The Nucleus ***61****, No. 2 (2024) 79-92*

https://doi.org/10.71330/thenucleus.2024.1404

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Internet of Vehicles Environment Verification of Authentication Protocols using Formal Analysis: A Survey

Khurram Khalid[1], Atta Ur Rahman[1], Ahtasham Sajid[1], Bibi Saqia[2], MumtazAli Shah[3*], Mujeeb ur Rehman[4]

[1]*Riphah Institute of Systems Engineering, Riphah International University, Islamabad, 46000, Pakistan*

[2]*Department of Computer Science, University of Science and Technology Bannu, 28100, Pakistan*

[3]*Depatrtment of Computer Science, University of Wah, Wah Cantt, 47040, Pakistan*

[4]*Department of Computer Science University of Management and Technology Lahore, Sialkot Campus, 51040, Pakistan*

ABSTRACT

The Internet of Vehicles (IoV) is becoming an interesting topic among researchers and it has emerged as a rapidly advancing field within Vehicular Ad-hoc Networks, facilitating intelligent communication between vehicles and the cloud through the integration of Internet of Things (IoT) technologies. The IoV surroundings face serious challenges due to the highly interrelated nature of vehicles and infrastructure in certifying privacy and security. Traditional approaches to authentication lack the strength required to protect against developing fears, leaving systems vulnerable to attacks. This survey addresses the gap by employing formal analysis approaches to prove authentication protocols, targeting to reinforce safety and confidentiality in IoV systems. The IoV communication model consists of Vehicle-to-Vehicle, Vehicle-to-Infrastructure, Vehicle-to-Personal Devices, and Vehicle-to-Cloud. Smart automobiles are equipped with cameras, radars, on-board units, and sensors to help reduce the number of accidents by giving drivers or autonomous vehicles up-to-date information on roads, traffic signals, and other pertinent entities. As human lives are at risk, security and privacy in the IoV communication paradigm are critical and cannot neglected. Security and privacy breaches may cause accidents because the attacker can inject false information into the system as the communication channel is open and unsecured. The researchers proposed many authentication protocols to provide secure communication between IoV entities. Although surveys on IoV security and privacy issues deal with communication and computation costs, they lack formal analysis of the authentication protocols. This survey reviews the informal analysis and formal analysis methods used by various authentication protocols. Furthermore, the challenges and future work are also included in this survey.

Keywords: *Internet of Vehicles, Security Requirements, Authentication Protocols, Formal Analysis, Informal Analysis*

1. Introduction

The transportation networks throughout the world are under tremendous strain. Due to the growing global population and the concurrent rise in the number of automobiles. With over one billion vehicles currently in use and projections reaching two billion by 2035, the resulting traffic jams and increased road accidents highlight the urgent need for innovative solutions [1]. The (WHO) reported in 2023 that approximately 1.19 million people lose their lives in automobile accidents each year. There are an additional 20 to 50 million non-fatal injury cases, many of which result in disability. WHO also pointed out some risk factors (speeding, non-use of motorcycle helmets, seat-belts and child restraints, distracted driving, unsafe road infrastructure, and unsafe vehicles) that should addressed to prevent deadly collisions and lower the number of severe injuries [2]. Previous informal analysis techniques in IoV safety are limited by their qualitative, subjective nature, which usually leads to insufficient security evaluations. They typically delivered a broad view of threats without rigorous verification against specific attacks, such as replay or impersonation, which limits their reliability. In contrast, the proposed survey and formal analysis systematically identify these gaps. By leveraging formal verification tools such, as AVISPA, BAN logic, and Scyther, the suggested study rigorously asses impotent security features integrity, confidentiality, and anonymity by reproducible tests and quantifiable. This certifies detailed safety validation against advanced adversarial processes improving confidence in IoV protocol strength. Transportation systems in real-world scenarios play an important role in people's daily lives. Since the opportunities in urban areas increasing day by day the use of vehicles is also increasing rapidly. There are 290 million registered vehicles in the United States in 2022. Thus, in the United States, cities are also adopting smart transportation technologies to tackle similar challenges [3]. Another example discussed in [4] is Riyadh the busiest city in Saudi Arabia, cities like Riyadh are experiencing significant traffic congestion due to rapid urbanization and an increasing number of vehicles on the road. To address these issues a perfect smart IoV system must be implemented. This system aims to analyze data from various sources, including sensors and cameras to enhance real-time traffic monitoring and provide timely updates to drivers, improving traffic flow and reducing delays. Consequently, the catastrophic expansion of the transportation system, researchers have combined technologies such as cloud computing, Vehicular Ad-hoc Networks (VANETs), and IoV.

1.1 Cloud Computing (CC)

CC provides on-demand resources for the users. The National Institute of Standards and Technology (NIST) defines cloud computing as "CC is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, such as (networks, servers, storage, applications, and services) that can be rapidly maintained and released with minimal management effort or service provider interaction" [5]. The NIST provided the 5 necessary characteristics, 3 service

[*] Corresponding author: mumtaz.ali@skt.umt.edu.pk

models, and 4 deployment models for cloud service providers (CSP) are shown in Fig.1.

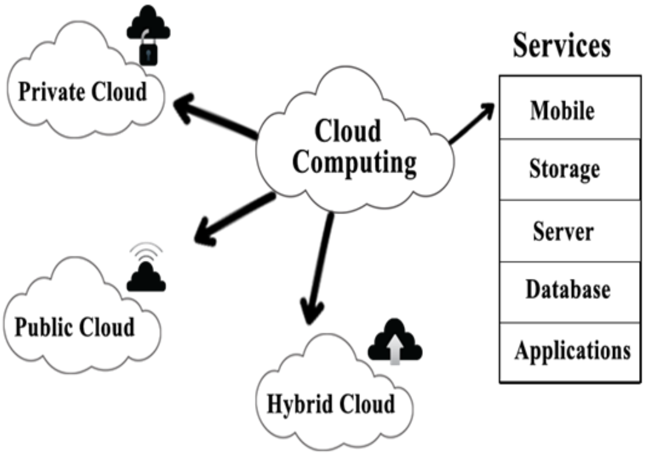

Fig.1 Cloud Computing Architecture

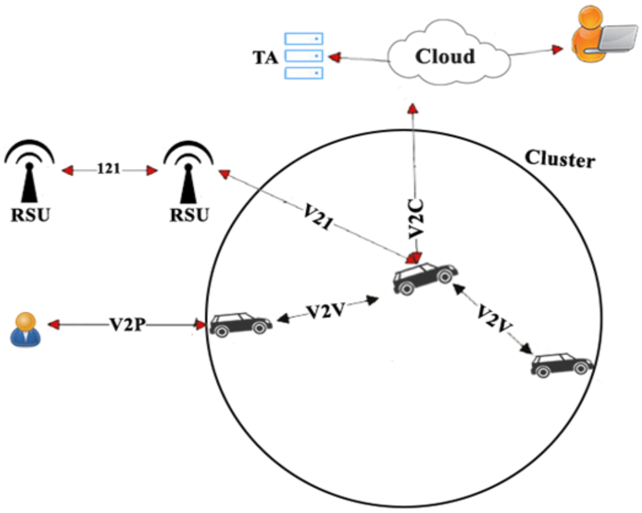

Fig.2. Iov Communication [6]

1.2 Vehicular Ad-Hoc Network

VANET is a type of wireless communication technology used in automobiles. These networks serve to improve traffic safety and efficiency in the current transportation systems by facilitating information exchange between vehicles and infrastructure. A VANET faces limitations in processing extensive information from sensors and devices in their environment, hindering global analysis. To tackle this issue, the progression towards the IoV aims to provide smart cars with multi-sensor platforms, strong computing units, and Internet connectivity. The proposed study enriched cooperation and communication between cars and other gear.

VANET achieves good outcomes in short-term usage like removing redundant data, still, they are not appropriate to control and assess worldwide information in large-scale situations due to their processing boundaries [7].

1.3 IoV Communication Model

The IoV is a well-known and hot area of research domain. The IoT and VANETs are integrated to structure the IoV, which delivers a useful solution to different traffic administration and driving challenges. Information technology assists a lot in providing the IoV, which enhances driving capability and efficiency in passenger safety. IoV-certifies improved associations and information sharing opens up new opportunities for updating techniques to traffic-concern problems, generating secure and effective mobility settings. Three important components play an essential role in the communication of the IoV: vehicular mobile Internet, intra-vehicular conversation, and inter-vehicular conversation [8]. Vehicle-to-infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Cloud (V2C), and Vehicle-to-Personal devices (V2P) are the diverse communication forms that generate a diverse vehicular network that is the IoV [9]. The smooth communication and interchange of data between automobiles, roadside units, personal gadgets, sensors, cloud, and infrastructure elements is made possible by this diversified network architecture. The basis for sophisticated and intelligent vehicle systems in the IoVis the integration of these communication components. Fig. 2 describes the communication entities involved in IoV.

i. V2I: The communication between cars and roadside structures, like traffic lights and signs, helps improve traffic control and safety. Vehicles with this system enabled are able to get critical information, like traffic updates and alerts, which ultimately enhances decision-making capabilities. Deploying V2I technology has the potential to substantially enhance the effectiveness of transportation networks, particularly in urban areas [10].

ii. V2P: In an attempt to make driving safer for everyone, Vehicle-to-Infrastructure (V2P) communication involves both pedestrians and vehicles. This can help reduce accidents by alerting vehicles when people are approaching and vice versa. Leveraging mobile and connected devices, V2P systems can provide real-time notifications and warnings, assisting in the development of safer [11].

iii. V2C: Refers to the information exchange between vehicles and cloud platforms. It enables vehicles to obtain various vehicle application services from cloud platforms, for example, navigation, monitoring, emergency rescue, and entertainment. These services are processed and calculated by cloud platforms and then sent to vehicles through Vehicle-to-Cloud (V2C) [12].

iv. V2V: Vehicles can directly interact with each other through communication, exchanging details about their direction, speed, and potential hazards. Applications like cooperative driving and accident avoidance, where vehicles may make judgments based on real-time information from other adjacent vehicles, depend heavily on this technology. Studies reveal that by empowering cars to react proactively to shifting road conditions, V2V communication can lower the chance of collisions and enhance overall traffic safety [13].

1.4 Contribution

This study conducts a thorough survey of authentication protocols within the IoV, focusing on the formal analysis of these protocols. It reviews existing literature to identify which research studies utilize specific tools and methodologies to verify the correctness and security of their proposed authentication mechanisms. The goal of the study is to further knowledge of the state of IoV authentication methods today and their efficacy in guaranteeing secure communications by pointing out the formal analysis using different strategies. This work highlights the significance of rigorous validation techniques in improving the security of IoV, which is crucial for directing future research and development in the field. The key points of this survey are as follows:

- Tool Usage: The survey identifies several methods and tools used in the literature to confirm the accuracy of IoV authentication protocols.
- Formal Analysis: It highlights how important formal analysis is for evaluating the security characteristics of authentication protocols, which is essential for spotting weaknesses and guaranteeing strong security measures.
- Survey Gaps: To the best of our knowledge, the formal analysis tools and techniques employed in IoV authentication protocol research have not been comprehensively surveyed. Consequently, our study aims to address this gap by leveraging the formal analysis methods utilized by researchers in this domain.

Challenges and Future Directions: This survey provides a valuable resource for researchers and practitioners working to develop more secure and effective IoV authentication protocols, including the verification of their correctness through formal analysis. The study offers guidance to support and advance future research in this field.

2. Methodology

The rationale underlying this study is predicated upon the accelerated advancement of the IoV and its burgeoning integration into our everyday lives. We survey to investigate the formal analysis methods employed by researchers to verify their IoV authentication protocols. By conducting a thorough examination of the existing literature, we endeavor to identify prevailing trends, proven best practices, and prospective areas warranting further research within this dynamically evolving field. This paper aims to thoroughly examine and resolve the following key research questions in the IoV environment:

i. What are the attacker's capabilities and types of security attacks?

ii. What are the security requirements and their solutions?

iii. What authentication protocols have been proposed, and how are they analyzed through informal and formal methods?

iv. What challenges need to be addressed in the context of authentication protocols?

2.1 Selecting and Reviewing Scholarly Sources

Thoroughly reviewing, evaluating, and incorporating pertinent academic literature is a crucial step in undertaking a robust scholarly investigation. This process entails thoroughly reviewing and synthesizing pertinent academic publications to establish a strong foundation for the study. To ascertain alignment with state-of-the-art research methodologies, we prioritized scholarly articles published within the past five years since 2024, concentrating on the topic of IoV authentication protocols. The identified digital repositories were thoroughly searched to procure the essential publications:

i. Google Scholar

ii. Springer

iii. IEEE Explorer

iv. ACM

v. MDPI

vi. Science Direct

vii. Semantic Scholar

2.2 Research Approach

A set of targeted keywords was employed to identify relevant articles. These keywords encompassed terms like "IoV security," "Internet of Vehicle security," "IoV authentication protocols," "IoV authentication protocols informal and formal analysis," and "Authentication protocols formal analysis tools." The search utilized Boolean operators (AND, OR) to refine the results and ensure comprehensive coverage of the topic.

2.3 Selection Criteria

The identification and assessment of articles and research papers were governed by the specific inclusion and exclusion criteria to maintain the relevance and integrity of the selected literature.

Inclusion Criteria:

- Articles must focus on the security aspects of the Internet of Vehicles, including authentication protocols and their analysis mechanisms.
- Papers must be published in well-regarded academic journals or conferences.
- Research from the past 5 years since 2024 was prioritized to capture the most recent advancements in the field.

Exclusion Criteria:

- To maintain consistency in language and comprehension, non-English publications were excluded from consideration.
- Articles without IoV authentication protocols were not considered.

- Articles that did not directly address security and privacy aspects within the IoV domain were also excluded.

3. Existing Surveys

The security and privacy related to the IoV system must be addressed, solved, and deployed properly because in IoV human lives are involved. Accidents could happen if an attacker injects erroneous data about traffic signals, traffic flow, or road conditions. It is crucial to know attackers and evaluate the likelihood that they may cause damage to a system.

3.1 Attacker Capabilities

Four categories can be used to differentiate the attackers, as their skills are described in [14]: 1) Insiders & Outsiders, The insider attackers who have been validated as network users. The outsider attackers with limited offensive capabilities are considered outsiders. 2) Malicious & Rational, The malicious attackers have no personal gain in targeting a system. The rational attackers aim to benefit themselves, their behavior is more predictable. 3) Active & Passive, to break a structure directs out signs. The passive attackers simply detect the system. 4) Local & extended, the local attackers employed an inadequate amount of entities and functioned in a restricted range. The extended attackers take control of numerous entities separate around the network, covering their reach. The IoV network faces pressures from the numerous attackers enclosed overhead. The variety of attacks could cooperation the reliability of the system, thus distressing its whole safety and reliability. Diverse safety attacks are enclosed in the subsequent section.

3.2 Security Attacks In IoV Environment

The IoV's vulnerability to sensitive cyber threats, including Distributed Denial of Service (DDoS) attacks and overhearing, offers the main apprehension. The threats in the IoV have exaggerated significance, risking both facility functionality and municipal security. The complex environment of these cyber hazards not only challenges the IoV's working usefulness but also increases the possibility of serious coincidences. Talking about these weaknesses is critical for guaranteeing the protected and consistent service of the IoV atmosphere. The following defines some key attacks defined in previous surveys [10, 4, 11, 12].

i. Eavesdropping attack: In this attack, user IDs, geolocation, and other pertinent data concerns to the IoV setting are inactively collected through the attacker. Without their realization or agreement, this data is misrepresented in contradiction of their privacy [15].

ii. Impersonation attack: The attacker signifies a genuine IoV object, misuses authentic identifications to gain illegal profits, and produces misperception within the IoV atmosphere. The attacker operates the data to their benefit.

iii. Man-in-middle (MITM) attack: The data integrity and privacy resolution of safety requests are disrupted through this attack. This kind of attack includes the aggressor introducing himself between two legally interactive objects or vehicles, attending in on their discussions, and varying or inoculating false evidence into the communications.

iv. Replay attack: This attack occurs when an attacker broadcasts earlier messages repetitively to deceive other IoV atmosphere objects. This deceitful practice goals to yield the benefit of replies.

v. Denial-of-service (DoS): Due to its huge distribution, this kind of attack extremely negotiates the obtainability of IoV facilities. Its main goal is to prevent legitimate users from using network resources and services, hence preventing their availability. This attack poses a serious problem since it stops genuine entities of IoV from communicating by interfering with the communication channel. Since timely information is crucial for preventing accidents, communication is key in life-critical safety applications. DDoS attacks are a type of DoS attack that carries greater severity than DoS attacks due to its distributive nature. Many hostile entities attack a legitimate entity in a DDoS.

vi. Sybil attack: The attacker creates a misleading environment by flooding the target vehicle with dummy vehicles via jamming a signal. Even when the target can easily follow the obvious path, the aggressor pressures them to monitor a diverse route. To conceal misleading reports, several fictitious identities are used, each supplied by a single attacker and mirroring actual nodes.

vii. Wormhole attack: An attack occurs when two or more malicious entities join forces on a network to construct a private tunnel through which data is forwarded from one malicious entity to another at an opposite end. It controls all packets that flow over that network, hiding the actual distances between them and compelling other legitimate entities to route through the tunnel that is built, leading to a safety breach.

viii. GPS spoofing attack: The Global Positioning System (GPS), relying on satellites, determines the precise location of vehicles by maintaining location tables that hold geographical coordinates and corresponding vehicular identities. In this attack, the attacker manipulates the position of the vehicles and thus fake locations are received by legitimate entities.

ix. Communication removal attack: The vigorous aggressor removes some of the communication conversation, influencing details regarding the state of the vehicle or the route. This attack affects the driver's decisions and results in mishaps.

x. Session linking attack: An attacker can use flaws to link two randomly selected vehicle sessions with other network entities using a session linking attack. Through a relatively simple calculation, this linkage may unveil all credentials associated with the sessions.

The researchers talked about a wide range of potential IoV environment security threats.

3.3 Security and Privacy Requirements

The digital world always has the possibility of attack and data breach because the attackers are also well equipped with tools and knowledge as the day passes. So, the attacks on IoV environments have the potential to create tragic mishaps. Consequently, the selection of encryption techniques must be undertaken with great care to ensure adequate security and privacy. Encryption techniques are vital for securing communications in the IoV, where sensitive data is transmitted between vehicles and infrastructure. Traditional symmetric encryption algorithms, such as AES, are commonly used due to their efficiency; however, they may not fully address the unique challenges of IoV environments [32]. Recent developments have introduced lightweight cryptographic protocols that are specifically designed for resource-constrained devices in IoV, ensuring both security and efficiency [33]. BBlockchain-based encryption techniques are being explored to provide decentralized security solutions, allowing for secure data sharing without relying on a central authority [34]. The integration of homomorphic encryption also allows for computations on encrypted data, preserving privacy while enabling data analysis [35]. These encryption techniques are crucial for ensuring the integrity, confidentiality, and authenticity of communications in the rapidly evolving IoV landscape. Therefore, security and privacy specifications are essential for evaluating and improving a network's resilience, especially when it comes to the IoV environment. In reaction to the serious attacks on IoV that have been mentioned above, researchers have looked into and put up a number of ways to improve security and privacy. Table 1 shows the summary of previous studies regarding security attacks on IoV. Table 2 represents the category of each attack highlighting the most dangerous attack types:

Table 1. Security Attacks in the IoV Environment

[16] in 2023	[6] in 2022	[17] in 2021	[18] in 2020
black hole cloaking	Impersonation attack	Man-in-the-middle attack	Message injection attack
grey hole creation	GPS spoofing attack	Traffic analysis attack	Cookie theft attack
Virus	Masquerading attack	Social attack	Flow of bogus information
Sybil	Man-in-middle attack	Eavesdropping attack	Man-in-middle attack:
Message Deception	Replay attack	Masquerading attack	Impersonation attack
GPS Intercepting	Message injection attack	Message tampering attack	DoS attack:
Masquerading	Cookie theft attack	Replay attack	Replay attack
Black Holes	Message manipulation attack	Illusion attack	Dissimulation of GPS attack
Worm Holes	Channel interference and Jamming attacks	Sleep deprivation	Sybill attack
Grey Holes	DoS	DoS/DDoS	Warm hole attack
Fraud	Eavesdropping attack	Jamming attacks	
Replay Attacks	Message holding attack	Intelligent cheater attack	Eavesdropping attack
Malware	False information flow	Jellyfish attack	Masquerading attack
Eavesdropping	Channel hindrance attack	Blackhole attack	Hardware intrusion attack
ID disclosure	Malware attack	Grayhole attack	Data falsification attack
Traffic monitoring	Physical Vehicle damage	Spamming attack	Channel hindrance attack
Spyware	Fuzzy attack	Greedy behavior attack	Fuzzy attack
Denied access	Sybil attack	Sybil attack	Malware attack
Malicious software	Guessing attacks	GPS spoofing	Session linking attack
	Wormhole attack	Tunneling attack	Guessing attacks
	Black-hole attack	Free-riding attack	Message holding attack
	Attack on fairness	Certificate/key replication attack	Message deletion attack
	Forgery attack	Repudiation attack	
	Session linking attack		

Table 2: Classification of Security Attacks in the Iov Environment

Attack Type	Description	Category
Black Hole Cloaking	Blocks legitimate data packets	Network Layer Attack

Impersonation Attack	Masquerades as another vehicle	Spoofing Attack
Man-in-the-Middle Attack	Intercepts and alters communication	Eavesdropping & Interception
Message Injection Attack	Inserts malicious messages	Injection Attack
Grey Hole Creation	Selectively drops packets	Network Layer Attack
GPS Spoofing Attack	Alters GPS data	Spoofing Attack
Traffic Analysis Attack	Monitors traffic for patterns	Privacy Attack
Cookie Theft Attack	Steals session data	Privacy Attack
Virus	Infects systems	Malware Attack
Masquerading Attack	Disguises identity	Spoofing Attack
Social Attack	Exploits social behaviors	Social Engineering Attack
Sybil Attack	Creates multiple fake identities	Spoofing Attack
Replay Attack	Re-sends captured messages	Replay Attack
DoS Attack	Floods network to deny service	Denial of Service
Wormhole Attack	Reroutes communication paths	Network Layer Attack
Eavesdropping	Listens to communications	Privacy Attack
Channel Interference/Jamming	Disrupts signals	Jamming/Interference
Malware	Infects devices	Malware Attack
False Information Flow	Propagates inaccurate data	False Data Injection
Hardware Intrusion	Compromises physical hardware	Physical Attack
Spamming Attack	Sends excessive messages	Denial of Service
Greedy Behavior Attack	Excessive resource consumption	Resource Exhaustion Attack
Guessing Attacks	Attempts to guess sensitive data	Guessing Attack
Forgery Attack	Creates forged identities or messages	Spoofing Attack
Repudiation Attack	Denies committed actions	Deception Attack

Table 3. Security Requirements, Attacks, and Solutions

Security Requirements	Attacks	Solutions
Confidentiality	Eavesdropping, Message holding, MITM	Encryption
Integrity	Identity Masquerading attack, Data Manipulation attack	ID-based cryptography, hash functions
Availability	DoS / DDoS, Malware, Jamming	PKI Infrastructure using Authentication, Antivirus-software, Spread-spectrum
Privacy	Privacy leakage, User ID disclosure, User's credentials exposure	Restrict access to sensitive data, Pseudonymous and Anonymization methods, Encryption
Authentication	Replay attack, Impersonation, Sybil	ID-based batch verification, Position-verification,

Table 4. Proposed Protocols: Informal & Formal Analysis

Proposed Protocols	Informal analysis: Attacks resistance using proposed protocols	Proposed work	Novelty	Results	Formal Analysis methods
[19]	Sybil attack, Spoofing attack,	Blockchain-based	Optimized PBFT	Meets IoV security	RoR model, and

	forgery attack, MITM attack, DDOS, Replay attack	distributed authentication for IoV. Decentralizes data processing and storage to reduce delays.	consensus algorithm for reusing authentication results. Reduces reliance on RSUs, refining system efficiency.	requirements. Reduces communication and computation costs.	AVISPA tool
[20]	Physical capture attacks, session key security, three-factor authentication mechanism	The paper proposes a secure and efficient Authentication and Key Establishment (AKE) scheme for IoV environments.	The paper identifies and addresses the security vulnerabilities of a previously proposed AKE scheme through logical and mathematical analyses.	The proposed scheme enhances the security properties and meets essential requirements, with AVISPA tool used for formal verification. The scheme ensures improved robustness.	AVISPA tool
[21]	Replay attack, MITM attack, Impersonation attack, Physical capture attack, session key security	The paper proposes a blockchain-based secure distributed authentication scheme for IoV, decentralizing data processing and storage to reduce communication delays and response time.	Smart contract technology is used for the automatic triggering of the authentication process. An optimized PBFT algorithm is designed to reuse authentication results.	The proposed scheme meets the security requirements of IoV, with reduced communication and computation costs, verified through formal security tools and SUMO simulation.	Scyther tool
[22]	MITM attack, Anonymity and Unlinkability, Traceability and Revocability, Replay attack, Impersonation Attack, Session Fixation Attack, Forward Secrecy, Colluding Attack Resistance	Proposes a Blockchain-Based Privacy-Preserving Authentication (BPA) scheme specifically designed for the IoV.	Utilizes blockchain technology for decentralized and secure authentication, ensuring privacy preservation while communicating across IoV networks.	The proposed BPA scheme enhances security and privacy in IoV environments, with efficient authentication mechanisms that reduce overhead and ensure user privacy.	RoR model, ProVerif tool
[23]	Anonymity and unlinkability, Perfect forward secrecy, Known key secrecy, Replay attacks, Password guessing attacks, Identity guessing attacks, Forgery attacks and impersonation attacks, RSU captured attacks	Proposes an improved V2I authentication protocol for IoV using Physical Unclonable Functions (PUF) and a three-factor secrecy strategy to resist attacks.	Introduces PUF for enhanced security against RSU attacks and a conditional privacy-preserving strategy for anonymity and tracking.	The proposed protocol demonstrates provable security under the random oracle model and achieves low computation and communication costs, providing enhanced security and privacy.	RoR model
[24]	Anonymity and un-traceability of the vehicle, withstand the DoS attack, and withstanding cloning attack	Proposes a new authentication protocol for the IoV environment that uses biometrics and Physical Unclonable Function (PUF) for security.	Introduces biometric key-based authentication to safeguard against smart card/device theft and PUF to resist cloning attacks.	Informal and formal analyses (RoR model and Scyther tool) verify the protocol's ability to withstand known attacks. The protocol offers low computation time and ensures security.	RoR model, and Scyther tool
[25]	Tag anonymity, Mutual authentication, Resistance against tag tracking, and Resistance against desynchronization attacks	Proposes a lightweight RFID security fast authentication protocol for IoV in traffic congestion scenarios, integrating ownership transfer in non-congestion situations.	Utilizes edge servers for authentication and combines ECC (Elliptic Curve Cryptography) and hash functions for secure private data protection in vehicles.	Formal analysis using the Scyther tool shows resistance to typical attacks. Experimentally, the scheme reduces calculation and communication overhead by 66.35% in congestion and 66.67% in non-congestion scenarios.	Scyther tool
[26]	Smart card theft attack, Unable to retroactively attack, Identity anonymity, Mutual authentication, Replay attack, and Traceability and non-repudiation	Proposes a mutual anonymous authentication and key agreement scheme for VANETs, based on elliptic curve cryptography.	Introduces a two-phase authentication: initial (with the first roadside unit) and subsequent authentication, which reduces computational complexity for vehicles already on the road.	Security analysis is performed using BAN logic and Proverif simulation, demonstrating that the scheme is secure. Performance analysis shows reduced computation and communication consumption compared to other methods.	BAN logic, and ProVerif tool

[27]	Resilience against on-broad unit physical capture attack, insider attack, replay attack, mutual authentication, and provides forward and backward secrecy	Proposes a new remote access control scheme for secure communication among vehicles in the (IoV) environment.	Introduces remote registration of vehicles and a two-phase mechanism: node authentication and key agreement using cryptographic techniques and pre-loaded information.	Security analysis (informal and formal) using AVISPA tool confirms that the scheme is secure against attacks like replay, man-in-the-middle, and impersonation. Additionally, the scheme shows lower computation and communication costs compared to existing methods.	Correctness proof using Theorems, and AVISPA tool
[28]	Stolen verifier, Vehicle anonymity, Session key security, Denial of service, and Replay attack	Proposes a Secure Message Authentication Protocol (SMEP-IoV) for information exchange among IoV entities using lightweight hash functions and encryption.	Utilizes lightweight symmetric hash functions and encryption operations to ensure secure and efficient authentication in IoV.	BAN logic is used for formal security analysis, and performance comparisons show that SMEP-IoV completes authentication in just 0.198 ms, demonstrating its lightweight nature and efficiency.	BAN logic
[29]	Known Key Attack, and OBU Physical Capture Attack	Proposes a mutual authentication and key agreement protocol for IoV-enabled Intelligent Transportation Systems (ITS) to ensure secure communications between connected entities.	Focuses on providing security, anonymity, and untraceability while ensuring low computational and communication overheads, tackling several known IoV attacks.	The proposed scheme is formally verified to be secure against several attacks (e.g., replay, impersonation, man-in-the-middle), has lower overhead compared to seven other schemes, and demonstrates better security and performance using NS2 simulations.	RoR model, and AVISPA tool
[30]	Session / Secret key disclosure attack, and Mutual Authentication	Proposes a secure and efficient message authentication protocol (IoV-SMAP) for communication in IoV-based smart cities, addressing security threats in IoV environments.	The IoV-SMAP protocol ensures user anonymity and mutual authentication, while resisting attacks like impersonation, secret key disclosure, and off-line guessing attacks.	Security of IoV-SMAP is validated using Real-or-Random (ROR) model and AVISPA simulations. The protocol is compared with existing schemes and is shown to provide better security and efficiency in an IoV-based smart city.	RoR model, and AVISPA tool
[31]	Password guessing attack, Man-in-the-middle attack, and Brute force attack	Proposes secure and lightweight communication protocols for various IoV communication components, including V2V, V2P, V2R, V2I, and V2S.	Focuses on developing secure and efficient protocols tailored for different IoV components, addressing security and efficiency in a highly dynamic IoV environment.	The protocols were implemented on a Desktop Computer and Raspberry Pi, demonstrating better performance than competing protocols in terms of communication, storage, computation, and battery consumption.	No Formal analysis

These specifications are derived from basic security objectives like availability, non-repudiation, confidentiality, data integrity, authenticity, and access control. The attacks and solutions related to these requirements shown in [18, 36] are provided in Table 3, and also explained in more detail in the section that follows:

Confidentiality: Information over IoV places a high value on confidentiality, making sure that data is only exposed to those who intend to see it and protecting sensitive information from unwanted access. Encryption is a vital component that ensures access is limited to authorized users, protecting the security and privacy of entities in the IoV environment. Encryption becomes essential to stop eavesdropping and prevent unwanted access when adversaries become a threat [16-18].

Integrity: In IoV environments, integrity is essential to accuracy and coherence. Data accuracy is threatened by attacks including viruses, masquerade, and message tampering. IoV environments are actively protected from active man-in-the-middle assaults because MITM attacks can modify the data. The integrity guarantees that message contents are unchanged and legitimate throughout the communication process [15].

Availability: The IoV entities need to be completely responsive at all times. More specifically, all of its parts have to work all the time. The most known attack is DoS and

DDoS attack that effects the availability of services needed by different entities in IoV environment.

Privacy: Modern cars have a need to protect private information that might compromise the privacy of drivers or passengers. The monitoring of the car's location, which is a type of sensitive data, serves as an example. This is problematic since many location services conflict with users' privacy concerns by requiring access to the car's position [37].

Latency: We have involved an in-depth conversation on how diverse authentication protocols effect message delays, mostly in high-mobility situations such as IoV, where real-time dealings are vital. Protocols that decrease handshake rounds and decrease re-authentication processes have been highlighted for their ability to improve system efficiency and lower latency.

Scalability: It is a critical concern in the IoV, particularly in the context of authentication protocols. As the number of connected vehicles rises, the need for efficient and secure authentication mechanisms becomes paramount. Traditional centralized authentication systems can become bottlenecks, leading to delays and vulnerabilities. To address this, decentralized approaches, such as those leveraging blockchain technology, have been proposed to distribute authentication tasks across multiple nodes, enhancing scalability while maintaining security [38]. Furthermore, federated learning-based protocols enable vehicles to collaboratively authenticate without sharing sensitive data, thereby reducing communication overhead and improving scalability [39]. These advancements underscore the necessity for scalable solutions that can adapt to the dynamic nature of IoV environments, ensuring secure and efficient communication among the ever-increasing number of vehicles [40].

Computational Overhead: We extended the examination of computational costs related to different authentication mechanisms, seeing the source restraints of IoV strategies like on-board units (OBUs). This proposed study stresses procedures that accomplish an optimal balance between low computational complexity and security certifying they are achievable for resource-limited devices without cooperating act.

Authentication: Authentication is essential for confirming the legitimacy of IoV entities communicating across a network. It keeps attackers from impersonating trustworthy nodes in order to modify or relay communications in an unethical manner. In authentication, the sender of the message can be verified using secrets only known to the sender like password, pin and cryptographic keys.

3.4 Security and Privacy in IoV through Authentication

Authentication is an initial requirement for any entity in the IoV environment who wants to join and then communicate with other entities. If any vehicle wants information about the road condition from roadside units (RSU), the distance of other objects, and the traffic flow information of a particular area then that vehicle must authenticate itself as a legitimate entity before starting any communication with other entities in the IoV. The entity after authentication establishes a session key with another entity. This symmetric session key is employed for communication in an unsecure channel. Therefore, authentication is the initial phase its significance ought to be given top consideration. The authors in [6] describe the IoV authentication is essential for identifying and verifying vehicles using credential-based systems that are supervised by a Trusted Authority (TA). Vehicles authenticate with Roadside Units (RSUs) as part of the procedure, and RSUs then submit requests to the TA for verification. For the IoV to guarantee data privacy, integrity, and general security, a strong authentication process is essential. Authentication is the initial line of defense against a variety of attacks, such as replay, Sybil, warm hole, impersonation, replay, message injection, and GPS spoofing. Threats to IoV authentication come from both intracluster and out-of-cluster techniques. Thus, these attacks immediately compromise the authentication mechanism if an attacker gains access to the secret credentials of real nodes. This breach allows unauthorized access to private data, which could result in dishonest behavior by network organizations. In [31] the authors describe IoV network model is consisting of the following 4 points:

- The IoV communication situation is limited to registered vehicles only.
- The VS is a TA. Its processing and storage capacities are also high. It can't be compromised.
- The OBUs and other entities also have storage and processing capabilities.
- The registered user never discloses their password to a stranger.

The VS is a TA initially registered all the communication entities of IoV. The registration involves 1) Vehicle registration, 2) RSU Registration, 3) Portable Device (Mobile) Registration, 4) Wireless Sensor Device Registration, and 5) Infrastructure Registration [31].

4. Existing IoV Authentication Protocols

The formal analysis of authentication methods in the context of the IoV is the main focus of this survey work. Examining the formal analysis of the latest authentication protocols is the primary goal. The goal of the study is to present a thorough overview of the most recent IoV authentication protocols, highlighting a formal analytical method used to verify the protocols. This will ultimately aid in the development of more durable and dependable authentication mechanisms for connected vehicles. Two main approaches often employed by academics to confirm their planned protocols are proper examination and casual assessment.

4.1 Informal Analysis of IoV Authentication Protocols

The IoV authentication protocols are examined informally by monitoring their application and structure regarding all aspects without using official statistical tools and mathematical proofs. Professionals in the safety examination process such as cryptographic approval assess how they are resistant to attacks such as DoS, MITM, session-key-security, replay attacks, impersonation, and Sybil, etc. The causal evaluation is an additional approach to help in detecting possible weaknesses in the IoV authentication process [41].

This paper also offers an informal examination of the most current IoV verification protocols, along with an assessment of their behavior on numerous attacks. The proposed work delivers visions into IoV authentication protocols by inspecting the efficiency of verification tools and their flexibility to conceivable attacks. Table 4 represents proposed protocols, informal and formal analysis, proposed work novelty, and results.

4.2 Formal Analysis of IoV Authentication Protocols

Formal analysis is essential for safeguarding the security and privacy of sensitive data transmitted among vehicles and infrastructure in IoV authentication protocols. By thoroughly examining the protocols, potential vulnerabilities can be detected and addressed prior to deployment, thereby thwarting attacks like impersonation, replay, and man-in-the-middle [42, 43]. The dynamic and highly mobile IoV environments, featuring frequent interactions, necessitate robust security measures to protect against unauthorized access and data breaches [44]. Furthermore, formal analysis provides a systematic framework for modeling and analyzing protocol behaviors under diverse attack scenarios, thereby enhancing the reliability of security claims [45]. This is especially vital in the context of the IoV, where security vulnerabilities can have grave safety implications [46]. Additionally, formal analysis can foster trust by ensuring that authentication processes are both effective and privacy-preserving [47]. Integrating formal analysis into the development of IoV authentication protocols is, consequently, crucial for cultivating a secure and trustworthy vehicular communication ecosystem.

To certify the consistency and safety of these key IoV objects, proper work of verification protocols is mandatory. Formal assessment is employed to identify and report any faults in the structure and application of verification protocols using statistical tools and verification measures. The main consequence of formal analysis is accuracy certification, which assurances that the validation protocol works as proposed and defends against diverse kinds of safety threats. Moreover, formal study helps in the initial exposure of errors throughout the design stage, permitting quick modifications and developments. The overall use of formal assessment in verification protocols is important for structuring consistent schemes, observing manufacturing standards, and defending against hidden breaches and unlawful admittance. The subsequent approaches are the important ones that a large number of public investigators employ for formal assessment:

Scyther: is a computerized tool employed for the confirmation of the safety protocols. It is proficient in facilitating in-depth analysis of information and examining safety standards like privacy, reliability, protocol availability, and authentication. The security protocol description language (SPDL) is employed using the scyther tool for the report of the protocols and the tests [48].

ProVerif: tool that inevitably tests cryptographic protocols' safety. Cryptographic primitives for instance digital signatures, symmetric and asymmetric encryption, and hash functions are supported, among others [49].

AVISPA: Automated Validation of Internet Security Protocols and Applications (AVISPA) tool instructions the correctness and defense standards of the protocols by a range of formal methods, such as model examination and representative study. AVISPA tool uses the "High-Language Protocol Specification Language" (HLPSL) for defining cryptographic protocols [50].

BAN Logic: Burrows, Abadi, and Needham (BAN) logic has guidelines and systems that are employed for defining and confirming the verification of main conversion between gatherings, several important agreement protocols employed BAN reason for studying the protocol genuineness [51].

ROR model: Real-Or-Random (ROR) model is employed to approve the session-key protection of authentication protocols [52].

This study aims to monitor the procedures that are presently being employed in the formal examination of the modern verification protocols used in the IoV settings for session keys well-known between objects to interconnection in an exposed and unsafe network.

5. Research Challenges, Impact of the Dynamic Nature, and Future Directions in IoV

The impact of the dynamic nature of the Internet of IoV has a significant impact on authentication protocols. We have delivered a broad conversation to address how issues like vehicle mobility, ad-hoc connections, and changing network topologies meaningfully effects the strategy and efficiency of authentication protocols. The field of IoV security is a dynamic and active one, with new research being introduced on a regular basis that offers innovative approaches to address the ever-changing problems in system security. In addition to helping to overcome current system constraints like computation and power resources, recent technology developments also create new opportunities for combining traditional standards with creative solutions to successfully handle security issues. The section that follows explores particular areas for future research in the field of IoV security.

5.1 Vehicle and Infrastructure Communication Security

It's critical to secure a connection between infrastructure and automobiles. Eavesdropping, message manipulation, and denial-of-service assaults are examples of threats. To safeguard communication channels, strong cryptographic protocols, intrusion detection systems, and safe key management systems should be developed on IoV environments.

5.2 Concerns about Privacy

User privacy is a problem with IoV because it involves the gathering and exchange of sensitive data. Privacy breaches may arise from unauthorized access to personal data. A key component of the Vehicular Cloud (VC) is privacy, which protects communication and information sharing in an encrypted manner and is therefore essential for building and preserving user trust in the IoV environments [15]. As a result, privacy-preserving techniques like data anonymization and anonymous authentication should be used to preserve user privacy while facilitating effective communication.

5.3 Authentication

The dynamic member fluctuations in the IoV make trustworthiness essential. To stop unauthorized entities from injecting false information, a strong authentication method is required. Authentication is crucial for secure communication between entities, especially in applications pertaining to traffic safety where an intruder could be a serious threat [14]. Building trust between entities improves the security of IoV. Addressing the limitations of traditional credential-based authentication, including password vulnerabilities and management complexities, is pivotal for a secure IoV environment. In order to accommodate the dynamic and ever-changing nature of IoV ecosystems, future research should concentrate on dynamic and multifactor authentication techniques, including password-less ways.

5.4 Blockchain

The decentralized nature of blockchain technology, which does away with the need for reliable third parties, has made it useful in the fields of IoV. It is necessary to work toward improving the benefits of blockchain technology, like decentralization, immutability, and transparency [18]. Blockchain in IoV provides immutable data integrity and safe identity retention. The creation of a blockchain-based authentication system to protect data in an IoV is a possible research problem.

5.5 Firmware and Security

Regarding Software and Firmware Security, the growing dependence of automobiles on software highlights the vital necessity of safeguarding in-car software and firmware. Remote attacks could occur from these components' exploitable vulnerabilities. Future efforts should concentrate on putting secure coding techniques, hardware-based security solutions, and constant monitoring into place in order to solve this and guarantee the continued confidentiality and integrity of software and firmware.

5.6 Large Quantity of IoV Entities Data

An enormous amount of data is produced by the sensors in the transportation environment, including cameras placed on vehicles and road sensors. It is difficult to manage real-time data from this vast amount of data. Fog computing has been suggested as a solution, however, it is still in its early stages [16].

5.7 Fog and Edge Computing

In the realm of the IoV, fog, and edge computing play a crucial role in enhancing authentication protocols. Fog and edge computing are essential for improving authentication protocols. Positioning computational resources nearer to the data origin facilitates more effective data processing, enhances response times, and diminishes latency. Furthermore, a straightforward, energy-efficient authentication methodology founded on Physically Unclonable Functions has been developed to safeguard communications between vehicles and roadside infrastructure. By improving resource allocation through the use of deep reinforcement learning in task offloading, IoV systems' efficiency is further raised. These developments emphasize how crucial it is to combine edge and fog computing with strong authentication methods in order to handle the particular difficulties presented by IoV environments. These advancements highlight the importance of combining fog and edge computing with robust authentication mechanisms to address the unique challenges posed by IoV environments [53-56].

5.8 Mobility, Ad-hoc Connections and Network Topology

The inherent dynamism of the IoV, marked by vehicle mobility, ad-hoc connectivity, and frequently changing network architectures, presents substantial obstacles for authentication protocols. The following points describe these challenges and their impact:

i. Vehicle Mobility: The high speed and constant movement of vehicles complicates consistent authentication. Vehicles frequently change network locations, necessitating rapid, seamless handover of authentication processes between different network points. For instance, protocols must quickly re-authenticate vehicles when they move from one RSU to another, which can cause delays if the system isn't optimized for highly mobile environments. In IoV the devices have very limited resources and therefore lightweight, fast protocols, such as those using cryptographic hash functions, are increasingly being proposed to address this issue by minimizing computational load and ensuring real-time performance [57-60].

ii. Ad-hoc Network Connections: IoV operates on an ad-hoc network, meaning vehicles establish direct, short-lived connections with nearby nodes. This unpredictability requires authentication protocols that can handle temporary, peer-to-peer interactions while ensuring security. Ad-hoc connections are particularly vulnerable to impersonation attacks and man-in-the-middle attacks, so protocols must incorporate measures like mutual authentication or session-key generation for secure communication [61-64].

iii. Dynamic Topologies: As vehicles move, network topologies are constantly changing, which makes it challenging to maintain a stable authentication process. Conditional privacy-preserving protocols are being developed to maintain security in these highly dynamic environments, ensuring that users' identities are protected even as network conditions shift. For instance, recent proposals have leveraged techniques like Physical Unclonable Functions (PUF) to enhance resilience against RSU capture attacks, while three-factor authentication helps protect against side-channel and impersonation attacks [*65*, *66*].

6. Conclusion

The IoV domain uses sophisticated communication technologies to improve road safety. Using real-time information, the IoV uses a complete communication approach to reduce accidents. Security and privacy lapses could result in casualties, so these issues must be addressed in IoV. The survey discusses security attacks like replay attacks, MITM attacks, Sybil attacks, and others on IoV environments.

The key elements of security like integrity, encryption, passwords, and cryptography confirm the validity of an entity. In addressing privacy issues in modern vehicles, protection measures are crucial. Safety monitoring is required especially in sensitive location data, driver, and vehicle identities.

The authentication protocols have been proposed by researchers to secure communication between IoV entities. The formal and informal analysis techniques are used to confirm the proposed authentication protocol. Formal authentication protocol analysis using mathematical models for design examination to ensure IoV entity dependability and security. Using detection and correction techniques of vulnerabilities such as replay attacks during the design phase, the formal analysis provides correct verification. Popular tools like Scyther, ProVerif, and AVISPA aid employed in the establishment of strong authentication protocols. The study addresses the significance of a thorough examination and also upcoming trends and difficulties in IoV security and privacy. The future work will be focused on further deep analysis of fog and edge computing in IoV safety which is another motivating and active research domain.

References

[1] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal,* vol. 5, no. 5, pp. 3701-3709, 2017.

[2] M. Abdelsalam and T. Bonny, "IoV road safety: Vehicle speed limiting system," in *2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, IEEE, pp. 1-6. 2019:

[3] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart transportation: an overview of technologies and applications," *Sensors,* vol. 23, no. 8, p. 3880, 2023.

[4] M. Humayun, S. Afsar, M. F. Almufareh, N. Jhanjhi, and M. AlSuwailem, "Smart traffic management system for metropolitan cities of kingdom using cutting edge technologies," *Journal of Advanced Transportation,* vol. 2022, no. 1, p. 4687319, 2022.

[5] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[6] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "Architecture, protocols, and security in IoV: Taxonomy, analysis, challenges, and solutions," *Security and Communication Networks,* vol. 2022, no. 1, p. 1131479, 2022.

[7] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Challenges of future VANET and cloud-based approaches," *Wireless Communications and Mobile Computing,* vol. 2018, no. 1, p. 5603518, 2018.

[8] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications,* vol. 20, p. 100182, 2019.

[9] P. Sharma, M. Patel, and A. Prasad, "A systematic literature review on IoVSecurity," *arXiv preprint arXiv:2212.08754,* 2022.

[10] S. S. Sepasgozar and S. Pierre, "Network Traffic Prediction Model Considering Road Traffic Parameters Using Artificial Intelligence Methods in VANET," *IEEE Access,* vol. 10, pp. 8227-8242, 2022.

[11] P. Sewalkar and J. Seitz, "Vehicle-to-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges," *Sensors (Basel, Switzerland),* vol. 19, 2019.

[12] M. Elassy, M. Al-Hattab, M. Takruri, and S. Badawi, "Intelligent transportation systems for sustainable smart cities," *Transportation Engineering,* p. 100252, 2024.

[13] S. Zeadally, J. A. G. Ibáñez, and J. Contreras-Castillo, "A tutorial survey on vehicle-to-vehicle communications," *Telecommunication Systems,* vol. 73, pp. 469 - 489, 2019.

[14] H. Goumidi, Z. Aliouat, and S. Harous, "Vehicular cloud computing security: A survey," *Arabian Journal for Science and Engineering,* vol. 45, no. 4, pp. 2473-2499, 2020.

[15] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey," *Wireless Communications and Mobile Computing,* vol. 2020, no. 1, p. 5129620, 2020.

[16] N. Tabassum and C. Reddyy, "Review on QoS and security challenges associated with the IoVin cloud computing," *Measurement: Sensors,* vol. 27, p. 100562, 2023.

[17] A. Verma, R. Saha, G. Kumar, and T.-h. Kim, "The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions," *Applied Sciences,* vol. 11, no. 10, p. 4682, 2021.

[18] P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges," *Ieee Access,* vol. 8, pp. 54314-54344, 2020.

[19] Z. Ma *et al.*, "A Blockchain-Based Secure Distributed Authentication Scheme for Internet of Vehicles," *IEEE Access,* 2024.

[20] K. Park, M. Kim, and Y. Park, "On the Security of a Secure and Computationally Efficient Authentication and Key Agreement Scheme for Internet of Vehicles," *Electronics,* vol. 13, no. 16, p. 3136, 2024.

[21] H. Vasudev, M. Shariq, S. K. Dwivedi, and M. Conti, "LightKey: Lightweight and Secure Key Agreement Protocol for Effective Communication in Internet of Vehicles," in *Proceedings of the 25th International Conference on Distributed Computing and Networking,* pp. 209-216, 2024.

[22] J. Li, Y. Lin, Y. Li, Y. Zhuang, and Y. Cao, "BPA: A Novel Blockchain-Based Privacy-Preserving Authentication Scheme for the Internet of Vehicles," *Electronics,* vol. 13, no. 10, p. 1901, 2024.

[23] Q. Xie and J. Huang, "Improvement of a Conditional Privacy-Preserving and Desynchronization-Resistant Authentication Protocol for IoV," *Applied Sciences,* vol. 14, no. 6, p. 2451, 2024.

[24] E. H. Nurkifli and T. Hwang, "Provably secure authentication for the internet of vehicles," *Journal of King Saud University-Computer and Information Sciences,* vol. 35, no. 8, p. 101721, 2023.

[25] Y. Gong *et al.*, "VASERP: an adaptive, lightweight, secure, and efficient RFID-based authentication scheme for IoV," *Sensors,* vol. 23, no. 11, p. 5198, 2023.

[26] Q. Yang, X. Zhu, X. Wang, J. Fu, J. Zheng, and Y. Liu, "A novel authentication and key agreement scheme for Internet of Vehicles," *Future Generation Computer Systems,* vol. 145, pp. 415-428, 2023.

[27] P. Bagga, A. K. Das, and J. J. Rodrigues, "Bilinear pairing-based access control and key agreement scheme for smart transportation," *Cyber Security and Applications,* vol. 1, p. 100001, 2023.

[28] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Security and Communication Networks,* vol. 2021, pp. 1-9, 2021.

[29] P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, K.-K. R. Choo, and Y. Park, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 2, pp. 1736-1751, 2021.

[30] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment," *IEEE access,* vol. 8, pp. 167875-167886, 2020.

[31] H. Vasudev, D. Das, and A. V. Vasilakos, "Secure message propagation protocols for IoVs communication components," *Computers & Electrical Engineering,* vol. 82, p. 106555, 2020.

[32] A. Aljumaili, H. Trabelsi, and W. Jerbi, "A Review on Secure Authentication Protocols in IOV: Algorithms, Protocols, and Comparisons," *2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT),* pp. 1-11, 2023.

[33] H. W. Haiyan Wang and H. M. Haiyan Wang, "A Lightweight V2R Authentication Protocol Based on PUF and Chebyshev Chaotic Map," *電腦學刊,* 2023.

[34] S. Roy, S. Nandi, R. Maheshwari, S. Shetty, A. K. Das, and P. Lorenz, "Blockchain-Based Efficient Access Control With Handover Policy in IoV-Enabled Intelligent Transportation System," *IEEE Transactions on Vehicular Technology,* vol. 73, pp. 3009-3024, 2024.

[35] B.D. Manh, C.-H. Nguyen, D. T. Hoang, and D. N. Nguyen, "Homomorphic Encryption-Enabled Federated Learning for Privacy-Preserving Intrusion Detection in Resource-Constrained IoV Networks," *ArXiv,* vol. abs/2407.18503, 2024.

[36] J. Deng *et al.*, "A Survey on Vehicular Cloud Network Security," *IEEE Access,* vol. 11, pp. 136741-136757, 2023.

[37] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Vehicular Communications,* vol. 10, pp. 13-28, 2017.

[38] Q. Xie, Z. Sun, Q. Xie, and Z. Ding, "A Cross-Trusted Authority Authentication Protocol for IoVBased on Blockchain," *IEEE Access,* vol. 11, pp. 97840-97851, 2023.

[39] P. Zhao, Y. Huang, J. Gao, L. Xing, H. Wu, and H. Ma, "Federated Learning-Based Collaborative Authentication Protocol for Shared Data in Social IoV," *IEEE Sensors Journal,* vol. 22, pp. 7385-7398, 2022.

[40] H. Han, S. Chen, Z. Xu, X. Dong, and J. Zeng, "Trust Management Scheme of IoV Based on Dynamic Sharding Blockchain," *Electronics,* 2024.

[41] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Security and Communication Networks,* vol. 2021, no. 1, p. 5554318, 2021.

[42] T. Lauser and C. Krauß, "Formal Security Analysis of Vehicle Diagnostic Protocols," *Proceedings of the 18th International Conference on Availability, Reliability and Security,* 2023.

[43] H. Sikarwar and D. Das, "A Novel MAC-Based Authentication Scheme (NoMAS) for IoV(IoV)," *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, pp. 4904-4916, 2023.

[44] J. Zhang, T. Li, M. S. Obaidat, C. Lin, and J. Ma, "Enabling Efficient Data Sharing With Auditable User Revocation for IoV Systems," *IEEE Systems Journal,* vol. 16, pp. 1355-1366, 2022.

[45] C. Jacomme and S. Kremer, "An Extensive Formal Analysis of Multi-factor Authentication Protocols," *2018 IEEE 31st Computer Security Foundations Symposium (CSF),* pp. 1-15, 2018.

[46] L. Li, J. Sun, Y. Liu, M. Sun, and J. S. Dong, "A Formal Specification and Verification Framework for Timed Security Protocols," *IEEE Transactions on Software Engineering,* vol. 44, pp. 725-746, 2018.

[47] U. Bodkhe and S. Tanwar, "BiOIoV: Biometric-based Secure Data Dissemination for IoV Ecosystem," *2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence),* pp. 677-682, 2023.

[48] C. J. Cremers, "The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols: Tool Paper," in *International conference on computer aided verification,*Springer, pp. 414-418, 2008.

[49] B. Blanchet, V. Cheval, X. Allamigeon, and B. Smyth, "ProVerif: Cryptographic protocol verifier in the formal model," ed, 2010.

[50] A. Armando, D. Basin, J. Cuellar, M. Rusinowitch, and L. Viganò, "Avispa: automated validation of internet security protocols and applications," *ERCIM News,* vol. 64, no. January, pp. 66-69, 2006.

[51] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems (TOCS),* vol. 8, no. 1, pp. 18-36, 1990.

[52] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, Proceedings 8*, Springer, pp. 65-84, 2005.

[53] M. Georgiades and M. S. Poullas, "Emerging Technologies for V2X Communication and Vehicular Edge Computing in the 6G era: Challenges and Opportunities for Sustainable IoV," *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT),* pp. 684-693, 2023.

[54] Y. Salami, V. Khajehvand, and E. Zeinali, "SAIFC: A Secure Authentication Scheme for IOV Based on Fog-Cloud Federation," *Security and Communication Networks,* 2023.

[55] S. G. Aarella, S. P. Mohanty, E. Kougianos, and D. Puthal, "Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing," *Proceedings of the Great Lakes Symposium on VLSI,* 2023.

[56] J. Bi, X. Xue, H. Yuan, and J. Zhang, "Latency-Minimized Computation Offloading in Vehicle Fog Computing with Improved Whale Optimization Algorithm," *2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC),* pp. 5003-5008, 2023.

[57] E. Khezri, H. Hassanzadeh, R. O. Yahya, and M. Mir, "Security challenges in IoV(IoV) for ITS: A survey," *Tsinghua Science and Technology,* 2024.

[58] Z. Yang, K. Zhang, L. Lei, and K. Zheng, “A novel classifier exploiting mobility behaviors for sybil detection in connected vehicle systems,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2626–2636, 2019.

[59] M. Tabany and M. Syed, "A Lightweight Mutual Authentication Protocol for Internet of Vehicles," *J. Adv. Inf. Technol,* vol. 15, pp. 155-163, 2024.

[60] Q. Xie, Z. Ding, and P. Zheng, "Provably secure and anonymous V2I and V2V authentication protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems,* vol. 24, no. 7, pp. 7318-7327, 2023.

[61] M. Ehtisham *et al.*, "IoV(IoV)-Based Task Scheduling Approach Using Fuzzy Logic Technique in Fog Computing Enables Vehicular Ad Hoc Network (VANET)," *Sensors,* vol. 24, no. 3, p. 874, 2024.

[62] R. Sohail *et al.*, "A machine learning-based intelligent vehicular system (IVS) for driver’s diabetes monitoring in vehicular ad-hoc networks (VANETs)," *Applied Sciences,* vol. 13, no. 5, p. 3326, 2023.

[63] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)," *Sensors,* vol. 23, no. 5, p. 2594, 2023.

[64] S. Masood *et al.*, "Detecting and preventing false nodes and messages in vehicular ad-hoc networking (VANET)," *IEEE Access,* 2023.

[65] Z. Liang, P. Yang, C. Zhang, and X. Lyu, "Secure and efficient hierarchical Decentralized learning for Internet of Vehicles," *IEEE Open Journal of the Communications Society,* 2023.

[66] P. Surapaneni, S. Bojjagani, and A. K. Maurya, "Handover-Authentication Scheme for IoV(IoV) Using Blockchain and Hybrid Computing," *IEEE Access,* 2024.