iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40598

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Internet of Vehicle (IOV) Security Issues and Their Solutions

Murtaza Rashid Wani[1], Jasdeep Singh[2]
[1]*M.Tech Scholar Computer Science Engineering, RIMT University Mandi Gobingarh, Punjab, India*
[2]*Assistant Professor Department of Computer Science Engineering, RIMT University Mandi Gobingarh, Punjab, India*

Abstract: ***The "Internet of Things" is a new paradigm that includes smart hospitals, smart cities, and home automation, among other services. The "Internet of Things" has turned a small-scale Vehicular Ad-hoc Network (VANET) into a highly scalable and controlled "Internet of Vehicle" that is based on the internet (IoV). The Internet of Automobiles (IoV) is a vehicular network idea that comprises of linked motors, users, and other smart devices.***
It aims to provide a range of safety and pleasure services. Depending on which directions and other data are sent to each vehicle, the IoV system equips them with various sensors that record various types of data and send it to a computer unit for computation and analysis. We present a model overview of the IoV system in this research. Because every system failure directly affects user safety on the Internet of Things, security becomes crucial. We look at security concerns, various security assaults, and solutions from an IoV perspective. We also provide a system that support for vehicle-to-infrastructure (V2I) communication in the Internet of Vehicles.
Keywords: Internet of vehicles, Vanet, Vehicle to infrastructure, Security challenges.

I. INTRODUCTION

The Internet of Automobiles, or IoV, is a complex network link that integrates vehicles, users, and other intelligent devices or "things" to the computer. Vehicles in the Internet of Things (IoV) are core nodes with processing and storage capabilities, unlike VANET.
The individuals who utilise the system, like as drivers, passengers, and even passers-by on the side of the highway, are known as users. A user's social profile can also help guideline systems.
In the Internet of Vehicles, vehicles are equipped with a variety of sensors that create a large amount of data, which is fed into a local compute unit and processed. Vehicles also include local storage for saving data for future use. Such data from each car in the vehicular cloud yields important data, which is subsequently transmitted on to each vehicle in question.
All sensors, gadgets, and machines placed in an IoT arrangement, such as a Smart Grid, can safely and effectively regulate power consumption, with humans serving as spectators. The difficulty of IoV is exacerbated by a number of reasons. Here are a few examples: Sensors (external/internal): On the outside of the automobile, security features like as cameras and parking sensors are installed, while within the car, automotive sensors such as brake sensors, low fuel, and tyre pressure sensors, among others, are installed.

Certain characteristics distinguish an IoV system from an IoT system. The following are the traits:

1) Mobility: Because a car is movable, it might lose connectivity or face wireless congestion at any time. Before an IoV system can be employed in real-world applications, these challenges must be solved.
2) The IoV system, which deals directly with user safety, places a high priority on user safety. Low overheads and latency are required, allowing messages to be transmitted in real time.
3) Hacker attacks: Cyber-attacks on a mobile or wireless system are always a possibility.

A. Internet of vehicles network model

The IOV model is made up of three distinct components. These let us visualise the IoV system as a whole network and understand its operations better. The three components of our IoV network model are as follows:
User.
Communication.
Cloud

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

1) The User

In an IoV system, clients who use IoV services are referred to as users. A user is the driver of the vehicle who receives traffic directions from the system. Other users include passengers in the automobile who are connected to IoV via their cellphones, computers, o r other smart devices. A user is someone who, for example, utilises IoV services to find out about cab availability in their neighbourhood. User services and services are divided into two categories:

a) Safety services

b) Commercial and entertainment services

Safety services are a primary priority for IoV because its main objective is to promote road safety and reduce the frequency of on-road incidents. IoV aims to offer a wide range of safety services, including:

Emergency call
Lane change warning
Auto breaking
Speed control
Real time traffic information
Car self-diagnostics
Car surveillance
Driving behavior analysis

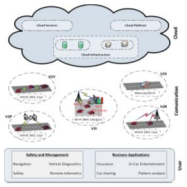


Figure 1 Internet of Vehicle network model

Everything from playing music based on the user's mood to carpooling is available as a commercial service in the IoV system. A list of some of these services is provided below.

Online music streaming
Advertisements
Local attractions, hotels, petrol pumps etc.
Connected drive
Fleet management
Car usage-based insurance
Toll payment

2) Communication is Essential

Because it allows all connected automobiles to share data and receive services from the internet cloud, communication is at the core of the IoV system. Integrating various communication technologies into one network is tough since numerous manufacturers create different devices and cars. It is incredibly difficult to link dissimilar technologies such as LTE and Wi-Fi. The Internet of Things (IoV) provides five different ways for its nodes to communicate with one another. The following are some instances of various communication styles..

Vehicle-to-Vehicle (V2V)
Vehicle-to-Infrastructure (V2I)
Vehicle-to-Roadside Units (V2R)
Vehicle-to-Sensors (V2S)
Vehicle-to-Personal Devices (V2T)

Wireless Access Technology is used to make all types of communication easier (WAT). In V2V, V2I, and V2R communication, IEEE WAVE, Wi-Fi, and 4G/LTE technologies are employed. V2T connection between autos and objects is enabled via in-car technology such as NFC and Car Play. In V2P communication, MOST/Wi-Fi is utilised to facilitate communication. The Internet of Things (IoV) is now commonly recognised as an umbrella term embracing numerous networks and communication technologies that function in a heterogeneous manner under one system...

The cloud represents the system's brain in our IoV paradigm, where all processing and analysis takes place and services are given to customers through multiple communication channels. A automobile is equipped with a bevy of sensors that continuously create large volumes of data. As a result, storing and processing data locally on each vehicle is no longer feasible, necessitating the use of cloud services. As indicated in the network model, the cloud is divided into three basic components:

Cloud Infrastructure

Cloud Services

Cloud Storage

Because the IoV system creates a large amount of data, cloud infrastructure provides storage space. Storage as a service, computation as a service, network as a service, and data as a service are just a few examples of cloud services. The cloud architecture also includes application servers for big data storage, processing, and analysis.

II. LITERATURE REVIEW

The current work by Contreras et al.2 is related to IoV in that the authors discuss IoV protocols, architectures, and standards but do not go into detail on security. Eiza and Ni3 discuss a more recent study in this area that focuses on the risks. The authors focused their investigation on cyber risks such as malware, auto mobile app-related risks, and on-board diagnostic (OBD) vulnerabilities, as well as possible remedies. Furthermore, while Zaidi and Rajarajan's work focused mostly on cryptographic-based countermeasures, their work is important for analyzing and comparing such cryptographic-based approaches. Azees et al.6 is a more recent and thorough study in this field.

In their study, Othmane et al.8 offered a taxonomy of security and privacy challenges for IoV. According to the authors, these aspects include data validity, device security, telecommunication connection secrecy, identity and responsibility, online privacy, and access control. The authors surveyed the recommended systems using their taxonomy. The authors of Parkinson et al.20 categorised and assessed the studies on protecting connected cars from cyber threats. Their main purpose was to identify and share knowledge gaps as well as future research goals in the field.

III. OBJECTIVES

1) We will discuss security issues, various security assaults, and solutions from an IoV perspective.

2) We also present an authentication mechanism for Vehicle-to-Infrastructure (V2I) communication in the Internet of Things, which allows for a secure connection between two nodes in the Internet of Things while also ensuring that no hostile node intrudes on the system.

3) In our solution, both the base station and the new vehicle entering the IoV network may use public key infrastructure to authenticate each other. cryptography

IV. METHODOLOGY

This section identifies the main network constituents and proposes an IoV network model. The building blocks of IoV in terms of network components better express the meaning and functions of IoV as a comprehensive heterogeneous network. The cloud, connection, and client are the three fundamental network characteristics of the Internet of Things (IoV) (see Fig. 2). The suggested IoV network model is depicted in Fig. 3 as a logical representation, replete with internal components for each element.

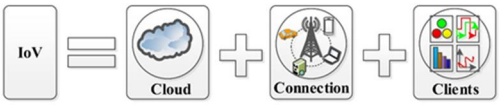


Figure 2 The three network elements of IoV.

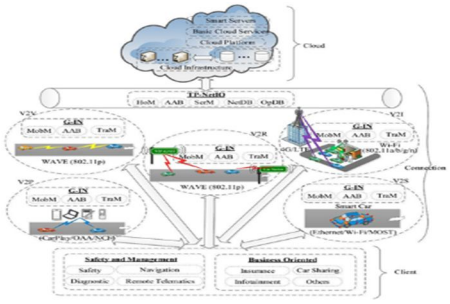


Figure 3 The network model of IoV with the three network elements.

The first element is the 'cloud,' which portrays IoV's brain. A number of services related to intelligent computing and processing are provided as fundamental cloud services. The platform on which the services are delivered is provided by cloud infrastructure. The second aspect of IoV is a trustworthy 'connection,' which is utilised to access cloud-based intelligent computing and processing services. A number of wireless access methods can be utilised to create a connection. As a result, client applications prioritise the use of wireless access methods. These components and their roles in IoV are discussed in further depth in the sub-sections that follow.

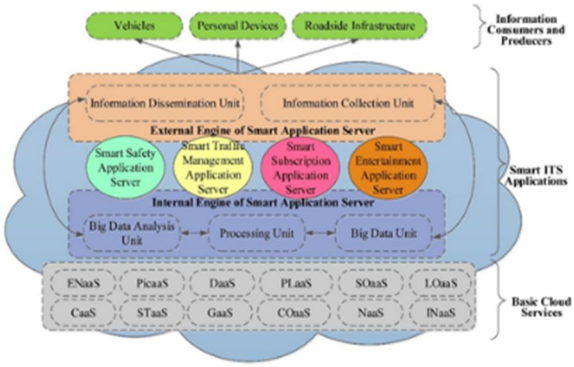


Figure 4 The role of cloud computing as three operation levels.

A. The Cloud

The volume of traffic-related data will drastically rise with the deployment of IoV. This is due to the fact that the vehicular network has been interconnected with numerous sorts of networks. A petabyte-scale information processing system would be required for a city's smart ITS to dynamically acquire, analyse, and disseminate real-time traffic information [4]. The cloud computing architecture is ideal for processing this type of data. A framework is proposed based on the concept of cloud-based application servers to emphasise the relevance of cloud computing as an element in IoV. (As seen in Fig. 4). The framework's three basic operational layers are basic cloud services, smart application servers, and information consumers and producers. The operational levels are cloud-based, with traffic data being uploaded, analysed, stored, and disseminated. The cornerstone for integrating cloud-based smart ITS application servers in the Internet of Things is basic cloud services. The three operational levels are explained below in terms of major components and responsibilities...

1) *Basic Cloud Services:* Some of the fundamental cloud services offered to smart traffic application servers include collaboration as a service (CaaS), storage as a service (STaaS), gateway as a service (GaaS), computing as a service (COaaS), network as a service (NaaS), and data as a service (DaaS). Smart ITS application servers are figured to be built and deployed on a cloud service that offers IoV apps with basic cloud services [7].
2) *Smart Its Application Servers:* Traffic safety, traffic management, service subscription, and entertainment are the four categories of IoV smart application servers [48]. Two types of processing engines are proposed for smart servers: internal and external engines. A big data unit, a big data processing unit, and a big data analysis unit make up the internal engine. The activities of all three units are carried out using the cloud platform's basic cloud services. An communication and information unit manages end-to-end service delivery to client applications, and an information collecting unit performs in-source data gathering.
3) *Information Consumer and Producer:* IoV smart devices such as autos, personal gadgets, and RSUs utilise the intelligent information provided by smart servers. The devices oversee gathering information from automobile traffic environments. The building of business models for organisations involved in insurance, automobile production and repair, and other Internet-based services is one of the most popular applications of data acquired by smart devices [9]. Cloud computing is one of the most important components in the design and development of IoV because of the purpose. The services supplied by the four smart application servers, which comprise smart safety, smart traffic control, smart enjoyment, and smart subscription, are at the heart of IoV [10]. The major task of cloud servers is to handle real-time huge traffic data and use artificial intelligence to make intelligent decisions for smart client applications [5]. The usage of a Real Time Operating System would be required to activate IoV services (RTOS). Google's plan to develop an Android-based RTOS for IoV with the help of the NOMA is also a viable solution.

B. The Connection

The 'connection' is used in the Internet of Automobiles to establish and maintain contact between the 'cloud' and automobiles in order to access cloud-based smart services. Because there are so many different types of networks to consider, such as VANETs, Wi-Fi, 3G/LTE, and satellite [13], interconnection among various networks is quite difficult. The primary components of a connection are the Third-Party Network Inter Operator (TPNIO) and the Internetworking Gateway (GIN). TPNIO is in charge of connection management, whereas GIN is in charge of the actual connection. The parts that follow go through both elements, as well as a preference for Wireless Access Technologies (WAT) for connection.

1) *Third Party Network Inter Operator (TPNIO):* In IoV, the need for direct Service Level Agreement (SLA) between network providers is reduced as a result of TPNIO [4]. The direct SLA is a challenging restriction to overcome in any heterogeneous network. TPNIO allows for seamless roaming without jeopardising the quality or security of network operator services. The five key components recommended for TPNIO are Global Handoff Manager (GHM), Global Authentication, Authorization, and Billing (GAAB), Service Management (SM), Network Database (NDB), and Operator Database (ODB). The logical connection between these pieces is depicted in Figure 5. The TPNIO components' operational duties are listed below.:

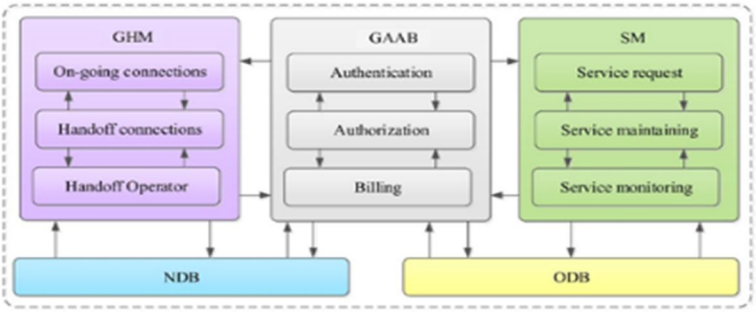


Figure 5 The logical relationship of the components of TPNIO.

2) *Global Handoff Manager (GHM):* The global handoff manager is responsible for smoothly transferring ongoing communications between any two IoV network providers. It's a global handoff manager that can handle IoV handoffs between two operators from various networks. GHM development is a hot issue in IoV, and efficient integration of heterogeneous network handoff modules might be viewed as a general strategy for achieving GHM [5]. • Global Scale Authentication, Authorization, and Billing (GAAB) The GAAB oversees authenticating a vehicle's credentials and granting network connection. GAAB is also in charge of usage-based pricing for network services. Because vehicles may belong to operators of many types of networks, GAAB's operations are intricate and difficult. As a result, the third-party notion is viewed as a TPNIO that aids GAAB with verification and pricing. • Management of Customer Service (SM) SM oversees delivering and monitoring vehicle service quality. It is based on a multi-network operator agreement on service quality. Through the implementation of a service quality agreement, it assists in the provision of guaranteed services to vehicles. To sustain service quality across diverse types of systems, continuous observation is essential. The concept of service quality rating might be utilised for quality control. • Network-wide database (NDB) NDB is a database of IoV-registered networks, as well as the technologies and protocols that they use. The database is used to identify a network and establish communications between different types of network operators. • Database of Operators (ODB) (ODB) The Operator Database (ODB) is a registry of registered operators for various IoV network types. There is no need for a direct SLA between these operators and TPNIO because they have a SLA with TPNIO. To maintain consistent service quality, the database is utilised to identify operators and their service level agreements (SLAs)..

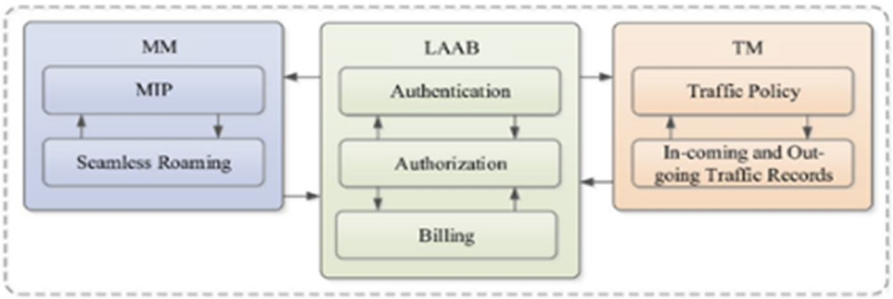


Figure 6 The logical relationship of the components of GIN.

3) *Gateway Of Internetworking (GIN):* Because of the various network conditions, several wireless access techniques are employed to build connections in IoV. The five types of vehicular networks in IoV are V2V, V2R, V2I, V2P, and V2S. Vehicle networks are represented using a variety of wireless access techniques (see Fig. 5). WAVE is the symbol for vehicle-to-vehicle and vehicle-to-remote communications in V2V and V2R networks. Vehicle-to-vehicle communication via Wi-Fi or 4G/LTE is referred to as V2I [6]. The V2P network refers to vehicle-to-vehicle communications that use Apple's CarPlay or Android's OAA (Near Field Communication) technology (NFC). The V2S network represents in-vehicle sensor communications over Ethernet, Wi-Fi, or Media Oriented System Transport (MOST) [7]. Client applications connect to these networks via the Gateway of Internetworking (GIN) to access the services of smart-based servers. Each vehicle network has its own GIN, which collaborates with the TPNIO to establish and maintain a connection. The three major components of GIN that have been mentioned are Mobility Management (MM), Local Authentication, Authorization, and Billing (LAAB), and Traffic Management (TM). The logical connection between these pieces is depicted in Figure 6. The following are the operational duties of these components:

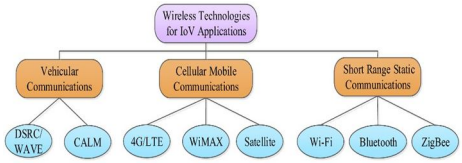


Figure 7 The classification of WAT for the applications of IoV.

V. SYSTEM ARCHITECTURE

Because the Internet of Things has such a direct influence on the lives of its users, security is a major concern. If the IoV system is breached, it might jeopardise safety by allowing hackers to take direct control of vehicles, perhaps leading in traffic accidents. There have been incidents in the past that have highlighted the significance of connected vehicle security issues. A group of hackers was able to remotely take control of a Jeep Cherokee's digital system, including the air conditioning and radio. They may also switch off the vehicle's engine. Tencent, a Chinese firm, was able to get control of a Tesla vehicle using its Wi-Fi connection, allowing them to operate the vehicle's brakes remotely. As the examples above demonstrate, security is a primary consideration in the Internet of Things. After that, we'll go through some of the most common hacking attacks in the IoV system.[16]

A. Security fundamentals

In most iov safety-related applications, messages are propagated, and they must be transmitted fast. A private and encrypted communication should not expose any personal information about the user, infringing on their right to privacy. There are four important security basics that must be adhered to in Iov..

1) *User Authenticity:* The source of a communication might be a valid or malicious node. The first step in improving the IoV system's security is to detect whether the node is genuine or malicious. The system should be able to distinguish between legitimate and malicious nodes and take action against the latter.
2) *User Anonymity:* Any information regarding a communication's origin should be deleted. To put it another way, the message's content should not reveal the sender's physical identify. The message sender's identity must be secured by the IoV system.
3) *User Integrity:* The data that the receiver receives should be identical to the data that the sender sends. The system should be able to confirm that the communication was not tampered with while in transit.
4) *Low Overhead:* The majority of IoV communications are time sensitive. If they do not reach the intended recipient within a specified length of time, they are worthless. As a result, while focusing on security, the IoV system must guarantee that overhead is not increased to the point that broadcasting takes longer and the system is no longer viable by the time it reaches its destination.

B. Types of attacks

A STRIDE model is proposed for information security, which categorizes security threats in sex categories:
Spoofing
Tampering
Repudiation
Information disclosure

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Denial of Service
Elevation of privileges

The above-mentioned dangers apply to the IoV system, which may be attacked using a number of methods such as network jamming, eavesdropping, infiltration, and so on. These attacks have the potential to harm the IoV system, compromising its stability and resilience, or, in the worst-case scenario, putting it to a halt and causing accidents. Some of the elements of the IoV system that make it vulnerable to such assaults are as follows:

Dynamic topology
Bandwidth limitation
Mobility of nodes
Non-uniform distribution
Large network
Nature of communication (wireless)

Now, let us discuss some of the common types of attacks in IoV.

1) *User Authenticity Attacks:* Sybil attack Sybil is based on a real-life case study of a lady with multiple personality disorder. In a Sybil attack, a single network node claims many identities. A single node with several identities may control multiple nodes at the same time in a wireless network, wreaking havoc on the system. Cars are regularly linked and withdrawn from the network due to the dynamic nature of IoV, offering hackers an opportunity to exploit the system. Masquerading attack.: Masquerading is an information security attack in which many nodes in an IoV system share the same ID. The attacker acquires a genuine ID before using it to gain unauthorised access to the system. The wormhole has launched an attack. When a hacker obtains access to a network, he or she uses it to steal packets from one site and send them to another. As a result, data intended for one node winds up in another, putting security at risk.
2) *Data availability Attacks:* Denial of Service.: In a denial of service (DoS) assault, the attacker tries to overload the system by flooding the network with redundant messages. As a result, legitimate requests are deleted from the network, affecting services.
3) *Channel Interference:* To bring an IoV system down, this hack takes advantage of a network's limited capacity and transmission power. The impact of such an attack is dictated by the targeted node. In an IoV system, a hacked automobile node will have a higher impact than a compromised base station or roadside device.
4) *Data Authenticity Attacks:* The phrase "data authenticity" refers to the fact that data from the source node corresponds to data received at the sink node. After gaining access to the system, the hacker collects packets being transferred, modifies them, and then retransmits them to the original address. Data authenticity threats may be divided into four categories:

Illusion attack
Camouflage attack
Replay attack
Message tampering

To secure communication between two entities in our IoV system, we need a robust and secure mechanism that should be able to withstand such variety of attacks.

VI. RESULTS

In this part, we present a mutual V2I authentication approach for autos connected to an IoV system. The base station authenticates an automobile while it is on the road and within range of one. Mutual authentication is the name given to the system since the vehicle does its own authentication via the base station to ensure it is not a forgery.

A. Authentication Mechanism

There are three types of authentication techniques that may be used in IoV scenarios. Additionally, a digital signature or the ID of a vehicle node can be used for validation, albeit this threatens the user's privacy.

B. RSU Based Authentication

RSU-based authentication services are mostly used in fixed infrastructure. For each vehicle, RSU generates a temporary anonymous certificate with a unique anonymous ID that is used for future V2V communication in the IoV network. A Trust Authority (TA) keeps track of these certificates and has the authority to remove them from the IoV system if a node is found to be malicious in the future. This strategy's shortcoming is the continual need for permanent infrastructure.

C. Pseudonym Based Authentication

When a pseudonym is used for authentication. Using this method, each vehicle in the network receives a list of public/private key pairs with PKI certificates. For V2V communication, each pair is given a unique pseudo-ID. The method's drawback is that it can only be used in a small-scale system. However, as the system gets more and more vehicles, the waiting list lengthens, and storage requirements expand.

D. Group Based Authentication

A vehicle does not send a message using its own ID while utilising group-based authentication. Cars are instead sorted into groups based on some characteristic, such as geography, and each group is assigned a unique ID. The IDs of the automobiles in the group are only accessible to the group manager, which might be beneficial if a vehicle is proven to be hazardous and must be removed from the system.

E. IoV System Overview

Figure 8 depicts a high-level perspective of our proposed IoV system. We see autos on the road and base stations evenly distributed along the route in this scenario. Several base stations are clustered together in the same region or area. In order for automobiles to connect to the network, many sensors and devices are deployed. A backbone network connects base stations to the internet. A local vehicular cloud is formed by vehicles in a region that can communicate with one another. The internet cloud, which includes cloud services, is at the top of the heap. A new vehicle must first complete mutual authentication with a nearby base station before joining the IoV system. When an automobile wishes to join the network, it sends a signal.

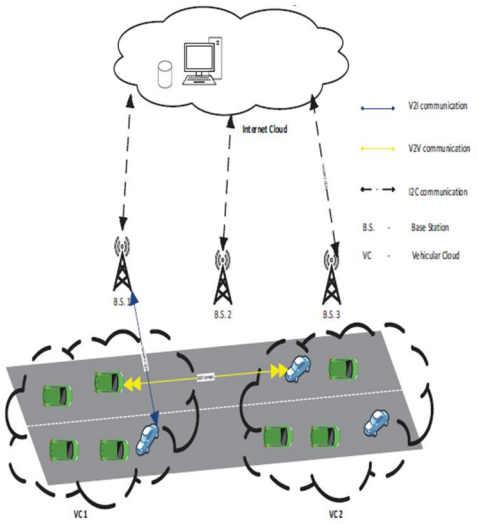
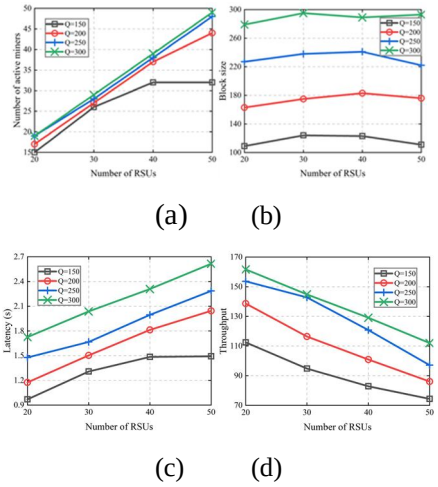


Figure 8 Internet of vehicle System overview

= To demonstrate the performance of our suggested techniques, we run massive simulations on a 64-bit Windows 10 PC with 16.0 GB RAM, an Intel(R) Core (TM) i7- 8700 CPU running at 3.20 GHz, and an NVIDIA GeForce GTX 1050.

Consider a base station with ten subchannels, each with a frequency of 2 MHz, an RSU frequency of 10-30 GHz, and a transmit power of 100 mW for each vehicle. Due to time constraint of transactions in the pool when Q (i.e., the value of transactions in the contract pool) increases, the V2I-enabled method favors to pick more effective members to gang up to such an optimum solution PIR and select more transaction records to form a block when the quantity of RSUs is fixed, as shown in Figures 9(a) and 9(b). When is fixed, the no of miners grows in lockstep with the number of RSUs, but the block size changes only little

In Figure 9 (c), the blockchain latency grows as Q grows for a certain number of RSUs, since more working miners and greater block sizes result in a larger delay. When Q is fixed, the blockchain latency requires many RSUs grows, and the no of miners grows, resulting in a bigger delay. When the number of RSUs is fixed, it can be shown in Figure 9(d) that the blockchain throughput grows as Q grows. The reason for this is because, while a greater Q produces more latency, the massive block size raises the block size ratio. and a considerable reduction in blockchain latency Because the block size fluctuates little while Q is constant, the blockchain throughput drops as the number of RSUs grows. Increasing latency, on the other hand, reduces blockchain throughput.



(a) (b)

(c) (d)

Figure 9. Performance evaluations in terms of the number of RSUs: (a) Number of active miners, (b) Block size, (c) Latency, and (d) Throughput.

The uploading time of NOMA (Non-Orthogonal Multiple Access) is always shorter than that of Orthogonal Frequency Division Multiplexing (OFDM) as the number of CHs rises, as shown in Figure 10. This is since with OFDM, having a lot of CHs produces a lot of queuing latency. Because each subchannel in NOMA may serve many CHs, the queuing latency is greatly reduced.

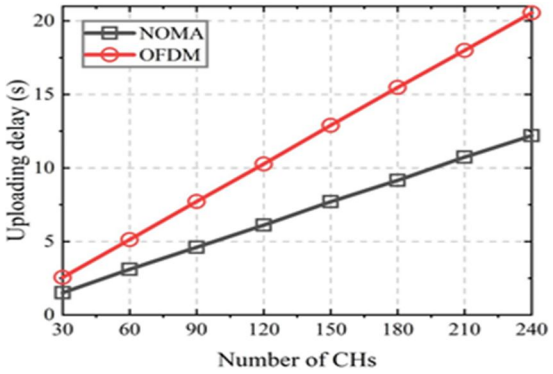


Figure 10. Uploading delay in BS based on NOMA and OFDM, respectively.

F. Assumptions

For our suggested IoV model, we will assume the following assumptions.

1) Each car communicates with its neighbors via DSRC.
2) The internet serves as the backbone network for all base stations.
3) A reputable government entity, such as the RTO, issues each vehicle with a unique certificate.
4) For IoV systems, there is a PKI architecture.

G. Proposed authentication scheme

A vehicle authenticates itself with the base station when it enters the network. The BSi certificate is requested by Vehicle Vi from the base station. After the verification is complete, Vehicle Vi sends a message. This email contains Vi's certificate, which is a self-generated symmetric key symmetric key signature. After then, the transmission is encrypted with BSi's ID, which employs an identity-based encryption approach. The encrypted message is then forwarded to the BSi base station. BSi decrypts the message and retrieves the contents using the NOMA and OFDM then verifies the vehicle's certificate using the RTO's public key. It then uses Vi's public key to verify the signature on the symmetric key. The vehicle is allowed authorised access to the IoV system if the symmetric key SKBSiVi is authenticated. BSi stores a mapped copy of Vi's public cryptographic SKBSiVi.to Vi's certification in the database. This copy may be required if the node is hacked or turns malicious in the future. The mapped copy might be used to remove Vi from the IoV system in this case.

H. Algorithm

IoV is a new research field with promising commercial prospects. Many car manufacturers have implemented IoV
IF Verification (Certificate (BSi)) = Valid,
Create Message MVi ,
where MVi includes Certificate (Vi),
Symmetric key SKViBSi and SignSK ;
MVi = {Certificate (Vi), SKViBSi and SignSK};
Encrypt MVi using ID(Vi);
Verify if Certificate (Vi) = Valid, using Public key (RTO).
key (RTO)
If Certificate (Vi) = Verified,
Verify SignSK using public key (Vi);
If Signsk = verified,
Verification successful.
Vi enters Range (BSi); Send Certificate (BSi) to Vi

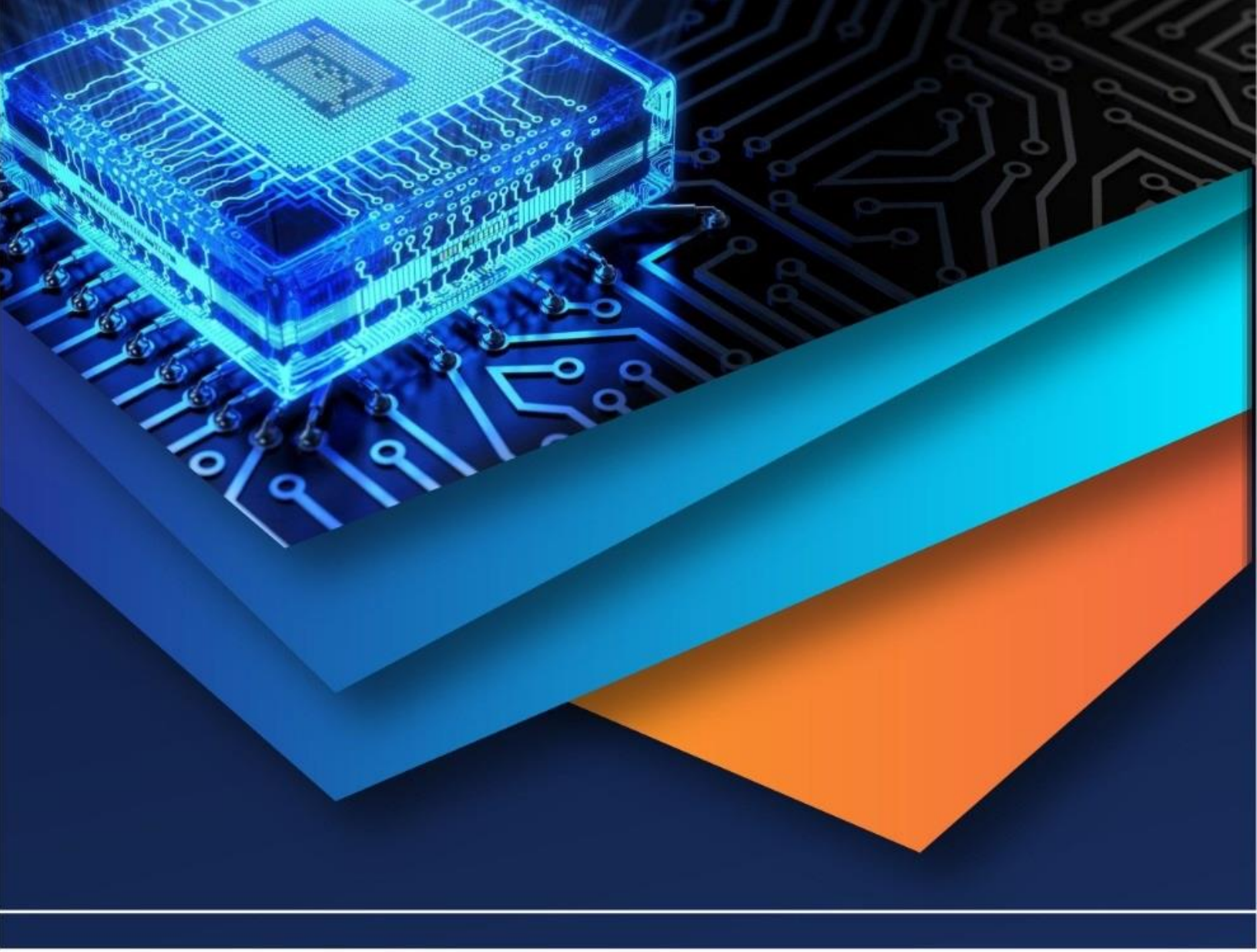
VII. CONCLUSIONS

IoV is a relatively new field of research with a lot of potential in terms of economics. To provide interactive services to their consumers, many automotive manufacturers have implemented IoV principles into their automobiles. Some major firms, such as Tesla, have designed their automobiles to operate almost entirely autonomously, with no human intervention. These options appear to be thrilling, but they are not without security issues.

The security and latency challenges of blockchain-enabled crowdsensing for 5G IoVs are the topic of this study. First, we formulate the optimization issues in our created system. A DRL-enabled method is presented to optimize the blockchain by selecting appropriate active miners and transactions in order to maximize safety and decrease latency. The NOMA subchannels are then allocated using a two-sided matching-based technique to minimizing the maximum uploading time. In comparison to OFDM, performance measurements show that our approach can strike a reasonable balance between blockchain latency and safety and significantly minimize uploading time. Our system's examination shows that it can safeguard user privacy, provide data security and integrity, withstand typical threats, and efficiently identify attackers.

REFERENCES

[1] La VH and Cavalli AR. Security attacks and solutions in vehicular ad hoc networks: a survey. IJANS 2014; 4:1–20.
[2] Contreras J, Zeadally S and Guerrero-Ibanez JA. Internet of vehicles: architecture, protocols, and security. IEEE Internet Things J 2017; 5: 3701–3709.
[3] Eiza MH and Ni Q. Driving with sharks: rethinking connected vehicles with vehicle cybersecurity. IEEE Vehic Tech Magazine 2017; 12: 45–51.
[4] Hamida EB, Noura H and Znaidi W. Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures. Electronics 2015; 4: 380–423.
[5] Zaidi K and Rajarajan M. Vehicular Internet: security & privacy challenges and opportunities. Future Internet 2015; 7: 257–275.
[6] Azees M, Vijayakumar P and Deborah LJ. A comprehensive survey on security services in vehicular ad-hoc networks. IET Intel Trans Syst 2016; 10: 379–388.
[7] Sakiz F and Sen S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks 2017; 61: 33–50.
[8] Othmane LB, Weffers H, Mohamad MM, et al. A survey of security and privacy in connected vehicles. In: Benhaddou D and Al-Fuqaha A (eds) Wireless sensor and mobile ad-hoc networks. London: Springer, 2015, pp.217–247.
[9] Butt TA, Iqbal R, Shah SC, et al. Social Internet of vehicles: architecture and enabling. Comp Electr Eng 2018; 69: 68–84.
[10] Lu Z, Liu W, Wang Q, et al. A privacy-preserving trust model based on blockchain for VANETs. IEEE Access 2018; 6: 45655–45664.
[11] Arif M and Ahmad S. Security issues in vehicular ad hoc network: a critical survey. In: Shakhovska N (ed.) Advances in intelligent systems and computing, vol. 624, pp.527–536. Singapore: Springer.
[12] Chauhan KK, Kumar S and Kumar S. The design of a secure key management system in vehicular ad hoc networks. In: 2017 conference on information and communication technology (CICT), Gwalior, India, 3–5 November 2017, pp.1–6. New York: IEEE.
[13] Dua A, Kumar N and Bawa S. A systematic review on routing protocols for vehicular ad hoc networks. Vehic Comm 1: 33–52.
[14] Reger L. Addressing the security of the connected car. NXP blog, 2014, https://blog.nxp.com/automotive/ addressing-the-security-of-the-connected-car
[15] Hackers demonstrate how to take control of cars. 20 jobs that will be replaced by technology. https://www.msn. com/en-gb/video/health and fitness/hackers-demonstrate how- to-take-control-of-cars/vi-BBlsiab (accessed 1 September 2018)
[16] Noori, Roman. (2021). Network Security Attacks and Countermeasures on Layer 2 and Layer 3 Network Devices. International Journal for Research in Applied Science and Engineering Technology. 9. 1173-1185. 10.22214/ijraset.2021.33462.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY