on finding optimal solutions.

Cryptography techniques often involve utilizing identifiers in data frames, detecting manipulations in sending time, and implementing message authentication to enhance security levels. Meanwhile, machine learning approaches utilize different algorithms to design frameworks and train models with relevant data. Security solutions can be developed at both the transfer layer and physical layer, but applying cryptography at the transfer layer may face constraints due to memory and computational limitations. Therefore, prioritizing security solutions at the physical layer could be advantageous.

Despite significant advancements in automotive protocols, several research challenges remain, including security against advanced attacks, bandwidth requirements, efficient attack detection and resolution, latency, compatibility issues, and cost. Designing efficient and robust security schemes capable of addressing various automotive protocol issues and protecting against a variety of security threats is essential.

This comprehensive survey systematically covered communication vulnerabilities in in-vehicle networks, proposed security methods based on machine learning algorithms and cryptography techniques, highlighted characteristics of in-vehicle protocols, and discussed an integrated multilayer security architecture for in-vehicle networks. Additionally, insights were provided on improving the security level in in-vehicle communication, along with discussions on future research directions. Both academia and industry have demonstrated significant concerns regarding the security of in-vehicle networks, and this systematic survey aims to provide a solid foundation for research and development teams to address security challenges and design enhanced solutions.

References:

[1]. Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. IEEE Access, 4, 5356–5373. [CrossRef]

[2]. Song, H. M., & Kim, H. K. (2021). Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data. IEEE Transactions on Vehicular Technology, 70, 1098–1108. [CrossRef]

[3]. Kang, S., Seong, J., & Lee, M. (2018). Controller area network with flexible data rate transmitter design with low electromagnetic emission. IEEE Transactions on Vehicular Technology, 67, 7290–7298. [CrossRef]

[4]. Maharjan, R., Chy, M. S. H., Arju, M. A., & Cerny, T. (2023, June). Benchmarking Message Queues. In *Telecom* (Vol. 4, No. 2, pp. 298-312). MDPI. https://doi.org/10.3390/telecom4020018

[5]. Chy, M. S. H., Arju, M. A. R., Tella, S. M., & Cerny, T. (2023). Comparative Evaluation of Java Virtual Machine-Based Message Queue Services: A Study on Kafka, Artemis, Pulsar, and RocketMQ. *Electronics*, *12*(23), 4792. https://doi.org/10.3390/electronics12234792

[6]. Rahman, M., Chy, M. S. H., & Saha, S. (2023, August). A Systematic Review on Software Design Patterns in Today's Perspective. In *2023 IEEE 11th International Conference on Serious Games and Applications for Health (SeGAH)* (pp. 1-8). IEEE. https://doi.org/10.1109/SeGAH57547.2023.10253758

[7]. Shivakumar, S. K., & Sethii, S. (2019). *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*. Apress.

[8]. Sethi, P. Karmuru, & Tayal.(2023). Analyzing and Designing a Full-Text Enterprise Search Engine for Data-Intensive Applications. *International Journal of Science, Engineering and Technology*, *11*. https://www.ijset.in/wp-content/uploads/IJSET_V11_issue6_628.pdf

[9]. Sethi, S., Panda, S., & Kamuru, R. (2023). Comparative study of middle tier caching solution. *International Journal of Development Research*, *13*(11), 64225-64229.

[10]. Gitte, M., Bawaskar, H., Sethi, S., & Shinde, A. (2014). Content based video retrieval system. *International Journal of Research in Engineering and Technology*, *3*(06), 123-129.

[11]. Gitte, M., Bawaskar, H., Sethi, S., & Shinde, A. (2014). Content based video retrieval system. *International Journal of Research in Engineering and Technology*, *3*(06), 123-129.

[12]. Sethi, S., & Shivakumar, S. K. (2023). DXPs Digital Experience Platforms Transforming Fintech Applications: Revolutionizing Customer Engagement and Financial Services. *International Journal of Advance Research, Ideas and Innovations in Technology*, *9*, 419-423.

[13]. Jhurani, J. REVOLUTIONIZING ENTERPRISE RESOURCE PLANNING: THE IMPACT OF ARTIFICIAL INTELLIGENCE ON EFFICIENCY AND DECISION-MAKING FOR CORPORATE STRATEGIES.

[14]. Jhurani, J. Enhancing Customer Relationship Management in ERP Systems through AI: Personalized Interactions, Predictive Modeling, and Service Automation.

[15]. Jhurani, J. DRIVING ECONOMIC EFFICIENCY AND INNOVATION: THE IMPACT OF WORKDAY FINANCIALS IN CLOUD-BASED ERP ADOPTION.

[16]. Smith, J. D. Influence of Self-Efficacy, Stress, and Culture on the Productivity of Industrial Sales Executives in Latin American Sales Networks.

[17]. Miah, S., Rahaman, M. H., Saha, S., Khan, M. A. T., Islam, M. A., Islam, M. N., ... & Ahsan, M. H. (2013). Study of the internal structure of electronic components RAM DDR-2 and motherboard of nokia-3120 by using neutron radiography technique. *International Journal of Modern Engineering Research (IJMER)*, *3*(60), 3429-3432

[18]. Rahaman, M. H., Faruque, S. B., Khan, M. A. T., Miah, S., & Islam, M. A. (2013). Comparison of General Relativity and Brans-Dicke Theory using Gravitomagnetic clock effect. *International Journal of Modern Engineering Research*, *3*, 3517-3520.

[19]. Miah, M. H., & Miah, S. (2015). The Investigation of the Effects of Blackberry Dye as a Sensitizer in TiO2 Nano Particle Based Dye Sensitized Solar Cell. *Asian Journal of Applied Sciences*, *3*(4).

[20]. Miah, S., Miah, M. H., Hossain, M. S., & Ahsan, M. H. (2018). Study of the Homogeneity of Glass Fiber Reinforced Polymer Composite by using Neutron Radiography. *Am. J. Constr. Build. Mater*, *2*, 22-28.

[21]. Miah, S., Islam, G. J., Das, S. K., Islam, S., Islam, M., & Islam, K. K. (2019). Internet of Things (IoT) based automatic electrical energy meter billing system. *IOSR Journal of Electronics and Communication Engineering*, *14*(4 (I)), 39-50.

[22]. Nadia, A., Hossain, M. S., Hasan, M. M., Islam, K. Z., & Miah, S. (2021). Quantifying TRM by modified DCQ load flow method. *European Journal of Electrical Engineering*, *23*(2), 157-163.

[23]. Miah, S., Raihan, S. R., Sagor, M. M. H., Hasan, M. M., Talukdar, D., Sajib, S., ... & Suaiba, U. (2022). Rooftop Garden and Lighting Automation by the Internet of Things (IoT). *European Journal of Engineering and Technology Research*, *7*(1), 37-43.

DOI: https://doi.org/10.24018/ejeng.2022.7.1.2700

[24]. Prasad, A. B., Singh, S., Miah, S., Singh, A., & Gonzales-Yanac, T. A Comparative Study on Effects of Work Culture on employee satisfaction in Public & Private Sector Bank with special reference to SBI and ICICI Bank.

[25]. Ravichandra, T. (2022). A Study On Women Empowerment Of Self-Help Group With Reference To Indian Context.https://www.webology.org/data-cms/articles/20220203075142pmwebology%2019%20(1)%20-%2053.pdf

[25]. Kumar, H., Aoudni, Y., Ortiz, G. G. R., Jindal, L., Miah, S., & Tripathi, R. (2022). Light weighted CNN model to detect DDoS attack over distributed scenario. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/7585457

[26]. Ma, R., Kareem, S. W., Kalra, A., Doewes, R. I., Kumar, P., & Miah, S. (2022). Optimization of electric automation control model based on artificial intelligence algorithm. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/7762493

[27]. Devi, O. R., Webber, J., Mehbodniya, A., Chaitanya, M., Jawarkar, P. S., Soni, M., & Miah, S. (2022). The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence. *Scientific Programming*, *2022*. https://doi.org/10.1155/2022/1473901

[28]. Al Noman, M. A., Zhai, L., Almukhtar, F. H., Rahaman, M. F., Omarov, B., Ray, S., ... & Wang, C. (2023). A computer vision-based lane detection technique using gradient threshold and hue-lightness-saturation value for an autonomous vehicle. *International Journal of Electrical and Computer Engineering*, *13*(1), 347.

[29]. Patidar, M., Shrivastava, A., Miah, S., Kumar, Y., & Sivaraman, A. K. (2022). An energy efficient high-speed quantum-dot based full adder design and parity gate for nano application. *Materials Today: Proceedings*, *62*, 4880-4890.https://doi.org/10.1016/j.matpr.2022.03.532

[30]. Pillai, A. S. (2023). Advancements in Natural Language Processing for Automotive Virtual Assistants Enhancing User Experience and Safety. *Journal of Computational Intelligence and Robotics*, *3*(1), 27-36.

[31]. Rahman, S., Mursal, S. N. F., Latif, M. A., Mushtaq, Z., Irfan, M., & Waqar, A. (2023, November). Enhancing Network Intrusion Detection Using Effective Stacking of Ensemble Classifiers With Multi-Pronged Feature Selection Technique. In *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-6). IEEE. https://doi.org/10.1109/ETECTE59617.2023.10396717

[32]. Latif, M. A., Afshan, N., Mushtaq, Z., Khan, N. A., Irfan, M., Nowakowski, G., ... & Telenyk, S. (2023). Enhanced classification of coffee leaf biotic stress by synergizing feature concatenation and dimensionality reduction. *IEEE Access*.

https://doi.org/10.1109/ACCESS.2023.3314590

[33]. Irfan, M., Mushtaq, Z., Khan, N. A., Mursal, S. N. F., Rahman, S., Magzoub, M. A., ... & Abbas, G. (2023). A Scalo gram-based CNN ensemble method with density-aware smote oversampling for improving bearing fault diagnosis. *IEEE Access*, *11*, 127783-127799. https://doi.org/10.1109/ACCESS.2023.3332243

[34]. Irfan, M., Mushtaq, Z., Khan, N. A., Althobiani, F., Mursal, S. N. F., Rahman, S., ... & Khan, I. (2023). Improving Bearing Fault Identification by Using Novel Hybrid Involution-Convolution Feature Extraction with Adversarial Noise Injection in Conditional GANs. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3326367

[35]. Latif, M. A., Mushtaq, Z., Arif, S., Rehman, S., Qureshi, M. F., Samee, N. A., ... & Al-masni, M. A. Improving Thyroid Disorder Diagnosis via Ensemble Stacking and Bidirectional Feature Selection. https://www.techscience.com/cmc/v78n3/55928/html

[36]. Gunasekaran, K. P., Babrich, B. C., Shirodkar, S., & Hwang, H. (2023, August). Text2Time: Transformer-based Article Time Period Prediction. In *2023 IEEE 6th International Conference on Pattern Recognition and Artificial Intelligence (PRAI)* (pp. 449-455). IEEE. https://doi.org/10.1109/PRAI59366.2023.10331985

[37]. Gunasekaran, K., & Jaiman, N. (2023, August). Now you see me: Robust approach to partial occlusions. In *2023 IEEE 4th International Conference on Pattern Recognition and Machine Learning (PRML)* (pp. 168-175). IEEE. https://doi.org/10.1109/PRML59573.2023.10348337

[38]. Kommaraju, V., Gunasekaran, K., Li, K., Bansal, T., McCallum, A., Williams, I., & Istrate, A. M. (2020). Unsupervised pre-training for biomedical question answering. *arXiv preprint arXiv:2009.12952*. https://doi.org/10.48550/arXiv.2009.12952

[39]. Bansal, T., Gunasekaran, K., Wang, T., Munkhdalai, T., & McCallum, A. (2021). Diverse distributions of self-supervised tasks for meta-learning in NLP. *arXiv preprint arXiv:2111.01322*. https://doi.org/10.48550/arXiv.2111.01322

[40]. Mahalingam, H., Velupillai Meikandan, P., Thenmozhi, K., Moria, K. M., Lakshmi, C., Chidambaram, N., & Amirtharajan, R. (2023). Neural attractor-based adaptive key generator with DNA-coded security and privacy framework for multimedia data in cloud environments. *Mathematics*, *11*(8), 1769. https://doi.org/10.3390/math11081769

[41]. Padmapriya, V. M. (2018). Image transmission in 4g lte using dwt based sc-fdma system. *Biomedical & Pharmacology Journal*, *11*(3), 1633. https://dx.doi.org/10.13005/bpj/1531

[42]. Padmapriya, V. M., Thenmozhi, K., Praveenkumar, P., & Amirtharajan, R. (2020). ECC joins first time with SC-FDMA for Mission "security". *Multimedia Tools and Applications*, *79*(25), 17945-17967. https://doi.org/10.1007/s11042-020-08610-5

[43]. Padmapriya, V. M., Sowmya, B., Sumanjali, M., & Jayapalan, A. (2019, March). Chaotic Encryption based secure Transmission. In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)* (pp. 1-5). IEEE. https://doi.org/10.1109/ViTECoN.2019.8899588

[44]. Padmapriya, V. M., Thenmozhi, K., Praveenkumar, P., & Amirtharajan, R. (2022). Misconstrued voice on SC-FDMA for secured comprehension-a cooperative influence of DWT and ECC. *Multimedia Tools and Applications*, *81*(5), 7201-7217. https://doi.org/10.1007/s11042-022-11996-z

[45]. Padmapriya, V. M., Thenmozhi, K., Avila, J., Amirtharajan, R., & Praveenkumar, P. (2020). Real Time Authenticated Spectrum Access and Encrypted Image Transmission via Cloud

Enabled Fusion centre. *Wireless Personal Communications*, *115*, 2127-2148. https://doi.org/10.1007/s11277-020-07674-8

[46]. Padmapriya, V. M., Priyanka, M., Shruthy, K. S., Shanmukh, S., Thenmozhi, K., & Amirtharajan, R. (2019, March). Chaos aided audio secure communication over SC-FDMA system. In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)* (pp. 1-5). IEEE. https://doi.org/10.1109/ViTECoN.2019.8899413