IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131102

Analysis of Vehicle-To-Everything (V2X) Communication to Enhance Driver Safety and Compliance Automation

Adeola Agbonyin

Electrical Engineer, Technical Product Owner, Arlington Virginia, United States

Abstract: Vehicle-to-Everything (V2X) communication is examined in this paper as a revolutionary strategy for improving driver safety and guaranteeing automated adherence to traffic laws. The real-time information exchange between cars infrastructure and pedestrians made possible by V2X technology is essential for preventing collisions and enhancing traffic control. Although traffic flow optimization and accident prevention are two areas where V2X exhibits great promise security flaws inconsistent standards expensive infrastructure and privacy issues are impeding its development. To protect V2X communication the study emphasizes a careful examination of current security protocols and the requirement for strong countermeasures. In order to create universally compatible systems global coordination is necessary to overcome standardization challenges caused by diverse regional protocols such as DSRC and C-V2X. Furthermore, putting V2X infrastructure into place is expensive especially when retrofitting already-existing urban landscapes. The study also looks at potential future directions indicating that adding artificial intelligence could improve V2Xs adaptive and predictive capabilities further supporting driver safety and legal compliance. A thorough grasp of the developments and difficulties in V2X communication is the goal of this paper which also highlights the fact that resolving these issues is crucial to realizing the full potential of the technology. To create a more secure interconnected and effective transportation ecosystem worldwide cooperation between governments businesses and research institutions will be essential.

Keywords: V2X Communication, Driver Safety, Compliance Automation, Security Challenges, Traffic Management Optimization

1. INTRODUCTION

Vehicle-to-Everything (V2X) connectivity is remodeling how automobiles engage with their environment and paving the manner for a more secure and extra effective riding enjoy in the hastily evolving transportation scene. V2V, or car-to-vehicle Infrastructure-to-car (V2I) V2X generation consists of some of communique protocols, which include Vehicle-to-Pedestrian (V2P) and Vehicle-to-Cloud (V2C). Through the facilitation of actual-time facts go with the flow between outside networks and car infrastructure, this networked framework enhances situational focus and decision-making skills. Given the pressing issues of traffic congestion, road safety, and inefficient traffic management, creative solutions are crucial. There are more cars on the road as cities develop denser, which raises the risk of crashes and other traffic-related mishaps. In order to solve these problems V2X communication allows cars to exchange vital data including navigational information traffic conditions and accident alerts. This connectivity creates a more adaptable transportation system that improves traffic flow lessens environmental impact and increases road safety. Systems created to reduce risks for all users of the road including cyclists and pedestrians put safety first in V2X applications. To prevent collisions and safeguard vulnerable road users V2P initiatives make use of cutting-edge sensors and communication technologies. Additionally V2I communication improves the way that cars and infrastructure interact by giving drivers crucial information about the state of the roads and impending traffic signals. V2X communication is a key component of the automotive industry's shift toward a future defined by electric connected autonomous and shared vehicles or ACES. V2Xs integration of cutting-edge technologies promotes compliance automation and improves driver safety by guaranteeing that automobiles follow operating procedures and traffic laws. This analysis will look at the many advantages of V2X communication including how it could transform compliance automation and driver safety. A thorough grasp of these technologies will enable us to see how V2X can improve the quality of life in our increasingly urbanized world by fostering a more efficient and safe transportation environment. Figure 1 shows the various applicational fields of V2X communications.[1][2]

DOI: 10.17148/IJARCCE.2024.131102

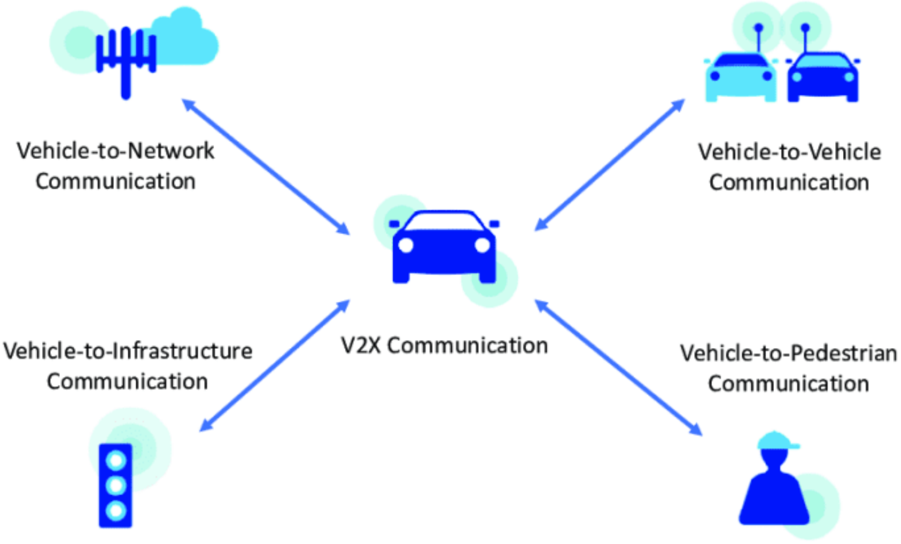
Vehicle-to-Network Communication
Vehicle-to-Vehicle Communication
V2X Communication
Vehicle-to-Infrastructure Communication
Vehicle-to-Pedestrian Communication

Fig. 1. V2X communications

2. LITERATURE REVIEW

Vehicle-to-Everything (V2X) communique is transforming street protection and compliance automation by means of permitting interconnected structures to speak important records, thereby enhancing situational cognizance and choice-making in real time. This literature survey covers the diverse aspects of V2X communique, specializing in its potential to enhance motive force protection and permit automatic compliance with traffic guidelines. Sources from Encora, Cyient, Automotive Technology, and ResearchGate offer insights into V2X's applications, technical mechanisms, and protection demanding situations, highlighting its effect on modern-day transportation.

OVERVIEW OF V2X COMMUNICATION TECHNOLOGY

Vehicle-to-automobile (V2X) communication permits communique among cars and their environment. Among its severa versions are Vehicle-to-Pedestrian (V2P) Vehicle-to-Infrastructure (V2I) Vehicle-to-Network (V2N) and Vehicle-to-Vehicle (V2V). These elements facilitate statistics manipulation among cars tourists pedestrians and even networks of clever towns. They help with infrastructure as properly (e. G. Three. 3. Symptoms and warnings). The most extensively used V2X era requirements are Dedicated Short-Range Communication (DSRC) and Cellular V2X (C-V2X). Although both standards enable real-time data transfer their range and network dependence differ. Whereas C-V2X is cellular-based and gains from wider network coverage and integration with cellular networks for increased reach DSRC uses direct short-range communication channels. By providing updates on traffic conditions upcoming road hazards and potential obstacles the real-time data exchanged via V2X can improve driver awareness. V2X could drastically lower traffic accidents by giving drivers and autonomous car systems the information they need to respond before collisions happen according to Encoras analysis. This is especially important for self-driving cars whose safe navigation depends on consistent and trustworthy data input. Through shared data V2X enables vehicles to see beyond their immediate line of sight reducing the chance of accidents caused by blind spots or slow reaction times and enabling earlier responses to hazards.

ENHANCING DRIVER SAFETY WITH V2X

Vehicles equipped with V2X technology can make decisions on their own in dangerous circumstances. For instance a car can alert other cars in the vicinity when it notices an obstruction or an abrupt slowdown in traffic enabling them to change their speed and prevent possible collisions. Cyients research indicates that this is especially helpful for a larger implementation of Automated Driver Assistance Systems (ADAS). Automatic emergency braking adaptive cruise control collision alerts and lane departure warnings are just a few of the many safety features that ADAS systems can support with V2X data. These characteristics make driving more dependable and allow for quick reactions to abrupt changes in traffic conditions. Additionally automated traffic law compliance is supported by V2X communication which lessens the need for human intervention and enhances regulatory adherence. For example without requiring driver input V2I communication can notify cars of impending speed limits or road construction zones and change the vehicles speed accordingly. All road users will be safer as a result of cars constantly adhering to traffic laws. Encora highlights the advantages of this compliance automation in circumstances that call for prompt actions to avoid collisions like slowing down close to crosswalks or stopping at red lights when visibility is poor.

TRAFFIC MANAGEMENT AND EFFICIENCY

Since V2X innovation makes it conceivable to utilize transportation framework more successfully it moreover altogether makes strides activity administration. The interconnecting of V2X empowers foundation and vehicles to participate to progress activity stream reduce clog and utilize less fuel. V2X empowers energetic steering which decreases activity jams by empowering vehicles to reroute in reaction to current activity conditions agreeing to Car Innovation. V2X frameworks help drivers in finding the foremost effective courses to their goals and maintaining a strategic distance from delays by determining activity designs and conceivable blockage focuses. Moreover V2X can help in maximizing the timing of activity signals encouraging more consistent moves and cutting down on crossing point hold up times. In order to meet wants of cars drawing closer the crossing point V2I communication empowers activity signals to adjust their cycles in reaction to real-time activity information. This methodology contributes to more economical urban situations by cutting down on emanations and fuel utilization in expansion to travel times. Also V2X-enabled cars can run at ideal speeds to cut down on stop-and-go activity which brings down contamination and increments fuel productivity. For cities looking to progress natural supportability and portability V2X is an basic innovation since of these characteristics.

SECURITY CONCERNS IN V2X COMMUNICATION

In spite of the fact that V2X communication has numerous points of interest there are security issues that have to be be settled to guarantee tried and true and secure operations. ResearchGate highlights that V2X frameworks are defenseless to potential cyberthreats like spoofing information altering and unauthorized get to since of their open nature. These perils may cause malicious disturbance of V2X communication channels which may lead to untrue data and jeopardized security. A programmer might for occurrence modify V2X information to manufacture activity circumstances which would cause robotized frameworks to form unsafe choices. V2X frameworks require solid security measures such as encryption verification and information approval strategies to decrease these dangers. Whereas confirmation makes sure that as it were authorized gadgets can get to the V2X arrange encryption makes a difference protect the keenness of information that's transmitted. Moreover it has been recommended that V2X communication utilizing blockchain innovation can create unchangeable records of information trades bringing down the plausibility of altering and ensuring that data is solid and precise. To cultivate open believe and advance far reaching selection of this innovation it is basic to ensure the steadfastness and security of V2X communication.

FUTURE OF V2X COMMUNICATION IN AUTONOMOUS VEHICLES

V2X innovation has more potential than fair its show employments particularly as independent cars multiply. For secure route independent cars incredibly depend on exact real-time information which V2X communication can supply on a bigger scale. Through information compatibility between vehicles, V2X can let independent cars make educated choices indeed in troublesome activity scenarios. For occasion, an independent vehicle can improve its security by altering its course in reaction to information from other vehicles within the region with respect to the condition of the street or the presence of people on foot. Future developments could improve autonomous systems responsiveness and adaptability by combining V2X with cutting-edge AI and machine learning algorithms. Vehicles can respond to novel or unexpected situations anticipate driver behavior and predict traffic patterns thanks to machine learning. As these systems develop V2X communication will be essential to the infrastructure that enables effective and safe autonomous driving. To assure the security and interoperability of V2X systems throughout numerous regions and automakers governments and regulatory corporations are also predicted to make a contribution through establishing standards and guidelines. Vehicle-to-Everything (V2X) communication has emerged as a transformative technology that complements motive force protection, promotes automation of compliance, and improves visitors control. Through the facilitation of real-time data sharing between pedestrians and automobile infrastructure, V2X improves situational cognizance and decreases the chance of accidents. While its influence on traffic management improves mobility and sustainability the technologys capacity to automate adherence to traffic laws also makes driving safer and more dependable. It is impossible to ignore the security issues with V2X though. To stop cyberthreats that could jeopardize safety and erode public trust it is crucial to guarantee the dependability and security of data within V2X networks. V2X communication will become more crucial

DOI: 10.17148/IJARCCE.2024.131102

as the automotive industry moves toward completely autonomous vehicles facilitating safe and effective transportation systems. Intelligent transportation systems that are safe and adaptable to changing circumstances will develop as a result of V2Xs continued integration with AI and machine learning. Figure 2 shows various types of V2I communication. [3]-[10]

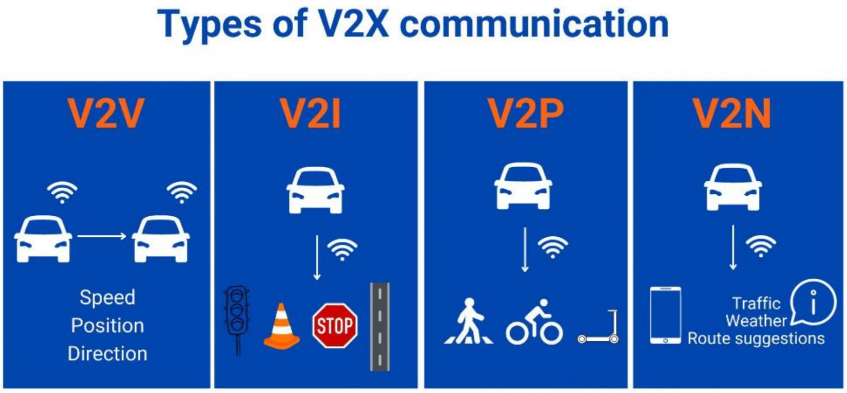

Fig. 2. V2X Communication Types

3. METHODOLOGY

The technique for an "Investigation of Vehicle-To-Everything (V2X) Communication to Improve Driver Security and Compliance Robotization" includes a multi-phase investigate approach planned to analyze V2X communication's security challenges, compliance components, and adequacy in security improvement. This technique comprises orderly writing survey procedures, risk classification, and a amalgamation of existing security measures and standardization endeavors, drawing from broad investigate over differing sources and stages.

PHASE 1: SYSTEMATIC LITERATURE REVIEW

The goal of this first stage is to gather and sift through pertinent research on V2X security and how it affects road safety and compliance. The current analysis draws from prestigious databases such as Google Scholar IEEE Xplore ACM Digital Library Scopus ScienceDirect and Wiley Online Library building on approaches outlined in related research endeavors such as the examination of 150 sources in V2X security. Studies covering the period of technological advancement in V2X from 1994 to 2023 are included in the literature. Notably we screen articles for direct V2X relevance concentrating on the threats challenges and mitigation strategies related to vehicular communication security. To keep the studys scope firmly within the domain of vehicular communication security research addressing general wireless sensor or mobile networks is excluded. Furthermore because hardware and system failures present a serious risk to compliance automation we restrict our attention to anomalous system behaviors brought on by malevolent intent. By classifying findings into threat classifications security/privacy concerns and industry standards that define secure V2X systems the literature review lays the groundwork for a thorough examination of how V2X improves automated driving safety and compliance.

PHASE 2: CLASSIFICATION OF V2X SECURITY CHALLENGES

Gathering and sorting relevant research on V2X security and its impact on road safety and compliance is the aim of this initial phase. The current study builds on methods described in related research projects such as the review of 150 sources in V2X security and uses prestigious databases like Google Scholar IEEE Xplore ACM Digital Library Scopus ScienceDirect and Wiley Online Library. Included in the literature are studies that span the years 1994–2023 when V2X technology advanced. Specifically we filter articles for direct V2X relevance focusing on the risks difficulties and solutions associated with the security of vehicular communication. Research addressing general wireless sensors or mobile networks is not included in order to maintain the studys focus firmly within the field of vehicular communication security. Furthermore we focus only on unusual system behaviors caused by malicious intent because hardware and system failures pose a significant risk to compliance automation. The literature review establishes the framework for a comprehensive analysis of how V2X enhances automated driving safety and compliance by grouping findings into threat classifications security/privacy concerns and industry standards that define secure V2X systems.

PHASE 3: EVALUATION OF STANDARDIZATION EFFORTS

The interoperability and dependability of V2X communication systems across various manufacturers environments and regulations depend on standardization. In this phase the literature synthesis examines current and planned V2X standardization initiatives. Encoras observations indicate that it is difficult to achieve consistency in V2X standards because technology differs by region (e. g. 3. Chinas C-V2X and the USs DSRC. Therefore the methodology includes a review of guidelines for secure V2X protocols such as IEEE 1609 as well as an analysis of standardization bodies such as the International Organization for Standardization (ISO) the Society of Automotive Engineers (SAE) and the European Telecommunications Standards Institute (ETSI). standards x. In order to ensure that V2X systems are secure scalable and meet safety and regulatory standards this phase evaluates the contributions made by these organizations. By examining these standards this phase offers insights into possible gaps in standardization that may affect the global deployment of V2X particularly with regard to automated compliance and driver safety. Figure 3 shows the difference between Direct and indirect V2X communications.

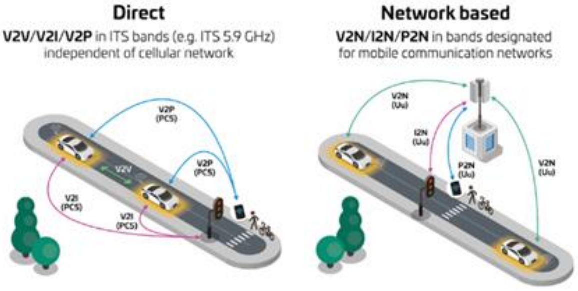
Direct
V2V/V2I/V2P in ITS bands (e.g. ITS 5.9 GHz) independent of cellular network
V2P (PC5)
V2P (PC5)
V2V
V2I (PC5)
V2I (PC5)
Network based
V2N/I2N/P2N in bands designated for mobile communication networks
V2N (Uu)
I2N (Uu)
P2N (Uu)
V2N (Uu)

Fig. 3. Direct and indirect V2X communications

PHASE 4: INVESTIGATION OF MISBEHAVIOR DISCOVERY APPROACHES

The fourth organize looks at distinctive misbehavior location procedures that are essential to discover and halt pernicious action in V2X systems. A scientific classification of discovery strategies is included in this examination and it is separated into the taking after categories. 1. Signature-based discovery is constrained in its capacity to recognize modern assaults but it can distinguish known risk marks to recognize recognizable sorts of malevolent movement. 2. Distinguishing odd designs or behaviors that wander from normal framework operations and may be signs of security dangers is known as anomaly-based location. 3. Combining signature and anomaly-based methods cross breed approaches offer a more intensive discovery since they can diminish wrong positives and offer a more extensive risk scope. The viability productivity and reasonableness of these location strategies in V2X settings are evaluated. Inquire about on misbehavior location from the scholarly community and industry sources is utilized to supplement this scientific categorization highlighting the preferences and impediments of the discovery models in UTILIZE NOWADAYS.

PHASE 5: REVIEW OF STATE-OF-THE-ART V2X SECURITY ARRANGEMENTS

Beside distinguishing dangers this organize involves analyzing current V2X security arrangements and countermeasures which contrast enormously depending on the innovation (e. g. G. DSRC as contradicted to C-V2X) as well as legitimate orders. The writing survey gives data for a exhaustive appraisal of security arrangements with an accentuation on information judgment techniques confirmation conventions and encryption procedures. Solid encryption and secure confirmation are fundamental for anticipating undesirable get to to V2X information concurring to ponders from Cyient and Car Innovations. This stage particularly looks at: The utilize of end-to-end encryption for V2X information secures communications from being capturing or changed.

Confirmation Conventions: Tough verification instruments to confirm the authenticity of framework and vehicles that are communicating maintaining a strategic distance from undesirable get to.

DOI: 10.17148/IJARCCE.2024.131102

Information Astuteness Checks: Confirmation procedures to ensure the exactness and constancy of information being exchanged whereas securing against infusion or information adjustment assaults. This stage examines the reasonability and value of a extend of security arrangements in different sending scenarios counting cloud-based interruption discovery frameworks and blockchain-based V2X security systems.

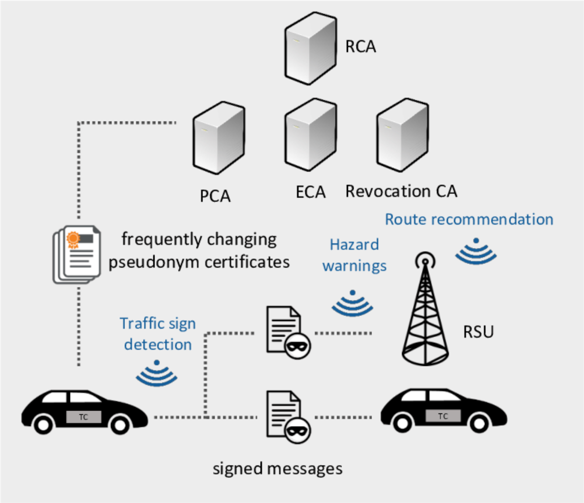

Fig. 4. A V2X security solution based on PKI

PHASE 6: IDENTIFICATION OF OPEN ISSUES AND FUTURE RESEARCH DIRECTIONS

In Figure 4, a PKI based V2X security solution is proposed. Recognizing the inadequacies of current investigate and arrangements this organize pinpoints conceivable bearings for assist examination. For illustration there are crevices in accomplishing real-time discovery and reaction capabilities inside V2X frameworks indeed in spite of the fact that current arrangements offer fundamental security functionalities. Uncertain issues incorporate the trouble of striking a adjust between security prerequisites and computational stack in situations with restricted assets and making beyond any doubt that territorial benchmarks work consistently together. To make strides discovery precision and reaction to unused dangers future investigate headings explore the joining of machine learning (ML) and counterfeit insights (AI) models into V2X security systems. Moreover in arrange to advance development in V2X security and standardization this stage requires multi-stakeholder participation between automakers telecom companies and government organizations.

PHASE 7: COMPARATIVE ANALYSIS WITH RELATED STUDIES

Last but not least a comparative analysis places this study in the larger context of V2X research. This approach places the results of this analysis in context by contrasting them with those of related surveys highlighting differences in the breadth of technological coverage regulatory focus and security threat coverage. Using resources like ResearchGate to highlight group efforts to address V2X vulnerabilities this phase includes a discussion of government business and academic initiatives that support V2X security. In order to provide a more comprehensive understanding of the potential of V2X communication to improve safety and compliance this phase shows how the analysis both builds upon and departs from the body of existing literature by comparing the studys findings with earlier research. This methodology offers a methodical way to assess V2X communication in order to enhance compliance automation and driver safety. It covers standardization analysis threat classification literature review and security solutions through a multi-phase process. By highlighting open issues revealing gaps and offering insights into cutting-edge technologies the study lays the groundwork for further research into dependable secure V2X systems. [11][12][13][14]

4. RESULTS & DISCUSSION

Various imperative discoveries from the subject Investigation of Vehicle-To-Everything (V2X) Communication to Upgrade Driver Security and Compliance Mechanization highlight how progressive V2X is for advancements in security activity administration and car security. Utilizing the assets provided the taking after are critical comes about.

DOI: 10.17148/IJARCCE.2024.131102

1. Expanded security on the streets. By empowering real-time information sharing between automobiles foundation and other street components V2X communication effectively brings down mishap rates by conveying early notices of possibly perilous circumstances. To anticipate collisions and increment street security drivers can advantage from this expanded situational mindfulness by being way better able to expect impediments potential hazards and indeed changes within the climate. As Cyient focuses out joining communication between vehicles and foundation (V2I and V2V) inside V2X comes about in a organized street environment where all parties respond rapidly to conceivable threats.

2. Robotized Bolster for Direction and Compliance. By permitting robotized speed alterations path direction and signaling adherence based on current street conditions and lawful prerequisites V2Xs advanced communication system makes it simpler to comply with activity directions. Accomplishing standardized authorization of activity laws bringing down human blunder and empowering more secure driving hones may all be made conceivable by these highlights which move forward compliance without solely depending on driver input. Usually particularly supportive in urban settings with complicated activity laws and fluctuating speed limits.

3. Way better dealing with of activity. The capacity of V2X to way better control activity stream is one of its vital comes about as Encora talks about. V2X can make strides travel times and lower fuel utilization by optimizing activity signals based on data from vehicles and activity foundation. Indeed amid top hours smoother stream is made conceivable by V2Xs dynamic street stack adjusting which brings down emanations and makes the activity framework more biologically inviting. V2X is a useful tool for policymakers and urban planners trying to establish sustainable transportation networks because of these advantages.

4. Increasing Security and Privacy Issues. V2X has benefits but because it requires strong data protection it also creates new security issues. The reliability of real-time information vital to road safety can be jeopardized by cyberthreats such as data tampering and spoofing which can affect the communication systems in V2X. In order to keep V2X a dependable tool for safety and compliance automation ResearchGate highlights the need for secure communication protocols and authentication procedures to stop unwanted access.

5. The Development of Standardization Initiatives. According to a number of sources interoperability in V2X technologies depends on standardization. When taking into account regional variations in technologies such as Cellular-V2X (C-V2X) in China and Dedicated Short-Range Communication (DSRC) in the US the absence of unified global standards currently presents a challenge. Standardization will facilitate smooth cross-border communication allowing V2X technology to be widely adopted and efficiently regulated. These standards are anticipated to evolve to fill security interoperability and data management gaps as V2X technologies advance.

6. Possibility of Autonomous Car Assistance. V2X establishes the foundation for autonomous vehicles by enabling real-time communication between automobiles and infrastructure. In order to achieve fully autonomous driving autonomous systems must be able to understand and communicate with their environment which requires this communication backbone. According to Cyients in-depth analysis V2X can serve as a dependable data stream for self-driving cars enabling them to function more safely and effectively by maintaining constant connectivity with their surroundings. Seven. Future Paths for Research. Integration with AI-driven misbehavior detection and real-time response systems that dynamically adjust to new threats are two unexplored research areas in this field which is still developing. By filling in these knowledge gaps V2X will be able to grow safely and build a robust system that can handle the increasing complexity of connected and driverless cars. V2Xs long-term survival depends on industry and academic efforts to achieve this scalability while reducing computational load. To sum up improvements in V2X communication have the potential to significantly affect traffic efficiency driver safety and regulatory compliance. Even though V2X presents security and standardization issues it provides a framework for a networked future in which infrastructure and automobiles collaborate to improve global transportation networks. [15][16][17]

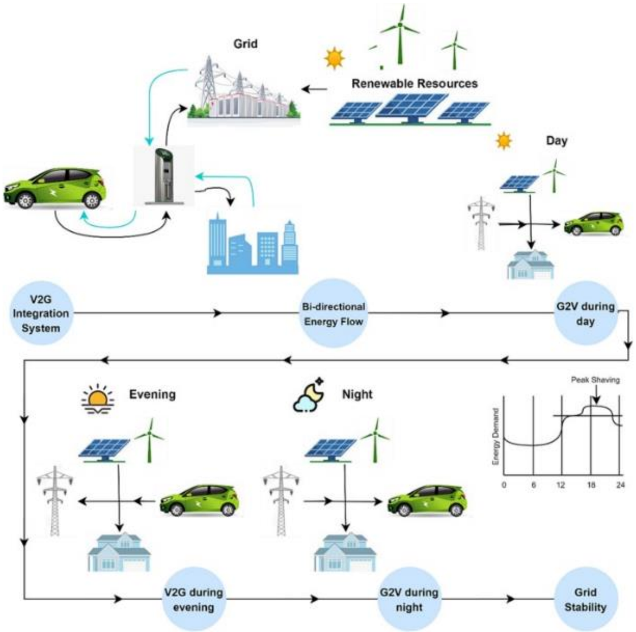

Fig. 5. Vehicle to Everything (V2X) Technology for Sustainable EV Adoption

5. CHALLENGES

Vehicle-to-Everything (V2X) technology has several obstacles to overcome before it can be widely used. V2X networks are susceptible to data spoofing cyberattacks and unauthorized access making security a top priority. These risks may jeopardizing car safety and result in private data being misused. Given the requirement for low-latency communication, it is very much imperative but also difficult to ensure strong security measures such as encrypting and authentication protocols. Another major challenge is standardization also. The implementation of multiple protocols such as Cellular-V2X (C-V2X) and Dedicated Short-Range Communications (DSRC) makes it difficult to achieve worldwide interoperability. Widespread adoption is restricted and compatibility is complicated by the fact that different manufacturers and nations support different technologies. Another obstacle is infrastructure costs particularly when it comes to modifying roads and cities to facilitate V2X communication. Network sensor and connectivity infrastructure setup and maintenance require a lot of resources especially in developing nations. Another problem is data privacy since V2X systems gather a lot of personal and vehicle data. A critical necessity is striking a balance between strict privacy protections and data use for safety. Finally because V2X depends on behavioral shifts and confidence in automated systems driver adaptation is difficult. In order for V2X to be widely accepted users must be educated on its advantages and safety features. When taken as a whole these difficulties highlight the necessity of a multifaceted strategy that incorporates public acceptance regulatory support and technological innovation in order to fully realize the potential of V2X communication. Vehicle to Everything (V2X) Technology for Sustainable EV Adoption is essential in future days, as shown in Figure 5. [18][19]

6. CONCLUSION

In rundown Vehicle-to-Everything (V2X) communication has the potential to revolutionize the transportation industry by progressing driver security mechanizing compliance and opening the entryway to totally coordinates transportation biological systems. Vehicle-to-vehicle (V2X) communication upgrades situational mindfulness brings down the chance of mischances and licenses proactive responses to street dangers by empowering vehicles to communicate with one another the encompassing foundation and indeed people on foot. Robotized compliance frameworks too empower adherence to activity laws upgrading generally street security and decreasing authorization workloads. Nevertheless there are a number of significant obstacles to the widespread use of V2X technology. To safeguard the integrity of information shared comprehensive countermeasures are necessary to address security flaws like the possibility of cyberattacks and data tampering. Regional preferences for communication protocols such as DSRC in the U. S. make matters more complicated due to standardization issues. S. and C-V2X in China impede interoperability and restrict the V2X systems ability to scale globally. International standardization initiatives are essential to filling in these gaps and guaranteeing a smooth globally compatible framework. Financial and logistical obstacles also arise from infrastructure requirements especially when it comes to retrofitting cities and highways with the technology required to facilitate V2X communications. Strategic investment and meticulous planning are necessary for the large-scale development of this infrastructure particularly in rural or resource-constrained areas. In order to improve predictive capabilities and misbehavior detection V2X will likely integrate artificial intelligence and advanced data analytics in the future. To reach its full potential V2X technology will require ongoing advancements in infrastructure security and user adaptation. Governments businesses and academic institutions can work together to make transportation systems safer and more intelligent globally through V2X. V2X has a clear vision: a networked environment that promotes compliance improves safety and streamlines traffic flow. In addition to facilitating V2X adoption resolving present issues will lay the groundwork for intelligent transportation in the future.

REFERENCES

[1]. Y. Fang et al., “A survey of security challenges in V2X: Vehicular communication for safety and security,” IEEE Trans. on Intelligent Transportation Systems, vol. 21, no. 12, pp. 5146-5162, 2020.

[2]. L. Zhang, “Vehicle-to-Everything (V2X) technology in intelligent transportation systems: A review,” Electronics, vol. 11, no. 1, pp. 109, 2022.

[3]. W. Li et al., “5G C-V2X technology for autonomous vehicle applications: A comprehensive review,” IEEE Access, vol. 9, pp. 96454-96479, 2021.

[4]. Y. Sun, S. Du, and J. Song, “Security and privacy in V2X communications: A survey,” IEEE Trans. on Vehicular Technology, vol. 69, no. 12, pp. 14945-14957, 2020.

[5]. M. Sepulcre et al., “Integration of V2X communications in intelligent transportation systems,” IEEE Trans. on Vehicular Technology, vol. 69, no. 10, pp. 11350-11365, 2020.

[6]. Srivastava, P. K., and Anil Kumar Jakkani. "Non-linear Modified Energy Detector (NMED) for Random Signals in Gaussian Noise of Cognitive Radio." International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy. Singapore: Springer Nature Singapore, 2020.

[7]. A. Bazzi et al., “Vehicular communications and the new 5G technology: A survey,” MDPI Sensors, vol. 20, no. 3, pp. 636, 2020.

[8]. Srivastava, Pankaj Kumar, and Anil Kumar Jakkani. "FPGA Implementation of Pipelined 8× 8 2-D DCT and IDCT Structure for H. 264 Protocol." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.

[9]. M. Shirvanimoghaddam, “Challenges and opportunities in C-V2X: A review of autonomous systems,” IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 66-73, 2021.

[10]. Vaza, Rahul N., Amit B. Parmar, Pankaj S. Mishra, Ibrahim Abdullah, and C. M. Velu. "Security And Privacy Concerns In AI-Enabled Iot Educational Frameworks: An In-Depth Analysis." Educational Administration: Theory and Practice 30, no. 4 (2024): 8436-8445.

[11]. B. Liu, X. Wang, and L. Zhu, “Improving urban traffic management using V2X technologies: Challenges and opportunities,” IEEE Access, vol. 8, pp. 127684-127700, 2020.

[12]. M. A. P. Vilela, “Security and privacy issues in V2X communications: A survey,” IEEE Network, vol. 34, no. 6, pp. 1-7, 2020.

[13]. T. Qiu et al., “Vehicle-to-everything (V2X) applications: Frameworks, challenges, and enabling technologies,” IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2876-2888, 2020.

[14]. R. K. Teja and M. S. Iqbal, “Enabling smart transportation systems with V2X: Safety, security, and standardization challenges,” Future Internet, vol. 13, no. 5, pp. 126, 2021.

[15]. K. Abboud et al., “Interworking of DSRC and C-V2X for secure V2X communications,” IEEE Trans. on Vehicular Technology, vol. 69, no. 10, pp. 11240-11254, 2020.

[16]. D. Sabella et al., “Role of V2X in the 5G ecosystem: A security perspective,” IEEE Network, vol. 34, no. 6, pp. 105-111, 2020.

[17]. F. M. Hessar et al., “Security and privacy in V2X communications: Survey on cybersecurity challenges,” IEEE Communications Magazine, vol. 58, no. 8, pp. 88-93, 2020.

[18]. R. Liu, “Artificial intelligence in V2X communication: Enhancing safety and compliance,” Electronics, vol. 10, no. 2, pp. 215, 2021.

[19]. G. Z. Chen et al., “A review of misbehavior detection in V2X networks: Current state and future directions,” IEEE Wireless Communications, vol. 28, no. 4, pp. 82-88, 2021.