IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 May 2023, accepted 28 May 2023, date of publication 1 June 2023, date of current version 7 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3281844

RESEARCH ARTICLE

Blockchain Integration for IoT-Enabled V2X Communications: A Comprehensive Survey, Security Issues and Challenges

P. MURALIDHARA RAO[1], (Member, IEEE), SRINIVAS JANGIRALA[2], (Member, IEEE), SARASWATHI PEDADA[3], ASHOK KUMAR DAS[4], (Senior Member, IEEE), AND YOUNGHO PARK[5], (Member, IEEE)

[1]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
[2]Jindal Global Business School, O. P. Jindal Global University, Sonipat, Haryana 131001, India
[3]Department of Computer Science and Engineering, GITAM School of Technology, GITAM University, Visakhapatnam 530045, India
[4]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad 500032, India
[5]School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, Republic of Korea

Corresponding authors: Ashok Kumar Das (iitkgp.akdas@gmail.com) and Youngho Park (parkyh@knu.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605.

ABSTRACT In V2X (vehicle-to-everything) communication, there is a two-way communication among the vehicle(s) and other Internet of Things (IoT)-enabled smart devices around it that may change how we need to drive. Due to the advancement of Information and Communications Technology (ICT) and the rapid development of IoT in transportation, traditional applications are converted to intelligent applications. In V2X communications, the collected information from the IoT smart devices and other sources passes through low-latency, high-bandwidth, high-reliability links. With the future adoption of the 5th generation mobile network (5G) and beyond networks, V2X continues to produce a huge volume of data. However, collecting and storing data securely in blockchain-based storage are extremely needed for immutability and transparency. In this survey article, the convergence of IoT, V2X and blockchain technologies, and various security challenges and their countermeasures are discussed. Next, we discuss various V2X applications and their respective services. Moreover, IoT-V2X architecture and its enabling technologies are discussed in this article. In addition, we also provide a comprehensive analysis of various security mechanisms. Finally, we provide some important challenges and issues of Blockchain for Intelligent Transportation System (BITS).

INDEX TERMS Vehicle-to-everything (V2X), Internet of Things (IoT), blockchain, attacks, security.

I. INTRODUCTION

Of late, the Internet of Things (IoT) has emerged to provide a wide range of services in complex domains such as climatic monitoring, transportation, industrial services, healthcare monitoring, and smart city applications. The IoT can be formed as a global network of interconnected devices uniquely identified and addressable based on standard protocols. On the other hand, the IoT comprises a network of physical devices that can communicate and compute sensory data. With the rapid development of IoT in transportation, conventional applications are being transformed into intelligent applications. The Intelligent Transportation System (ITS) is predicted to evolve due to significant advancements in IoT technologies that connect vehicles to remote servers via gateways. Most automobile manufacturers now manufacture networking, communication, sensing visualization, and data processing technologies to enrich user experience and safety to promote autonomous vehicles [1]. Connected vehicles have evolved into a viable idea that offers significant solutions. In ITS all vehicles must be equipped with internet capabilities that allow connecting to adjacent

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

access points. After smartphones, linked vehicles surpassed smartphones as the third most popular and rapidly growing type of connected device. Furthermore, the term ''vehicles-to-everything'' refers to connected devices and communication technology (V2X), and the network architecture is shown in Fig. 1. The primary objective of IoT-V2X is to bring advanced solutions to enable traffic management and road safety. It provides many applications and services to increase traffic efficiency, road safety, and user experience. Besides, collision warning and autonomous driving imply autonomous vehicles generate massive amounts of data that is exchanged through vehicle sensors using high-bandwidth and high-reliability networks. Every vehicle has a sensor unit that transmits data to other vehicles and infrastructure like traffic lights, parking spots, and pedestrians. The primary goal of V2X technology is to increase road safety, energy efficiency, and traffic efficiency [2]. On-road car traffic has increased dramatically in major cities during the last decade. As a result, traffic and road accidents are rising in cities and highways, posing serious socio-economic issues [3].

According to data published by the ''National Highway Traffic Safety Administration (NHTSA)'' [4], approximately 40 thousand people die annually from traffic accidents. Advances in ITS could significantly reduce various concerns, including highway collisions, city traffic, and so on. The NHTSA believes using V2X technology would reduce traffic accidents across the country [5]. According to recent research by Hallegatte [6], a decrease of one million crashes might result in a 26 billion USD annual cost savings. Furthermore, V2X assists intelligent services by enabling physical cellular and wireless networks to establish seamless connectivity between vehicles and roadside units. The 4G, 5G and 6G make a significant resolution in broadly developing the V2X applications. V2X provides promising characteristics, like low latency, high bandwidth, extensive support, and wide range capacity to improve connectivity amongst vehicles and access points. The V2X delivers beneficial services for the enhancement of ITS with these technological advancements. However, connectivity and transmission via public channels create several adversarial *Advr* opportunities. As a result, major socioeconomic concerns arise, and the *Advr* can acquire access to automobiles to misappropriate the resources. Thus, intelligent systems demand novel authentication mechanisms to safeguard vehicles and sensitive information.

Authors in [7] devised a robust authentication scheme to enable secure communication and proper mutual authentication. The authors then presented an advanced, reliable authentication strategy to safeguard vehicle sensor networks in [8], proving that their scheme withstands potential attacks. Besides, Tan et al. [9] suggested an upgraded strategy to safeguard against chosen-identity and no-message attacks (CID-CMA) using a different approach.

The future generation of cellular networks improves message delivery performance. Although numerous advanced authentication systems are based on complex pairing, identity-based schemes have been proposed. Cui et al. [10] devised a secure authentication mechanism to withstand various potential attacks and mitigate computational overheads for 5G-enabled networks.

A. RECENT WORKS

Data communication performance is drastically improved over the generation, including 5G and 6G. Identity based and group key based authentication schemes [11], [12], [13], [14] were proposed to address various issues in vehicle networks. Unfortunately, these schemes cannot meet the desired requirements of current vehicular systems. The authors in [10] presented a solution to this problem and designed a lightweight message authentication technique for 5G-enabled vehicle networks.

V2X architectures, communication, and other relevant applications and services have been the subject of numerous recent research papers. Besides, numerous other security issues in V2X environments need to be addressed in message communication, data storage and availability. Recent research on V2X communication technologies relating to short-range and cellular communication technologies was presented in [15]. Moreover, communication channels and protocols for vehicular networks were used in various aspects, such as device authentication, roadside units, and vehicle authentication were discussed in [16].

Traffic-related data, such as that pertaining to current traffic conditions and road construction, is gathered and shared through ''vehicular ad hoc networks (VANETs)''. Moving from a centralized to a decentralized strategy has been popular recently. The authors in [17] conducted a thorough literature review of blockchain-based VANET systems, emphasizing the use of various blockchain technologies in various situations, as well as the corresponding difficulties and research prospects. The V2X communication platforms are made possible by contemporary vehicular wireless technology, which enables information to be sent between cars at any time, from any location to any network. Despite the advantages, V2X apps face significant security and privacy challenges, which is a reasonable concern given that intrusions in automotive communication networks and applications are prevalent.

The authors in [18] presented a detailed description of the V2X ecosystem. Additionally, they examine key security and privacy issues, ongoing standardization efforts, and existing defense mechanisms for the V2X domain. Additionally, the authors in [19] presented a thorough analysis of V2X applications, services, and other associated ITS requirements, with less emphasis on security. The primary application of V2X technologies is now supported by major automotive, telecommunications, and transportation companies: only short-range communications. Dedicated short-range communications (DSRC) and Cellular-V2X, which are based on ''3rd Generation Partnership Project (3GPP) long-term evolution (LTE)/5G NR'' and IEEE 802.11p, respectively.

TABLE 1. Existing related works.

Reference	Research Objective	Problem Discussed	Limitations
[21]	Presented existing security solutions for V2X	Threat analysis, security and privacy for V2X communication technologies	Application scenarios and services were not discussed
[22]	Mobile edge computing state-of-the-art advancements for vehicular networks	Discussed various methods that improve performance of IoT-V2X, including reliability, loss of network connectivity, massive data handling, offloading, network availability and coverage	Lack in covering performance metrics, security and privacy concerns
[23]	Survey on blockchain-based VANET systems	Applications of blockchain for vehicular technologies, various research challenges were addressed	Security and evaluation were not considered.
[24]	Security of 5G-V2X	Security reflex function is addressed to elevate the usage of 5G over V2X, various current research challenges were presented	Discussed more network specifications, not considered applications and services
[25]	Edge-based intelligent networks for Internet of Vehicles (IoV)	Addressing security problems in Intelligent Internet of Vehicles (IIoV), networking, offloading, intelligent mobility-aware caching	Lack proper analysis for evaluating offloading services, and blockchain was not discussed
[26]	Applications of blockchain or hash chain in IoT-V2X communication technologies	Security and safety, security requirements, blockchain applications	Not much details about performance metrics, security evaluation, and future directions
[27]	Blockchain for V2X: applications and architectures	Provided an overview of V2X and Blockchain. Explored potential applications of V2X and architectures	Did not explore much about security and privacy concerns. IoT security is not considered as V2X requires it as a default condition
[28]	Blockchain for vehicular IoT	Explained fundamentals of Blockchain for a vehicular environment. Reviewed several existing research efforts of Blockchain. Discussed research problems and technical issues	Did not deal with application perspectives, and security and privacy challenges were not also focused

Although DSRC has deployments, C-V2X is anticipated to see more extensive trials and transfers in 2021.

Later, the authors in [20] examined the necessity for integrating IoT-based technologies into contemporary ITS solutions and provided insight and a study of the two primary V2X technologies, DSRC and C-V2X, as well as their basic characteristics, drawbacks, and limits. In addition, they discussed security concerns and difficulties with IoT-based V2X solutions. In Table 1, we then discussed the research objective; the problem discussed and the limitations of various existing relevant schemes.

B. MOTIVATION AND CONTRIBUTIONS

Data comes from sensors, through fog devices, and onto a centralized cloud server in traditional Internet of Things (IoT) ecosystems. One point of failure, a bottleneck in data flows, privacy concerns owing to third-party administration of cloud servers, and challenges in frequently updating firmware for millions of smart devices from a security and maintenance standpoint are just a few of the problems that come up. Blockchain solutions protect against single points of failure, trusted third parties, and other problems. This has motivated experts to investigate how IoT can use blockchain technology. In the context of intelligent transportation, and other applications, recent state-of-the-art advancements in blockchain for IoT, cloud IoT, and fog IoT are analyzed in this article. Therefore, we have structured this article to highlight the necessity of security and privacy.

This survey's purpose is to provide researchers with a comprehensive overview of V2X Blockchain Integration, key technologies and methods while also assisting them in understanding how recent works are addressed. There exist numerous research works and related survey articles. However, there are still various aspects that need to be addressed in such a way as to meet the requirements of advanced V2X technologies. We then present a comprehensive survey that focuses on multi-dimensional requirements of IoT-V2X-Blockchain technologies with the following contributions:

- The focus of this survey work is on the most recent trends and developments in the V2X era, as well as original contributions from the research community. It also covers technical information on key 5G advancements.
- This work describes the development of V2X technologies. Additionally, several aspects of the development of V2X technologies are examined.
- This study presents a descriptive taxonomy and discusses the growing applications, research groups, and research areas in the V2X blockchain integration.
- This survey analyses the advantages, applications, major technologies, and important aspects of the current sensor networks with the emergence of requirements in the mobile networks era.
- Issues and concerns related to security are then explored.
- Finally, this survey concludes with some recommendations for the future open challenges.

The current survey concentrates on implementation concerns, challenges, and essential themes. In contrast, this survey includes the most recent breakthroughs by researchers and state-of-the-art methodologies. With the core technologies boosting the development and manufacture of 5G goods, several recent relevant articles are highlighted.

C. OUTLINE

This survey article is organized as follows. We discuss the state of art mechanisms for the V2X-Intelligent

Transport System (ITS) in Section II. IoT-V2X architectures and enabling technologies were discussed in Section III. Later on, we systematically studied security and privacy by considering various security issues, challenges, countermeasures, performance analysis, and future vision in Section IV. In Section V, we highlight important challenges and issues of blockchain for ITS. Lastly, Section VI concludes the article.

II. V2X-INTELLIGENT TRANSPORT SYSTEM: STATE-OF-THE-ART

A. INTELLIGENT TRANSPORT SYSTEM

The world has evolved from the IoT to the IoE, bringing significant communication technology advancements. Besides, IoT improvements have equipped smart devices to promote advanced solutions throughout the last decade. They largely employed vehicle monitoring and tracking services, which are increasingly demanding. A vehicle driver can use WSN to get the information that necessitates safe driving situations such as vehicle speed, accidents, emergencies, and traffic congestion. As a result, because information can be transmitted over a public channel, a driver or traffic controller may be subject to various attacks. As a result, vehicle communications are also increasingly vulnerable. According to recent studies [28], more than three billion people spend at least two to three hours on the road; transportation is becoming increasingly important. Traffic congestion, accidents, rising mortality, and other issues have plagued traditional transportation networks. As a result, Transport systems arise to provide data-driven services to vehicular systems to solve problems with traditional transportation systems. Currently, data is shared among vehicles, drivers, and RSUs can in turn helps to enhance information to develop new ITS capabilities and services [29]. Advanced transport management systems, traveler information systems, vehicle control systems, commercial vehicle management, and public and urban transport management system are six major components of data-driven ITS.

B. CONVERGENCE OF IoT, V2X AND BLOCKCHAIN TECHNOLOGIES

In the past two decades, the number of vehicles rapidly increased, increasing road traffic. The huge production of vehicles is also one of the reasons for increasing traffic on roads due to various social problems such as road accidents, air pollution, economic loss, loss of fuel, traffic jams, and time. Road accident is a major problem, and due to this, 1.5 million people die annually. The 2019-20 year accident report shows that 15 million people died in India, and 50 million were injured. Every country needs road safety policies to reduce the aforementioned issues. The national security agencies conceal sensitive information and security policies merge with ITS to promote large-scale services. The ITS aims to improve road traffic by eliminating difficulties. It alerts users to traffic jams, accident areas, slow and rapid speed zones, and real-time running information. It cuts travel time and improves safety and comfort. ITS promises to improve road safety and save time, cost, and pollution. ITS faces various security issues while communicating device vehicle and vehicle to vehicle. Blockchain technology is one of the emerging technologies, and it will address the security problems in the ITS network.

C. TARGETED FIELD

In this section, the transportation of vehicles on roads consists of various factors such as communication among vehicles, roadside unit (RSU), data centers connected via the internet and wireless communication. At this point, attackers may choose to tamper with or modify the data in communication among various vehicles or devices. Therefore, we need a secure Intelligent transport system (ITS) to provide secure communication.

Anusha et al. [30] devised a novel blockchain-enabled certificate-based authentication scheme for vehicle accident detection and notification in ITS (BCAS-VADN). The proposed mechanism addressed various potential attacks, but still, they need to include other adversaries, like non-repudiation and need to evaluate by considering data sets. Kumar et al. [31] presented a secure framework based on privacy preservation to address security and privacy challenges in cooperative intelligent transportation systems (C-ITS). Two modules, blockchain and deep learning were used in this technique. One was proposed and analyzed using the ToN-IoT and CICIDS-2017 network datasets and security and privacy concerns. The scalability and utility of the proposed one must be considered. Compared to recent strategies, addressing the numerous potential attacks is necessary. The authors in [32] presented SmartCoin, a novel vehicle incentive system based on a consortium blockchain. The proposed method intends to increase social welfare and transportation, reduce traffic congestion and road accidents, and develop a transportation network free of fraudulent information. Various mechanisms have been proposed for developing an effective ITS for secure and fast communication among various entities in transport.

Jabbar et al. [33] designed a Blockchain-based framework secure V2X communication and payment system. Their framework employs Ethereum to facilitate seamless and secure payment services at parking within the V2X environments. Their framework was experimentally tested to assess its computational costs, communication expenses and the real-time aspect.

New requirements, such as secure, smooth, and robust information exchange among cars in vehicular networks, are emerging with the rise of connected vehicles and an exponential expansion in online cab booking services. In this context, networked and autonomous vehicles a new concept are replacing the fundamental idea of vehicular networks. Because autonomous vehicles can rapidly access current information, they provide a better user experience

and aid in reducing traffic. However, unscrupulous users in the automotive Internet may misdirect all communications, and hackers may hijack smart gadgets to carry out a malicious ruse. As a solution, Rathee et al. [34] designed a secure blockchain-based protocol for connected and autonomous vehicles.

Oham et al. [35] designed a framework for securing small vehicles based on blockchain (B-FERL). B-FERL uses permissioned blockchain technology to control access to information for certain companies inside the ecosystem of linked vehicles. It also uses a challenge-response data exchange between vehicles and roadside devices to detect instances of in-vehicle network compromise. Only vehicles with a verifiable record on the blockchain can exchange messages in the vehicular network to enable authentic and legitimate communication. Quantitative analyses in a simulated environment demonstrate that B-FERL ensures an appropriate response time and needed storage space compatible with real-world conditions.

D. V2X-BLOCKCHAIN APPLICATION PERSPECTIVE

In this section, we discuss the transport applications developed using blockchain technology. We focus on blockchain-based ITS in particular. Jabbar et al. [36] conducted a systematic review on blockchain for ITS. The authors classified various research directions regarding security, communication, energy, transportation, payments and optimization. Then, Lei et al. [37] proposed a novel key management scheme using blockchain technology. The proposed scheme optimizes the efficiency and key transfer cost. However, the work does not consider security and privacy issues. The users require to decide the trade-off between security and privacy. In 2017, Johar et al. [38] proposed a blockchain-based novel pseudonym management scheme for ITS. Their mechanism shows better results regarding execution time, memory, and processing time. In this work, the authors did not include the potential attacks of RSU (Road side unit) in ITS. Various possibilities are presented for attackers for RSU. Blockchain technology is required to enhance the proposed mechanism.

E. REAL-TIME ISSUES AND CHALLENGES

1) PRESERVING DATA SECURITY ACROSS NODES IN IoT

IoT devices produce a large amount of data shared with other network nodes and embedded software. Blockchain provides a secure method for data distribution, which enhances data security and preserves the nodes' anonymity. The data is stored using cryptographic hashes in a tamper-proof block linked to the previous block. The adoption of blockchain in IoT presents challenges, like higher processing power of nodes, heterogeneous and diverse devices, and the absence of governing regulations and skills for blockchain development [39]. The solution for the various concerns requires collaboration and coordination between each entity of the IoT system. The data stored in a centralized cloud makes it vulnerable to attacks and single-point failures. The use of decentralized storage on the blockchain can mitigate this. Various properties of blockchain can be adopted for wireless sensor networks (WSN), which are limited in their power consumption capacity. The data produced by IoT devices can be considered transactions and is associated with a unique identity composed of device number and location. Each node receives information from the network, combine it with its data and redistributes it amongst other nodes, which is similar to a full node ledger of blockchain [40].

F. PRIVACY IN ELECTRONIC RECORD STORAGE AND SHARING

Security and accuracy are seen as essential requirements for electronic record storage. Data-sharing between various health organizations is often required for analytics purposes. A user's privacy must be preserved in such cases. The usage of a hybrid system involving private and consortium blockchain is proposed by Zhang et al. [41], which is an efficient way to address data security concerns. The private blockchain holds the data within the organization, while the consortium blockchain contains the keywords and is accessible to all organizations in the coalition. Access to such a database is based on cryptographic signatures. Attribute-based encryption (ABE) provides greater access security where the smart contract can facilitate transactions based on data and design the authorization structure. A combination of two attribute-based encryption algorithms: key-policy ABE (KP-ABE) used for access control for service providers and ciphertext policy ABE (CP-ABE) for individuals after patients consent is proposed by Pournaghi et al. [42]. Private blockchain provides an efficient mechanism to improve the right to revoke instant access in case of attribute-based encryption. Further, geospatial blockchain, which stores crypto-spatial coordinates along with the data, was proposed by Boulos et al. [43] for improving data accuracy where the traditional blockchain lacks such property.

1) DATA IMMUTABILITY AND AUTHORIZATION

Data privacy in elections is essential to instill trust in voters for an authentic election. The preconditions for an election are preserving data anonymity and preventing tampering with records. Lee et al. [44] proposed a model comprising a trusted third party and authentication organization for maintaining user privacy. The user interacts with the trusted third party, which verifies its identity from the authentication organization that maintains a record of all authorized voters. The trusted third party verifies the hash with the authentication organization without revealing the voter's identity. After verification, voters can cast votes in the form of a transaction. Time stamping prevents multiple transactions. Smart Contracts are irreversible applications that work on decentralized applications, like blockchain. Deploying smart contracts for voting ensures that the stored data is immutable and can be used for authorization. Hjalmarsson et al. [42]

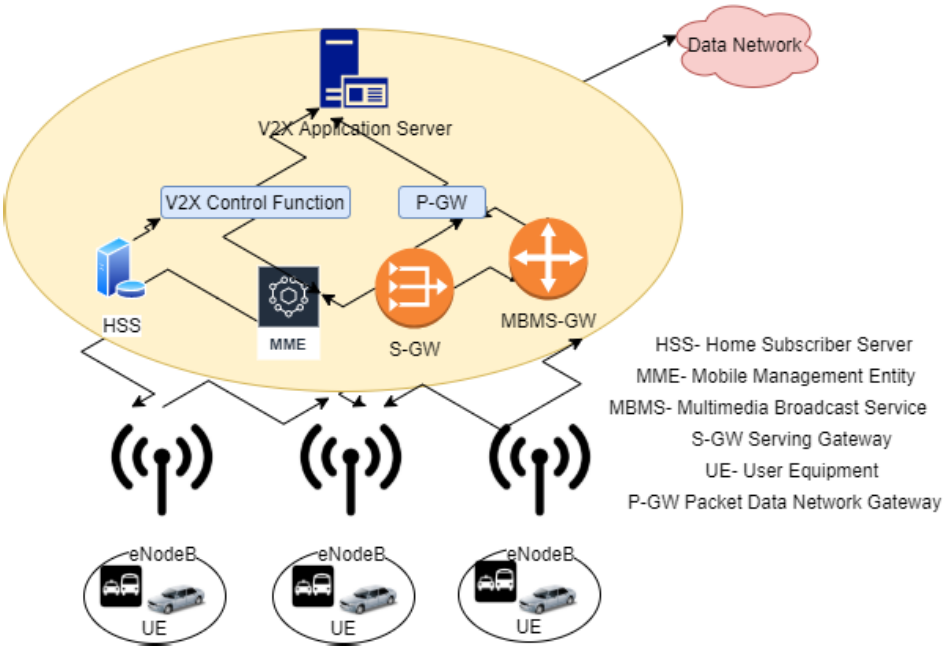

FIGURE 1. V2X network architecture.

presented a model utilizing the power of smart contracts. Smart contracts govern the interaction between voters and monitoring entities at various levels. The system offers work traceability, ensuring that forging data is impossible. Table 2 describes various security challenges addressed and depicts countermeasures.

G. V2X: COMMUNICATION STANDARDS AND PROTOCOLS

Short range wireless communication and cellular technologies major contributors of V2X systems. The wireless communication technologies were developed specifically for data transmission between vehicles, users, RSUs, and pedestrians. Wireless communication technologies works based on IEEE 802.11 p extension generated from a Wi-Fi version (IEEE 802-11). C-V2X or LTE-V2X employs the same SIM technology as your smartphone. These communication technologies were largely utilized for V2X applications including vehicle remote monitoring, tracking, and traffic management. as wireless connectivity is seamless, the driver can access vehicle information, and connected with V2X applications to receive notifications about vehicle speed, accidents warning, emergencies, and limited distances. The same level of services can be deliver through pedestrian mobile applications, car onboard devices, and roadside infrastructure RSUs. However, because of its traditional short-range communication and reliability, efficiency, and latency in mass traffic scenarios, DSRC is becoming a difficult issue for the improvement of the V2X communication system. Table 3 depicts various communication standards for short-range and long-range mediums along with properties.

Because of the limitations of DSRC, cellular communication technologies have become an important aspect of V2X communication. It improves performance while offering a diverse set of connections, allowing for enhanced coverage, capacity, and productivity. Furthermore, it can improve efficiency by allowing intermediate stations to relay data to all nodes. As a result, the strain can be reduced, and the communication system's latency can be improved. Different cellular communications standards are available depending on the pricing and deployment needs. 2G, 3G, 4G (LTE, LTE-A), and 5G are the four types. Assistance with traffic and information on traffic The basic goal of a traffic management program is to transfer information about road conditions collected by vehicles or roadside units to other vehicles, such as speed management, cooperative navigation, and improved routing.

H. V2X APPLICATIONS

As shown in Fig. 2, this section presents several V2X applications in ITS and vehicular communication technologies. These include entertainment, traffic management, autonomous driving, and road safety. For instance, traffic management includes, among other things, speed management, route data, and traffic data. Road safety issues such as dangerous crashes, intersection warnings, and others are covered. There are also automated speed control, automatic tracking, electronic stability control, and other elements for autonomous driving. Finally, audio, video, data visualization, automatic traffic optimization, entertainment, and comfort-related services are all included in infotainment.

TABLE 2. Security challenges and countermeasures.

Reference	Problem addressed	Techniques proposed	Limitations
[46]	Security of data in IoT	Mitigation of single-point failure in the cloud using decentralized storage. Cryptographic hashes along with the immutability property of Blockchain to eliminate IP spoofing.	Lack of interoperability between devices and restricted power capacity of nodes. Absence of standards and legal regulations for the usage of Blockchain.
[44]	Reliable system for data exchange	Developed a lightweight sensor chain-like system based on Blockchain for wireless sensor networks (WSNs)	Unlike a wired network, the mobile nodes in an IoT have a restricted-energy budget.
[47]	Securing IoT infrastructure using distributed ledger	Peer-to-Peer, tamper-resistant mechanisms were considered. The existing entities of the Internet autonomous system number (ASN) and DNS domain owners are considered peers.	The scalability of Blockchain is not being tested for the application.
[48]	Enhancing the security of vehicular communication system	Onboard unit in vehicle transmits messages to security managers (SM) periodically. Transmit messages in the form of transactions and unlike the traditional system, there is no need for a certification agency (CA).	Lacks privacy of data transmission between SMs
[49]	Providing security and privacy using Blockchain in an existing application.	The level of trust in the enhanced PGP, as proposed, relates to the number of bitcoins the entity can be trusted with.	High computational overheads

TABLE 3. Comparison of other cellular technologies with 6G.

Properties	LTE	LTE-A	5G	6G
Range	30 km	30 km	≈ 500 m	320 m outdoor
Frequency Band	700-2600 MHz	450 MHz-4.99 GHz	57.05-64GHz	94 GHz-3 THz
Channel Width	1,4,3,5,10,15,20 MHz	Up to 100MHz	2.16 GHz	410 MHz to 7.125 GHz
Latency	10 ms	–	1 ms	1000 times faster
Mobility Support	Very high	Very high	Ultra high	Extreme high
Bandwidth	50 Mbps	1 Gbps	20 Gbps	1 Tbps
Operational cost	Low	Low	Very low	Very low

1) CONTROLLING TRAFFIC

By allowing traffic assistance and raising traffic awareness, it can be done. A traffic management program's main objective is to disseminate information on the state of the road, as well as speed management, cooperative navigation, and enhanced routing, to other cars.

2) ROAD (HIGHWAY) SAFETY

These apps are made to provide drivers with accurate information about various scenarios that aren't always obvious, such as potential risks. There are two types of traffic management apps: ''time-critical applications'' and ''less time-critical applications.'' Hard safety was defined by time-critical applications, which were in charge of facilitating preventive actions to avoid crashes and hazards. In the future, less time-critical applications will be soft safety applications. Soft safety apps are not required to decide right away and inform the driver of their findings.

3) AUTONOMOUS DRIVING

These programmes enable the user to control the driving accessories or drive the automobile with our driver. These apps help drivers stay well-rested while travelling long distances. Additionally, it helps with resource optimization, electronic usage automation, and other processes.

4) INFOTAINMENT

These applications are specifically developed to enable Internet access so travelers can continue working without interruption. Web-based applications, audio-video streaming, and navigation services are available to passengers. For example, these apps can help you identify nearby medical establishments, eateries, and nearby petrol stations. Furthermore, these applications aid in the reduction of communication restrictions such as packet latency or packet loss. V2X communication contexts mostly influence these. Cellular technologies provide several benefits to low/short-range communication technologies in achieving low latency and a high packet delivery ratio.

III. IoT-V2X ARCHITECTURE AND ENABLING TECHNOLOGIES

Machine-to-machine (M2M) and Machine-to-human (M2H) connections are two types of IoT connections that differ from

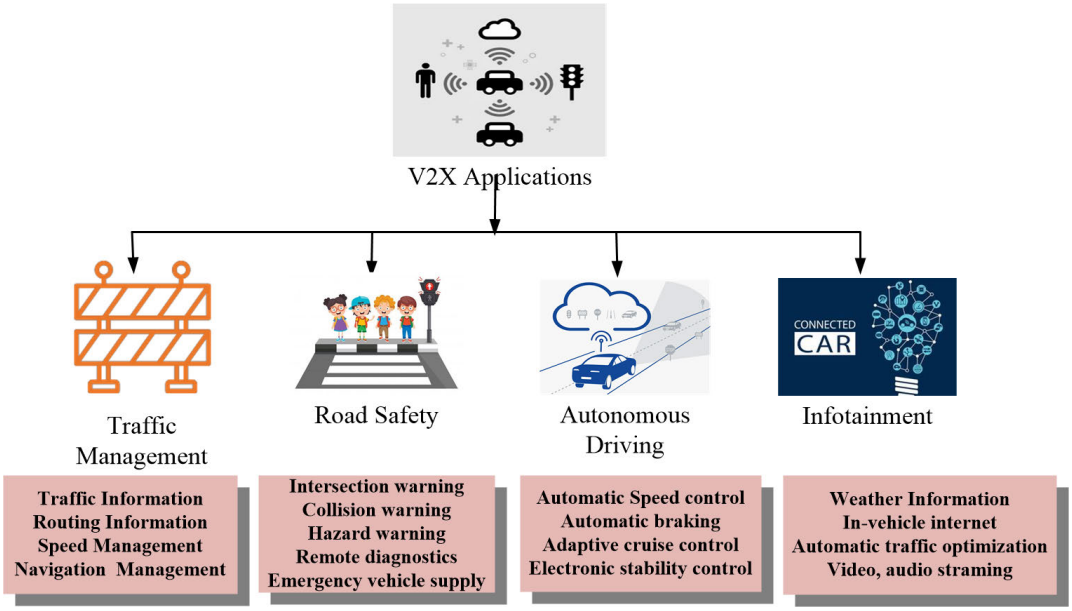

FIGURE 2. V2X applications and services.

standard Internet connections. M2M methods offer a variety of applications for locating, identifying, tracking, controlling, monitoring and transmitting data across heterogeneous devices. However, the correlation between physical gadgets has grown tremendously, and this has prevailed. Various authentication systems have been proposed, specifically to improve security efficiencies in the V-IoT. Furthermore, the V-IoT requires a lot of storage and computational power in the physical world to analyze a lot of real-time data. As a result, intermediate steps must be required, and indefinite storage is in high demand. Fig. 3 depicts the generic IoT-V2X software architecture. Vehicle to Infrastructure (V2I) is the data interchange between a car and equipment erected beside roads, commonly referred to as an RSU. V2I is commonly utilized to notify drivers about traffic conditions and emergency situations. Data is exchanged through vehicle sensors using high-bandwidth and high-reliability networks in the V2X system. Every automobile has a sensor that transmits data to other cars as well as infrastructures like traffic lights, parking spots, and pedestrians. V2V is a communication technique that helps to avoid collisions. It makes use of VANETs, which are wireless networks that allow vehicles to communicate and share information about their driving habits.

The IoT-V2X is made up of a number of components, including interface drivers that allow processing devices and hardware to communicate. The Graphical User Interface (GUI)Â is employed to enhance the control abstraction of the application and display pertinent data on the display device. The operations and functionalities of the V2X communication system are defined by API, the lowest level of programming. API is mostly utilized for operating system software integration. Radio module configuration and key settings are set via RF IC registers. Using graphical data representation enables digital processing and its outcomes in devices and signals. To set up communication between the CPU unit and the hardware, use Data Stream options. To quickly check and boot known settings, use framework state load/save. A signal clock setup is also used to set the clock signals. (Field Programmable Gate Array) FPGA code configuration is used to load firmware codes. Finally, Initialization creates the necessary parameters and resets the framework to its initial state. Hardware controls are used as a group for framework controls.

A. 5G NETWORKS

4G could not properly meet new difficulties such as increased capacity, higher data rate, massive device connectivity, lower latency, cheaper cost, and consistent QoE provisioning because of the exponential increase in user demand. Cellular network enhancements are required to satisfy these needs, prompting network operators to seek solutions for introducing 5G mobile networks. Furthermore, 5G infrastructures offer specialized network solutions for the automotive, agriculture, and energy industries. Dedicated Short Range Communication (DSRC) is a wireless communication system allowing automobile and infrastructure communication. DSRC allows for secure, high-speed communication without a cellular network. The DSRC technology was created with vehicular communications in mind. It is a widely standardized short/medium-range technology that operates in the 5.9 GHz frequency. The 3GPP-developed radio access technology (RAT) for 5G contains two frequency ranges: FR1, which runs below 6 GHz, and FR2, which operates

above 24 GHz and into the extremely high-frequency range above 50 GHz. The new air interface for 5G has been called 5G NR by 3GPP (New Radio).

5G development has moved forward, because it makes it easier for mobile devices to connect to the Internet of Things (IoT) and work together, especially for large-scale wireless sensor networks (WSNs). 5G cellular technology aimed to have high peak data speeds, low latency, reliability, and network capabilities [48]. With the development of 5G networks, individuals can connect and share information between terminals and mostly everyday objects. Statistics reported in [49] indicated that by the end of 2020, more than 50 billion sensor devices will be connected to the Internet around the world.

The 5G-V2X vehicles that will be available starting in 2025 employ different chips, frequencies, and software than the LTE-V2X vehicles of today. It seems sensible that the challenging start-up phase entirely slows down many inventions. For instance, automotive inventor, Tesla, has abstained entirely from V2X communication [50]. From the user's point of view, 5G can do many new things, such as having a high bandwidth of 10 Gbps, low latency of one millisecond, a channel width of 2.16 GHz, support for ultra-high mobility, and low operational costs. Because of these changes, the Quality of Service (QoS) and Quality of Experience (QoE) are much better. Table 3 compares the characteristics of 5G cellular networks in detail to those of LTE and LTE-A.

B. 6G NETWORKS

Future 6G wireless has attracted tangential research attention. As more individuals accept this change to an indefinite workplace, 5G will become more commercially viable. Increased Internet usage, as a result, highlights the need for improved connectivity to handle the increasing demand for uncompromising network specifications. This is necessary to enable new technologies like the Industrial Internet of Things and extended networked autonomous cars. Besides, data rates in the range of terabits per second and a latency of under 1 ms are expected with 6G. With 107 connections per km^2, it is anticipated that it will power the Internet of Everything. With a higher frequency range than the mm-wave spectrum (30-300 GHz) used in 5G, 6G will use 300 GHz to 10 THz spectrum to accomplish this. Because the sub-6GHz area is already overcrowded, it is vital to investigate a higher frequency spectrum. The Terahertz spectrum not only allows for more spectrum but it also results in higher data speeds that are desirable for 6G networks. However, transmission distance is constrained by substantial path loss when using a higher frequency spectrum.

6G enables decentralized, cooperative environmental sensing applications made possible by blockchain technology. These abilities can be used for things like smart cities, transportation, and protecting the environment for the green economy. It is expected that 6G internet will be available for sale in 2030. The technology makes the most of the distributed radio access network (RAN) and the terahertz (THz) spectrum so that capacity, latency, and spectrum sharing can all be improved. The technologies that will drive 6G are the Terahertz (THz) band, artificial intelligence, optical wireless communication (OWC), 3D networking, unmanned aerial vehicles (UAV), and wireless power transfer [51]. It is expected that 6G technology will have faster speeds, less latency, and more bandwidth than 5G [52]. This will increase productivity and open up new automation, AI, and IoT opportunities by instantly sending massive amounts of data across decentralized networks. Khan et al. 2021 show how blockchain and 6G will affect future communication systems. The authors of this work divide these application requirements into two main groups [53]. In the first group, Requirement Group I (RG-I), authors include performance-related requirements like data rates, latency, reliability, and massive connectivity. In the second group, Requirement Group II (RG-II), authors include security-related requirements like data integrity, non-repudiation, and auditing. With blockchain and 6G, networks would be less centralized, and resources would be shared more. This would help reach the goals of RG-I. The RG-II requirements of 6G applications can also be easily met by choosing the right type of blockchain and consensus method. This study shows that combining blockchain and 6G is an elegant way to make communication in the future safe and everywhere.

Khan et al. [53] evaluate current developments made to allow 6G systems. The authors establish a taxonomy based on the most important enabling technologies, use cases, new machine learning techniques, communication technologies, networking technologies, and computer technologies. Moreover, the authors identify and solve unanswered research concerns, including adaptive transceivers based on artificial intelligence, intelligent wireless energy harvesting, decentralized and secure commercial models, intelligent cell-less architecture, and distributed security [54]. The authors suggest various ways to overcome these problems, such as deep Q-learning and federated learning-based transceivers, blockchain-based secure business models, homo-morphic encryption, and authentication techniques based on distributed ledgers.

Aggarwal et al. [55] conducted a study on security issues with blockchain and 6G technology. Mainly, UAVs are commonly utilized in dangerous areas. Hence, these devices need a secure network. In this article, we explore 6G technology's architecture, requirements, and use cases.

C. BLOCKCHAIN TECHNOLOGY

Blockchain is a data storage technique that renders system manipulation, theft, and fraud nearly impossible. A blockchain is a network of connected computer systems that contains multiple copies of a digital log of transactions. From easy-to-track operations to tamper-proof transaction records to lower transaction fees, blockchain solutions benefit the automobile industry payments in various ways.

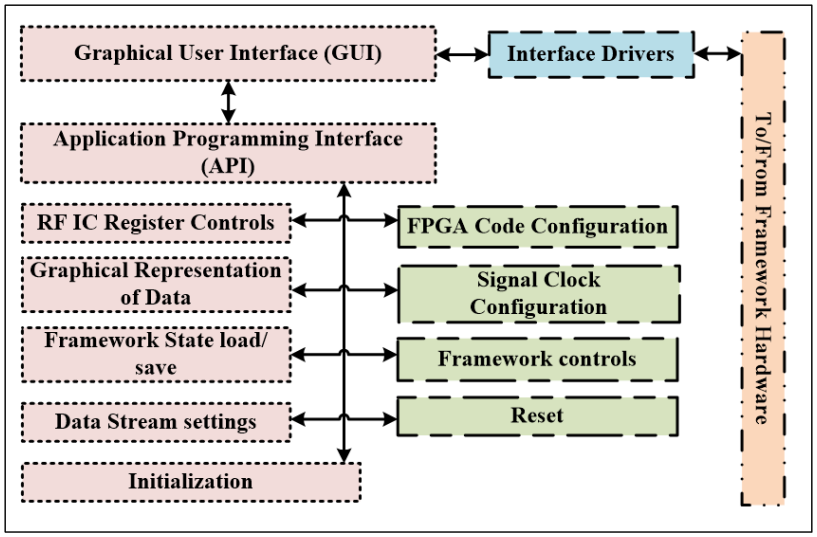

FIGURE 3. A generic IoT-V2X software structure [56].

TABLE 4. Security goals and properties.

Security goal	Properties	Adversarial acts	Counteractions
Mutual authentication	Secure authentication, Anonymous remote authentication	FN, RA, NC, DDoS, MiTM	-Encryption standards -Location hiding -Digital signature -One-way hashing -Nonce -Access control -Identity based authentication -Group signatures -Multi-factor
Confidentiality	Privacy preservation, Secure session key management, Location privacy, Perfect secrecy	TA, TRA, MiTM, ED	
Integrity	Data protection, Information reliability	MiTM, FN, MNI	
Availability	Timely resource access	DoS, DDoS, DoSl	
Accountability	Trace track activity, Anonymity	TRA, TA, MNA, SNI, MNI	

Note: FN: Fake node, RA: Replay attack, NC: Node capture, DDoS: Distributed Denial-of-Service (DoS), DoSl: Denial-of-Sleep, MiTM: Man-in-the-Middle attack, TA: Tampered attack, ED: Eavesdropping, SNI: Sensor node injection attack, TRA: Tampered routing attack, MNA: Mass node authentication, MNI: Mass node injection.

However, while designing any blockchain-based solution, three issues in particular demand special consideration. Blockchain technology ensures complete transparency and expedites the transfer of car ownership. A smart contract is another feature of blockchain that allows the seller and buyer to enforce a goods transaction without needing a mediator.

The decentralized ledger of blockchain could allow driverless cars to access vital traffic data instantly and more precisely. The use of smart contracts, made possible by blockchain technology, may simplify paying for tolls, repairs, and vehicle insurance. Because the real-time autonomous decisions must be made in a split second, 5G's low latency characteristic enables cars to receive information at fast rates and react quickly to avoid obstacles. Autonomous vehicles using the 5G technology must be widely accessible to be put into use. Tesla's semi-autonomous driving capabilities are presently available. However, they only use the network as a secondary mode of communication [57]. Using encryption, specialized data structures, peer-to-peer (P2P) networks, game-theoretical incentives, and fault-tolerant consensus algorithms, a blockchain is a form of a distributed state machine that enables users to agree on changes to the state of a global database. Users can create complicated applications that leverage the shared database by using smart contracts, which let them set the rules for database updates through software programs.

There are various possible uses for the blockchain technology in the V2X industry. Various automobile industry stakeholders include car manufacturers, insurance companies, and governmental organizations. Stakeholders can agree on a blockchain technology protocol in which they all take part in maintaining the common ledger, each checking its contents and keeping records to ensure it is not being abused. The open nature of blockchains enables a broad range of users to use the system on an even playing field without anyone being disadvantageous. Blockchains also provide precise data auditing, which is crucial for many V2X applications, particularly accident investigations [26].

D. CLOUD COMPUTING

Cloud computing is developing into the automotive Internet of Things market, enabling autonomous car technology to be

developed. Cars will be able to interact with one another via the cloud to avoid accidents and update traffic information and maps. A self-driving car (also known as an autonomous car or a driverless car) is a vehicle that travels between destinations without the assistance of a human driver using a mix of sensors, cameras, radar, and artificial intelligence (AI). A typical high-tech cloud-based system for autonomous vehicles combines traditional cloud computing with access to and use of self-driving vehicles through the cloud's standard parts. One of the options is Vehicular Cloud Computing (VCC). VCC is a novel hybrid technology that significantly impacts traffic management and road safety by making fast decisions using vehicular resources like computers, storage, and the internet [58].

E. FOG AND EDGE COMPUTING

Edge computing is a processing that is carried out at or close to the source of the data, as opposed to relying on the cloud at one of 10 data centers to perform all the work. This doesn't mean the cloud will disappear. It serves as a warning that the cloud is getting closer. Autonomous vehicle connectivity to the edge can improve security and productivity, lower accident rates, and ease traffic congestion. These vehicles have a variety of sensors, which produce a large amount of data that needs to be processed quickly. The VFC (vehicular fog computing) uses the idle resources of vehicle-loaded computer systems to provide computing services at the network's edge. VFC-related task scheduling and resource allocation have recently received a lot of attention. Edge computing is better suited for applications that require quick and consistent responses. That group includes autonomous vehicles. In fact, applying processing at the edge can reduce the quantity of data that needs to be transferred, resulting in even faster reaction times.

IV. V2X: SECURITY AND PRIVACY

As the demand for ITS and related services grows, so does the need for an attack plane. The IoT and V2X have become vulnerable as a result of technological improvements. Furthermore, the insecure wireless communication channel has been used to connect cars, controlling systems, RSUs, and other associated facilities. As a result, an attacker could do harmful actions throughout the connection formation and communication phases. As a result, this section discusses numerous security issues, requirements, and potential V2X attacks. Table 4 depicts various security goals, properties and possible counteractions presented here. The short forms used in adversarial acts can be referred to in Section IV.

A. SECURITY CONCERNS

The following are the important security concerns.

- *Adaptive Scalability:* A vast volume of data is generated and transmitted in the V-IoT context for further processing. However, because of the dynamic node addition, the increasing device consumption puts the present system at risk. As a result, there is a desire for secure node authentication procedures that simplify the sensing device addition phase while maintaining security.
- *Energy:* Many IoT devices are resource constrained, particularly those with limited battery capacity. When no activity is detected, these devices can automatically save energy by turning on the power-saving mode. However, the majority of the gadgets are utilized for continuous monitoring. As a result of this restriction, imposing high-level security on these IoT systems is extremely challenging.
- *Dynamic Network Topology:* The mobility of V2X makes the dynamic nature of vehicular commutation technologies and their topologies hard. It is difficult to offer comprehensive security solutions that can survive multiple threats. Vehicles typically travel from one area to another at great speeds, making it difficult to offer adequate protection.
- *Heterogeneity:* We realized that we utilize a variety of gadgets for our convenience, such as IoT sensors, RFID systems, cell phones, and so on. The computing, communication, and storage capacities of these devices may vary. As a result of these IoT devices, designing a secure authentication becomes difficult.
- *Defending against Attacks:* Vehicle communication networks are designed to support various applications and services. The vehicle must be connected to the Internet to provide all essential services. Furthermore, the car must broadcast fundamental private information, such as the vehicle's identity and other associated data. As a result, authorizing the vehicle requires high security, and it should not be exposed to potential assaults.
- *Future Technology Adoption:* It must be compatible with emerging technologies that use the existing system. It enables future technology security, which is becoming an increasingly important challenge. The existing system requirements determine how security and privacy are integrated.
- *Latency:* Due to the widespread usage of DSRC and cellular communication technologies, latency may cause challenges in V2X commutation. Furthermore, each vehicle may communicate additional data. As a result, processing the data before sending it to the destination is a significant load. As a result, latency concerns may diminish the efficiency of V2X systems.
- *User Trust and Privacy:* To maintain vehicle safety against numerous risks, user trust and privacy have recently become more worrying. The participants do not want any adversarial model to be able to attack their cars. As a result, several safeguards have been made to ensure that the user's activities are trusted and private. PKI is one of the most well-known security technologies for ensuring user privacy. It ensures that the user's private activities resist various assault models.
- *Data Priority:* Data received from hundreds of nodes should be prioritized by the V2X communication

network. Prioritization, buffering, and queuing techniques should be used in data processing to ensure a reliable and efficient data transmission link. Data received from security-critical sectors must be treated with the utmost care to avoid network collateral harm. As a result, data priority must be treated with extreme caution to avoid network collateral harm.

B. SECURITY REQUIREMENTS

In the following, we discuss various security requirements.

- *Maintaining Message Confidentiality:* It is one of WSN's most important security services. It relates to ensuring that information is not shared with anybody else and that only authenticated users can access the data. The use of public-key cryptography to ensure the integrity of sensitive data is a well-known norm. However, this strategy requires more resources in terms of computing and transmission costs. Furthermore, because WSNs have limited resources, this strategy cannot withstand known attacks. As a result, for WSN, multiple security protocols based on cryptographic approaches using symmetric-key cryptography have been developed. It ensures that unauthorized users do not have access to sensitive information [59].
- *Mutual Authentication:* It allows IoT devices to recognize the integrity of other IoT devices and establish secure communication. However, there are a few basic requirements for the authentication mechanism, including the lightweight scheme. Because many IoT devices have limited computation, processing, storage, and battery power, they are resource-intensive. It should use a multi-factor authentication technique rather than a single authentication scheme. As a result, the schema should be useful because it supports multi-factor authentication, which places additional strain on IoT devices. To improve security, the authentication schema involves integrating encryption techniques, such as ''RSA-based public key cryptosystem'' [60], ''Secure Hash Agorithm (SHA)'' [61], ''Advanced Encryption Standard (AES)'' [62], and ''Elliptic Curve Cryptography (ECC)'' [63]. In recent years, ''access control, authentication and key management'' are widely-used two main security mechanisms in providing security in IoT-enabled environments [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80].
- *Integrity:* It ensures that data is generated and that data received during transmission and storage is unaltered.
- *Access Control:* It ensures that IoT devices cannot access information that they are not authorized to see. It is the backbone technology that ensures information security and can withstand various security threats. The basic purpose of access control is to efficiently monitor resource access and prevent unwanted information flow. Data can be exchanged continually and shared between people and devices in IoT environments.
- *Availability:* It ensures that IoT services are available when needed, even when there are resource limits such as power outages or DoS assaults.
- *Data Accuracy:* It guarantees that the data sent by the sensors is as fresh as possible. The freshness feature ensures that every message received is current. It necessitates using recent data sets and ensures that no attacker will respond with an old message.
- *Non-repudiation:* Its goal is to ensure that communication parties' data transfer cannot be rejected while transmitting a previously transmitted message. This might be considered when the communication parties have agreed to the contract.
- *Device Security Resistance:* Because all of the devices are linked, an attacker can physically capture one if it is compromised. As a result, they can get their hands on the device's private credentials. Furthermore, an attacker collects secret session keys sent between the user and IoT devices. As a result, the compromised node should not affect the network's security. As a result, some security methods must be implemented to protect non-compromised devices. To withstand device security, robust authentication and key agreement processes must be designed.

C. POTENTIAL ATTACKS

A compromise of an Internet of Things (IoT) system is known as an IoT attack. Devices, networks, data, and users are all examples of this. A cyber attack can use an IoT attack to steal information. They can take control of an automated or IoT system and shut it down. Fig. 4 depicts possible attacks in IoT-V2X environments and the following potential attacks. We have thoroughly reviewed possible attacks in IoT environments at various application domains [81].

D. COUNTERMEASURES

Over the past ten years, several security techniques for protecting vehicle networks have been developed. The most secure methods were also developed especially for authenticating the vehicle and its driver. The autos communicate with other vehicles, nearby units, and control systems using an insecure wireless channel. As a result, cars using the V2X communication system are susceptible to numerous attacks, such as replay, masquerade, side-channel, and impersonation attacks. To protect the V2X communication system, strong and secure remote authentication is needed. Several security measures have been implemented in recent years, including identity-based, password-based, two-factor, three-factor, and multi-factor authentication. Table 5 depicts security challenges.

The authors developed an effective key distribution system for data fusion in heterogeneous networks in [95]. Their schemes define the multi-trust layer data fusion trust

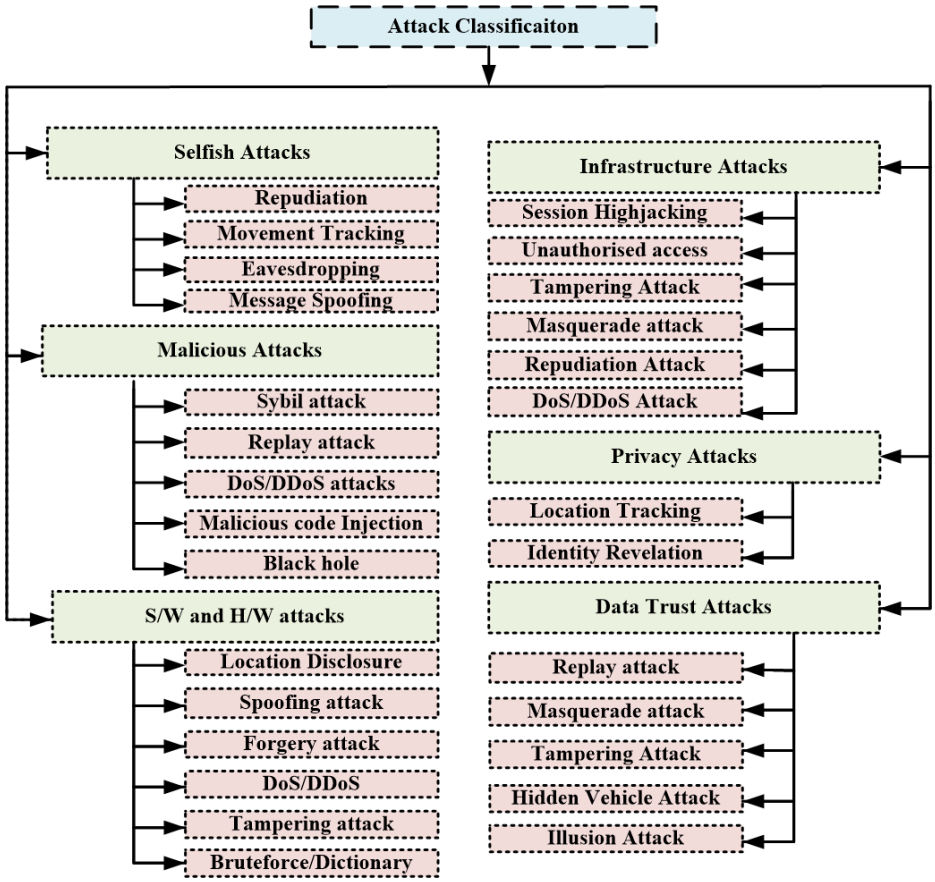

FIGURE 4. Attacks classification for V2X environment [81].

TABLE 5. Blockchain security challenges and countermeasures.

Requirements	Challenges	Vulnerabilities	Countermeasures
Prevent data loss	Attacks on a centralized cloud; Manipulation of data; Prevent future manipulation	Single point failure; Insider attack; IP spoofing; Forward tampering	[40], [44], [48]
Access control	Authenticity validation; Denial of Service (DoS); Delay in revocation of the right to access; Pseudo anonymity	Impersonation attack/phishing; Jamming; Unauthorized access; Identification by linking transaction details	[43], [44], [45], [49]
Data transmission	Data transfer in the network; Secure data sharing	Replay attacks; Man-in-the-Middle (MiTM) attack	[40], [42], [48]

architecture. For V2X communication, Wang et al. [96] presented physical layer authentication based on an adaptive Kalman filter. The Sage-Husa adaptive Kalman filter, which can dynamically modify statistical properties, is used in their mechanism. For safe V2X communications, Rigazzi et al. [97] developed an improved certificate revocation list distribution. Their mechanism was designed to implement the architecture of a certificate authority's certificate revocation list. By activating tailored filters that create a significant overhead reduction with a preset rate of false positives, certificate revocation list (CRL) compression can be achieved. A safe resource allocation technique for V2X was proposed by Ahmed et al. [98]. Ulybyshev et al. [99] developed a secure communication technique for autonomous V2X systems as a result. Their system ensures role-based and attribute-based access control, as well as encrypted data search. Cheng et al. [100] suggested a privacy-preserving Blockchain-based remote attestation security paradigm for V2X. As a result, various alternative security techniques have become typical in V2X contexts. Table 6 shows various countermeasures to withstand various potential attacks in V2X environments.

E. PERFORMANCE EVALUATION

In this section, we have performed a comprehensive analysis of various mechanisms by considering the various parameters such as computational cost, communication cost and execution time based on the "MIRACL Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library" [101]. The following parameters have

TABLE 6. Countermeasures to withstand potential attacks in V2X environments.

Attacks	[7]	[84]	[10]	[85]	[86]	[87]	[88]	[89]	[90]	[91]
NC	✓	✓	×	✓	×	×	×	×	×	×
DoSl	✓	✓	×	×	✓	✓	×	✓	✓	✓
DoS	✓	✓	✓	×	×	×	✓	✓	✓	✓
DDoS	×	×	×	×	×	×	×	×	×	×
MNI	×	×	×	✓	✓	✓	✓	×	✓	✓
FDI	✓	✓	✓	✓	×	×	×	✓	✓	✓
FN	✓	✓	×	×	×	×	✓	✓	✓	✓
RA	✓	×	✓	✓	✓	×	✓	✓	×	×
MiTM	×	×	✓	×	×	✓	✓	✓	×	×
SCA	✓	✓	✓	×	✓	✓	×	✓	×	×
SA	✓	×	✓	✓	×	✓	×	✓	✓	✓
BFA	✓	✓	✓	×	✓	✓	✓	×	×	×
MNA	✓	✓	✓	✓	×	✓	×	✓	✓	✓
TA	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
JA	✓	✓	✓	✓	×	×	✓	✓	✓	✓
UIA	✓	✓	✓	✓	✓	×	×	×	×	×
ED	✓	✓	✓	×	×	×	✓	✓	✓	✓
TRA	✓	×	×	×	×	✓	✓	✓	✓	✓

Note: NC: Node capture, DoSl: Denial-of-Sleep, DoS: Denial-of-Service, DDoS: Distributed Denial-of-Service, MNI: Mass node injection, FDI: False data injection, FN: Fake node, RA: Replay attack, MiTM: Man-in-the-Middle attack, SCA: Side-channel attack, SA: Sybil attack, BFA: Brute-force attack, MNA: Mass node authentication, TA: Tampered attack, JA: Jamming attack, UIA: User impersonation attack, ED: Eavesdropping, TRA: Tampered routing attack.

TABLE 7. Performance evaluation of various security schemes.

Reference	Scheme	Total Computation Cost	Communication Cost	Execution Time
[10]	Lightweight authentication for 5G enabled VANET	$T_{EM}+ 2T_{EA} + 2T_H$	672 bits	0.976 ms
[91]	Smart lightweight privacy preservation scheme for UAV	$19T_H + 12T_X$	1352 bits	1.182 ms
[92]	Three-factor authentication	$3T_{EM} + 21T_H$	1856 bits	1.283 ms
[93]	Edge-assisted lightweight authentication	$6T_{EM} + 10T_{EA} + 4T_H$	2496 bits	13.68 ms
[94]	Cost-efficient privacy-preserving authentication	$4T_{EM} + 2T_H$	1440 bits	26.2 ms
[95]	Lightweight device authentication for edge-based IoT	$32T_H$	2400 bits	10.24 ms
[96]	Lightweight privacy-preserving V2I authentication	$T_{AES} + 2T_H$	–	1.93 ms

Note: T_{EM} : "time for performing a scale multiplication in an ellptic curve"; T_{EA} : "time for performing a point addition in an ellptic curve"; T_H : "time for performing a cryptographic hash operation"; T_X : "time for performing an XOR operation"; T_{AES} : "time for performing a symmetric encryption operation using Advanced Encryption Standard (AES)" [64].

been considered to calculate computation cost in the existing schemes that were depicted in Table 7. In addition, we have considered propagation delay, block processing time and storage cost from the blockchain perspective.

1) **Computation cost:** The computational time is the overall time it takes the simulator to run the framework from beginning to end. A millisecond is a time interval that is measured in milliseconds. BCAS-VADN technique optimizes the computation cost. it achieves 226 milliseconds and 227 milliseconds respectively. The proposed scheme performed better than existing techniques [30]. Smart coin-based scheme performed better than existing for reducing the computation cost [32].
2) **Communication cost:** The storage space required for storing communicating factors including hash code, ciphertext, as well as other parameters is referred to as communication cost. For the BCAS-VADN approach, it takes 1856 bits for 2 messages and for 3 messages 2400 bits [30]. By using Smart coin it reduces the communication cost [32]. we observed from existing papers need to optimize the communication cost for ITS.
3) **Security features and functionality comparison:** Security and privacy and their functionality-based issues are addressed in with traditional mechanisms. after adding the blockchain technology effectively it addressed and solved by considering various potential attacks. we have done a comparative study from the existing mechanism not satisfied in all directions. security and privacy of data in networks is still an open research problem.
4) **Propagation delay:** The time it takes for a message to travel from sender to receiver is known as propagation delay. When the number of vehicles on the road rises,

i.e., when traffic becomes congested, the propagation delay increases because packets take longer to reach their destination in a congested network. We observed that required reducing the propagation delay.

5) **Block processing time:** The block processing time refers to the time it takes miner nodes to process a block, including mining and verification. SmartCoin does not use high-performance cryptographic computation like PoW. It also doesn't follow the PBFT consensus algorithm's significant message overhead. The Smart-Coin, on the other hand, uses a time-saving round-robin system to choose the next block inviter. Furthermore, as compared to state-of-the-art procedures, block construction and verification take very little time. As a result, when compared with existing approaches, SmartCoin's block processing time is extremely low [32].
6) **Storage cost:** The cost of storing values such as the encryption key, hash, and other parameters is referred to as the storage cost. Bytes are the measurement unit for storage costs. For Smart coin storage cost is 100 bytes [32]. In this research, we observed that still, storage cost reduction is an open research problem.

V. FUTURE VISION

Blockchain is an emerging technology that has been widely used in various applications and domains. The performance of Blockchain technology is anticipated to be a topic of interest in research. This section mainly focused on the challenges and issues of Blockchain for ITS.

1) **Improving the performance of BITS:** The Blockchain-based ITS consists of various requirements such as Throughput, Network bandwidth and transaction Latency. Due to the poor scalability, the network connectivity failures problem will arise like single point failures. and Security and privacy issues are open research problems for Blockchain-based ITS.
2) **Machine Learning with BITS:** Machine learning has been known to be an efficient method for supporting future BITS. As a foundation for artificial intelligence, machine learning has been applied in various fields, including speech recognition, medical diagnosis, and computer vision. It has also transformed BITS services by allowing them to learn from training data, draw data-driven conclusions, give decision assistance, and forecast network performance improvements. Using various Machine Learning algorithms for BITS will give better results regarding abnormal activity detection and performance.
3) **Big data with BITS:** Big data analysis has become a critical data analytical tool for maximizing the value of the information in huge amounts of Blockchain ITS data due to rapid advancement in BITS applications. In terms of diversity, velocity, and volume of Blockchain data, Blockchain-based Internet of Vehicles (BIoV) is predicted to rise exponentially in the future [102], [103]. Big data analysis facilitates the adoption of BIoV systems by enabling a number of solutions, including analytics, data cleansing, and storage. This is one of the future research areas for Blockchain-based transport applications.
4) **BITS in 5G:** The 5G technology adopted for BITS enhances performance in all aspects. The mobile industry is working on creating and deploying the 5G network, which is expected to transform businesses and societies. Massive data connections, high system throughput, low operational expenses, energy conservation, low network latency, and high data rate are all major benefits of the innovation. Moreover, new technology architectures employed in 5G wireless networks, such as cloud computing, device-to-device (D2D) communications, network slicing, network function virtualization (NFV), and software-defined networking (SDN), have presented new security issues. From the above observations, BITS consists of various future challenges for researchers.

VI. CONCLUDING REMARKS

With the integration of 5G, 6G and Blockchain technologies, the V2X systems provide significant intelligent services that can help minimize accidents, provide extended quality of service, and quick access to connected vehicles. However, the advancements in the scale of connectivity of 5G and 6G networks may open doors to attack surfaces and increase multiple adversarial opportunities. This study aimed to conduct a thorough, systematic literature analysis focusing on V2X to analyze the crucial elements of safe and secure IoT environments. This study thoroughly analyzed various V2X communication standards, applications, and underlying technologies to address various security issues, challenges, and countermeasures. Firstly, the state-of-the-art functionalities for the IoT-V2X were specifically discussed to visualize an ITS. Next, we discussed IoT-V2X architecture with underlying technologies including Blockchain. We then examined important security aspects to achieve high-security efficiencies, such as requirements, concerns, primitives, system models, and attacks. A few important assessments were performed to determine security performances and counteractants to support the well-functioning of IoT-V2X. Lastly, we provided a future vision for enhancing the research works in line with the integration of IoT-V2X-Blockchain.

Our outcome's substantial impact on the research field emphasizes the importance of integrating IoT and Blockchain to assure seamless, secure and tamperproof data collection, processing and storage. As we focus on V2X technologies, we must analyze secure authentication and access control mechanisms to employ safety. For instance, IoT allows Internet-connected devices to transmit data to private blockchain networks to produce tamper-proof shared transaction records. Each transaction can be independently validated to prevent disputes and foster confidence among all users of

a permissioned network. Increasing privacy agreements and securing device communication channels are benefits of combining blockchain and IoT. Human-to-human and human-to-device communications are made possible by this technology. As a result, Blockchain technology develops an open database that demonstrates who has access and who is transacting. Later on, Blockchain technology may be utilized for transferring user data between platforms and systems quickly and securely. There is still research going on to minimize the computational complexities by targeting performance at its best. However, there are pitfalls in handling multi-level integration of IoT and other underlying technologies. Our future studies target to analyze deeper into the development of sustainable environments.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the associate editor for providing their valuable suggestions and comments which helped them to improve the article significantly.

REFERENCES

[1] W. Kassab and K. A. Darabkh, "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *J. Netw. Comput. Appl.*, vol. 163, Aug. 2020, Art. no. 102663.

[2] V. Elangovan, W. Xiang, and S. Liu, "A real-time C-V2X beamforming selector based on effective sequence to sequence prediction model using transitional matrix hard attention," *IEEE Access*, vol. 11, pp. 10954–10965, 2023.

[3] S. L. A. Shajith, H. R. Pasindu, and R. K. T. K. Ranawaka, "Evaluating the risk factors in fatal accidents involving motorcycle—Case study on motorcycle accidents in Sri Lanka," *Engineer, J. Inst. Eng.*, vol. 52, no. 3, p. 33, Dec. 2019.

[4] (2022). *National Highway Traffic Safety Administration*. Accessed: May 2022. [Online]. Available: https://www.nhtsa.gov/

[5] S. L. Kok and S. Siripipatthanakul, "The challenges and opportunities of Geely: A marketing case study," Tech. Rep., 2023.

[6] O. E. J. Wing, W. Lehman, P. D. Bates, C. C. Sampson, N. Quinn, A. M. Smith, J. C. Neal, J. R. Porter, and C. Kousky, "Inequitable patterns of US flood risk in the anthropocene," *Nature Climate Change*, vol. 12, no. 2, pp. 156–162, Feb. 2022.

[7] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Veh. Commun.*, vol. 9, pp. 64–71, Jul. 2017.

[8] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar. 2021.

[9] H. Tan, W. Zheng, P. Vijayakumar, K. Sakurai, and N. Kumar, "An efficient vehicle-assisted aggregate authentication scheme for infrastructureless vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, May 30, 2022, doi: 10.1109/TITS.2022.3176406.

[10] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6417–6428, Aug. 2019.

[11] L. Dang, J. Xu, X. Cao, H. Li, J. Chen, Y. Zhang, and X. Fu, "Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 4, pp. 1–16, 2018.

[12] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018.

[13] M. Han, L. Hua, and S. Ma, "A self-authentication and deniable efficient group key agreement protocol for VANET," 2016, *arXiv:1611.09009*.

[14] Q. Li, C.-F. Hsu, K.-K. R. Choo, and D. He, "A provably secure and lightweight identity-based two-party authenticated key agreement protocol for vehicular ad hoc networks," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, Dec. 2019.

[15] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent advances and challenges in security and privacy for V2X communications," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 244–266, 2020.

[16] E. Ahmed and H. Gharavi, "Cooperative vehicular networking: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 3, pp. 996–1014, Mar. 2018.

[17] S. K. Dwivedi, R. Amin, A. K. Das, M. T. Leung, K.-K.-R. Choo, and S. Vollala, "Blockchain-based vehicular ad-hoc networks: A comprehensive survey," *Ad Hoc Netw.*, vol. 137, Dec. 2022, Art. no. 102980.

[18] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (V2X) communication platforms," *IEEE Trans. Intell. Vehicles*, vol. 5, no. 4, pp. 693–713, Dec. 2020.

[19] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Veh. Commun.*, vol. 12, pp. 50–65, Apr. 2018.

[20] K. Kiela, V. Barzdenas, M. Jurgo, V. Macaitis, J. Rafanavicius, A. Vasjanov, L. Kladovscikov, and R. Navickas, "Review of V2X–IoT standards and frameworks for ITS applications," *Appl. Sci.*, vol. 10, no. 12, p. 4314, Jun. 2020.

[21] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Comput. Netw.*, vol. 151, pp. 52–67, Mar. 2019.

[22] L. Bréhon–Grataloup, R. Kacimi, and A.-L. Beylot, "Mobile edge computing for V2X architectures and applications: A survey," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108797.

[23] V. Sharma, I. You, and N. Guizani, "Security of 5G-V2X: Technologies, standardization, and research directions," *IEEE Netw.*, vol. 34, no. 5, pp. 306–314, Sep. 2020.

[24] S. S. Musa, M. Zennaro, M. Libsie, and E. Pietrosemoli, "Convergence of information-centric networks and edge intelligence for IoV: Challenges and future directions," *Future Internet*, vol. 14, no. 7, p. 192, Jun. 2022.

[25] H. Farran, D. Khoury, and L. Bokor, "A comprehensive survey on the application of blockchain/hash chain technologies in V2X communications," *Infocommunications J.*, vol. 14, no. 1, pp. 24–35, 2022.

[26] J. Meijers, P. Michalopoulos, S. Motepalli, G. Zhang, S. Zhang, A. Veneris, and H. Jacobsen, "Blockchain for V2X: Applications and architectures," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 193–209, 2022.

[27] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "Blockchain for the Internet of Vehicles: A decentralized IoT solution for vehicles communication using Ethereum," *Sensors*, vol. 20, no. 14, p. 3928, Jul. 2020.

[28] F. L. Paxson, "The highway movement, 1916–1935," *The Amer. Historical Rev.*, vol. 51, no. 2, pp. 236–253, 1946.

[29] S. Padam and S. K. Singh, "Urbanization and urban transport in India: The search for a policy," Tech. Rep., 2004, doi: 10.2139/ssrn.573181.

[30] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. Park, "Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems," *IEEE Sensors J.*, vol. 21, no. 14, pp. 15824–15838, Jul. 2021.

[31] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16492–16503, Sep. 2022.

[32] L. Vishwakarma and D. Das, "SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100429.

[33] 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 J.*, vol. 21, no. 14, pp. 15807–15823, Jul. 2021.

[34] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, p. 3165, Jul. 2019.

[35] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, "B-FERL: Blockchain based framework for securing smart vehicles," *Inf. Process. Manag.*, vol. 58, no. 1, Jan. 2021, Art. no. 102426.

[36] R. Jabbar, E. Dhib, A. B. Said, M. Krichen, N. Fetais, E. Zaidan, and K. Barkaoui, "Blockchain technology for intelligent transportation systems: A systematic literature review," *IEEE Access*, vol. 10, pp. 20995–21031, 2022.

[37] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[38] S. Johar, N. Ahmad, A. Durrani, and G. Ali, "Proof of pseudonym: Blockchain-based privacy preserving protocol for intelligent transport system," *IEEE Access*, vol. 9, pp. 163625–163639, 2021.

[39] A. Erdem, S. O. Yildirim, and P. Angin, *BlockchainBlockchainfor Ensuring SecuritySecurity, PrivacyPrivacy, and TrustTrustin IoTIoTEnvironments: The State of the Art*. Cham, Switzerland: Springer, 2019, pp. 97–122.

[40] M. N. K. Boulos, G. Peng, and T. VoPham, "An overview of GeoAI applications in health and healthcare," *Int. J. Health Geographics*, vol. 18, no. 1, Dec. 2019.

[41] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 140, Aug. 2018.

[42] S. Pournaghi, M. Bayat, and Y. Farjami, "A novel and secure model for sharing protected health record (PHR) based on blockchain and attribute based encryption," *Electron. Cyber Defense*, vol. 8, no. 1, pp. 101–124, 2020.

[43] V. Skwarek, "Blockchains as security-enabler for industrial IoT-applications," *Asia Pacific J. Innov. Entrepreneurship*, vol. 11, no. 3, pp. 301–311, Dec. 2017.

[44] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—Review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, Aug. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/17/5874

[45] Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of Things (IoT) of smart home: Privacy and security," *Int. J. Comput. Appl.*, vol. 182, no. 39, pp. 3–8, Feb. 2019.

[46] A. Hari and T. V. Lakshman, "The internet blockchain: A distributed, tamper-resistant transaction framework for the internet," in *Proc. 15th ACM Workshop Hot Topics Netw.*, Nov. 2016, pp. 204–210.

[47] A. Draper, A. Familrouhani, D. Cao, T. Heng, and W. Han, "Security applications and challenges in blockchain," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–4.

[48] C. Shin, E. Farag, H. Ryu, M. Zhou, and Y. Kim, "Vehicle-to-everything (V2X) evolution from 4G to 5G in 3GPP: Focusing on resource allocation aspects," *IEEE Access*, vol. 11, pp. 18689–18703, 2023.

[49] J. Ye, L. Xiang, and X. Ge, "Spatial–temporal modeling and analysis of reliability and delay in urban V2X networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 3, pp. 1752–1765, May 2023.

[50] G. J. Dimitrakopoulos, L. Uden, and I. Varlamis, *The Future of Intelligent Transport Systems*. Amsterdam, The Netherlands: Elsevier, 2020.

[51] A. Bazzi, C. Campolo, V. Todisco, S. Bartoletti, N. Decarli, A. Molinaro, A. O. Berthet, and R. A. Stirling-Gallacher, "Toward 6G vehicle-to-everything sidelink: Nonorthogonal multiple access in the autonomous mode," *IEEE Veh. Technol. Mag.*, vol. 18, no. 2, pp. 50–59, Jun. 2023.

[52] J. Gallego-Madrid, R. Sanchez-Iborra, J. Ortiz, and J. Santa, "The role of vehicular applications in the design of future 6G infrastructures," *ICT Exp.*, Mar. 2023.

[53] A. H. Khan, N. Ul Hassan, C. Yuen, J. Zhao, D. Niyato, Y. Zhang, and H. V. Poor, "Blockchain and 6G: The future of secure and ubiquitous communication," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 194–201, Feb. 2022.

[54] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, and C. S. Hong, "6G wireless systems: A vision, architectural elements, and future directions," *IEEE Access*, vol. 8, pp. 147029–147044, 2020.

[55] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5416–5441, Apr. 2021.

[56] K. Kiela, M. Jurgo, and R. Navickas, "Structure of V2X-IoT framework for ITS applications," in *Proc. 43rd Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2020, pp. 229–234.

[57] M. R. Patruni and P. Saraswathi, "Securing Internet of Things devices by enabling Ethereum blockchain using smart contracts," *Building Services Eng. Res. Technol.*, vol. 43, no. 4, pp. 473–484, Jul. 2022.

[58] P. M. Rao and P. Saraswathi, "Evolving cloud security technologies for social networks," in *Security in IoT Social Networks*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 179–203.

[59] B. D. Deebak, F. H. Memon, S. A. Khowaja, K. Dev, W. Wang, N. M. F. Qureshi, and C. Su, "A lightweight blockchain-based remote mutual authentication for AI-empowered IoT sustainable computing systems," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6652–6660, Apr. 2023.

[60] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[61] *National Institute of Standards and Technology (NIST)*, Secure Hash Standard FIPS PUB 180-1, U.S. Department of Commerce, Apr. 1995, Accessed: Mar. 2021. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[62] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback, and J. F. Dray Jr., "Advanced encryption standard," Tech. Rep., 2001, doi: 10.6028/NIST.FIPS.197.

[63] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Des., Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 173–193, Mar. 2000.

[64] N. Radhakrishnan and M. Karuppiah, "An efficient and secure remote user mutual authentication scheme using smart cards for telecare medical information systems," *Informat. Med. Unlocked*, vol. 16, Jan. 2019, Art. no. 100092.

[65] A. K. Das and B. Bruhadeshwar, "An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system," *J. Med. Syst.*, vol. 37, no. 5, p. 9969, Oct. 2013.

[66] S. Chatterjee and A. K. Das, "An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks," *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1752–1771, Jun. 2015.

[67] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card," *Peer-Peer Netw. Appl.*, vol. 9, no. 1, pp. 171–192, Jan. 2016.

[68] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K. R. Choo, and Y. Park, "Certificateless-signcryption-based three-factor user access control scheme for IoT environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3184–3197, Apr. 2020.

[69] M. Wazid, S. Thapliyal, D. P. Singh, A. K. Das, and S. Shetty, "Design and testbed experiments of user authentication and key establishment mechanism for smart healthcare cyber physical systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Mar. 29, 2022, doi: 10.1109/TNSE.2022.3163201.

[70] B. Bera, A. K. Das, W. Balzano, and C. M. Medaglia, "On the design of biometric-based user authentication protocol in smart city environment," *Pattern Recognit. Lett.*, vol. 138, pp. 439–446, Oct. 2020.

[71] A. K. Das, N. R. Paul, and L. Tripathy, "Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem," *Inf. Sci.*, vol. 209, pp. 80–92, Nov. 2012.

[72] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100075.

[73] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.

[74] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," *IEEE Access*, vol. 5, pp. 25808–25825, 2017.

[75] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K. R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8739–8752, Oct. 2019.

[76] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment," *Comput. Commun.*, vol. 166, pp. 91–109, Jan. 2021.

[77] A. K. Das, "A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks," *Int. J. Inf. Secur.*, vol. 11, no. 3, pp. 189–211, Jun. 2012.

[78] A. K. Das, "A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications," *Netw. Sci.*, vol. 2, nos. 1–2, pp. 12–27, May 2013.

[79] A. Msolli, N. Ajmi, A. Helali, A. Gassoumi, H. Maaref, and R. Mghaieth, "New key management scheme based on pool-hash for WSN and IoT," *J. Inf. Secur. Appl.*, vol. 73, Mar. 2023, Art. no. 103415.

[80] G. Thakur, P. Kumar, S. Jangirala, A. K. Das, and Y. Park, "An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment," *IEEE Access*, vol. 11, pp. 26877–26892, 2023.

[81] P. M. Rao and B. D. Deebak, "Security and privacy issues in smart cities/industries: Technologies, applications, and challenges," *J. Ambient Intell. Humanized Comput.*, pp. 1–37, Feb. 2022.

[82] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," *Exp. Syst. Appl.*, vol. 41, no. 5, pp. 2559–2564, Apr. 2014.

[83] H. Zhao, M. Zhang, K. Gao, T. Mao, and H. Zhu, "A multi-channel cooperative demand-aware media access control scheme in vehicular ad-hoc network," *Wireless Pers. Commun.*, vol. 104, no. 1, pp. 325–337, Jan. 2019.

[84] R. Ali, A. K. Pal, S. Kumari, M. Karuppiah, and M. Conti, "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring," *Future Gener. Comput. Syst.*, vol. 84, pp. 200–215, Jul. 2018.

[85] T. Gao, Y. Li, N. Guo, and I. You, "An anonymous access authentication scheme for vehicular ad hoc networks under edge computing," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 2, Feb. 2018, Art. no. 155014771875658.

[86] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Comput. Netw.*, vol. 104, pp. 137–154, Jul. 2016.

[87] Q. Zhang, Y. Gan, L. Liu, X. Wang, X. Luo, and Y. Li, "An authenticated asymmetric group key agreement based on attribute encryption," *J. Netw. Comput. Appl.*, vol. 123, pp. 1–10, Dec. 2018.

[88] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, and W. Zhuang, "Reinforcement learning based PHY authentication for VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3068–3079, Mar. 2020.

[89] B. D. Deebak and F. Al-Turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," *Comput. Commun.*, vol. 162, pp. 102–117, Oct. 2020.

[90] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K.-R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018.

[91] M. Yahuza, M. Y. I. Idris, A. W. A. Wahab, T. Nandy, I. B. Ahmedy, and R. Ramli, "An edge assisted secure lightweight authentication technique for safe communication on the Internet of Drones network," *IEEE Access*, vol. 9, pp. 31420–31440, 2021.

[92] T. A. Shah, F. Algarni, I. Ullah, A. M. Abdullah, F. Noor, and M. A. Khan, "Cost-efficient privacy-preserving authentication and key management scheme for Internet of Vehicle ecosystem," *Complexity*, vol. 2022, pp. 1–8, Jun. 2022.

[93] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment," *Sensors*, vol. 19, no. 24, p. 5539, Dec. 2019.

[94] S. Lv and Y. Liu, "PLVA: Privacy-preserving and lightweight V2I authentication protocol," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6633–6639, Jul. 2022.

[95] H. Qiu, M. Qiu, Z. Lu, and G. Memmi, "An efficient key distribution system for data fusion in V2X heterogeneous networks," *Inf. Fusion*, vol. 50, pp. 212–220, Oct. 2019.

[96] J. Wang, Y. Shao, Y. Ge, and R. Yu, "Physical-layer authentication based on adaptive Kalman filter for V2X communication," *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100281.

[97] G. Rigazzi, A. Tassi, R. J. Piechocki, T. Tryfonas, and A. Nix, "Optimized certificate revocation list distribution for secure V2X communications," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–7.

[98] K. J. Ahmed and M. J. Lee, "Secure resource allocation for LTE-based V2X service," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11324–11331, Dec. 2018.

[99] D. Ulybyshev, A. O. Alsalem, B. Bhargava, S. Savvides, G. Mani, and L. B. Othmane, "Secure data communication in autonomous V2X systems," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2018, pp. 156–163.

[100] C. Xu, H. Liu, P. Li, and P. Wang, "A remote attestation security model based on privacy-preserving blockchain for V2X," *IEEE Access*, vol. 6, pp. 67809–67818, 2018.

[101] (2020). *MIRACL Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library*. Accessed: Jun. 2022. [Online]. Available: https://github.com/miracl/MIRACL

[102] S. M. Hatim, S. J. Elias, R. M. Ali, J. Jasmis, A. A. Aziz, and S. Mansor, "Blockchain-based Internet of Vehicles (BIoV): An approach towards smart cities development," in *Proc. 5th IEEE Int. Conf. Recent Adv. Innov. Eng. (ICRAIE)*, Dec. 2020, pp. 1–4.

[103] A. Hemmati, M. Zarei, and A. Souri, "Blockchain-based Internet of Vehicles (BIoV): A systematic review of surveys and reviews," *Secur. Privacy*, p. e317, Apr. 2023, doi: 10.1002/spy2.317.

P. MURALIDHARA RAO (Member, IEEE) received the B.Tech. degree in computer science and engineering from Jawaharlal Nehru Technological University (JNTU), Kakinada, India, in 2012, and the M.Tech. degree in software engineering from JNTU, Hyderabad, India, in 2014. He is currently pursuing the Ph.D. degree with the Vellore Institute of Technology, Vellore, India. He is also an Assistant Professor with the Vellore Institute of Technology. He has published several articles in international journals. His research interests include wireless sensor networks and network security. He is an active member of IAENG professional bodies.

SRINIVAS JANGIRALA (Member, IEEE) received the Bachelor of Science and Master of Science degrees from Kakatiya University, India, in 2003 and 2008, respectively, the Master of Technology degree from IIT Kharagpur, in 2011, and the Ph.D. degree from the Department of Mathematics, IIT Kharagpur, in 2017. He is currently an Associate Professor with the Jindal Global Business School, O. P. Jindal Global University, Haryana, India. Prior to this, he was also a Research Assistant with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology (IIIT) Hyderabad, Hyderabad, India. His research interests include blockchain technology and applications, information security, cryptocurrency, and supply chain. He has authored 30 papers in international journals and conferences in his research areas.

SARASWATHI PEDADA received the B.Tech. and M.Tech. degrees in computer science and engineering from Jawaharlal Nehru Technological University (JNTU), Kakinada, India, in 2014 and 2016, respectively. She is currently pursuing the Ph.D. degree with GITAM University, Visakhapatnam, India. She is also an Assistant Professor with the Department of Computer Science and Engineering, GITAM Institute of Technology, GITAM University. She has published several articles in international journals and also published more than five book chapters in Elsevier Academic Press. Her research interests include wireless sensor networks and networks security.

ASHOK KUMAR DAS (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, IIIT Hyderabad, Hyderabad, India. He was also a Visiting Faculty of the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. His current research interests include cryptography, system and network security, including security in smart grid, the Internet of Things (IoT), the Internet of Drones (IoD), the Internet of Vehicles (IoV), cyber-physical systems (CPS), cloud computing, intrusion detection, blockchain, and AI/ML security. He has authored over 350 papers in international journals and conferences in the above areas, including over 300 reputed journal articles. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has been listed in the Web of Science (Clarivate^{TM}) Highly Cited Researcher 2022 in recognition of his exceptional research performance. He was/is on the editorial board of IEEE Systems Journal, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He has served as a program committee member for many international conferences. He also served as one of the Technical Program Committee Chair for the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in June 2019, and the second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, in October 2020. His Google Scholar H-index is 77 and i10-index is 219 with over 16,860 citations.

YOUNGHO PARK (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea in 1989, 1991, and 1995, respectively. He is currently a Professor with the School of Electronics Engineering, Kyungpook National University. From 1996 to 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. His research interests include information security, computer networks, and multimedia.