IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

623+Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Security of 6G enabled Vehicle-to-Everything Communication in Emerging Federated Learning and Blockchain Technologies

MYOUNGSU KIM[1], INSU OH[1], KANGBIN YIM [1], MAHDI SAHLABADI[2] and ZARINA SHUKUR[2]

[1]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea
[2]Center of Cyber Security, Faculty of Information Science and Technology at Universiti Kebangsaan Malaysia (UKM), Malaysia

Corresponding author: Mahdi Sahlabadi (e-mail: sahlabadi@ieee.org).

This work was supported in part by the National Research Foundation of Korea (NRF) Grant by the Korean Government [Ministry of Science and ICT (MSIT)] under Grant NRF-2021R1A4A2001810, and in part by the Soonchunhyang University Research Fund.

ABSTRACT Sixth-generation (6G) communication is emerging as seamless and massive connecting of almost everything. Therefore, vehicles, being extensively linked with human mobility, require a technological pace for compatibility with the 6G era. 6G will also potentially revolutionize the Vehicle-to-Everything (V2X) communication. However, this modernization will surface several security challenges in the complex heterogeneous architecture of V2X communication in 6G. Similarly, the expansion of V2X also introduces unconventional security risks and vulnerabilities. This paper aims to provide an overview of the security challenges and solutions for V2X communication in the upcoming 6G era to visualize the future of this research domain. This paper discusses the architecture and standards utilized in 6G enabled V2X communications and provisions a comprehensive analysis of V2X security in Confidentiality, Integrity, Availability, Authentication and Access Control (CIA^3) domains. Thereby, we analyze the impact of the emerging technological concepts of Blockchain and Federated Learning (FL) in 6G enabled V2X communication. Thereby, we suggest a Blockchain-enabled FL based generic security architecture for V2X communication in 6G networks. At the conclusive end, the review highlights key lessons learned and the future research directions in the domain of security of V2X communications in the 6G including; Privacy in 3D Fog Computing, Privacy in Augmented Reality, C. Secure Software Defined Networking (SDN), Physical Layer Security In THz Spectrum, SUMO (Simulation of Urban MObility) and Intrusion Detection using AI.

INDEX TERMS V2X; security; 6G; Federated Learning, Blockchain.

I. INTRODUCTION

The emergence of the Sixth-generation (6G) communication technology is poised to revolutionize the ways of interaction with everything around us. This technology promises seamless and massive connectivity, enabling everything from autonomous vehicles to smart cities and beyond. Presently, vehicles, being increasingly linked to human mobility, require several technological advancements to keep up with the demands of 6G communication [1].

In particular, 6G has the potential to revolutionize Vehicle-to-Everything (V2X) communication, which includes various concepts such as Connected Autonomous Vehicles (CAVs), Internet of Vehicles (IoV), Intra-vehicular communication, and Vehicle-to-Vehicles (V2V) communication. These advancements are modernizing the concept of transportation, by provisioning safer and more efficient transportation [2]. V2X communication includes the exchange of data between a vehicle and other entities in its environment, including other vehicles, infrastructure, and even pedestrians. V2X communication is designed to enhance the safety and efficiency of transportation systems by allowing vehicles to communicate with each other and with their surroundings in real-time [3]. V2X communication is primarily dependent on wireless communication technologies such as Dedicated Short-Range Communications (DSRC) based on Road Side Units (RSUs), WiFi, and mobile network communication. These technologies involve vehicles exchanging data with each other and with infrastructure over short and long distances, respectively.

TABLE I
THE IMPACTFUL RESEARCH PROJECTS BASED ON V2X COMMUNICATION.

Year	Project	Scope	Impact
2005	Unity [4]	Develops 3D technology and VR visualization tools to streamline physical navigation of autonomous vehicles.	• Promoting modern concepts such as DigitalTwin, • Partnership with Audi and Toyota
2009	Waymo [5]	Builds self-driving vehicles, offering commuters for use in personal and commercial spaces. Based on a research project conducted by Google,	• Provide assets to use for press and educational purposes. • Provides Open Dataset for V2X.
2016	Auto X [6]	Provides an AI-enabled platform offering solutions for self-drive vehicles and grocery delivery services	• Backed by Alibaba • Operating a fleet of robo-taxis in Shenzhen • Roll out a fleet of robo-taxis for China and other countries in Asia.
2017	May Mobility [7]	Autonomous driving technology to make transportation "safer, greener and more accessible. Employs a drive-by-wire system that can be integrated into most platforms	• Real-time, on-board simulations lead to emergent behaviors that allow every vehicle to drive safely in each and every situation. • Partnership with Toyota
2020	Motional [8]	Ensures 360-degree visibility and object detection. Moreover, it also employs ML and a cloud-based infrastructure to collect and process vehicular data	• It is a joint venture between automotive technology expert Aptiv and vehicle manufacturing leader Hyundai Motor Group • Provides fully driverless vehicles • Integration into mobility networks for autonomous ride-hail and delivery services
2023	Cruise [9]	Self-driving cars use data visualization to allow cars to track objects around	• Addresses challenges in hardware, AI, embedded systems, simulation, and infrastructure. • Promotes All-electric, driverless rides •

V2X communication is considered a potential technological candidate for playing a significant role in the development of autonomous vehicles and smart transportation systems, as it can provide vehicles with the information they need to operate safely and efficiently in complex environments [10].

Currently, several autonomous vehicle projects have been pursued by renowned companies, which depict extensive utilization of communication technologies. The automotive industry is currently experiencing significant technological advancements with a groundbreaking objective of creating intelligent and self-driving cars. These types of vehicles can be categorized as either Automotive Vehicles or Connected Vehicles. In the United States, the term Connected Vehicles (CVs) is used for communication between cars [11], while in EU countries, V2X concept is referred as Cooperative Intelligent Transport Systems (C-ITS) [12]. The scope of the most prominent industrial works based on V2X communication is briefed in Table 1.

However, with these technological uplifts surface several challenges, particularly, security in complex and heterogenous architecture in networks of V2X in 6G [13]. V2X communication is a critical technology that enables communication between vehicles, pedestrians, infrastructure, and other devices. However, 6G communication is expected to enhance road safety and improve transportation efficiency. But, as V2X in 6G is also probable to surface various unconventional risks and vulnerabilities [14]. The fundamental security challenge in V2X communication is ensuring the confidentiality, integrity, availability, authentication and access control (CIA^3) in data transmission between vehicles and infrastructure. Therefore, accurate and secure communication is an extreme requirement for the safe operation of autonomous. Cybersecurity threats such as eavesdropping, altering, and Denial-of-Service (DoS) attacks can compromise the integrity of V2X communication, leading to potential safety hazards on the road.

To address these security challenges, various measures are being developed, including secure communication protocols, encryption techniques and intrusion detection systems. Additionally, it is important to establish a comprehensive security framework that incorporates all aspects of V2X communication, including hardware, software, and network infrastructure [15]. The advent of 6G holds the potential to revolutionize vehicular concepts including; CAVs, IoV, V2V communication, and more. However, this transformation introduces significant security challenges, particularly in the context of the complex V2X communication architecture. Therefore, this paper aims to provide an in-depth analysis of the security challenges within V2X communication in the upcoming 6G era, proposing a novel security architecture to address these concerns. The core problem addressed in this paper is the security of V2X communication in the context of 6G networks [16]. As vehicles become increasingly connected and autonomous, their vulnerability to security breaches and cyber-attacks rises.

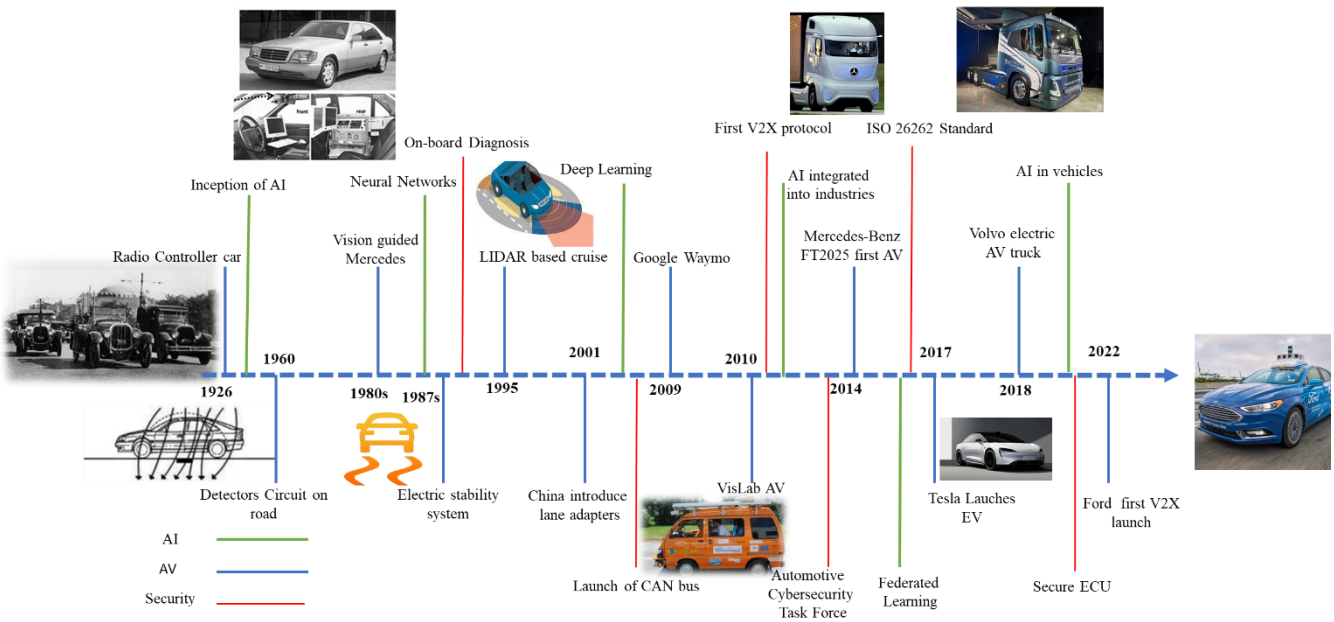

FIGURE 1. **Time line of technological evolution of AI, AV and vehicular security**

Figure 1 describes the technological evolution of AI, vehicular technology and security in vehicular communication. Vehicular technologies face unique challenges and constraints, such as safety, regulation, and consumer trust, which can slow down their advancement compared to other technology sectors. While progress is being made, the cautious and complex nature of the automotive industry contributes to the perception of lagging. Similarly, the automotive industry often experiences longer product development cycles compared to other technology sectors. Developing, testing, and bringing a new vehicle to market can take several years. This extended timeline can slow down the integration of cutting-edge technologies in vehicles. Similarly, the rate of adoption for new vehicular technologies often depends on consumer acceptance and trust. Consumers may be more cautious when it comes to entrusting their safety to advanced AI systems in vehicles, which can slow down the integration of these technologies.

The diverse and heterogeneous nature of V2X communication in 6G networks introduces unconventional security risks, potentially jeopardizing the CIA[3] domains of vehicular systems [17]. Ensuring the security of V2X communication is paramount to enable the safe and reliable operation of future vehicular networks [18]. The review addresses how the novel features of 6G networks, such as higher data rates, ultra-low latency, and massive device connectivity, impact the security landscape of V2X communication. The paper delves into the unique security requirements of V2X communication, considering aspects such as real-time communication, authentication of vehicles, and protection against cyber threats. Further, the analysis explores how emerging technologies like Blockchain and Federated Learning can be harnessed to enhance V2X security.

A. Related Previous Surveys / Reviews in the Literature

Recently, there has been a momentous increase in the count of research articles published on V2X communication in 6G networks, covering a wide range of topics including networking enhancements, applications, and security. With the advancement of technology, computer communication is moving towards 6G networks, and over the last three years, research in this area has reached unprecedented levels. We conducted a comprehensive search of SCOPUS and Web of Science databases to shortlist publications related to this topic and found that only seven previous surveys from 2019 to 2023 focused specifically on security in V2X communication. The recent study [19] provides an overview of V2X communication architecture for incorporating collaborative learning to augment cyber security.

Several works presented similar surveys / review, however, these studies lack a systematic security analysis with respect to V2X in 6G technologies. Moreover, the review does not cover the recent research spectrum in V2X security domain related to FL and the concepts of blockchain in 6G enabled V2X. Similarly, existing related literature works also lack discussion on the joint emerging security architecture of FL and blockchain in V2X enabled 6G communication.

The authors in the study [20] provided a detailed discussion on V2X security enhancement through blockchain technologies and discussed challenges for Beyond 5G communication. However, the study does not cover the security domain for threat analysis and countermeasures other than blockchain. Moreover, the study also has not covered the

utilization of FL in V2X communication. The study [21] focused on 6G enabled vehicular network enhancement with Deep Learning (DL) techniques. Although, the study comprehensively covers the architectural element in V2X communication, however, contains only a brief discussion on the security requirements and challenges. The study also does not cover FL implementation and challenges for V2X communication.

The authors in [22] provide a comprehensive review of 6G empowered V2X communication with a specific focus on reflecting surfaces. The only partially covers the security of V2X communication concerning the physical layer. However, the study does not provide a details security landscape for threats and countermeasures. Likewise, FL and blockchain emerging technologies are not included in the scope. The survey [23] provides a consolidated view of Machine Learning (ML) based approaches for 6G enabled secure vehicular network. However, the survey does not provide a comprehensive view of security issues in V2X communication. Similarly, the study also does not cover blockchain technology in V2X domain.

The study [24] is a security assessment of V2X integration with 6G networks. However, it does not systematically cover the complete security architecture such as countermeasures and intrusion detection systems etc. The also does not cover the blockchain and FL technologies. The authors in [25] survey provide a comprehensive discussion on 6G security and privacy issues. However, it does not provide a focused analysis of 6G security concerning V2X communication. In this study, V2X architecture is not discussed with blockchain and FL. In contrast, our survey is unique in that it offers a critical analysis of existing research on security architecture, standards, challenges, and pertinent future research directions in 6G-enabled V2X communication. The unique aspect of our survey is the systematic security analysis through CIA^3 model and analysis of countermeasures in all the architectural elements of 6G enabled V2X communication.

TABLE II
RELATED PREVIOUS SURVEYS AND REVIEW ARTICLES
Annotations: "√" shows Comprehensively covered, "0" shows Partially covered, X" shows Not covered

Ref.	V2X Security	6G	FL	Blockchain	Focus	Limitations
[19]	√	0	0	X	Mainly AI specific opportunities for attack mitigation have been discussed.	• Lacks a systematic security analysis with respect to 6G technologies • Does not cover the research spectrum in V2X security domain. • Does not blockchain technology
[20]	√	0	X	√	Focus only discussion on V2X security enhancement through blockchain technologies.	• Does not fully cover the security domain for threats and countermeasures • Does not cover FL in V2X
[21]	√	X	X	√	Focuses on 6G enabled vehicular network enhancement with Deep Learning (DL) techniques but contains only a brief discussion on security.	• Partial discussion on the security requirement • Does not cover security challenges • FL is not discussed in the domain of V2X
[22]	0	0	X	X	Provides a review of 6G empowered V2X communication with a specific focus on reflecting surfaces with partially covering physical security.	• Only partially covers the security of V2X communication • Does not provide a details security landscape for threats and countermeasures • Does not cover FL and blockchain in V2X
[23]	0	0	0	X	Discussed Machine Learning (ML) based approaches for 6G enabled secure vehicular network.	• Does not provide a comprehensive view of security issues in V2X communication • Does not cover blockchain in V2X
[24]	0	0	X	X	A security assessment of V2X integration with 6G networks. However, it does not systematically cover all security domains	• Does not systematically cover the complete security architecture, countermeasures and intrusion detection systems • Does not cover FL and blockchain in V2X
[25]	0	0	√	√	Provides a discussion on 6G security and privacy issues. However, it partially covers V2X communication.	• Does not provide a focused analysis of 6G security • V2X architecture is not discussed with blockchain and Federated Learning

B. Scope and Contributions

The literature review in this paper focused mainly on the keywords,"V2X security schemes", "V2X authentication techniques", "V2X access control system", and "V2X confidentiality ", which were used to search for the latest literature on various platforms such as, Web of Science, Google Scholar, IEEE Xplore, SCOPUS and ACM Digital Library. The goal was to identify proposed security schemes for 6G-enabled vehicular networks, and the shortlisted works were reviewed based on their reputation, relevance, originality, date of publication (between 2019 and 2023), and significance in the specific area. The review primarily includes papers on 6G V2X communication that specifically discuss security mechanisms as their main subject. The search was initiated on 11/11/22 and continued until submission for acceptance. The significant contributions of the survey are:

1) This article presents a focused discussion on V2X communication architecture for emerging technological concepts in 6G. Moreover, the 6G enabled V2X ecosystem is presented in pictorial form for a broader overview. Further, this article provides an outline of the standardization approach in V2X and further analyzes the requirements on 3GPP release 18 to augment the next-generation networking concepts in 6G communication.
2) With the above premise, this study presents a comprehensive security analysis based on CIA^3 Model. This discussion of CIA^3 is summarized in Table 3 to Table 7.
3) After a detailed overview of the security paradigm of V2X in 6G networks, this article deliberated the role of emerging technologies of Blockchain and Federated Learning (FL) for the security architecture of V2X in 6G networks. Moreover, this article presents a generic security architecture based on Blockchain and FL for compatibility with dynamic V2X environments and 6G heterogeneous networks. Thereby, this review deliberates upon lessons learned.
4) After a comprehensive analysis of security in V2X, this study highlights potential future research directions, including,1) V2X 6G Network Privacy in 3D Fog Computing, 2) V2X 6G Network Privacy in Augmented Reality, 3) Secure SDN architecture in V2X 6G network,4) V2X Physical Layer security in THz spectrum and 5) Blockchain-based distributed security in V2X.

C. Paper Structure and Organization

The review proceeding of this paper is structured as follows. Section 2 discusses V2X architectural details in 6G networks. Section 3 presents an outline of standardization in V2X communication and a discussion regarding security requirements. Section 4 is the main focus of this review for a comprehensive CIA^3 based security analysis of V2X communication. Section 5 highlights the role of emerging technologies of Blockchain and FL for a security architecture for V2X in 6G networks. Moreover, Section 6 includes the proposed security architecture. Section 7 deliberates future research directions. This review article concludes in Section 8. Figure 2 depicts the overall structure and organization of this review.

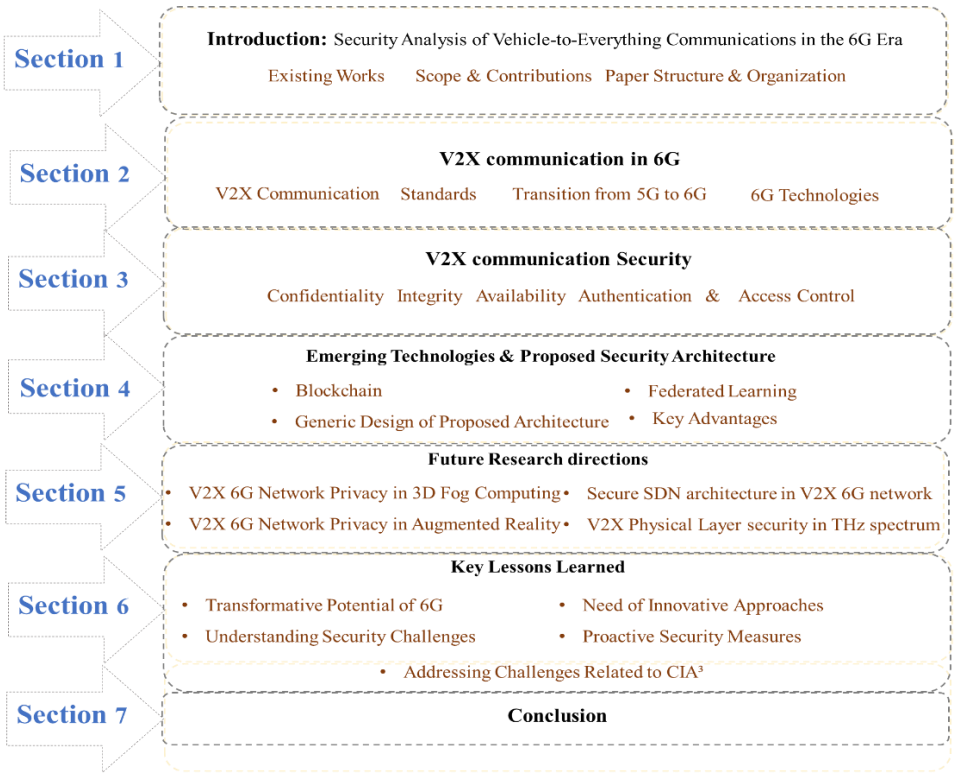

FIGURE 2. Structure and Organization of this paper

II. V2X COMMUNICATION in 6G

A. V2X COMMUNICATION

V2X communication encompasses all the communication technologies that enable V2V and V2I communication. These technologies can provide information to drivers and other vehicles in real-time alongside improving safety and efficiency and reducing traffic congestion [26]. V2V communication provisions vehicles to conversation information with each other including, speed, position, and direction of travel. V2V communication can enable vehicles to avoid collisions by coordinating their movements and optimizing traffic flow [27]. V2V communication can also be employed for coordinated movements between vehicles, such as merging onto a highway or crossing an intersection [28].

Similarly, V2I communication, on the other hand, allows vehicles to connect with infrastructure, such as Road Side Units (RSUs) traffic lights or road signs. This can provide drivers with real-time information about road conditions, congestion, and potential hazards. Moreover, V2I communication can disseminate alerts among drivers in advance for an accident or roadwork ahead, allowing them to adjust their route or speed to avoid disruption. Similarly, in case of traffic jams or congestion, V2I communication can provide drivers with real-time information about the cause and duration of the delay, allowing them to make appropriate to alter their route and optimize travel time [29]. The anticipated growth in autonomous vehicles and the various communication and digital applications required to support them. As the count of connected and autonomous vehicles increases, there will be a greater demand for services such as 3-D videos, holographic display systems, immersive entertainment, and improved in-car infotainment [30]. These developments will thrust the capacity bounds of current wireless networks and pose unconventional challenges to V2X networks in terms of bandwidth, delay, signals coverage, spectral utilization, energy consumption, cost competence, AI level, virtualization, and predominately security [31].

The Figure 3 illustrates the emerging network architecture for V2X communication, encompassing several key planes. In the user interface plane, it highlights various communication types, such as V2V, V2Pedestrian, and Vehicle-to-Grid connections. The data plane comprises intra-vehicle networks, pedestrian networks, EV grid networks, and vehicle-to-UAV networks. The routing plane showcases technologies like Edge computing, SDN, cloud computing, and intelligent network management. All of these elements are vital for enabling seamless V2X communication and fostering an intelligent transportation system.

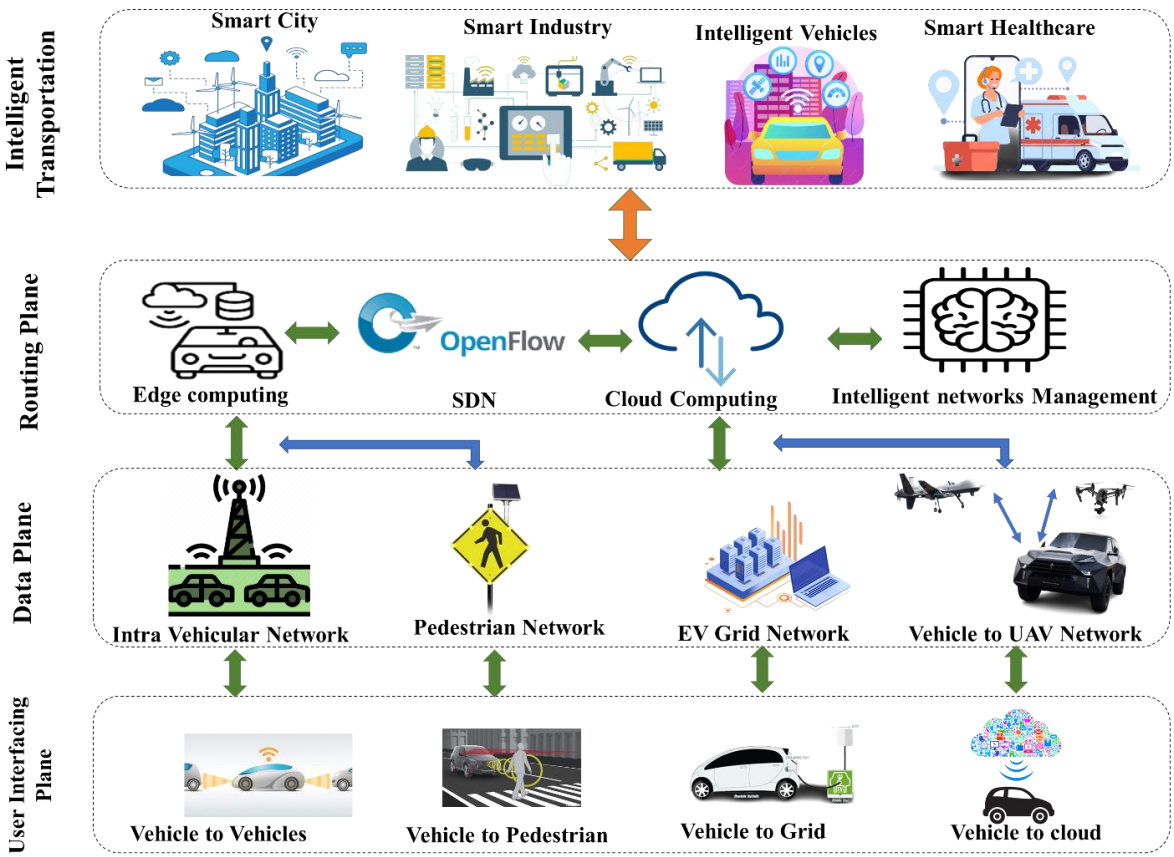

FIGURE 3. V2X communication emerging network architecture

B. V2X STANDARDS

The advancement and establishment of C-V2X technology involve multiple organizations, with primary contributions stemming from the 3rd Generation Partnership Project (3GPP), the European Telecommunications Standards Institute (ETSI), the Institute of Electrical and Electronics Engineers (IEEE), and the 5G Automotive Association (5GAA). IEEE is a well-known organization responsible for developing a wide range of technical standards, including those related to communication technologies. In the context of V2X communication, the IEEE 802.11 Working Group is relevant. This working group has developed the IEEE 802.11p standard, which is designed for short-range communication in vehicular environments. IEEE 802.11p operates in the 5.9 GHz frequency band and is commonly used for V2X communication. ETSI is another organization that plays a role in formulating V2X communication standards, particularly in the context of ITS. ETSI's Technical Committee for ITS has developed standards for cooperative ITS communications, including ITS-G5, which is based on IEEE 802.11p technology. ITS-G5 standards focus on enhancing road safety, traffic efficiency, and environmental sustainability through V2X communication [32].

The 3GPP is a collaborative organization that develops standards for cellular communication technologies, including 2G, 3G, 4G (LTE), and 5G. While 3GPP has not been directly involved in developing V2X communication standards, it has considered the integration of V2X concepts into cellular networks to enhance communication between vehicles and other road users. The initial V2X standard by 3GPP was based on LTE (Long Term Evolution) and 5G NR (New Radio) air interfaces. The initial work on LTE V2X was done under Release 14 (Rel. 14), which was further improved in Release 15 (Rel. 15). The 3GPP then approved a Study Item (SI) under Rel. 15 to evaluate and compare proposals for LTE and NR V2X. The standardization and development of Rel. 16 NR V2X was the precursor to this SI. The assessment procedure and conventions for LTE and NR V2X were developed under this SI. The 3GPP introduced a new SI and a work item (WI) to formulate the initial set of 5G NR V2X standards in Rel. 16 [27]. Thereby, this approach by 3GPP produced the primary set of 5G NR V2X details. These details were made part of the 3GPP technical specifications (TS) [33].

The 5G NR standard was originally developed under Release 15, however, the Sidelink (SL) communication capabilities were not included. Sidelink refers to the direct communication between User Equipments (UEs) or terminal nodes without the data passing through the network. The requirements of such use cases cannot be covered by the LTE V2X standard. Therefore, NR V2X SL was developed to complement LTE V2X SL communications. Overall, the introduction of NR V2X SL expands the capabilities of 5G technology to support new applications in the V2X domain. In the context of NR V2X, UEs can include vehicles, RSUs, or mobile devices carried by pedestrians. The 5G NR standard introduces V2X communications initially through Release 16 as the first version, including SL communications, based on the 5G NR air interface [34].

The 18th release and beyond refer to the next phases of development for the 3rd Generation Partnership Project (3GPP), an organization responsible for creating the technical standards for mobile telecommunications. These phases will focus on defining new use cases, SI, and WI towards the 6th Generation (6G) of mobile networks by 2030. The development of 6G will involve significant advancements in wireless communication technologies to enable faster data speeds, reduced latencies, and improved reliability than the existing 5G networks. The intricacies involved in V2X communication, which refers to the communication between vehicles and other entities such as infrastructure, pedestrians, and other vehicles, will be a crucial area of focus for 6G development [35].

The 3GPP will work on defining new use cases for 6G, which will include applications that require ultra-reliable, low-latency communication such as autonomous driving, telemedicine, and industrial automation. The SI will focus on research and analysis of various technical aspects of 6G networks, including new radio access technologies, spectrum usage, and network architecture. WI will involve the development of technical specifications and standards for 6G networks. This will include the design of new hardware and software components, protocols for V2X communication, and the incorporation of unconventional technologies such as AI and ML into the network [36]. The use of high-frequency radio waves in the 20-100 GHz range is usually referred to as millimeter wave systems. These frequencies are currently being explored for use in 5G wireless communication systems, with future releases of 3GPP expected to utilize even higher frequency bands up to 100 GHz. Terahertz wireless communication, which involves frequencies in the range of 100-300 GHz, is also an area of active research for potential use in 6G wireless [37]. One significant challenge of THz level higher frequency bands for mobile communication is the typical requirement of directional transmissions. The energy of mm-Wave must be focused in a narrow beam to reach the intended receiver. Therefore, achieving beamforming in heterogeneously dense networks is challenging due to the requirement of precise alignment between the transmit and receive apertures [38].

Moreover, one of the key objectives of 6G evolution is to increase the data rate of sidelink communication by adding the carrier aggregation (CA) feature. Carrier aggregation allows for the combination of multiple carriers to increase data throughput. By introducing CA in sidelink communication, the data rate can be significantly improved, enabling faster and more reliable communication between V2X devices [39]. Similarly, another objective is to extend sidelink operation to unlicensed spectrum.

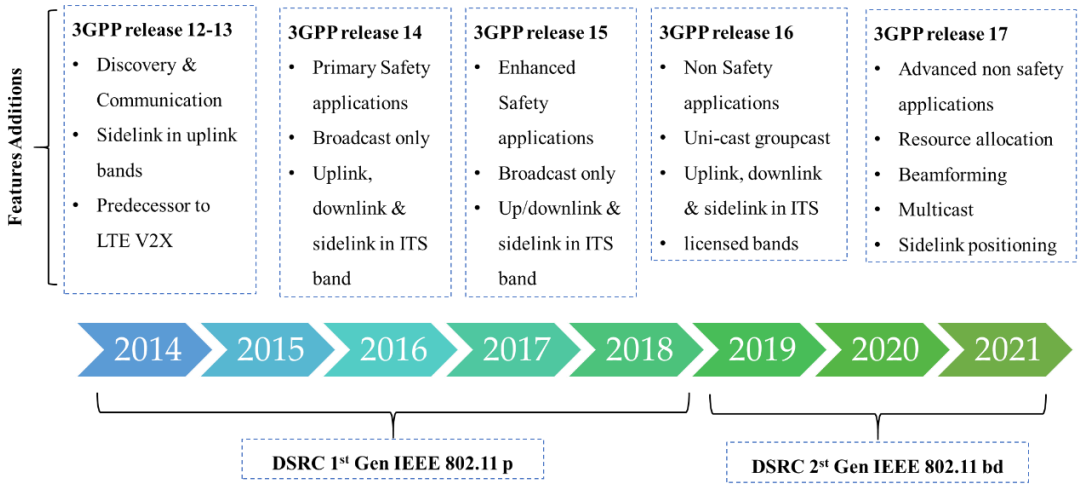

FIGURE 4. Timeline of Standards in V2X communication architecture

Unlicensed spectrum refers to the radio frequency spectrum that is not owned or licensed by any specific entity. It can enable V2X devices to communicate using frequencies that are not allocated to any particular organization, which can lead to increased efficiency and reduced congestion in licensed bands [40]. The frequency range 2 (FR2) refers to the millimeter-wave spectrum, which provides high-frequency bands with wide bandwidths that are suitable for high-speed communication. Enhancing sidelink support in FR2 can provide improved performance and reliability for V2X devices, especially in high-speed scenarios [41].

Moreover, 3GPP will analyze the procedure to provision LTE V2X and NR V2X devices co-existence in the common frequency channel. LTE and NR are two different cellular technologies that are used for wireless communication. Supporting both technologies in the same frequency channel can provide greater flexibility and interoperability for V2X devices, allowing them to communicate with each other regardless of their cellular technology [42]. 3GPP allows the elective use of security implementation based on their ability to meet the required services. This means that the implementation of security measures is not mandatory in all cases [43]. However, 6G may require mandatory end-to-end encryption; thereby, it will pose a challenge in maintaining QoS in all services and applications. Moreover, upgrading all current security protocols to support quantum-safe standards may be costlier. Therefore, it may not be feasible to upgrade all existing security protocols to support quantum-safe standards in a short time. Encryption operation through expanded key space may have a substantial effect on power consumption and storage requirements. It will surface several concerns for resource-constrained devices such as smartphones and IoT devices [44].

3GPP is responsible for developing standards for mobile communications technologies and should work more closely with researchers who use formal methods to investigate and verify the security of software and networks. By doing so, potential security vulnerabilities can be identified and addressed before the standard is released. Formal methods are mathematical techniques used to rigorously analyze and prove the correctness of software and systems. By using formal methods, researchers can identify potential security vulnerabilities and design more secure systems. This can help to ensure that mobile communication technologies are more secure and less vulnerable to cyber-attacks [45]. Figure 4 shows the timeline of Standards in V2X communication architecture.

C. V2X TRANSITION FROM 5G TO 6G TECHNOLOGIES

In the realm of telecommunications, the transition from 4G to 5G networks marked a significant leap in terms of speed, connectivity, and the ability to support a wide range of applications. However, as technology continues to advance, the next frontier in wireless communication is already on the horizon: 6G networks. Building upon the foundations established by their predecessors, 6G networks are poised to redefine the boundaries of connectivity and introduce novel concepts to address emerging challenges and opportunities. The evolution from 4G to 5G brought about an increase in data speeds and capacity, enabling faster downloads, seamless streaming, and improved overall connectivity. 6G is expected to continue this trend by providing even higher data rates and capacity, enabling unprecedented real-time data transfer and communication capabilities [46]. 5G significantly reduced latency, enabling near-instantaneous communication and responsiveness. 6G aims to further reduce latency, enabling applications that require URLLC for scenarios such as remote surgery, autonomous vehicles, and critical industrial processes. While 4G and 5G networks primarily focused on utilizing the sub-6 GHz spectrum, 6G is expected to expand into higher frequency bands, such as the terahertz range. This will facilitate higher data rates and capacity, albeit with shorter propagation distances.

6G technology presents both exciting opportunities and unique challenges in the context of vehicular networks compared to the established 5G vehicular scenarios. The key opportunities lie in ultra-low latency and ultra-high data rates, which can enable real-time, high-definition communication between vehicles and infrastructure, leading to safer and more efficient transportation. 6G's improved positioning accuracy and sensing capabilities can enhance autonomous driving and traffic management. However, the challenges are substantial. Ensuring the reliability and security of vehicular communication is paramount, as even small disruptions can have life-threatening consequences. The massive scale of connected vehicles and the need for continuous, uninterrupted connectivity demand robust infrastructure. Furthermore, regulatory and standardization hurdles must be addressed to achieve seamless global compatibility.

D. 6G TECHNOLOGIES

6G ecosystem includes revolutionizing concepts of enhanced Mobile Broad-Band (eMBB), Secure Ultra-Reliable Low-Latency Communications (SURLLC), Un-Conventional Data Communications (UCDC), Big Communications (BigCom) and Three-Dimensional Communications (3DCom) [47]. Figure 5 shows a picturized ecosystem of 6G enabled V2X communication.

eMBB refers to an advanced mobile network technology that offers higher data rates, improved spectral efficiency, and enhanced coverage to support data-intensive applications such as video streaming, virtual reality, and gaming. The enhanced capabilities provided by eMBB with higher data rates, greater capacity, and improved coverage, 6G networks will ensure that even the most data-intensive applications remain seamlessly connected. Likewise, UCDC includes non-traditional methods of communication to transmit data over networks such as wireless sensor communication, ad-hoc networks and machine-to-machine communication. UCDC introduces unconventional ways of data transmission, such as using wireless signals for sensing and imaging, opening doors to innovative applications in healthcare, agriculture, and security. SURLLC refers to a type of communication that provides extremely high reliability, low latency, and secure communication links. SURLLC enables real-time communication for applications requiring ultra-reliable low-latency connections, allowing for remote surgeries, autonomous vehicles, and industrial automation. Whereas, 3DCom refers to a type of communication technology that enables the transmission of information in three dimensions. 3DCom enables communication in three-dimensional space, enhancing location-based services, augmented reality experiences, and more immersive interactions. This can include technologies such as holographic displays. Moreover, BigCom includes the use of big data analytics techniques to analyze and optimize communication networks such as network optimization, traffic prediction, and anomaly detection. BigCom tackles the challenges posed by the exponential growth of data, enabling efficient processing and transmission of vast amounts of information. 6G networks promise a multitude of benefits that will transform industries and society as a whole [48]. As 6G networks continue to evolve, they hold the potential to revolutionize various industries and transform the way we connect, communicate, and interact with the world [49].

E. 6G TECHNOLOGIES IN V2X

The current 5G NR-based V2X networks may not be able to meet these requirements of emerging intelligent communication and quantum computing technologies. In addition, traditional V2X communication networks can only provide partial integration with intelligent networks. Therefore, a significant paradigm shift is required to pace with extra versatile and diversified network approaches as compared to traditional communication networks. This shift is expected to start with the emerging 6G wireless communication network to unify terrestrial and non-terrestrial networks such as satellite and airborne communication networks [50].

6G is expected to bring together various technologies like millimeter-wave communications, terahertz frequencies, and integrated satellite systems. Integrating these technologies into V2X communication systems can introduce complexities, making network deployment and management more challenging. While 6G technology advances, there will still be existing vehicles and infrastructure using older communication systems. Ensuring smooth interoperability between 6G-enabled V2X systems and legacy technologies is a challenge that needs to be addressed [51]. The adoption of new technologies often comes with regulatory and standardization hurdles. The development of regulations and standards for 6G-enabled V2X communication systems must balance innovation with safety and security considerations. Despite 6G's focus on low latency, the stringent real-time requirements of V2X communication systems (especially for autonomous vehicles) may still pose challenges in terms of achieving the ultra-low latency needed for split-second decision-making [52].

The potential benefits of 6G enabled V2X is an intelligent wireless communication system that aims to achieve the revolutionized concept of Intelligent Transportation Systems (ITS). The key features of 6G enabled V2X include the integration of complex technologies such as Reconfigurable Intelligent Surfaces (RIS) enabled air interfaces, resource allocation, decision-making, cloud computing, Software Defined Networking (SDN), quantum computing and various vehicular communication technologies. 6G aims to enhance the Quality of Service (QoS) of vehicular communication systems by using airborne networks and satellites in low Earth orbit to augment the V2X systems with significantly enlarged and seamless coverage. This will help to significantly improve the QoS parameters, specifically in certain low-coverage areas that are not part of traditional terrestrial communication

systems. Additionally, edge or fog computing and caching are game-changing technologies for the swift adaption of V2X communication in resource-constrained devices. They can achieve high-speed computation, highly accurate decisions, and longer battery life. The adoption of Visible Light Communication (VLC) in V2X networks will augment the traditional RF-based communications to achieve ultra-wide bandwidth, reduced setup cost, less power consumption, and improved security [53]. VLC in 6G will enable user-driven connectivity through an intelligent and autonomous service platform for ITS by enabling an unprecedented travel experience for passengers as well as drivers [54].

Moreover, potentially the 6G communications can enable beyond imagination ultrahigh data rates leading to several gigabits per second by utilizing mm-wave technology, VLC, and THz communications. Additionally, emerging state-of-the-art multicarrier frameworks and the latest resource allocation schemes will support ultralow latency and reliable data transmission through multiple radio access technologies, For ubiquitous vehicular access and massive connectivity, are two promising wireless paradigms such as Non-Orthogonal Multiple Access (NOMA) [55] and satellite or UAV based V2X. Moreover, the integration of sensing and localization in communication networks will contribute to precise positioning and velocity estimation respectively up to cm-lev and cm/s-level. Similarly, vehicle interfacing with intelligent infrastructure will augment with ability to handle the complex physical and electromagnetic conditions in heterogenous networks [56].

Similarly, the potential recipients of 6G enabled V2X are electric vehicles (EVs). EVs are a recent focus automotive industry at the global level to counter fossil fuel diminution, global warming and environmental pollution. With 6G V2X, power optimization through various driving modes for EVs can significantly enhance the battery life and travel range [57]. Similarly, EV battery integration with cloud-based computation or machine learning (ML) can improve monitoring and remotely configure required changes [58]. Intelligent Reflecting Surfaces (IRS) can be used to improve V2X communication in coverage-limited scenarios, such as when operating at high-frequency bands like millimeter-wave or THz, or in unfavorable propagation conditions where the communication links are obstructed. The use case scenario is an out-of-coverage traffic intersection, where buildings and other obstructions can block V2V communication links, leading to degraded communication performance. In such a scenario, IRS can be used on the walls of buildings and at the intersection in the infrastructure [59]. The reflecting elements of the IRS can be fine-tuned to enhance the communication coverage of transmitting vehicles in perpendicular streets. By introducing enhanced multipath propagation, IRS can improve vehicular channel conditions and increase transmission coverage, resulting in better V2V communication performance. The signal-to-noise ratio in V2V links is sensitive to distance and quickly reduces away from the intersection due to blockages; therefore, the use of IRS can mitigate this issue [60]. The authors in [61] conducted a case study to evaluate the effectiveness of the IRS in improving vehicular communication in a scenario with a high traffic density of 60 vehicles/km. The study shows that the utilization of IRSs can 25% improve the signal of vehicles with line-of-sight (LOS) links, compared to a scenario without IRS. Figure 6 shows the 6G network architecture integrated with V2X communication.

.

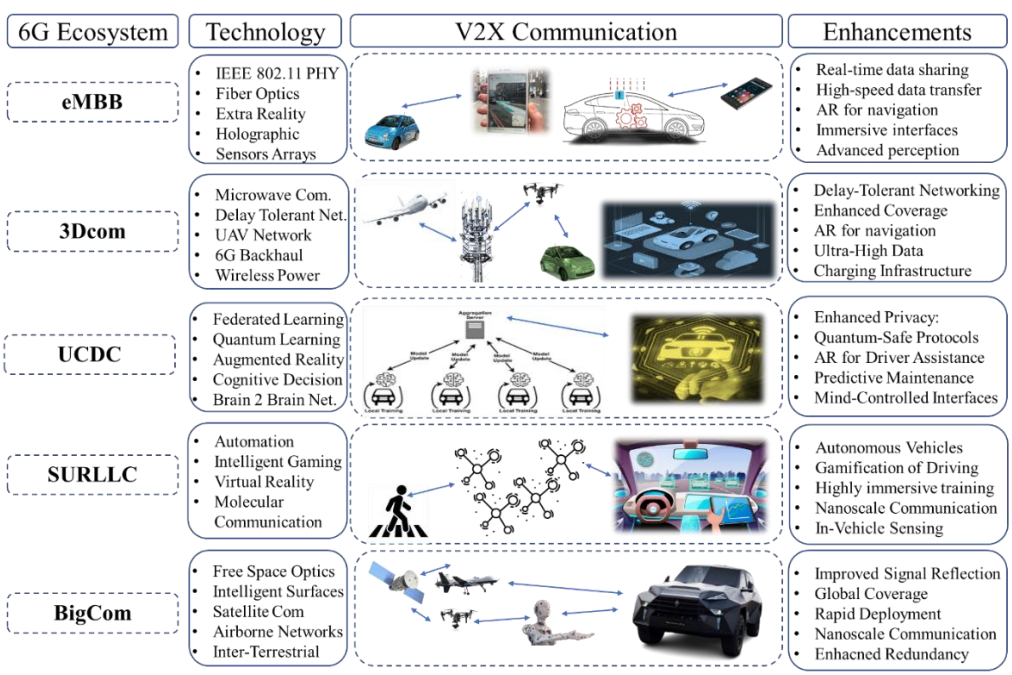

FIGURE 5. Ecosystem of V2X communication in 6G networks

III. V2X COMMUNICATION SECURITY

Ensuring the security of V2X communication is extremely critical for the safety and privacy of individuals as well as vehicles. Data transmitted between vehicles and infrastructure should be encrypted to prevent unauthorized access and data interception. Vehicles and infrastructure without a secure authentication can leverage illegitimate entities to interfere recklessly. Therefore, access to the V2X network must be restricted to authorized entities only. Similarly, data integrity is mandatory to ensure that data has not been modified during the transmission process [62]. V2X communication can reveal sensitive information, such as the location and behavior of vehicles. Therefore, anonymity techniques are explored to protect the privacy of individuals. Likewise, the firmware and software in vehicles and infrastructure are required to be securely updated regularly to address vulnerabilities and cyber threats. V2X communication architecture needs redundant systems in place to ensure that any individual subsystem is not becoming the single point of failure for the whole system [63]. Encryption techniques used in 6G networks must be designed to provide stronger security and resist attacks from quantum computers, which are expected to become more common in the future.

Similarly, applications involved in V2X communications depend on the transmission of information with other vehicles or the roadside infrastructure to provision important services such as collision avoidance, traffic management, and improved navigation. However, this exchange of information also presents a potential security risk, as attackers can intercept, modify or insert fake information in the communication. These vulnerabilities can lead to serious consequences such as accidents or traffic congestion [64]. Furthermore, V2X communication shares location information with other vehicles and traffic infrastructure. Any ill manipulation of location information is expected to cause devastating results. Moreover, unencrypted location information can lead to serious privacy issues for users. Therefore, securing V2X communication is crucial to ensure the safe and reliable operation of V2X-based applications [65].

The CIA^3 model is an extensively used framework for evaluating the security of a system. It is an acronym for Confidentiality, Integrity, Availability, Authentication, and Access Control. The model provides a comprehensive approach to evaluating the security of a system, and it is used by security professionals to ensure that a system is secure against all possible threats [66]. Security and protection of V2X communication must deal with sensitive information. Therefore, CIA^3 security model can be employed as an inclusive outline for evaluating the security of V2X communication in 6G networks. In subsequent sub-sections, we provide a detailed of different attack scenarios and CIA^3 model-based security analysis of V2X communication in 6G.

A. ATTACK SCENARIOS IN V2X

The V2X communication domains such as V2V, V2I, V2P and V2C provide numerous benefits, such as improving road safety, traffic efficiency, and overall transportation experience. However, they also introduce security vulnerabilities that can be exploited by malicious actors. Some of the pertinent attack scenarios in V2X communication are as follows:

- Denial of Service (DoS) Attacks: Attackers may transmit radio frequency interference to disrupt V2X communication, causing Jamming. This can lead to accidents and chaos on the road if vehicles and infrastructure can't communicate effectively. Similarly, Attackers can flood the V2X network with excessive messages, overwhelming the communication channels and causing legitimate messages to be lost or delayed, known as Flooding [62].
- Eavesdropping: Attackers may intercept V2X messages to gather sensitive information, such as location data or emergency signals. This information can be used for various malicious purposes, including tracking individuals or planning physical attacks [67].
- Message Tampering: Malicious actors can alter or inject false messages into the V2X network. For example, they might send fake traffic signals or manipulate the information related to a vehicle's speed or direction. This can lead to accidents or traffic congestion [68].
- Replay Attacks: Attackers capture legitimate V2X messages and replay them at a later time. For instance, an attacker can capture a legitimate emergency braking message and replay it to confuse or slow down nearby vehicles, potentially causing accidents [69].
- Spoofing and Impersonation: In spoofing attacks, attackers mimic legitimate entities (e.g., other vehicles or infrastructure) to deceive V2X participants. They can send false messages that mislead vehicles or infrastructure into taking unsafe actions [70].
- Sybil Attacks: In a Sybil attack, an attacker creates multiple fake identities within the V2X network, potentially overwhelming it with bogus messages or undermining trust within the system [71].
- Malware and Software Exploits: Infected vehicles or infrastructure components can spread malware or become victims of software exploits. These can compromise the safety and security of the entire V2X ecosystem [72].
- Physical Attacks on Infrastructure: Physical attacks on V2X infrastructure, such as tampering with roadside units or traffic lights, can disrupt communication and cause traffic chaos or accidents [73].
- Privacy Violations: Attackers may exploit V2X communication to track the movements and behavior of individuals, violating their privacy. This information can be used for stalking or other malicious purposes [74].

- Data Manipulation: Attackers can manipulate V2X data to create fake traffic congestion or accidents, leading to inefficient routing decisions and potential gridlock [75].

B. CONFIDENTIALITY IN V2X

Next-generation In V2X communication, the privacy and confidentiality of user data are of paramount importance. Primary public safety messages, such as traffic lights and speed limits, do not require data confidentiality. However, other V2X messages, such as private vehicle-to-vehicle messages, require data confidentiality to ensure user privacy, including user identity and positional information [76]. In 6G networks, V2X communication will continue to be critical for enabling connected and autonomous vehicles to communicate with each other and with infrastructure. However, wireless communication in vehicular environments is also prone to various security threats to the confidentiality of transmitted messages. To prevent passive attacks, primary encryption and authentication mechanisms are used in V2X communication.

However, ensuring confidentiality in V2X has become extremely complex due to the heterogeneous nature of 6G network alongside unconventional technologies such as AI, quantum computing, fog computing etc. [77]. Anonymization is a technique used to protect the identity of users by removing any personally identifiable information (PII) from the data before transmitting it over the network [78]. However, the security and privacy requirements of V2X communication is lawful identity resolution or de-anonymization, which refers to the ability to identify the real-world identity of a user or entity behind a pseudonym or anonymous identifier. This requirement is necessary for law enforcement purposes, such as investigating traffic violations or accidents. The authors in [79] define a broader set of technical details for lawful identity resolution in V2X communication. Similarly, Pseudonymization is another technique that can be used to replace PII with a pseudonym or unique identifier before transmitting the data over the network, allowing the data to be used for analysis and optimization of the V2X communication system while still protecting the privacy of users [80]. The study [81] suggested a framework based on blockchain and Name Data Network (NDN) technologies to provide verifiable secure V2X communication without using the confidential information of users. Instead, the framework uses non-confidential information such as the number plate of the vehicle for accountability of the communications. However, it is still probable to extract personal credentials from the number plat of vehicles, therefore, it is widely researched to shift to intelligent number plates based on QR codes or barcodes for all CAVs to preserve user privacy [82].

Similarly, the authors in [83] proposed an authentication system to provide privacy and security guarantees by jointly using several techniques such as attribute signature, multi-receiver encryption (MRE), and message authentication code.

However, MRE requires more computation and communication resources compared to traditional encryption techniques, which can increase the processing time and network bandwidth requirements.

In addition, physical security measures can also be employed to ensure data confidentiality in the network and protect against physical attacks on the network. The study [84] presented a phased-array physical layer security (PLS) scheme for millimeter-wave (mmWave) communications in cybertwin-driven V2X applications. The scheme aims to reduce computational complexity by randomly swapping the pre-calculated initial weight vector elements, instead of directly calculating a new weight vector. However, randomly swapping the weight vector can result in degraded system performance, as the new weight vector may not be optimized for the specific system requirements. Similarly, the authors in [85] propose an analytical framework for assessing the security performance of two association schemes in vehicular networks, including, the smallest-distance association (SDA) scheme and the largest-power association (LPA) scheme. The SDA scheme associates the vehicle with the closest RSU, while the LPA scheme associates the vehicle with the RSU with the strongest received signal power. The analytical results show that the LPA scheme outperforms the SDA scheme in terms of confidentiality. However, the suggested beamforming requires significant processing power and can be a complex technique to implement. Therefore, it is challenging problem to integrate into certain resource constraint systems or to optimize for specific applications. Table 3 provides a summarized view of the above-discussed research works.

TABLE III
THE PROMINENT RESEARCH WORKS ON CONFIDENTIALITY IN V2X.

Ref.	Technique	Attributes	Limitations
[81]	Uses non-confidential information such as the number plate	• Based on blockchain and NDN technologies • Verifiable secure V2X communication	• Extraction of personal credentials from number plat of vehicle • Does not cover the concept of intelligent number plates based on QR codes or barcodes
[83]	MRE	• Jointly use Attribute signature, MRE and multi-receiver message authentication code along with	• Requires more computation and communication resources
[84]	PLS	• Phased-array • Cybertwin-driven V2X • Randomly swapping the pre-calculated initial weight vector elements • Reduce computational complexity	• Degraded system performance due to randomly swapping the weight vector
[85]	LPA	• Assessment of the security performance • LPA scheme outperforms the SDA	• Requires significant processing power • Complex implementation

C. *INTEGRITY* IN V2X

Data integrity is critical in V2X communication to ensure that the information transmitted between vehicles and infrastructure is accurate, reliable, and consistent. Without data integrity, the safety and effectiveness of V2X communication systems can be compromised, leading to potential accidents and system failures [86]. The authors in [87] proposed a technique for verifying the integrity of real-time sensor data and detecting and localizing any tampering. The technique is based on semi-fragile data hiding, which involves inserting a binary watermark into the sensor data using a 3-dimensional quantization index modulation (QIM) technique. The decision-making unit can then use the watermark signature to detect and localize the tampering. The technique is specifically designed for LiDAR data, which is used in various applications such as autonomous driving.

In the 6G networks, the challenges of ensuring data integrity and reliability in V2X communication remain important. Digital signatures used in 6G networks must also be designed to resist attacks from quantum computers, which can potentially break traditional cryptographic techniques used for signature verification [88]. The authors in [89] proposed a framework based on multi-layered edge-enabled V2X system models. To ensure the integrity of the data, the framework also includes a blockchain-based data integrity management scheme. This scheme ensures that the data remains secure and tamper-proof by storing the data in a decentralized and immutable ledger. However, Multi-layered edge with blockchain can be computationally expensive and require significant resources, which can limit its scalability. Moreover, multi-layered edge architecture requires multiple technologies and protocols to be integrated and work together seamlessly. Achieving interoperability can be challenging and require significant collaborative efforts.

Similarly, The study [90] suggests blockchain based design to evaluate the integrity of received data by considering the reputation score of the data sender. However, the accuracy of the reputation score depends on the quality and reliability of the data being used to calculate it. If the data is incomplete, inaccurate, or biased, the reputation score may not be an accurate reflection of the data sender's trustworthiness. Likewise, the authors in [91] blockchain technology to enhance the security and efficiency of a remote data integrity checking (RDIC) scheme for big data. Using RSA digital signature and blockchain, the scheme achieved a lightweight blockchain-based RDIC scheme. RSA digital signature is susceptible to security vulnerabilities such as quantum computing-based brute-force attacks, side-channel attacks, and attacks on the underlying cryptographic algorithms. Similarly, Blockchain technology face regulatory and computational energy challenges in some jurisdictions, which can limit its adoption and potential use cases.

Standardization of communication protocols and data formats is also critical in the context of data integrity in 6G networks. With the increasing diversity of devices and applications that may participate in V2X communication, it is important to have standardized protocols and formats that can ensure interoperability and data integrity across different systems [92]. The authors in [93] a protocol, named Outlier Detection, Prioritization and Verification (ODPV) to address data integrity attacks in ITS applications using the isolation forest algorithm for detection of outliers, fuzzy logic for prioritizing outliers and C-V2X communications to validate the outliers. However, the performance of the isolation forest algorithm can degrade in high-dimensional data due to the increased computational complexity and sparsity of the data. Moreover, Fuzzy logic can struggle with complex data relationships that may require more sophisticated models to accurately capture the underlying patterns. The study in [94] proposed a Karatsuba-based ECC (Elliptic Curve Cryptography) processor for security architecture to ensure a high level of data integrity and privacy in various forms of V2X communication. Karatsuba-based ECC requires more memory than traditional ECC techniques, as it involves precomputing some values and storing them in memory for later use. This can be a limitation for resource-constrained systems, such as embedded devices with limited memory

TABLE IV
THE PROMINENT RESEARCH WORKS ON INTEGRITY IN V2X.

Ref.	Technique	Attributes	Limitations
[87]	Semi-fragile data hiding and binary watermark	• Real-time sensor data detecting and localizing for any tampering • 3-dimensional QIM	• Designed specifically for LiDAR data
[89]	Multi-layered edge with blockchain	• Data in a decentralized and immutable ledger • Secure and tamper-proof	• Computationally expensive • Require significant resources • Limited scalability
[90]	Blockchain	• Reputation score • Reflection of the data sender's trustworthiness	• Low performance with incomplete, inaccurate, or biased
[91]	RSA and blockchain	• Remote data integrity check • Digital signature • Computationally efficient	• Vulnerable to quantum computing based brute-force attacks • Side-channel attacks,
[93]	ODPV	• Outliers are detected Isolation forest algorithm • Outliers are prioritize the Fuzzy logic	• Degraded performance in high-dimensional data • Increased computational complexity
[94]	Karatsuba-based ECC	• Ensure a high level of data integrity and privacy	• Requires more memory than traditional ECC techniques

The development of new communication standards, such as 6G NR-V2X, will play a crucial role in enabling V2X communication in 6G networks. Moreover, these standards must be designed to address the specific challenges and requirements of V2X communication, such as real-time data transmission, reliability, and security. Therefore, ensuring data integrity and reliability will continue to be a critical challenge in V2X communication in 6G networks, and the development of new techniques and standards will be necessary to meet data integrity challenges [95]. Table 4 provides a summarized view of above discussed research works.

D. AVAILABILITY IN V2X

Data availability is the ability of a communication system to ensure that data is accessible and usable when needed. In 6G networks, ensuring real-time data transmission and high network availability in V2X communication systems will remain critical requirements [96]. However, 6G networks are expected to introduce new capabilities and unconventional features to achieve the forecasted next generation QoS through technologies such as IRS, intelligent beamforming and NOMA [97]. These techniques can help to ensure that data is transmitted reliably and with low latency, even in the presence of interference. The study [98] suggested, in order to ensure that the system can provide a consistent level of performance across different channel qualities, the count of reflecting elements used to serve users near or far can be derived based on the specific channel conditions in IRS enabled V2X communication. It can improve availability through optimized power allocation to maximize the sum-rate of data transmission to all users. However, the performance of IRS is heavily dependent on the availability and accuracy of channel state information (CSI). Any errors or uncertainties in CSI can affect the performance of IRS, particularly in dynamic V2X environments where the channel conditions are constantly changing. Likewise, the authors in [99] proposed an optimization framework for reducing the total transmit power of Backscatter (BC)-NOMA cooperative V2X networks while ensuring the quality of service. This framework involves jointly optimizing the transmit power of both the base station and the roadside units, along with the reflection coefficient, to minimize the overall transmit power. The optimization is performed using an iterative sub-gradient method by iteratively updating the optimization variables until minimum transmission power is achieved under both perfect and imperfect channel state information.

Similarly, out of several key features of 6G communication will be their ability to support ultra-low latency and high-bandwidth communication in real-time data transmission in V2X communication systems. Therefore. V2X in 6G networks must be designed to leverage low-latency and handle high-bandwidth connectivity to support time-critical applications such as emergency services and collision avoidance [100]. Moreover, 6G networks are designed to provision massive numbers of connected devices, which presents scalability challenges for ensuring high network availability in V2X communication. Therefore, integrated and heterogeneous scenarios of a large number of devices and users in 6G require maintaining high availability to minimize the impact of downtime on V2X communication systems [101]. The authors in [102] proposed a framework called Federated Learning and edge Cache-assisted Cybertwin (FLCC) for providing individual user-specific services in 6G-V2X. The FLCC framework utilize both edge cooperation and optimizations by employing a Federated Multi-agent Deep Reinforcement Learning-based (FM-DRL) algorithm. The framework augments the network availability by a caching mechanism based on the Federated Reinforcement Learning-based Edge Caching (FREC) algorithm to acquire the required training datasets with minimum bandwidth and computational load on resource-constrained systems in vehicles. FL involves training models on distributed data, which raises concerns about data privacy and security. However, the proposed FLCC framework requires incorporation of appropriate privacy-preserving measures such as Differential Privacy (DP), Secure Multi-Party Computation (SMPC) and Homomorphic Encryption (HE) to protect user privacy from inference attacks.

In 6G networks, ensuring data availability in V2X communication becomes even more crucial due to the growing demand for high-speed, reliable communication services. To support time-critical applications; therefore, V2X communication systems must be designed with redundancy and fault tolerance mechanisms to handle the event of hardware or software failures and minimize downtime of critical services [103]. The study [104] suggested a Byzantine-Fault-Tolerant Consensus via Reinforcement Learning (RL) for permissioned Blockchain implementation to optimize the mobility during blockchain transactions in a V2X communication. The proposed scheme performs optimum channel selection and switching by a vehicle as a fault-tolerant measure for maximum availability in the network. Byzantine fault tolerance algorithms typically require a large amount of computational resources to achieve consensus. This can be a limiting factor for systems with limited resources or high-performance requirements. Moreover, Byzantine fault tolerance assumes that nodes in the system can detect and isolate malicious behavior. Therefore, it can be difficult to detect and respond to malicious behavior, particularly if the behavior is sophisticated or disguised.

Similarly, to ensure network availability, V2X communication systems in 6G networks should consider continuous real-time monitoring techniques to identify issues [105]. Moreover, load balancing techniques are potential solutions to distribute traffic across multiple nodes to ensure that no single node becomes overwhelmed, which helps ensure that data services remain available even under heavy load. V2X communication systems must be designed with intelligent load-balancing schemes to handle increasing

volumes of data from multiple devices and support a growing number of users without compromising on data availability [106]. QoS mechanisms are also essential for ensuring data availability in V2X communication to prioritize time-critical applications, such as emergency services and collision avoidance. To withstand interference from other wireless networks and environmental factors, V2X communication systems in 6G networks must be designed with resiliency to interference. The authors in [107] propose an algorithm for scheduling multiple users in 6G ultra-massive MIMO systems in V2X communication using block diagonalization (BD) precoding techniques, which are sensitive to the correlation between channels. The algorithm uses a mathematical technique called the Pearson coefficient to calculate the channel matrix into a vector form to measure the channel quality based on their noise enhancement factor. The algorithm jointly considers the correlation between the channels of different users and their channel quality to select the users with the highest quality channels while minimizing the correlation between channels. This approach ensures that high-quality channels are selected while reducing interference between channels due to correlation. However, the Pearson coefficient measures the linear association between variables but does not capture the strength or direction of the relationship. This can limit its usefulness in complex heterogenous networks where the strength or direction of the correlation is important. Moreover, the coding scheme BD requires a significant amount of computation, particularly for large MIMO systems. This can be a limiting factor for real-time applications or systems with limited computational resources such as IoVs.

Moreover, the associated technologies in 6G communication such as cloud computing, SDN, network virtualization, AI and fog computing can provision backup and recovery procedures in V2X to restore data services quickly in the event of a failure and minimize downtime [108]. Table 5 provides a summarized view of above discussed research works.

E. AUTHENTICATION IN V2X

Data authentication is to verify the identity of the sender and confirm that the data is not tampered with in the process of transmission. V2X communication requires fast and reliable authentication mechanisms to ensure that time-critical applications such as emergency services and collision avoidance can be supported. Authentication mechanisms must be designed to work quickly and efficiently to minimize delays and ensure that data is transmitted in real-time [109]. The authors in [110] proposed a multicast service model for vehicles to securely connect them to a content provider using distributed keys in RAN enabled mobile network. The proposed scheme ensures authentication and protection of multicast service data and key distribution while maintaining anonymity and protocol attack resistance. However, as the number of group members increases, the complexity of managing group keys and member authentication also increases, causing scalability issues. Moreover, the compatibility of the multicast authentication scheme with different network architectures and technologies can be a challenge, particularly in heterogeneous network environments.

In the context of 6G networks, the challenges and requirements for data authentication in V2X communication are complex as compared to previous generations of wireless networks. 6G networks are expected to introduce new capabilities and features that may impact the design and implementation of authentication mechanisms such as AI, quantum computing, fog computing etc [111]. The authors in [112] propose a blockchain-based scheme for cellular vehicle-to-everything (C-V2X) ecosystems in the context of 6G networks. The scheme utilizes network function virtualization (NFV) to optimize edge-resource allocation. Further, the data aggregation through 6G sensors is securely performed at the data plane, and the aggregated data is transmitted to the NFV control plane. The aggregated data is then used to allocate resources to connected autonomous smart vehicles (CASVs) through edge nodes.

TABLE V
THE PROMINENT RESEARCH WORKS ON AVAILABILITY IN V2X.

Ref.	Technique	Attributes	Limitations
[98]	CSI in IRS	• Provides a consistent level of performance • Optimized power allocation to maximize the sum-rate of data	• Heavily dependent on the availability and accuracy of CSI • Errors or uncertainties in CSI can affect the performance
[99]	BC-NOMA	• Joint optimization of the power at both BS and RSUs • Iteratively updating the optimization variables until minimum transmission power	• Coverage and reliability of the system • Channel estimation issue in high mobility or multipath fading
[102]	FLCC	• Focused on personalized service • Optimized edge cooperation • Enhanced caching mechanism • Minimum bandwidth and computational	• Vulnerable to inference and model poisoning attacks without appropriate privacy-preserving measures
[104]	BFTC visa RL and Blockchain	• Performs optimum channel selection and switching • Optimize the mobility during blockchain transaction	• Require a large amount of computational resources • Assumed implementation of detection and response to malicious behavior
[107]	Pearson coefficient	• Calculate the channel matrix into a vector form to measure the channel quality • Reduced interference	• Not compatible with complex heterogeneous networks • Requires a significant amount of computation

The proposed scheme provides an efficient and secure method for data aggregation and resource allocation, which is essential for the reliable operation of CASVs in C-V2X ecosystems. However, allocating resources efficiently and effectively to different NVFs can be a challenging task, particularly in large-scale networks. Moreover, ensuring compatibility between different VNFs from different vendors can be a challenging task, particularly in heterogeneous network environments.

One of the key features of 6G networks is their ability to support ultra-low latency and high-bandwidth communication, which is essential for time-critical applications such as V2X communication. Therefore, authentication mechanisms must be designed to incur minimum delay to ensure that data is transmitted in real-time [113]. The authors in [114] propose a secure authentication scheme for vehicle-to-everything (V2X) communication, which aims to provide a high degree of security in different types of vehicular communication (V2V, V2I, V2N). The proposed approach uses lightweight cryptographic algorithms to safely receive all keys and messages from roadside units (RSUs), vehicles, and the network. The proposed scheme provides an efficient and secure method for authenticating V2X communication while ensuring lower computation and operational costs. However, Lightweight cryptographic algorithms are designed to be computationally efficient, but they may not provide the same level of security in emerging quantum computing paradigms in 6G networks.

In addition, 6G networks are expected to introduce new security threats, such as quantum-based attacks, that may require the development of new authentication mechanisms [115]. Similarly, privacy concerns are also expected to be a key consideration in 6G networks, given the sensitive nature of the data exchanged during authentication in V2X communication. Therefore, authentication mechanisms must be designed to protect user privacy and prevent unauthorized access to sensitive data [116].

The authors in [117] propose a group-based handover authentication strategy for 6G heterogeneous networks to improve efficiency and security. The system includes the user equipment (UE), access points such as gNB and eNB, authentication servers and blockchain. To access network services, the UE must first perform initial authentication and key negotiation with the local server. The proposed scheme then performs handover authentication and batch authentication for individual and group users, depending on the number of users. The scheme uses blockchain and aggregated signature technologies to achieve global switching authentication and D–H key exchange to enhance security and decrease one-by-one authentication time. However, Implementing and managing aggregated signatures can be a complex task, particularly in terms of key management and secure communication. Similarly, aggregated signatures can introduce performance overhead due to the additional computation and communication required for signature aggregation, which can affect the overall performance of the system.

Moreover, the limited computational resources of vehicles and devices participating in V2X communication may pose challenges to the design and implementation of authentication mechanisms in 6G networks [118]. Therefore, only resource-efficient authentication mechanisms are expected to work efficiently to minimize the impact on device performance. Similarly, secure key management mechanisms are the most complex part of authentication in V2X communication systems for ensuring that only authorized entities can access and use encryption keys [119]. Likewise, digital signatures are suitable to authenticate data and ensure tampered-free transmission in V2X communication [120]. V2X communication systems are expected to be compatible with digital certificates to ensure compatibility with legacy security architecture. Digital certificates provide a way to verify the identity of the sender and ensure that data is transmitted securely through trust in a Certification Authority (CA). V2X communication systems can use certificates for secure communication protocols such as TLS (Transport Layer Security) [121]. Table 6 provides summarized view of above discussed research works.

TABLE VI
THE PROMINENT RESEARCH WORKS ON AUTHENTICATION IN V2X.

Ref.	Technique	Attributes	Limitations
[110]	Multicast service model	• Protection of multicast service data and key distribution • Maintains anonymity and protocol attack resistance	• Complex key management • Scalability issues • Compatibility issues in a heterogeneous network
[112]	Blockchain	• Utilizes NFV to optimize edge-resource allocation • Secure data aggregation • Efficient resource allocation	• NVF has scalability issues • Compatibility issues between different VNFs
[114]	Lightweight cryptography	• low computation and operational costs • Secure distribution of all keys and messages from RSUs	• Vulnerable to quantum computing based attacks
[117]	Group-based handover with blockchain	• Performs handover authentication and batch authentication • Uses aggregated signature and D–H key exchange for global switching	• Increased complexity • Requires high computational resources

F. ACCESS CONTROL IN V2X

Access control refers to the process of controlling the actions a user can take after authentication in a network or system. Access control systems typically use a set of allowed or prohibited rules or policies to restrict the actions for a given user or group of users. The purpose of access control is to limit the scope of an authenticated user in a system or resource. Access control in V2X communication in 6G networks faces several challenges due to the unique characteristics of the communication environment [122]. V2X communication in 6G networks may involve a wide range of devices with different communication capabilities and security requirements. Access control mechanisms in V2X communication are required to work seamlessly across these heterogeneous devices and ensure that only authorized entities can access sensitive data [123]. The authors in [124] proposed a blockchain-based access control ecosystem for managing large data sets and protecting against data breaches. The ecosystem gives asset owners sovereign control over access control. The Linux Foundation's Hyperledger Fabric blockchain to implement smart contracts or transaction processing functions. By using a blockchain-based access control ecosystem, the proposed system offers enhanced security, transparency, and immutability than traditional access control systems. However, although Hyperledger Fabric supports private channels and transactions, the level of privacy is not as strong as some other blockchain platforms. Moreover, Hyperledger Fabric it may not scale well for extremely high transaction volumes in dense and massive 6G V2X connectivity.

Massive connectivity is the hallmark of 6G communication, which presents scalability challenges for access control mechanisms. Access control mechanisms in V2X communication must be designed to scale up to support large numbers of devices and users while maintaining efficient and reliable operation [125].

The authors in [126] proposed a protocol called Network Coding-based Medium Access Control protocol (NC-MAC) for supporting V2V beacon broadcasting using distributed network coding. The protocol combines feedback mechanisms, the process of retransmission and coding in the network to improve broadcasting reliability. The NC-MAC protocol improves communication reliability and scalability in various situations, including roads with clusters of urban vehicles. However, network coding introduces additional overhead due to the need for encoding and decoding packets, which can increase latency and reduce throughput. Moreover, network coding introduces new security challenges, such as the potential for attacks on the coding coefficients used for packet encoding and decoding.

Likewise, V2X communication in 6G networks must support real-time applications such as autonomous driving and traffic management. Access control mechanisms is to operate quickly and efficiently to minimize delays and ensure that real-time applications can be supported [127] . Moreover, 6G communication may face several unconventional security threats, including hacking, data breaches, and denial-of-service attacks. Therefore, critical safety requirements of V2X communication necessitate robust access control mechanisms to detect and prevent these threats [128]. The authors in [129] proposed a multi-dimensional Discrete-Time Markov Chain (DTMC)-based models for analyzing the efficiency of IEEE 802.11p and C-V2X Mode 4 protocols at MAC layer. The models consider periodic cooperative awareness messages (CAMs) and event-driven (decentralized environmental notification messages) DENMs, to obtain closed-form solutions for the steady-state probabilities. The solution includes expressions for key performance metrics for performance enhancements for both standards IEEE 802.11p and C-V2X Mode 4 in terms of delay, collision probability, and channel utilization. However, DTMC models assume that the system has no memory, meaning that the future state of the system depends only on the current state and not on the past. This assumption may not hold in all cases and can limit the accuracy of the model predictions. Moreover, multi-dimensional DTMC models arehighly complex and require significant computational resources to solve and analyze which can be a challenge for resource-constraint IoVs.

TABLE VII
THE PROMINENT RESEARCH WORKS ON ACCESS CONTROL IN V2X.

Ref.	Technique	Attributes	Limitations
[124]	Hyperledger Fabric blockchain	• High security, transparency, and immutability • Gives sovereign control to asset owners	• Hyperledger Fabric is less strong as compared other blockchains • Scalability issues in massive connectivity
[126]	NC-MAC	• Performs V2V beacon broadcasting using distributed network coding • Combines feedback mechanisms, retransmissions, and network coding • improves reliability and scalability	• Additional overhead due to encoding • Increased latency and reduce throughput • Vulnerable to encoding based attacks
[129]	DTMC	• Analyzes MAC layer performance of IEEE 802.11p and C-V2X Mode 4. • Employs CAMs and DENMs for the steady-state probabilities	• Limited accuracy of the model predictions due no memory • require significant computational resources • Increased complexity
[130]	IND-sID-CCA	• DL-based techniques to filter malicious packets • Identity-based encryption	• Computationally intensive • Limited scalability • Compatibility issues

Similarly, V2X communication involves the exchange of sensitive data, which raises privacy concerns. Therefore, access control mechanisms must be designed to protect user privacy and prevent unauthorized access to sensitive data [131]. The authors in [130] proposed a solution for the incorporation of an authentication mechanism for addressing the security issues in VANETs. The approach uses identity-based encryption for access control and deep learning-based techniques to filter malicious packets. The identity-based encryption technique INDistinguishability under selective-ID Chosen-Ciphertext Attacks (IND-sID-CCA) secure along with the deep learning algorithm provides accuracy of 99.72% to detect malicious packets. However, IND-sID-CCA secure IBE systems can be computationally intensive, especially for large-scale deployments with many users. This can impact the system's performance and scalability. Moreover, IND-sID-CCA secure IBE systems may not be compatible with other security mechanisms or protocols, which can limit their interoperability with other systems. V2X communication in 6G networks must comply with regulations such as data protection laws, which may present challenges for access control mechanisms. Access control mechanisms must be designed to comply with these regulations while ensuring that data is transmitted securely [132]. Table 7 provides a summarized view of above discussed research works.

IV. V2X SECURITY IN EMERGING TECHNOLOGIES

As we approach the 6G era, several emerging technologies are poised to transform the way devices communicate and interact with each other. The most prominent of these technologies, blockchain and FL are particularly most impactful. In subsequent subsection, this article elaborates the impact of these technologies on 6G enabled V2X communication.

A. BLOCKCHAIN IN 6G ENABLED V2X

Blockchain is a distributed ledger technology that enables secure and transparent transactions without the need for intermediaries. It is often associated with cryptocurrencies like Bitcoin, but its potential extends beyond finance. In a 6G context, blockchain could be used to securely and efficiently manage the vast amounts of data generated by the network devices that will be ubiquitous in the 6G era. One of the key benefits of blockchain is its ability to establish trust in a decentralized network. Each block in the chain contains a cryptographic hash of the previous block, making it impossible to modify or tamper with the data stored in the chain. This immutability makes blockchain an ideal platform for securing sensitive data and ensuring that it is not tampered with [133]. The authors in [134] proposed a blockchain based solution that involves developing a formal mathematical model for a system that considers the interconnectedness of objects and V2X information channels. The solution also includes an algorithm that is designed to efficiently offload traffic to a mobile edge computing (MEC) server. The focus of the work is on energy efficiency, which is an important consideration in V2X communication. The proposed work aims to improve the efficiency and effectiveness of V2X communication in terms of data transfer and processing. The proposed work has the potential to contribute to the advancement of V2X technology and could have practical applications in areas such as smart transportation systems.

Blockchain is an emerging technology that could play a significant role in enabling secure and efficient V2X communication. One of the primary challenges of V2X communication is ensuring the security and privacy of the data transmitted between vehicles and infrastructure. Blockchain is a distributed ledger technology that offers a secure and transparent way to manage data. By using blockchain, V2X communication can be made more secure, transparent, and tamper-proof. In a blockchain-based V2X system, each vehicle and infrastructure node would have a unique digital identity, which would be recorded on the blockchain. The blockchain would then be used to manage the communication between nodes, ensuring that data is only shared with authorized parties [20].

Another benefit of blockchain-based V2X communication is that it enables the creation of decentralized applications that can run on a blockchain network, enabling secure and transparent transactions without the need for intermediaries. In the context of V2X communication, decentralized applications could be used to enable secure and efficient micropayments between vehicles and infrastructure, such as tolls or parking fees. Furthermore, blockchain could enable the creation of new business models and revenue streams in the V2X ecosystem.

For example, a blockchain-based V2X system could allow vehicle owners to monetize their data by sharing it with authorized third parties in exchange for compensation [135]. The authors in [136] proposed a method for integrating blockchain technology into vehicular networks to improve cybersecurity. The proposed method uses a decentralized, collaborative system to dynamically create communities that can revoke malicious vehicles in real-time, which helps to address challenges such as Sybil and faking position attacks. The article presents analytical models of the system of real-time revoking certificates and examines the solution's impact on these types of attacks. The proposed method was tested using real V2X hardware, and the experiments demonstrated the feasibility and benefits of real-time revocation via vehicle communities.

However, several challenges need to be addressed before blockchain can be effectively implemented in V2X communication, including issues related to scalability, privacy, interoperability, standardization, and the integration of blockchain with existing V2X systems. Overcoming these challenges will require collaboration between industry stakeholders, as well as further research and development in the field of blockchain technology for V2X communication.

B. FEDERATED LEARNING IN 6G ENABLED V2X

6G networks are considered intelligent networks because they are expected to be designed with advanced technologies, such as artificial intelligence (AI), machine learning, and edge computing. These technologies enable the network to adapt to changing user needs and dynamically allocate network resources to support various applications and services. Intelligent networks are designed to be more flexible, resilient, and efficient than traditional networks. They can automatically adjust to changing traffic patterns and optimize the use of network resources, providing faster and more reliable connectivity to users. Additionally, intelligent networks can provide new services and applications that were not possible with earlier generations of wireless networks [137].

FL is a machine learning technique that allows multiple devices to collaboratively learn from a shared model while keeping their data private. In the context of V2X communication, federated learning could be used to train machine learning models on the massive amounts of data generated by vehicles and infrastructure, leading to more accurate predictions and better decision-making[138]. The authors in [139] propose a new approach called consensus-driven FL (C-FL) for PointNet-compliant deep ML architectures and Lidar point cloud processing for road actor classification. The approach is modular and decentralized, which is evaluated by simulating a V2X network based on the Collective Perception Service (CPS) for mutual sharing of the PointNet model parameters. The performance evaluation considers the impact of the vehicular network's degree of connectivity, the benefits of continual learning, convergence time, and loss/accuracy tradeoffs with heterogeneous training data. The proposed method has the potential to improve the accuracy and efficiency of road actor classification in V2X networks by leveraging a decentralized approach to FL.

One of the primary challenges of V2X communication is ensuring the privacy of the data transmitted between vehicles and infrastructure. Federated learning allows for the training of machine learning models without the need for data to be shared, thus ensuring data privacy. Instead, the machine learning models are sent to the devices themselves, which then contribute their learnings back to the central model. This approach ensures that sensitive data is not exposed, while still allowing for the creation of accurate machine learning models [140].

Moreover, FL enables distributed machine learning, allowing for more efficient use of computational resources. Instead of relying on a central server to train machine learning models, FL distributes the workload across multiple devices, resulting in faster and more efficient training. This distributed approach is particularly useful in the context of V2X communication, where the amount of data generated is massive and constantly growing [141]. The authors in [142] proposed a novel privacy-preserving computing model called AFLPC, which is designed for asynchronous FL in 5G-V2X scenarios. The model utilizes an adaptive differential privacy mechanism to protect data privacy while minimizing noise. Additionally, we proposed a weight-based asynchronous FL aggregation update method that controls the proportion of parameters submitted by users with different training speeds and updates the aggregation parameters of lagging users to reduce the negative impact on the model caused by varying speeds. Experiments demonstrate that the proposed approach effectively ensures the credibility and privacy of asynchronous federated learning in 5G-V2X scenarios while improving the model's utility.

Similarly, FL could be used in the creation of predictive maintenance models for vehicles. By using machine learning models trained on data from multiple vehicles, predictive maintenance models could be developed that identify and predict issues before they occur. This approach could help to reduce maintenance costs, improve vehicle safety, and prolong the life of vehicles [143]. However, FL in V2X communication faces several challenges, including the heterogeneity of data and the varying computational capabilities of the different vehicles and roadside units. Similarly, ensuring the privacy of the data while facilitating effective collaboration among the participants is also a significant challenge. Moreover, communication problems such as high latency and intermittent connectivity can also impact the learning process. Likewise, maintaining consistency and accuracy of the learned model across all participants while managing the efficient aggregation of model updates from different sources is also a challenge. Additionally, avoiding overfitting and data imbalance is crucial to ensure that the learned model generalizes well to new data.

C. BLOCKCHAIN ENABLED FL BASED SECURITY IN 6G ENABLED V2X

The incorporation of blockchain technology and FL can significantly enhance their roles within 6G scenarios when compared to their utilization in 5G contexts. In 6G, blockchain can play a crucial role in securing and managing the vast amount of data generated by an even more extensive network of connected devices. Its decentralized, immutable ledger can provide a trust layer for transactions and data exchange, ensuring data integrity and privacy, which is especially vital in the context of critical applications like autonomous vehicles and remote healthcare. FL, on the other hand, becomes more relevant in 6G due to its ability to train machine learning models across a multitude of edge devices while preserving data privacy. This becomes essential as 6G supports a massive number of IoT and edge devices, making it inefficient and potentially insecure to centralize data for training. Federated learning allows devices to collaboratively train models while keeping data on the device, mitigating privacy concerns.

Blockchain-enabled FL is a potential approach to improve the security architecture of 6G-enabled V2X communication

networks. The FL framework uses a distributed learning approach where multiple devices collaborate to train a shared model without sharing sensitive data. The blockchain component is used to ensure the integrity of the learning process and to manage access to the shared model. This architecture can enhance the privacy and security of V2X networks by ensuring that sensitive data remains secure while still allowing for the efficient sharing of knowledge. With the implementation of blockchain-enabled FL, V2X networks can achieve a higher level of security, which is crucial for the safe and reliable operation of autonomous vehicles and other connected devices [144].

Intelligent connected vehicle (ICV) generate vast amounts of data within the V2X environment, which can be harnessed securely and efficiently through decentralized techniques such as FL. However, traditional FL systems are susceptible to attacks and fail to meet the security requirements for practical use. If compromised or malicious ICV uploads incorrect or low-quality local model updates to the central aggregator, this could lead to a decrease in the accuracy of the global model, which would reduce drivers' safety and efficiency. Therefore, ensuring the security of FL in V2X environments is critical to protecting the privacy of drivers and enhancing the reliability and safety of the overall system.

The increasing use of software and wireless interfaces in the vehicular networks built by interconnected vehicles and transportation infrastructure has made them susceptible to cyber-attacks. To mitigate this risk, intrusion detection systems (IDSs) can be customized to efficiently detect such attacks. Machine learning approaches have made significant progress in detecting malicious attack traffic in vehicular networks. In the study [145] a cooperative intrusion detection mechanism is proposed that involves distributing the training model to edge devices such as connected vehicles and roadside units (RSUs). By using a federated-based approach, the resource utilization of the central server is reduced, while maintaining security and privacy. The proposed mechanism also utilizes blockchain for the storage and sharing of the training models to ensure the security of the aggregation model. Through this approach, the training process becomes more efficient and secure, making it suitable for use in distributed environments with limited computing resources.

It is important to note that none of the existing blockchain-enabled FL solutions have fully addressed and examined the security architecture requirements in the CIA^3 domain. This means that current solutions may not provide a robust and comprehensive security mechanism to protect the integrity and privacy of the data during the FL process. There is a need for an integrated security architecture that covers all aspects of the CIA^3 domain to ensure a secure and reliable FL system that can be applied to various use cases, including in the ICVs. Therefore, in the next section, this study presents a Blockchain enabled FL based generic security architecture for V2X communication.

D. PROPOSED GENERIC SECURITY ARCHITECTURE

Blockchain and FL technologies are emerging as joint manifestations of secure intelligent networks in 6G communication. FL can improve the privacy of blockchain networks by allowing multiple entities to collaborate on training machine learning models while keeping their data decentralized and secure. This means that sensitive data remains on local nodes and is not shared across the entire blockchain network, reducing the exposure of data to potential security breaches This proposed architecture considers the security requirements of CIA^3 domains as a highly dynamic phenomenon due to heterogeneous network and vehicular domains such as IoV, V2V communication, infrastructure, Vehicle to UAV links etc. Extremely foolproof and strong security measures result in various compromises to legitimate uses, complexity, network overload and computational costs. Therefore, the proposed architecture suggests the employment of Blockchain as foundational implementation through CIA^3; However, the dynamic requirements are to be controlled, monitored and adjusted through FL techniques for the least compromise on legitimate users and network services. The proposed architecture suggests real-time modification in security settings and security protocol through FL. The proposed architecture stands to provide a broader prospect in the context of 6G communication networks. It suggests a unique approach to addressing security concerns by combining blockchain and Federated Learning technologies. While both blockchain and FL have been used in various domains, their joint application in the context of secure intelligent networks for 6G communication is relatively new and represents a novel approach to enhancing security and privacy.

E. DESIGN OF PROPOSED ARCHITECTURE

The proposed architecture suggests a hierarchical implementation of FL, starting from IoV (e.g., connected vehicles) and extending to core networks (e.g., cloud servers). The goal of FL models in this architecture is to learn from available data and real-time scenarios to generate an efficient hierarchy. This includes selecting the optimal Roadside Units (RSUs), vehicles, and other infrastructure as part of the FL process. These local models are then hierarchically aggregated and updated in a cluster-level global model, and ultimately in an overall global model. The proposed architecture also takes into consideration the selection of optimum miners for the Blockchain, a decentralized ledger technology that can be used for secure data sharing and verification in FL. The security settings for the FL process, such as confidentiality, integrity, authentication, and access control, are adjusted based on the specific requirements of the different services and applications in the IoV ecosystem. Moreover, the security domain in CIA^3 does not need to be simultaneously covered for all aspects of FL in the proposed architecture. For example, in the case of safety and hazard-related information broadcast, confidentiality may not be a primary requirement, but integrity

and authentication are necessary. Access control requirements are also continuously changing based on the type of vehicles and corresponding services, such as law enforcement, health services, disaster management, schools, etc.

The primary use of blockchain technology is authentication and integrity based on immutability and distributed ledger. This means that blockchain is commonly used to ensure that data is secure, cannot be altered, and is stored across a network of computers, making it tamper-proof. However, availability, confidentiality, and access control can be added to the blockchain through conventional schemes. This implies that traditional security measures can be used in conjunction with blockchain to enhance its functionality and security. The relationship between these conventional security schemes and blockchain, as well as any adjustments needed, will be governed through FL. The implementation of blockchain in a holistic manner can result in challenges related to resource utilization. This means that effectively utilizing resources such as computing power, storage, and network bandwidth may be difficult in a comprehensive blockchain implementation.

Similarly, the major aim of FL in the context of blockchain implementation is to optimize the adjustment of the blockchain based on several features extracted from V2X communication systems. V2X communication systems allow vehicles to communicate with each other, as well as with infrastructure and other entities, for various purposes such as improving road safety and traffic efficiency. Some of the features that can be used for optimizing blockchain implementation, such as the number of vehicles, vehicle concentration, perceived threat, available resources, interference, vehicle speeds, and load balancing. These features can provide valuable insights and data points for adjusting the blockchain implementation to better meet the specific needs and requirements of the V2X communication systems. The number of vehicles and vehicle concentration can indicate the scale of the V2X communication system, and adjusting the blockchain accordingly can help ensure efficient data processing and storage. Perceived threat refers to the potential risks and vulnerabilities in the V2X communication system, and optimizing the blockchain implementation can enhance security measures to mitigate these threats. Similarly, Available resources, interference, and vehicle speeds can impact the performance and efficiency of the V2X communication system, and optimizing the blockchain can help ensure optimal resource allocation and data transmission.

However, the integration of blockchain technology and FL holds significant promise in addressing compatibility challenges within the dynamic V2X environment and the complex 6G heterogeneous networks. By utilizing blockchain's decentralized and tamper-resistant nature, data integrity and security can be ensured in V2X communications, fostering trust among vehicles, infrastructure, and users [146]. FL complements this by enabling collaborative model training across various network nodes without centralized data sharing, preserving individual privacy and reducing communication overhead. This combination allows for real-time updates and model refinements to adapt to the rapidly changing conditions of V2X and 6G networks, enhancing overall system efficiency and responsiveness [147].

FL will enable adjustments in the blockchain implementation based on features extracted from the local data of the collaborating entities. This means that each entity will adjust the blockchain implementation based on its specific needs, requirements, and local conditions, leading to a more customized and optimized blockchain network. Moreover, FL will facilitate interoperability between different blockchain networks by allowing entities to collaborate on machine learning models without sharing their data. This can enable cross-chain collaborations and data sharing, leading to enhanced interoperability between different blockchain networks. Similarly, Blockchain's decentralized and tamper-resistant nature could enhance data integrity and authentication within VLC networks, safeguarding sensitive information exchanged between vehicles and infrastructure. Additionally, FL, with its privacy-preserving capabilities, might enable collaborative model training while preserving individual data privacy. However, challenges such as the high computational demands of Blockchain and FL, as well as the latency-sensitive nature of V2V and V2I communication, should be carefully addressed for practical implementation. Thus, while the concept holds promise, a thorough analysis of performance, efficiency, and real-time constraints is imperative before adopting this security architecture in VLC systems [139]. Moreover, implementing a smart transportation system with unique digital identities using VLC and blockchain requires a systematic approach. Each vehicle and infrastructure node would be equipped with a unique digital identity, possibly through RFID tags or QR codes, which would be associated with their VLC transmitters. These digital identities ensure that each entity is distinguishable and can be tracked. VLC technology utilizes light signals for communication. Each entity's VLC transmitter would encode data into light signals, such as LED light pulses. These signals can carry information like location, status, and identity, enabling communication between vehicles and infrastructure nodes. The generated data from VLC communication, including digital identities and relevant information, would be securely stored on a blockchain. As VLC communication can be affected by environmental factors, a consensus mechanism is crucial to validate the accuracy of transmitted data [148].

The association of digital identities with corresponding VLC devices can be achieved through a process known as device registration. During registration, each VLC device is assigned a unique identifier that serves as its digital identity. When a VLC device is powered on and initiates communication, it broadcasts its digital identity along with its operational parameters, allowing receiving devices to recognize and establish an association with it. This association enables secure and accurate communication between VLC devices within the network [149].

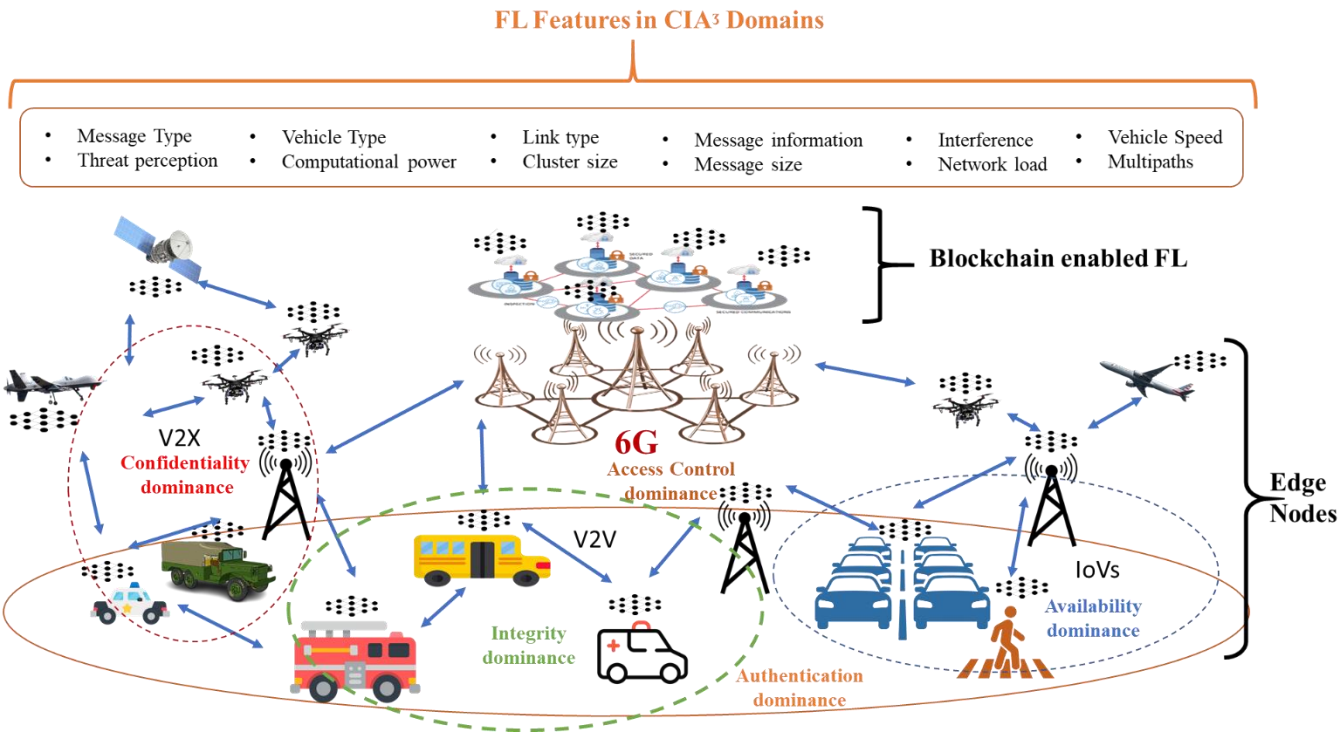

FIGURE 6. **Proposed Architecture for FL enabled V2X communication with Security dominance clusters**

The proposed architecture aims to intelligently identify the security implementation requirements and ensure the security should be as per the dominating domain out of all the CIA^3 domains. It is particularly observed that Authentication is a holistic requirement. However, other domains switch their dominance as per the infrastructure and the participating entities. The design of the proposed architecture has been pictorially presented in Figure 4. The effectiveness of the proposed architecture would involve a combination of technical testing, evaluation against established metrics, user feedback, and validation through the academic and research community. In this review, the architecture has been proposed to demonstrate that the novel approach has the potential to provide a secure, privacy-preserving, and efficient solution for 6G networks in the context of dynamic security requirements of FL and blockchain enabled V2X communication.

F. KEY ADVANTAGES OF PROPOSED ARCHITECTURE

The proposed architecture, which combines blockchain and FL technologies for secure intelligent networks in 6G communication, offers several key advantages over traditional architectural models:

1) IMPROVED PRIVACY

One of the primary advantages is enhanced privacy. Traditional architectural models may involve centralized data storage and processing, which can pose risks to data privacy. In the proposed architecture, FL allows multiple entities to collaborate on training machine learning models without sharing their sensitive data across the entire network. This decentralized approach minimizes the exposure of data to potential security breaches and enhances privacy.

2) CUSTOMIZATION AND ADAPTABILITY

The architecture allows for real-time modification of security settings and protocols through FL. Each entity can adjust the blockchain implementation based on its specific needs and requirements, resulting in a more customized and optimized network. This adaptability is crucial in addressing the dynamic security requirements of 6G communication.

3) EFFICIENT RESOURCE UTILIZATION

Traditional blockchain implementations can pose challenges related to resource utilization, including computing power, storage, and network bandwidth. The proposed architecture aims to optimize the blockchain based on features extracted from V2X communication systems, such as the number of vehicles, perceived threats, available resources, and more. This optimization helps ensure efficient resource allocation and data processing.

4) ENHANCED DATA INTEGRITY AND SECURITY

Blockchain's decentralized and tamper-resistant nature is leveraged to ensure data integrity and security in V2X communications. The combination of blockchain and FL enables real-time updates and model refinements to adapt to changing conditions, enhancing overall system efficiency and responsiveness.

5) INTEROPERABILITY

The architecture facilitates interoperability between different blockchain networks by allowing entities to collaborate on machine learning models without sharing their data. This enables cross-chain collaborations and data sharing, which can enhance interoperability between different blockchain networks.

6) UNIQUE DIGITAL IDENTITIES

The use of unique digital identities for vehicles and infrastructure nodes, associated with VLC transmitters and securely stored on the blockchain, helps distinguish and track entities. This can improve the accuracy and security of VLC communication.

7) FLEXIBILITY BASED ON DOMAINS

The proposed architecture intelligently identifies the security implementation requirements and adapts based on the dominating domain within the CIA^3 (Confidentiality, Integrity, Authentication, Availability, Access Control) framework. This flexibility ensures that security measures are tailored to the specific needs and conditions of different domains.

V. FUTURE RESEARCH DIRECTIONS

After a detailed overview of the existing research landscape in the above sections under the scope of secure V2X in 6G networks, we critically identified potential challenges and future research directions in subsequent paragraphs that require focus from both academia and industry to overcome these challenges

A. V2X ENABLED 6G NETWORK PRIVACY IN 3D FOG COMPUTING

Implementation of 6G-enabled 3D fog computing will require the deployment of unconventional heterogeneous infrastructure to support the massive amounts of data and extremely low latency connectivity [150]. The 6G enabled 3D fog computing for V2X communication would require a highly complex network infrastructure with multiple layers of communication nodes to enable seamless connectivity. This would require significant investment in infrastructure and maintenance to ensure that the network can handle the high volume of data transmission. This infrastructure will require scalable, reliable, and secure design [151]. Similarly, with the massive amounts of data generated by 6G-enabled 3D fog computing, effective security measures and data management will be essential to avoid vulnerabilities and cyber threats [152]. With the huge expansion in the use of connected devices, security becomes a major challenge for 6G enabled 3D fog computing for V2X communication. Hackers can exploit vulnerabilities in the system, resulting in data breaches or network failures. Ensuring data privacy and security in this scenario requires robust security measures at all levels of the network. Therefore, future research is required to develop algorithms and tools to process and analyze, the security strength of V2X 3D fog computing in 6G.

B. V2X 6G NETWORK PRIVACY IN AUGMENTED REALITY

Augmented reality (AR) is a potential technology to enhance V2X communication and provisions drivers with real-time conceivable data of the road infrastructure and vehicles around them, such as road conditions, traffic signs, and hazards, displayed directly in their field of view, without obstructing their view of the road. AR overlays real-time digital information on top of the physical environment, which may involve sensitive or personal information [22]. To ensure privacy, 6G-enabled V2X communication with AR should provide secure and privacy-protected data transmission, processing, and storage. Moreover, 6G-enabled V2X communication with AR requires a robust security mechanism to protect the data transmitted between vehicles and infrastructure, as well as the AR devices. This includes securing the communication channel, authentication, encryption, and intrusion detection and prevention. As augmented reality becomes more prevalent in V2X communication, it will be essential to develop privacy-enhancing technologies to protect sensitive information [153]. Future research could focus on developing new technologies such as secure multi-party computation, homomorphic encryption, and differential privacy to ensure data privacy. Future research could focus on developing new trust models and mechanisms that can effectively manage trust in the complex and dynamic AR enabled V2X environment.

C. SECURE SDN ARCHITECTURE IN V2X 6G NETWORK

SDN enabled architecture relies on a centralized controller to manage the network and enforce security policies. This creates a single point of failure and may increase the vulnerability of the network to attacks [154]. Moreover, SDN enabled secure architecture may face scalability issues when deployed in large-scale V2X networks. As the network grows, managing security policies and ensuring secure communication becomes increasingly complex, which may limit the ability of SDN-based security solutions to scale effectively [155]. Similarly, SDN is a relatively new technology, and security measures are still being developed. Conventional security measures that are available for traditional networks do not apply to SDN-based architecture in V2X 6G network, resulting in a gap in security measures that need to be addressed [156]. Moreover, the lack of standards can lead to inconsistencies in security measures and make it difficult to ensure compatibility between different systems. V2X communication involves the exchange of sensitive information, such as location data and personal identification. As the number of devices and entities in the V2X network increases, it becomes challenging to ensure secure authentication and access control. Therefore, it is important to develop secure and scalable mechanisms for

security framework to insure the requirement of CIA^3 model in SDN enabled V2X networks.

D. V2X PHYSICAL LAYER SECURITY IN THZ SPECTRUM

Accurate estimation of channel parameters is essential for secure V2X communication. However, the presence of obstacles, reflections, and multipath fading can lead to channel estimation errors, which can be used by attackers to exploit the security of the communication network [157]. Similarly, V2X communication relies on wireless signals, which can be easily jammed or interfered with, leading to disruption or complete breakdown of the communication [158]. Attackers can use jamming or interference to prevent legitimate communication or to force the communication to take a less secure route [159]. V2X communication relies on several physical layer techniques such as beamforming, MIMO, and OFDM, which can be vulnerable to attacks such as spoofing, frequency jamming, and injection attacks. These attacks can lead to data manipulation, interception, or destruction [160]. Future research is required to explore new MIMO beamforming algorithms that can optimize the transmission of secure V2X signals while minimizing the impact of interference. Similarly, new methods for channel modeling and estimation are can improve the efficiency and security of MIMO-based V2X communication.

E. V2X AND SUMO (Simulation of Urban MObility)

Integrating a security architecture based on both Blockchain and Federated Learning (FL) into the SUMO (Simulation of Urban MObility) simulator is feasible, though it demands careful attention to several critical aspects. Firstly, incorporating FL mechanisms within SUMO enables decentralized model training using data from various sources, enhancing privacy and efficiency. Secondly, integrating Blockchain protocols ensures secure and tamper-proof data sharing among connected vehicles and infrastructure. This decentralized trust model enhances data integrity and prevents unauthorized modifications [161]. Lastly, designing a simulated V2X communication infrastructure within SUMO is essential to accurately emulate real-world interactions, allowing for the testing and refinement of the security architecture in a controlled environment. This endeavor would necessitate a comprehensive approach that integrates FL, Blockchain, and V2X components seamlessly to address the complexities of urban mobility security effectively [162].

F. INTRUSION DETECTION IN V2X USING AI

In the context of V2X communications, leveraging machine learning techniques for anomaly detection, intrusion detection, and security analytics holds great promise. To effectively detect and mitigate emerging threats and attacks, a combination of supervised and unsupervised models should be employed. Supervised models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), can learn from labeled data to recognize known attack patterns. Unsupervised models like autoencoders and generative adversarial networks (GANs) can capture anomalies by learning the normal behavior of V2X communications and identifying deviations from them [163]. A hybrid approach integrating both types of models enables the system to detect and respond to both known and unknown threats, enhancing the robustness of the security framework. However, the primary challenge would be the availability of real-life datasets for optimally training the AI models.

VI. KEY LESSONS LEARNED

The main lessons learned from this study revolve around recognizing the potential of 6G communication for vehicular networks, understanding the security challenges and analyzing innovative solutions like Blockchain and Federated Learning by discussion on a generic architecture. The following subsections provide discussion on several key lessons learned from this study related to 6G communication for vehicular networks and its associated challenges.

A. TRANSFORMATIVE POTENTIAL OF 6G

The study highlights the importance of recognizing the transformative potential of 6G communication for vehicular networks. This implies understanding the significant advancements and capabilities that 6G can bring to V2X communication, which can have a profound impact on the transportation and automotive industry. 6G, the next generation of wireless technology, can revolutionize vehicular communication in several ways. Firstly, it underscores the importance of staying ahead of technological advancements, as 6G is poised to bring unprecedented capabilities in specific communication domains including, eMBB, SURLLC, UCDC, BigCom and 3DCom.

Secondly, recognizing 6G's potential emphasizes the need to invest in research and development. To harness the full benefits of 6G, research into its applications and security challenges is crucial. This lesson highlights the importance of continual innovation and exploration in the field of telecommunications and vehicular networks. Furthermore, understanding the transformative potential of 6G for vehicular networks also highlights the need for cross-disciplinary collaboration. Engineers, computer scientists, and transportation experts must work together to fully leverage 6G's capabilities. This underlines the significance of multidisciplinary approaches in addressing the complex challenges posed by 6G in V2X communication.

B. UNDERSTANDING SECURITY CHALLENGES

The study emphasizes the importance of understanding the security challenges posed by the expansion of V2X communication in the 6G era. As technology advances, it also introduces new vulnerabilities and risks that must be thoroughly comprehended to develop effective security solutions. One of the primary lessons is that the security

challenges in 6G vehicular networks are multifaceted and constantly evolving. As technology advances, so do the tactics of malicious actors. It is crucial to remain adaptive in security measures accordingly. Lessons from 6G security challenges include the need for continuous monitoring, enhancement in threat intelligence and the ability to adjust security protocols in real-time. Security Information and Event Management (SIEM) systems, anomaly detection algorithms, and real-time monitoring tools will play a vital role in identifying and mitigating security breaches

C. NEED OF INNOVATIVE APPROACHES

The rapid advancement of 6G technology demands innovative solutions to fully harness its transformative potential. Vehicular networks stand to benefit immensely from the low-latency, high-bandwidth capabilities of 6G. Secondly, the conventional methods for ensuring the confidentiality, integrity, and availability of data may no longer suffice in the 6G era. This is where innovative technologies like Federated Learning and blockchain come into play. Federated Learning enables collaborative machine learning without compromising sensitive data, while blockchain provides a secure and decentralized ledger for managing transactional data.

By integrating these technologies, an unconventional security architecture can be created, which not only safeguards V2X communication but also minimizes compromises on legitimate users and network services. To effectively address the security challenges in 6G V2X communication, an unconventional security architecture is deemed necessary. This architecture should incorporate Blockchain and Federated Learning to mitigate risks while ensuring the continuity of legitimate users and network services. The study suggests innovative architecture to emphasize the possibility for joint utilization of Blockchain and Federated Learning. Blockchain is proposed as a technology for creating a secure and decentralized ledger to manage transactional data, while Federated Learning is recommended for collaborative machine learning tasks that keep sensitive data localized. These solutions aim to enhance the security of V2X communication in 6G networks.

D. PROACTIVE SECURITY MEASURES

The study underscores the significance of proactively implementing security measures to ensure the safety and integrity of V2X communication. Waiting for security breaches to occur is not ideal; rather, a proactive approach to security is essential in the 6G era. the integration of advanced technologies such as Federated Learning, which allows collaborative machine learning while preserving data privacy, and Blockchain, which provides a secure and decentralized ledger, can significantly enhance the security of vehicular networks in the 6G era. These technologies enable not only data protection but also the creation of trust and transparency in transactions. Moreover, a deep understanding of the complex security challenges and unconventional risks that come with 6G V2X communication is essential.

E. ADDRESSING CHALLENGES RELATED TO CIA^3

The study mentions that the security challenges encompass issues related to CIA^3, which typically stands for Confidentiality, Integrity, Availability, Authenticity, and Accountability. These are crucial aspects for ensuring the overall security of vehicular networks in the 6G era. Protecting sensitive data and ensuring it remains confidential is paramount. Lessons include the need to encrypt and securely store V2X communication data, ensuring that only authorized entities have access to it. The data exchanged in V2X communication must remain unchanged and trustworthy. Lessons here highlight the importance of data validation mechanisms, ensuring data hasn't been tampered with during transmission or storage. For Vehicular Networks to function effectively, data and services must be readily available. The lesson is to design systems that are resilient to disruptions and capable of providing continuous service even in the face of attacks or failures. It is essential to verify the authenticity of communication participants and data sources. Key lessons involve implementing robust authentication mechanisms to ensure that only legitimate entities can participate in the network. Incorporating Federated Learning and Blockchain into 6G Vehicular Networks presents innovative solutions to address these CIA^3 challenges. Federated Learning allows machine learning to take place on decentralized and localized data sources, preserving data confidentiality and integrity. Blockchain technology provides a secure and immutable ledger for transactional and authentication data, enhancing data authenticity and accountability.

VII. CONCLUSION

In conclusion, as 6G communication emerges and expands, it brings with it the potential for massive connectivity between almost everything, including vehicles. The modernization of vehicles and their concepts, such as CAVs, IoV, intra-vehicular communication, and V2V communication, will require technological advancements to keep up with the 6G era. However, this expansion of V2X communication also introduces security risks and vulnerabilities that need to be addressed. As technology continues to evolve and expand, new security risks and vulnerabilities may arise, and it will be essential to develop new and improved security solutions to mitigate these risks. This paper has provided an overview of the security challenges and solutions for V2X communication in the upcoming 6G era. It has discussed the architecture and standards utilized in V2X communication and analyzed V2X security in the CIA^3 domains, which include confidentiality, integrity, availability, authentication, and access control. Finally, the paper highlights challenges and future research directions in the domain of security of V2X communications in the 6G era.

REFERENCES

[1] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55-61, 2020.

[2] M. Noor-A-Rahim *et al.*, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proceedings of the IEEE*, vol. 110, no. 6, pp. 712-734, 2022.

[3] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (V2X) communication platforms," *IEEE Transactions on Intelligent Vehicles*, vol. 5, no. 4, pp. 693-713, 2020.

[4] M. Szalai, B. Varga, T. Tettamanti, and V. Tihanyi, "Mixed reality test environment for autonomous cars using Unity 3D and SUMO," in *2020 IEEE 18th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 2020: IEEE, pp. 73-78.

[5] X. Hu, Z. Zheng, D. Chen, X. Zhang, and J. Sun, "Processing, assessing, and enhancing the Waymo autonomous vehicle open dataset for driving behavior research," *Transportation Research Part C: Emerging Technologies*, vol. 134, p. 103490, 2022.

[6] D. Coffin, S. Oliver, and J. VerWey, "Building vehicle autonomy: Sensors, semiconductors, software and US competitiveness," 2019.

[7] S. Vozar and A. Wyglinkski, *Sensors for Autonomous Vehicles*. IEEE, 2019.

[8] P. Schmitt *et al.*, "nuReality: A VR environment for research of pedestrian and autonomous vehicle interactions," *arXiv preprint arXiv:2201.04742*, 2022.

[9] https://getcruise.com/ (accessed 19 March, 2023, 2023).

[10] T. Petrov, L. Sevcik, P. Pocta, and M. Dado, "A performance benchmark for dedicated short-range communications and LTE-based cellular-V2X in the context of vehicle-to-infrastructure communication and urban scenarios," *Sensors*, vol. 21, no. 15, p. 5095, 2021.

[11] K. Jadaan, S. Zeater, and Y. Abukhalil, "Connected vehicles: an innovative transport technology," *Procedia Engineering*, vol. 187, pp. 641-648, 2017.

[12] K. Sjoberg, P. Andres, T. Buburuzan, and A. Brakemeier, "Cooperative intelligent transport systems in Europe: Current deployment status and outlook," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 89-97, 2017.

[13] J. Partala, "Post-quantum cryptography in 6G," *6G Mobile Wireless Networks*, pp. 431-448, 2021.

[14] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, and J. Zhou, "A systematic survey of attack detection and prevention in Connected and Autonomous Vehicles," *Vehicular Communications*, p. 100515, 2022.

[15] M. Sahlabadi, R.-C. Muniyandi, Z. Shukur, F. Qamar, and S.-H.-A. Kazmi, "Process Mining Discovery Techniques for Software Architecture Lightweight Evaluation Framework," *Computers, Materials \& Continua*, vol. 74, no. 3, pp. 5777--5797, 2023. [Online]. Available: http://www.techscience.com/cmc/v74n3/50886.

[16] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957-975, 2020.

[17] S. H. A. Kazmi, R. Hassan, F. Qamar, K. Nisar, and A. A. A. Ibrahim, "Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions," *Symmetry*, vol. 15, no. 6, p. 1147, 2023.

[18] J. Wang, K. Zhu, and E. Hossain, "Green Internet of Vehicles (IoV) in the 6G era: Toward sustainable vehicular communications and networking," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 391-423, 2021.

[19] P. K. Sharma, D. Vohra, and S. Rathore, "Security and Privacy in V2X Communications: How Can Collaborative Learning Improve Cybersecurity?," *IEEE Network*, vol. 36, no. 3, pp. 32-39, 2022.

[20] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, 2020.

[21] A. Mekrache, A. Bradai, E. Moulay, and S. Dawaliby, "Deep reinforcement learning techniques for vehicular networks: Recent advances and future trends towards 6G," *Vehicular Communications*, vol. 33, p. 100398, 2022.

[22] W. U. Khan *et al.*, "Opportunities for intelligent reflecting surfaces in 6G-empowered V2X communications," *arXiv preprint arXiv:2210.00494*, 2022.

[23] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292-307, 2019.

[24] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks," in *2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC)*, 2021: IEEE, pp. 154-158.

[25] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384-2428, 2021.

[26] E. Farsimadan, F. Palmieri, L. Moradi, D. Conte, and B. Paternoster, "Vehicle-to-everything (V2X) communication scenarios for vehicular ad-hoc networking (VANET): an overview," in *Computational Science and Its Applications–ICCSA 2021: 21st International Conference, Cagliari, Italy, September 13–16, 2021, Proceedings, Part VIII 21*, 2021: Springer, pp. 15-30.

[27] K. Kiela *et al.*, "Review of V2X–IoT standards and frameworks for ITS applications," *Applied sciences*, vol. 10, no. 12, p. 4314, 2020.

[28] G. Giambene, M. S. Rahman, and A. Vinel, "Analysis of V2V sidelink communications for platoon applications," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 2020: IEEE, pp. 1-6.

[29] B. Yu, S. Bao, F. Feng, and J. Sayer, "Examination and prediction of drivers' reaction when provided with V2I communication-based intersection maneuver strategies," *Transportation research part C: emerging technologies*, vol. 106, pp. 17-28, 2019.

[30] F. von Laffert, "3-D Lighting Technologies," *ATZelectronics worldwide*, vol. 15, no. 6, pp. 50-55, 2020.

[31] A. R. Abdellah, A. Muthanna, M. H. Essai, and A. Koucheryavy, "Deep Learning for Predicting Traffic in V2X Networks," *Applied Sciences*, vol. 12, no. 19, p. 10030, 2022.

[32] S. Chen, J. Hu, Y. Shi, L. Zhao, and W. Li, "A vision of C-V2X: Technologies, field testing, and challenges with Chinese development," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3872-3881, 2020.

[33] M. H. C. Garcia *et al.*, "A tutorial on 5G NR V2X communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1972-2026, 2021.

[34] J. Kim, G. Noh, T. Kim, H. Chung, and I. Kim, "Link-level performance evaluation of mmWave 5G NR sidelink communications," in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, 2021: IEEE, pp. 1482-1485.

[35] G. Liu *et al.*, "Vision, requirements and network architecture of 6G mobile network beyond 2030," *China Communications*, vol. 17, no. 9, pp. 92-104, 2020.

[36] V.-L. Nguyen, R.-H. Hwang, P.-C. Lin, A. Vyas, and V.-T. Nguyen, "Towards the Age of Intelligent Vehicular Networks for Connected and Autonomous Vehicles in 6G," *IEEE Network*, 2022.

[37] Y. Xing and T. S. Rappaport, "Terahertz wireless communications: Co-sharing for terrestrial and satellite systems above 100 GHz," *IEEE Communications Letters*, vol. 25, no. 10, pp. 3156-3160, 2021.

[38] N. Shinohara, "Trends in wireless power transfer: WPT technology for energy harvesting, mllimeter-wave/THz rectennas, MIMO-WPT, and advances in near-field WPT applications," *IEEE microwave magazine*, vol. 22, no. 1, pp. 46-59, 2020.

[39] R. Shrivastava, S. Hegde, and O. Blume, "Sidelink Evolution Toward 5G-A/6G Future Considerations for Standardization of Group Communications," *IEEE Communications Standards Magazine*, vol. 7, no. 1, pp. 24-30, 2023.

[40] K. Ganesan, J. Lohr, P. B. Mallick, A. Kunz, and R. Kuchibhotla, "NR sidelink design overview for advanced V2X service," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 26-30, 2020.

[41] J. W. Park, J.-Y. Hwang, S. Lim, Y. Yang, and S.-W. Lee, "Coexistence study on 5G V2X in mmWave," in *2021 International*

Conference on Information and Communication Technology Convergence (ICTC), 2021: IEEE, pp. 716-718.

[42] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, "Challenges and solutions for cellular based V2X communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 222-255, 2020.

[43] Y. Chen *et al.*, "Seeing the Forest for the Trees: Understanding Security Hazards in the {3GPP} Ecosystem through Intelligent Analysis on Change Requests," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 17-34.

[44] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G security: Opportunities and challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021: IEEE, pp. 616-621.

[45] Y. Wu, "Ethically Responsible and Trustworthy Autonomous Systems for 6G," *IEEE Network*, vol. 36, no. 4, pp. 126-133, 2022.

[46] C. Ranaweera, J. Kua, I. Dias, E. Wong, C. Lim, and A. Nirmalathas, "4G to 6G: Disruptions and drivers for optical access," *Journal of Optical Communications and Networking*, vol. 14, no. 2, pp. A143-A153, 2022.

[47] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?," *Nature Electronics*, vol. 3, no. 1, pp. 20-29, 2020.

[48] B. M. Shah, M. Murtaza, and M. Raza, "Comparison of 4G and 5G Cellular Network Architecture and Proposing of 6G, a new era of AI," in *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*, 2020: IEEE, pp. 1-10.

[49] Y. Lu, "Security in 6G: The prospects and the relevant technologies," *Journal of Industrial Integration and Management*, vol. 5, no. 03, pp. 271-289, 2020.

[50] M. Božanić and S. Sinha, *Mobile Communication Networks: 5G and a Vision of 6G*. Springer, 2021.

[51] M. Adhikari, A. Hazra, V. G. Menon, B. K. Chaurasia, and S. Mumtaz, "A roadmap of next-generation wireless technology for 6G-enabled vehicular networks," *IEEE Internet of Things Magazine*, vol. 4, no. 4, pp. 79-85, 2021.

[52] A. D. Abdullahi, T. Dargahi, and M. Hammoudeh, "Poster: Continuous Authentication in Highly Connected 6G-enabled Transportation Systems," in *2023 IEEE Vehicular Networking Conference (VNC)*, 2023: IEEE, pp. 171-172.

[53] J. Jia, P. Zou, F. Hu, Y. Zhao, and N. Chi, "Flexible data rate V2X communication system beyond 1.84 Gb/s based on MIMO VLC and radar integration," *Applied Sciences*, vol. 10, no. 19, p. 6636, 2020.

[54] S. Caputo, L. Mucchi, M. A. Umair, M. Meucci, M. Seminara, and J. Catani, "The Role of Bidirectional VLC Systems in Low-Latency 6G Vehicular Networks and Comparison with IEEE802. 11p and LTE/5G C-V2X," *Sensors*, vol. 22, no. 22, p. 8618, 2022.

[55] W. U. Khan, A. Ihsan, T. N. Nguyen, Z. Ali, and M. A. Javed, "NOMA-enabled backscatter communications for green transportation in automotive-industry 5.0," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7862-7874, 2022.

[56] Y. Shen, "Intelligent infrastructure, ubiquitous mobility, and smart libraries–Innovate for the future," *Data Science Journal*, vol. 18, no. 1, 2019.

[57] A. Gachhadar *et al.*, "Power Optimization in Multi-Tier Heterogeneous Networks Using Genetic Algorithm," *Electronics*, vol. 12, no. 8, p. 1795, 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/8/1795.

[58] P. Bhattacharya, S. Tanwar, U. Bodkhe, A. Kumar, and N. Kumar, "EVBlocks: A blockchain-based secure energy trading scheme for electric vehicles underlying 5G-V2X ecosystems," *Wireless Personal Communications*, vol. 127, no. 3, pp. 1943-1983, 2022.

[59] M. Noor-A-Rahim, G. M. N. Ali, Y. L. Guan, B. Ayalew, P. H. J. Chong, and D. Pesch, "Broadcast performance analysis and improvements of the LTE-V2V autonomous mode at road intersection," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9359-9369, 2019.

[60] A. Thomas, K. Deka, S. Sharma, and N. Rajamohan, "IRS-Assisted OTFS System: Design and Analysis," *IEEE Transactions on Vehicular Technology*, 2022.

[61] M. A. Javed, T. N. Nguyen, J. Mirza, J. Ahmed, and B. Ali, "Reliable communications for cybertwin-driven 6G IoVs using intelligent reflecting surfaces," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7454-7462, 2022.

[62] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, vol. 151, pp. 52-67, 2019.

[63] L. Gallo and J. Haerri, "Unsupervised long-term evolution device-to-device: A case study for safety-critical V2X communications," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 69-77, 2017.

[64] B. Brecht and T. Hehn, "A security credential management system for V2X communications," *Connected Vehicles: Intelligent Transportation Systems*, pp. 83-115, 2019.

[65] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent advances and challenges in security and privacy for V2X communications," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 244-266, 2020.

[66] L. Mauri and E. Damiani, "Stride-ai: An approach to identifying vulnerabilities of machine learning assets," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021: IEEE, pp. 147-154.

[67] K. Bian, G. Zhang, and L. Song, "Toward secure crowd sensing in vehicle-to-everything networks," *IEEE Network*, vol. 32, no. 2, pp. 126-131, 2017.

[68] J. Wang, Y. Shao, Y. Wang, Y. Ge, and R. Yu, "Physical layer authentication based on nonlinear kalman filter for v2x communication," *IEEE Access*, vol. 8, pp. 163746-163757, 2020.

[69] Y. Chen, M. Alam, and S. Mumtaz, "Aiden: Association-learning-based attack identification on the edge of V2X communication networks," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1377-1385, 2022.

[70] O. Sawade, I. Radusch, and M. Hauswirth, "V2x attack vectors and risk analysis for automated cooperative driving," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, 2021: IEEE, pp. 1-6.

[71] A. Afdhal, A. Ahmadiar, and R. Adriman, "Sybil Attack Detection on ITS-V2X System using a Realistic Traffic Model-based Approach," in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, 2022: IEEE, pp. 333-338.

[72] A. D. Kumar, K. N. R. Chebrolu, and S. KP, "A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities," *arXiv preprint arXiv:1810.04144*, 2018.

[73] J. Wang, Y. Shao, Y. Ge, and R. Yu, "Physical-layer authentication based on adaptive Kalman filter for V2X communication," *Vehicular Communications*, vol. 26, p. 100281, 2020.

[74] M. Tsukada, S. Arii, H. Ochiai, and H. Esaki, "Misbehavior detection using collective perception under privacy considerations," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, 2022: IEEE, pp. 808-814.

[75] E. Zadobrischi, M. Dimian, and M. Negru, "The Utility of DSRC and V2X in Road Safety Applications and Intelligent Parking: Similarities, Differences, and the Future of Vehicular Communication," *Sensors*, vol. 21, no. 21, p. 7237, 2021.

[76] T. Yoshizawa *et al.*, "A Survey of Security and Privacy Issues in V2X Communication Systems," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1-36, 2023.

[77] H. Ouamna, Z. Madini, and Y. Zouine, "6G and V2X Communications: Applications, Features, and Challenges," in *2022 8th International Conference on Optimization and Applications (ICOA)*, 2022: IEEE, pp. 1-6.

[78] M. Naderpour, "Privacy of V2X Communications."

[79] M. Naderpour, T. Meskanen, A. Paverd, and V. Niemi, "Auditable De-anonymization in V2X Communication," *Journal of ICT Standardization*, pp. 91–106-91–106, 2017.

[80] F. Haidar, F. Braiteh, L. Brigitte, A. Kaiser, and P. Urien, "Performance evaluation of pseudonym reload over cellular technology," in *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2021: IEEE, pp. 1-4.

[81] D. B. Rawat, R. Doku, A. Adebayo, C. Bajracharya, and C. Kamhoua, "Blockchain enabled named data networking for secure vehicle-to-everything communications," *IEEE Network*, vol. 34, no. 5, pp. 185-189, 2020.

[82] L. Woods, "Automated number plate recognition: data retention and the protection of privacy in public places," *Journal of Information Rights, Policy and Practice*, vol. 2, no. 1, pp. 1-21, 2017.
[83] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of network and computer applications*, vol. 116, pp. 42-52, 2018.
[84] M. He, J. Ni, Y. He, and N. Zhang, "Low-complexity phased-array physical layer security in millimeter-wave communication for cybertwin-driven V2X applications," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 4573-4583, 2021.
[85] T.-X. Zheng *et al.*, "Physical-Layer Security of Uplink mmWave Transmissions in Cellular V2X Networks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 11, pp. 9818-9833, 2022.
[86] Y. Koh, Y. Kim, M. Batzorig, and K. Yim, "Real Vehicle-Based Attack Dataset for Security Threat Analysis in a Vehicle," in *Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 17th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2022)*, 2022: Springer, pp. 137-146.
[87] R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle," *IEEE Access*, vol. 7, pp. 138018-138031, 2019.
[88] L. J. Vinita and V. Vetriselvi, "Federated Learning-based Misbehaviour detection on an emergency message dissemination scenario for the 6G-enabled Internet of Vehicles," *Ad Hoc Networks*, p. 103153, 2023.
[89] G. S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar, and K.-K. R. Choo, "BloCkEd: Blockchain-based secure data processing framework in edge envisioned V2X environment," *IEEE transactions on vehicular technology*, vol. 69, no. 6, pp. 5850-5863, 2020.
[90] P. Michalopoulos, J. Meijers, S. F. Singh, and A. Veneris, "A V2X Reputation System with Privacy Considerations," in *2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS)*, 2022: IEEE, pp. 8-14.
[91] H. Wang, D. He, J. Yu, N. N. Xiong, and B. Wu, "RDIC: a blockchain-based remote data integrity checking scheme for IoT in 5G networks," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 1-10, 2021.
[92] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the Internet of vehicles: Challenges and opportunities," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308-323, 2020.
[93] M. A. Javed *et al.*, "ODPV: An efficient protocol to mitigate data integrity attacks in intelligent transport systems," *IEEE Access*, vol. 8, pp. 114733-114740, 2020.
[94] A. Kamaraj, "Secured V2x Communication Using Optimized Prime Field Ecc Architecture," 2022.
[95] N. H. Mahmood *et al.*, "White paper on critical and massive machine type communication towards 6G," *arXiv preprint arXiv:2004.14146*, 2020.
[96] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Vehicular Communications*, vol. 12, pp. 50-65, 2018.
[97] S. Basharat, S. A. Hassan, H. Pervaiz, A. Mahmood, Z. Ding, and M. Gidlund, "Reconfigurable intelligent surfaces: Potentials, applications, and challenges for 6G wireless networks," *IEEE Wireless Communications*, vol. 28, no. 6, pp. 184-191, 2021.
[98] Z. Zhang, W. Duan, Y. Ji, and G. Zhang, "Power and Element Allocation Design for RIS–NOMA IoV Networks," *Electronics*, vol. 12, no. 4, p. 1003, 2023.
[99] W. U. Khan, M. A. Jamshed, A. Mahmood, E. Lagunas, S. Chatzinotas, and B. Ottersten, "Backscatter-aided NOMA V2X communication under channel estimation errors," in *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*, 2022: IEEE, pp. 1-6.
[100] P. N. Srinivasu, M. F. Ijaz, J. Shafi, M. Woźniak, and R. Sujatha, "6G Driven Fast Computational Networking Framework for Healthcare Applications," *IEEE Access*, vol. 10, pp. 94235-94248, 2022.
[101] D. Mishra, A. M. Vegni, V. Loscrí, and E. Natalizio, "Drone networking in the 6g era: A technology overview," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 88-95, 2021.
[102] S. B. Prathiba, G. Raja, S. Anbalagan, S. Gurumoorthy, N. Kumar, and M. Guizani, "Cybertwin-driven federated learning based personalized service provision for 6g-v2x," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 4632-4641, 2021.
[103] O. Vermesan *et al.*, "Advancing the Design of Fail-Operational Architectures, Communication Modules, Electronic Components, and Systems for Future Autonomous/Automated Vehicles," in *Intelligent System Solutions for Auto Mobility and Beyond: Advanced Microsystems for Automotive Applications 2020*, 2021: Springer, pp. 53-71.
[104] S. Kim and A. S. Ibrahim, "Byzantine-Fault-Tolerant Consensus via Reinforcement Learning for Permissioned Blockchain-Empowered V2X Network," *IEEE Transactions on Intelligent Vehicles*, 2022.
[105] R. Aissaoui, H. Menouar, A. Dhraief, F. Filali, A. Belghith, and A. Abu-Dayya, "Advanced real-time traffic monitoring system based on V2X communications," in *2014 IEEE International Conference on Communications (ICC)*, 2014: IEEE, pp. 2713-2718.
[106] T. Semong *et al.*, "Intelligent load balancing techniques in software defined networks: A survey," *Electronics*, vol. 9, no. 7, p. 1091, 2020.
[107] S. He, J. Du, and Y. Liao, "Multi-user scheduling for 6G V2X ultra-massive MIMO system," *Sensors*, vol. 21, no. 20, p. 6742, 2021.
[108] H. Cui, "A Novel Traffic Aware Data Routing Protocol in Vehicular Networks," Université d'Ottawa/University of Ottawa, 2022.
[109] M. Houmer, M. Ouaissa, and M. Ouaissa, "Secure authentication scheme for 5g-based v2x communications," *Procedia Computer Science*, vol. 198, pp. 276-281, 2022.
[110] R. Ma, J. Cao, Y. Zhang, C. Shang, L. Xiong, and H. Li, "A Group-Based Multicast Service Authentication and Data Transmission Scheme for 5G-V2X," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 23976-23992, 2022.
[111] E. S. Ali *et al.*, "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications," *Security and Communication Networks*, vol. 2021, pp. 1-23, 2021.
[112] P. Bhattacharya, A. Shukla, S. Tanwar, N. Kumar, and R. Sharma, "6Blocks: 6G-enabled trust management scheme for decentralized autonomous vehicles," *Computer Communications*, vol. 191, pp. 53-68, 2022.
[113] V. O. Nyangaresi, A. J. Rodrigues, and S. O. Abeka, "Efficient group authentication protocol for secure 5G enabled vehicular communications," in *2020 16th International computer engineering conference (ICENCO)*, 2020: IEEE, pp. 25-30.
[114] M. Houmer, S. Laqtib, and S. Eddamiri, "Lightweight and Secure Authentication Model for Vehicle to Everything (V2X) Communication Based on 5G Networks," *Journal of Mobile Multimedia*, pp. 1399–1424-1399–1424, 2022.
[115] A. Neish, T. Walter, and P. Enge, "Quantum-resistant authentication algorithms for satellite-based augmentation systems," *Navigation*, vol. 66, no. 1, pp. 199-209, 2019.
[116] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.-K. R. Choo, and H. Cai, "V2X security: A case study of anonymous authentication," *Pervasive and Mobile Computing*, vol. 41, pp. 259-269, 2017.
[117] M. Soni and D. K. Singh, "Blockchain-based group authentication scheme for 6G communication network," *Physical Communication*, p. 102005, 2023.
[118] V. Marojevic, "C-V2X security requirements and procedures: Survey and research directions," *arXiv preprint arXiv:1807.09338*, 2018.
[119] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Computer Networks*, vol. 169, p. 107093, 2020.
[120] M. Klaassen and T. Szuprycinski, "Security for V2X," *Automotive Systems and Software Engineering: State of the Art and Future Trends*, pp. 283-294, 2019.
[121] E. Verheul, C. Hicks, and F. D. Garcia, "Ifal: Issue first activate later certificates for v2x," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2019: IEEE, pp. 279-293.
[122] F. Salahdine, T. Han, and N. Zhang, "Security in 5G and beyond recent advances and future challenges," *Security and Privacy*, vol. 6, no. 1, p. e271, 2023.
[123] L. Wang and X. Liu, "Secure cooperative communication scheme for vehicular heterogeneous networks," *Vehicular Communications*, vol. 11, pp. 46-56, 2018.

[124] U. U. Uchibeke, K. A. Schneider, S. H. Kassani, and R. Deters, "Blockchain access control ecosystem for big data security," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018: IEEE, pp. 1373-1378.

[125] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1-5, 2020.

[126] H. Mosavat-Jahromi, Y. Li, L. Cai, and L. Lu, "NC–MAC: a distributed MAC protocol for reliable beacon broadcasting in V2X," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6044-6057, 2021.

[127] R. Ernst, D. Stöhrmann, A. Bendrick, and A. Kostrzewa, "Application-centric Network Management-Addressing Safety and Real-time in V2X Applications," *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 2, pp. 1-25, 2023.

[128] Q. Chen, A. K. Sowan, and S. Xu, "A safety and security architecture for reducing accidents in intelligent transportation systems," in *2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2018: IEEE, pp. 1-7.

[129] G. P. W. NBA, J. Haapola, and T. Samarasinghe, "A discrete-time Markov chain based comparison of the MAC layer performance of C-V2X mode 4 and IEEE 802.11 p," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2505-2517, 2020.

[130] Z. Zhou, A. Gaurav, B. B. Gupta, M. D. Lytras, and I. Razzak, "A fine-grained access control and security approach for intelligent vehicular transport in 6g communication system," *IEEE transactions on intelligent transportation systems*, vol. 23, no. 7, pp. 9726-9735, 2021.

[131] A. Didouh, Y. El Hillali, A. Rivenq, and H. Labiod, "Novel centralized pseudonym changing scheme for location privacy in V2X communication," *Energies*, vol. 15, no. 3, p. 692, 2022.

[132] U. Datta, A. Kalam, and J. Shi, "The strategies of EV charge/discharge management in smart grid vehicle-to-everything (V2X) communication networks," *Advanced Communication and Control Methods for Future Smartgrids*, vol. 177, 2019.

[133] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6G communications," *Digital Communications and Networks*, vol. 6, no. 3, pp. 261-269, 2020.

[134] A. Vladyko, V. Elagin, A. Spirkina, A. Muthanna, and A. A. Ateya, "Distributed edge computing with blockchain technology to enable ultra-reliable low-latency V2X communications," *Electronics*, vol. 11, no. 2, p. 173, 2022.

[135] R. Jabbar, N. Fetais, M. Kharbeche, M. Krichen, K. Barkaoui, and M. Shinoy, "Blockchain for the Internet of vehicles: how to use blockchain to secure vehicle-to-everything (V2X) communication and payment?," *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15807-15823, 2021.

[136] A. Didouh, H. Labiod, Y. El Hillali, and A. Rivenq, "Blockchain-based collaborative certificate revocation systems using clustering," *IEEE Access*, vol. 10, pp. 51487-51500, 2022.

[137] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, "Artificial-intelligence-enabled intelligent 6G networks," *IEEE Network*, vol. 34, no. 6, pp. 272-280, 2020.

[138] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46-51, 2020.

[139] L. Barbieri, S. Savazzi, M. Brambilla, and M. Nicoli, "Decentralized federated learning for extended sensing in 6G connected vehicles," *Vehicular Communications*, vol. 33, p. 100396, 2022.

[140] K. Tan, D. Bremner, J. Le Kernec, and M. Imran, "Federated machine learning in vehicular networks: A summary of recent applications," in *2020 international conference on UK-China emerging technologies (UCET)*, 2020: IEEE, pp. 1-4.

[141] S. B. Prathiba, G. Raja, S. Anbalagan, K. Dev, S. Gurumoorthy, and A. P. Sankaran, "Federated learning empowered computation offloading and resource management in 6G-V2X," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3234-3243, 2021.

[142] J. Huang *et al.*, "AFLPC: an asynchronous federated learning privacy-preserving computing model applied to 5G-V2X," *Security and Communication Networks*, vol. 2022, 2022.

[143] B. Qolomany, K. Ahmad, A. Al-Fuqaha, and J. Qadir, "Particle swarm optimized federated learning for industrial IoT and smart city services," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, 2020: IEEE, pp. 1-6.

[144] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4734-4746, 2020.

[145] H. Liu *et al.*, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6073-6084, 2021.

[146] S. Otoum, I. Al Ridhawi, and H. Mouftah, "A Federated Learning and Blockchain-Enabled Sustainable Energy Trade at the Edge: A Framework for Industry 4.0," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3018-3026, 2022.

[147] M. Zrikem, I. Hasnaoui, and R. Elassali, "Vehicle-to-Blockchain (V2B) Communication: Integrating Blockchain into V2X and IoT for Next-Generation Transportation Systems," *Electronics*, vol. 12, no. 16, p. 3377, 2023.

[148] D. P. M. Osorio *et al.*, "Towards 6G-enabled internet of vehicles: Security and privacy," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 82-105, 2022.

[149] B. Gera, Y. S. Raghuvanshi, O. Rawlley, S. Gupta, A. Dua, and P. Sharma, "Leveraging AI-enabled 6G-driven IoT for sustainable smart cities," *International Journal of Communication Systems*, p. e5588.

[150] M. Katz, M. Matinmikko-Blue, and M. Latva-Aho, "6Genesis flagship program: Building the bridges towards 6G-enabled wireless smart society and ecosystem," in *2018 IEEE 10th Latin-American Conference on Communications (LATINCOM)*, 2018: IEEE, pp. 1-9.

[151] K. RAGHUNANDAN, R. DODMANE, K. BHAVYA, N. K. RAO, and A. K. SAHU, "Chaotic-Map Based Encryption for 3D Point and 3D Mesh Fog Data in Edge Computing."

[152] A. Almaiah and O. Almomani, "An investigation of digital forensics for shamoon attack behaviour in FOG computing and threat intelligence for incident response," *J. Theor. Appl. Inf. Technol*, vol. 15, p. 98, 2020.

[153] N. M. Alzahrani and F. A. Alfouzan, "Augmented reality (AR) and cyber-security for smart cities—A systematic literature review," *Sensors*, vol. 22, no. 7, p. 2792, 2022.

[154] A. Abuarqoub, "A review of the control plane scalability approaches in software defined networking," *Future Internet*, vol. 12, no. 3, p. 49, 2020.

[155] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet," *IEEE Access*, vol. 8, pp. 91028-91047, 2020.

[156] Y. He *et al.*, "D2D-V2X-SDN: Taxonomy and architecture towards 5G mobile communication system," *Ieee Access*, vol. 9, pp. 155507-155525, 2021.

[157] K. Luo, X. Zhou, B. Wang, J. Huang, and H. Liu, "Sparse Bayes tensor and DOA tracking inspired channel estimation for V2X millimeter wave massive MIMO system," *Sensors*, vol. 21, no. 12, p. 4021, 2021.

[158] S. Tariq, H. Al-Rizzo, M. N. Hasan, N. Kunju, and S. Abushamleh, "Stochastic versus ray tracing wireless channel modeling for 5G and V2X applications: Opportunities and challenges," *Antenna Systems*, pp. 1-16, 2021.

[159] B. Kihei, H. Wilson, and M. Fall, "Experimental results of detecting primitive jamming attacks using machine learning in vehicle-to-everything communication networks," in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 2021: IEEE, pp. 530-535.

[160] W. M. R. Shakir, J. Charafeddine, H. Al Satai, H. Hamdan, S. Haddad, and J. Sayah, "Opportunistic Schedule Selection for Multiuser MIMO FSO Communications: A Security-Reliability Trade-off Perspective," *IEEE Photonics Journal*, 2023.

[161] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A blockchain based federated learning for message dissemination in vehicular networks,"

IEEE Transactions on Vehicular Technology, vol. 71, no. 2, pp. 1927-1940, 2021.
[162] A. Boualouache and T. Engel, "Federated learning-based scheme for detecting passive mobile attackers in 5G vehicular edge computing," *Annals of Telecommunications*, pp. 1-20, 2022.
[163] C. I. Nwakanma *et al.*, "Explainable artificial intelligence (xai) for intrusion detection and mitigation in intelligent connected vehicles: A review," *Applied Sciences*, vol. 13, no. 3, p. 1252, 2023.

MYOUNGSU KIM received the B.S. degree from the Department of Information Security Engineering, Soonchunhyang, Asan, South Korea, in 2016. He is currently a Ph.D. candidate at the Department of Information Security Engineering, Soonchunhyang University. His research interests include vulnerability analysis, mobile baseband security, automotive security, and V2X security.

INSU OHreceived the B.S. and M.S. degrees from the Department of Information Security Engineering, Soochunhyang University, Asan, South Korea, in 2018 and 2020, respectively, where he is currently pursuing the Ph.D. degree with the Department of Information Security Engineering. His research interests include vulnerability analysis, mobile baseband security, automotive security, and V2X security.

KANGBIN YIM received the B.S., M.S., and Ph.D. degrees from the Department of Elec- tronics Engineering, Ajou University, Suwon, South Korea, in 1992, 1994, and 2001, respectively. He is currently a professor at the Department of Information Security Engineering, Soonchunhyang University. His research interests include malware analysis, vulnerability identification, code obfuscation, secure architecture, and mobile baseband and automotive security.

Mahdi Sahlabadi, an IEEE Senior Member, holds a Ph.D. in Industrial Computing from the National University of Malaysia. His academic journey includes research positions at the Japan Advanced Institute of Science and Technology (JAIST), Singapore Management University (SMU), Sharif University of Tehran (SUT), University Kebangsaan Malaysia(UKM), and Soonchunhyang University (SCH), South Korea. His areas of research interest are process mining, software architecture, cybersecurity, and quality assurance.

ZARINA SHUKUR received the Ph.D. degree from the University of Nottingham, in 1999. She is currently a Professor at the Center for Cyber Security Studies, Universiti Kebangsaan Malaysia. Her research interests include formal methods and cybersecurity.