Original Article

Blockchain-Based Internet of Things Security and Reliability via SDN-Enabled 5G-VANETs

Dr N Srikanth Reddy[1], Leopoldo, Choque-Flores[2], Praveen Ponia[3], Mukta Sandhu[4], Dr. Yogesh Mahajan[5], Dr Chanakya Kumar[6]

[1]Assistant Professor, SOM, Presidency University, Bangalore, srikanthreddyn@presidencyuniversity.in

[2]Universidad Cesar Vallejo, Lchoquef@ucv.edu.pe

[3]Ibri College of Applied Science, Ibri, Oman, Praveen.ibr@cas.edu.om

[4]Shri Vishwakrma Skill University, Palwal, India, Mukta.sandhu@gmail.com

[5]Assistant Professor, Department MBA, Symbiosis Centre for Management and Human Resource Development, Symbiosis International University, Symbiosis Infotech Campus, Plot No. 15, Rajiv Gandhi Infotech Park, MIDC, Hinjewadi, Pune, Maharashtra, yogesh_mahajan@scmhrd.edu

[6]Associate Professor, Indira School of Business Studies PGDM, Pune, chanakya.kumar@indiraisbs.ac.in

Corresponding Email: srikanthreddyn@presidencyuniversity.in

DOI: 10.47750/pnr.2022.13.S09.057

Abstract

New opportunities for vehicular Internet of Things (IoT) services using current and modern rational transportation system, along with newer challenges for vehicular ad-hoc networks (VANETs). Along with improved network performance, a workable and trustworthy security system is required to handle trust management while maintaining user privacy. A key technology for extremely dependable, low-latency wireless communication services is the newly developed 5G mobile communication system. Additionally, the software-defined network (SDN) design allows for network control and worldwide data collection within the 5G-VANET. As a result, real-time IoT services for monitoring and reporting on transportation can be effectively supported. Both open the door for a cutting-edge automobile security system.

This paper investigates the security and privacy issue in the transportation system and the vehicular IoT environment in SDN-enabled 5G-VANET. A blockchain-based security framework is created to support the vehicular IoT services, such as real-time cloud-based video reporting and trust management on vehicular messaging, due to the decentralised and immutable nature of blockchain. The 5G-VANET model with SDN support and the framework's scheduling processes are specifically illustrated in this study. The outcomes of the numerical simulation also demonstrate that it is possible to detect malicious vehicular nodes or communications while maintaining acceptable overhead and network performance impacts in large-scale scenarios. We show how our design considerably ensures a secure and reliable vehicle IoT environment with user privacy preserved through case studies and theoretical analysis.

Keywords: Blockchain, 5G-VANET, IoT, security and privacy, SDN, trust.

I. INTRODUCTION

A. BACKGROUND OF THE VEHICULAR IOT IN SDN-ENABLED 5G-VANET

The current intelligent transportation system needs vehicle ad hoc networks to manage new opportunities and constraints (VANETs). To keep people's trust and protect their privacy, a reliable and effective security solution is needed. The network will also operate more effectively. Cellular services are now more dependable and appropriate thanks to new 5G mobile communication technology. [1,2,3] A unified platform is used by the 5G network's user-centric networking philosophy to satisfy service requirements [4]. As a result of the development of millimetre-wave [5] and huge multiple-input multiple-output (MIMO) arrays [6,] the newly assigned spectrum enables new air interfaces with improved spectral and energy efficiency. A strategy that makes use of both already-existing infrastructure and the anticipated access methods is also made possible by 5G. Users now have access to a greater variety of services. [7]

The 5G-VANET is able to run its network and collect data on a global scale because it uses software-defined network (SDN) architecture. IoT services provide real-time reporting and tracking of shipments. Both give customers access to cutting-edge techniques for making cars safer. [8] On a 5G-VANET, which is made possible by SDN, this study explores security and privacy in IoT and transportation systems (IoT). A blockchain-based security architecture has been developed to enable

automotive IoT services, including real-time cloud-based video reporting and trust management on vehicular communications. Blockchain is decentralized and cannot be altered. [4]

Some preliminary studies have looked into the integration of SDN with VANET. For instance, SDN offers an adaptive edge computing solution with regressive admission control and fuzzy weighted queueing to monitor and respond to changes in quality of service (QoS) in automotive networks [9]. In order to encourage the transmission of data, a cooperative data scheduling scheme that is integrated at road side units (RSUs) has also been created [10]. This scheme takes advantage of the synergy between vehicle-to-network (V2N) and vehicle-to-vehicle (V2V) communications. SDN can therefore greatly improve IoT services in a vehicle setting.

This paper discusses the 5G-VANET model that supports SDN and the scheduling algorithm for the blockchain-based architecture. The outcomes of the numerical simulation also demonstrate the existence of malicious vehicle nodes or communications, the accuracy of the overhead, and the impact of these factors on the network's performance under heavy load. We demonstrate how our solution offers vehicles a dependable and secure Internet of Things (IoT) environment while preserving user privacy through case studies and theoretical research.

B. SECURITY AND TRUST CONCERNS IN THE VEHICULAR IOT ENVIRONMENT

Security for IoT on vehicles has grown in importance and received more attention. Because of the advancements in on-board sensing, processing, and communication capabilities, vehicles are becoming more autonomous. Vehicle networks are thus able to report information to the information operation or management centre and share enormous volumes of messages (such as high-definition films) among cars. Transmission of emergency data and messages enables new IoT services [11]. Furthermore, these warnings improve the administration's awareness of traffic problems, which improves the transportation system's safety.

Conversely, it is challenging for cars in a VANET to collaborate and build confidence because they are effectively strangers to one another. The VANET's tremendous mobility and diversity make it challenging to rule out malicious vehicles or incorrect behavior in complex situations. Rogue automobile nodes' dissemination of false information puts the entire transportation system at risk. When a route is congested or has recently been in an accident, they can claim it is clear. Only dependable machinery and vehicles must send service connections in a secure IoT environment created by the VANET network. These communications need to be precise, trustworthy, and unchangeable. No one wants their personal information to be made public. Thus, each step of the message collection and delivery process must protect user privacy. Future development of car IoT services [12] will also need collaborative intelligence, spatiotemporal sensitivity, and trust without a centralized authority.

A blockchain-based architecture is viewed as a workable choice in this essay. This architecture allows cars to have Internet of Things features like cloud-based live video streaming and secure texting between vehicles. An authorization is required for a vehicle to access the 5G-VANET. The legitimacy of the vehicle is confirmed by authorities who supply authentic private keys and public key certificates. If the car is found to be legal, it will be allowed to keep going while streaming real-time footage of the road. The method separates vehicle authentication data from the user identifying data to maintain user anonymity. The user cannot identify the driver or the other passengers. One vehicle transmits data on traffic and road conditions every minute. Authorities will examine all pertinent camera footage and traffic alerts after a collision.

The following list of the most important contributions:

We are initially creating a blockchain-based system for managing the trust. For the car to share information about road conditions with other vehicles, the traffic condition identifier must also be uploaded along with the video. The accuracy of an automobile's traffic broadcasts will be checked by other vehicles to prevent an attacked car from causing congestion by broadcasting false or malicious information. The distance between the vehicle that scores a tag and the vehicle that sends it through RSU is used to calculate a tag's trust value and pack it into blocks.

This method uses proof-of-work and proof-of-stake to repeat elections (2). Only accurate traffic reports will be kept, while inaccurate ones will be deleted. Malevolent cars, or automobiles that disturb traffic order by providing a significant volume of false road information, will be temporarily outlawed once their source is identified as the system. Law-abiding drivers' safety and anonymity are of vital significance.

A semi-centralized system to govern the integrity of video and road conditions is constructed and tested using centralized authentication and distributed trust management based on blockchain technology—theoretical analysis and numerical proof back up the framework's genius and scalability.

The report is divided into the following sections: The second sentence introduces the pertinent work. The third section provides a general explanation of the suggested system model. The security features of a blockchain network are covered in Chapter IV. The test results and a risk assessment are discussed in Section V. Section VI is the sixth and last section of the essay.

II. RELATED WORK

Videoconferencing and similar services are required for vehicle networks. [13]. Real-time traffic footage may now be sent and stored thanks to VANET's integration of 5G. [14]. Automotive systems and industrial mobile computers have acknowledged the advantages of IoT cloud services. [15]. It could be challenging to establish the facts after a traffic collision from a forensic and investigative standpoint due to the numerous blind spots of roadside CCTV cameras. All cars connected to the network must take part in road monitoring, multi-angle real-time monitoring, and road condition reporting to guarantee data security in a VANET. The paper suggests a semi-decentralized strategy for upholding trust after examining the advantages and disadvantages of centralized, decentralized, and semi-decentralized systems.

CENTRALIZED TRUST MANAGEMENT SYSTEM

Suppose every vehicle in the VANET connects to the camera system and takes on the role of road security manager and supervisor. In that case, it will be much simpler to investigate traffic accidents. This would greatly simplify the investigation of automobile accidents. Furthermore, it reduces the serious safety problems that can arise when someone is watching, which is a huge advantage. The [18] team is now working on a cloud-based video gathering and analysis platform called Kestrel. It accomplishes this while gathering video data by utilizing comparatively affordable visual qualities. It allows for constant surveillance within a video network made up of stationary and moving cameras, which helps overcome confusing paths. It also connects the visual features of each vehicle. An Internet of Things that is large-scale and employs numerous hops can use a backpressure scheduling technique, which is also demonstrated in reference [19].

It will be much simpler to follow the information on the present condition of the roads if a search engine bases its results on the user's identification; however, this may jeopardize the privacy of video producers. Finding volunteers to send in the film will be challenging if there isn't already a well-established mechanism to handle the situation. People who use their vehicles as witnesses might not be aware that the videos recorded inside them can be used as evidence. Therefore, it is imperative to develop a method of gathering traffic data that considers people's privacy concerns while also allowing moving vehicles to send videos and data on the roadways. [13]. The revolutionary approach provided by the 17.1 can be used to record and distribute videos while you're on the go. This article describes how new network technologies affect wireless broadcasting in various 5G networks and suggests a novel system model for 5G-VANET. Thanks to technology improvements that verify the vehicle and encrypt the data, cars can now record and share road footage. It also shields the identity of the car involved in the event and the privacy of any video footage.

DISTRIBUTED TRUST MANAGEMENT SYSTEM

Distributed system management enables hiding the route of a vehicle. View-map is an autonomous public service that enables anyone to add anonymous DashCam videos, according to Reference [13]. A dashCam is a camera that can be mounted on a vehicle and records the inside and outside of the vehicle. Each movie in [13] is displayed as a view profile to safeguard users' privacy (VP). In the system's retrieval, validation, and reward procedures, Anonymous VP takes the place of its owner. Actual users of the system assess their dependability. Users can obtain virtual cash through distributed trust management without being aware of its source. This safeguards the privacy of the travel routes of video vehicles. A trust management system can be used to monitor road conditions continuously as well as to record videos that can be used as evidence in car accidents. [20] suggests that a blockchain-based system may be used to assess the accuracy of traffic information provided by moving automobiles. Using this technique, neighboring autos can assess the correctness of the route information given by moving vehicles. Each RSU tries to add information to a block and send it to the blockchain. The system allows vehicle-to-vehicle communication and mutual validation to ensure that vehicles reliably report traffic conditions. This method, however, makes it impossible to determine whether the vehicle's name is accurate. Furthermore, road data may be hidden or altered if an RSU is intentionally

attacked, such as by someone modifying the collected data. This will lead to the acquisition of false information about the state of the roads.

A BLOCKCHAIN-BASED DECENTRALIZED TRUST MANAGEMENT SYSTEM

Centralized trust management is advantageous for gathering information about traffic circumstances and conducting follow-up investigations while maintaining user privacy. On the other hand, if dishonest vehicles disseminate incorrect information on the highways, it might be hazardous. Moreover, by analyzing the communication between cars, distributed trust management may verify data integrity like traffic reports and other information. The VANET, however, cannot verify that the car in question is who it purports to be because vehicles connected to the VANET do not go through a single identification process.

This study recommends a blockchain-based, semi-decentralized trust management system. It collects protected videos, sends them to the cloud, and records verified traffic data in the blockchain. As the blockchain election node, the RSU node is advised because of its ability to reach consensus quickly and reliably. The integrity of the blockchain is maintained even if only one RSU node is attacked. No matter how hard the attacker RSU tries, it will never be able to record bogus data on the blockchain covertly. Only authorized vehicles can access the VANET in this configuration. The system will then allow users who have requested key pairs to switch recorded movies and route data. Each communication transmitted by a vehicle must be digitally authenticated using the vehicle's specific digital signature to prevent the transmission of fake or fraudulent traffic data. Then, other vehicles verify that the said road conditions are accurate. Any automobiles VANET determines to be potentially harmful will be put on a blocklist and reported to the police. The method safeguards the integrity of the information sources while preserving user privacy.

SYSTEM MODEL

OVERVIEW OF THE SDN-ENABLED 5G-VANET ARCHITECTURE

An SDN-enabled 5G-VANET system model and a HetNet architecture are shown in Figures 1 and 2, respectively.

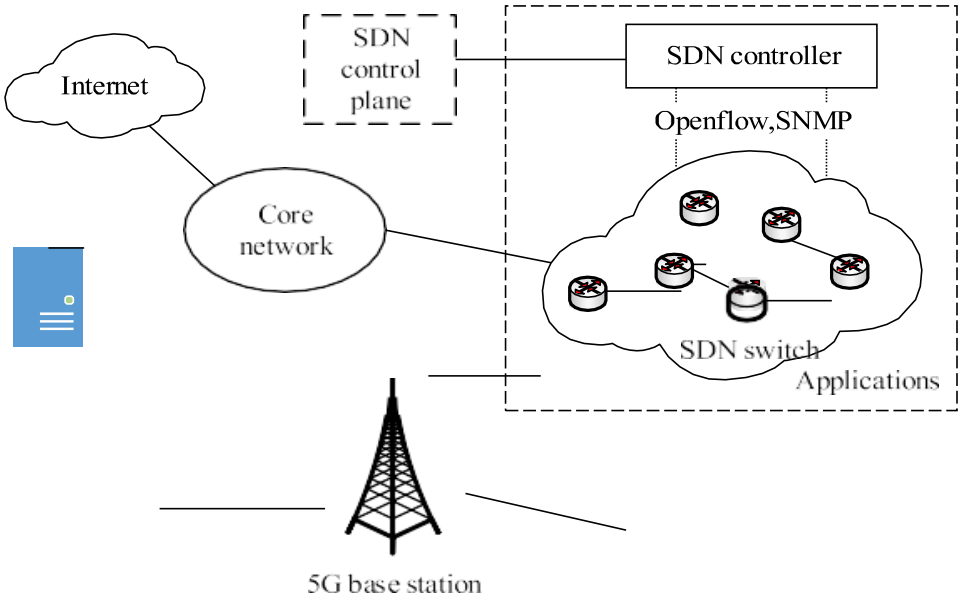

FIGURE 1. Integrating SDN into the 5G-VANET system

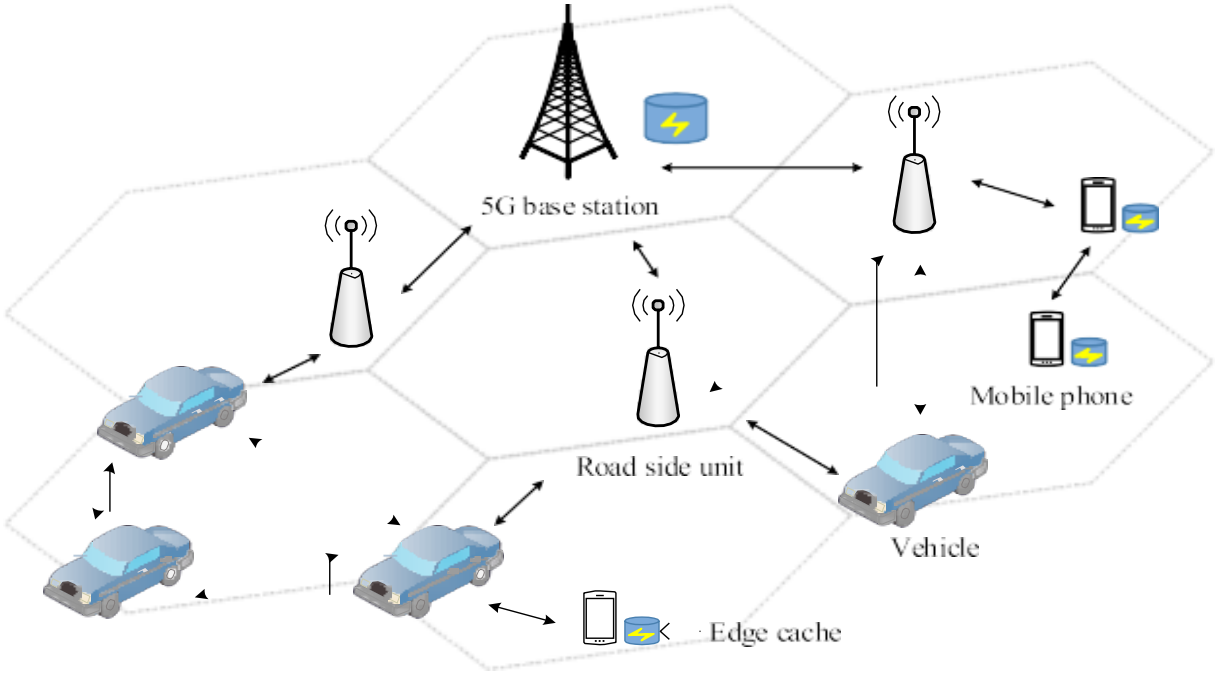

FIGURE 2. Radio Access Network in the 5G-VANET system.

This architecture includes numerous node types, such as remote subscriber units (RSUs), 5G base stations (gNBs), and units mounted on moving vehicles (OBUs). RSUs are intended to function as 802.11p wireless access points (APs), enabling communication amongst OBUs within the service region. The Department of Motor Vehicles and the Trustworthy Authority (TA) are also a part of the core network; both are linked to the Internet by the video cloud server, which stores video reports (DMV). The 802.11p network's limitations in terms of low capacity, poor scalability, and intermittent connectivity are why the VANET depends on gNBs to give people high-speed wireless Internet access. The vehicle-to-vehicle (V2V) communication that enables data sharing between vehicles is also considered in this design. As a result, a vehicle can use other vehicles as relays if it is outside or very close to the edge of the RSU or gNB service region.

High-capacity fiber optic backhaul cables and the OpenFlow protocol govern all Russ and gNBs by a centralized SDN controller. This is done to manage the 5G-VANET globally using a set of uniform policies. All vehicles, RSUs, and gNBs are part of the SDN data plane. The data and control planes are not in contact with one another. The SDN controller moves network control functionality from the infrastructure to the control layer. Applications for automobiles that organize and manage traffic can be set up using the SDN controller. Global policies like mobility, user authentication, and traffic management are under the jurisdiction of the SDN controller. The controller's policies are carried out in the data plane. It is possible to see the entire service area and utilize programmable applications to conduct operations across several domains by separating the data plane from the control plane. One way the HetNet architecture encourages communication and information sharing is through this. The infrastructure can update the general network policies on its own or request updates from the network administrator after a predetermined time.

NETWORK OF AUTOMOTIVE BLOCKCHAINS

Traditional, centrally controlled network architecture does not adequately safeguard user privacy and is frequently open to intrusion. However, due to its decentralized structure, blockchain has been hailed as a game-changing method for data and privacy protection. A decentralized database known as a blockchain keeps track of an expanding number of linked blocks. Without a central bank, distributed node trading keeps a consistent record. Bitcoin, the first cryptocurrency established by Satoshi Nakamoto, is largely credited for revolutionizing the financial sector. A peer-to-peer network manages each node, identified by a public key (PK). Nodes communicate with one another through transactions, which are broadcast to the entire network and encrypted by PKs. Any node on the blockchain can verify a transaction by comparing the signer's signature to their private key (PK).

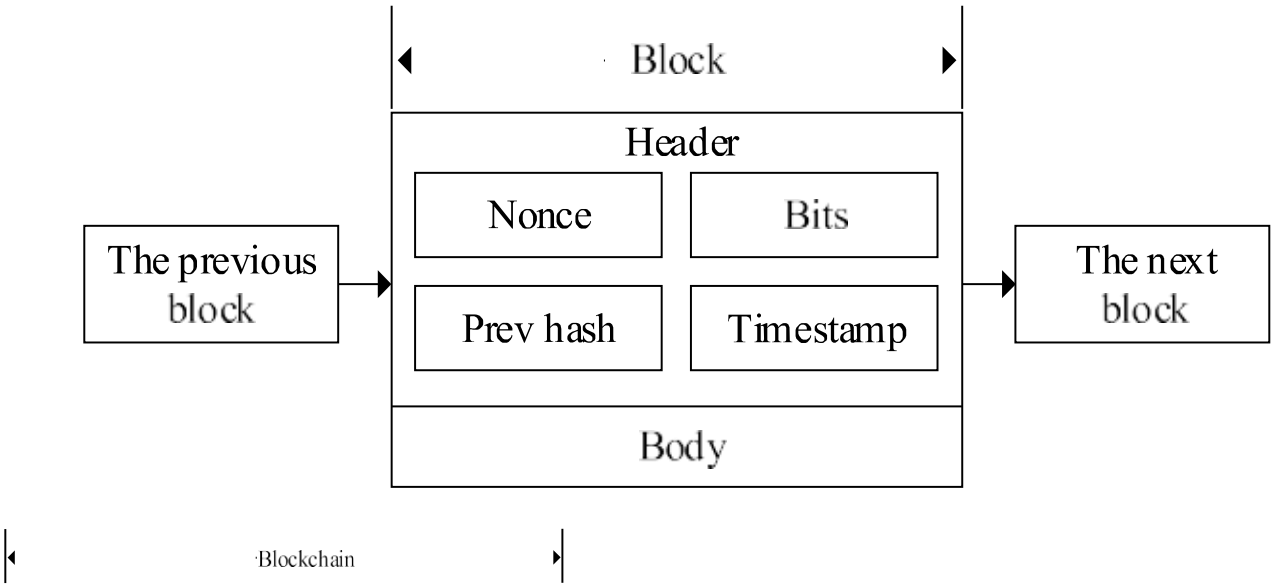

FIGURE 3. The Structure of a blockchain.

We developed a blockchain-based infrastructure for 5G-VANETs that uses SDN to provide security and privacy. A blockchain is maintained by an overlay P2P network of cars, RSUs, and gNBs (5G base stations). The onboard computer of the car features a real-time video service that shows the movement of traffic and enables data exchange between nearby vehicles. We think that blockchain technology can make source communications traceable and immutable. Transportation, as a result, is much safer and more effective.

A platform for communication that offers real-time video reports

IV. Blockchain-based security framework

A.1) VEHICLE ENROLLMENT

The 5G-VANET assigns each vehicle a SIM (subscriber identity module) number. ID is the number on the SIM card. One vehicle may utilize one ID at a time. The operator's database also contains the device number for the vehicle. The device number is represented in this case by Dat. Use Ia as an example to demonstrate how to register a vehicle. A Jb cannot go online when it enters the system unless the operator confirms that the Ebu and ID have not been altered. The specific symmetric key UFQ for the registration process is then randomly selected by Jb.

This article claims that the DMV is the only place where you can find SIM and license plate numbers. The term "ovn" here refers to a car's license plate number. DMV requests that Jb be registered in a letter to BU. It is crucial to remember that the END is alone in mapping a vehicle's ovn and ID. This aids in hiding its real identity. As a result, BU is only aware of Jb 's ID number, not who they are. To determine whether Jb 's public and private keys are already available, BU looks through its repository, which houses key pairs.

Additionally, it confirms the public-key certificate for Jb is legitimate. The public-key certificate and private key encrypted by TEP will be given to other vehicles by BU if the certificate expires or if there are no key pairs for the Jb in the repository. The first algorithm summarises vehicle registration.

2) A ROAD CONDITION REPORT

After registering, the inbuilt camera of the Jb was utilized to capture visual information that was then used to create the message digest [21]. On average, the procedure is carried out once every minute. The letters placed stand for the place, but ubhn.k, where k is a date, stands for the state of the road. Jb uses UFQ to encrypt the video's hash value and sign minute-specific data. The message is then transmitted to the Y nearby nodes using Jb. The STV is a Node Y, just like other vehicles. If a node close to Jb receives the message, it will verify the message's authenticity and legal identity using Jb 's public-key certificate.

Before being sent via the RSU to the gNBs, the message will be transmitted to other nodes for verification. In phases, the encrypted data will be sent to the cloud server. If the STV next to the Jb runs out of storage space, $n(n \geq 1)$ more vehicles will carry the message. The message will be examined to see if it is valid at each hop. An algorithm could be used to produce the road report. Because only the source car and the cloud server may view the video, data transportation is secure. As a result, if the cloud server is directly attacked or the intermediary nodes alter the video data, a message-digest method is offered. The authentication must verify the message digest's digital signature because a hostile node might supply fake video content. In addition to recording its video, a car must provide vital information to other nearby vehicles, such as its driving style and the state of the road. False alerts could endanger other vehicles and greatly limit the system's value. As a result, blockchain transactions were used to regulate vehicle-to-vehicle communications. Every communication may be discovered on the blockchain and connected to the device transmitted because all records are permanent. The system will punish misbehaving cars to ensure that message source node using this service are held accountable. The total number of blockchain transactions is shown in the message number.

Algorithm 1 Vehicle Registration

Input:

Input:

Initial vehicle Jb

TM’s public key QVCUB

A random symmetric key UFQ

Time b // validity period of the registration

Output:

Jb’s public-key certificate Qdfsub

Jb’s public key QVCb

Jb’s private key QSJb

1. Jb entered the VANET.

2.Operator select Ebu from the DATABASE.

3.where ID = ID of Jb

4.If Ebu! = Ebu of Jb 's then =

5: Fails

6: else

7. Jb can be accessed via the Internet.

8: end if

9: Jb do

10: Use QVCUB to encrypt UFQ as En(UFQ)

11: send (Num of Jb, ID of Jb, and En(UFQ)) to the NOP

12: NOP do

13: insert into IDENTITY_ PAIRS (Num, ID)

14: select Num of Jb, ID of Jb.

15. Where not exists (select * from IDENTITY_ PAIRS where Num = Num of Jb and ID = ID of Jb s)

16: Use BCDLB to encrypt UFQ and Jb 's ID as En(UFQ, Jb 's ID).

17.Send En(UFQ, Jb ID) to BU.

18: BU do

19: Decrypt En(UFQ, ID of Jb)

20. Choose * from KEY_PAIRS.

21.if not exists (QVCb QSJb) then

22. Issue (QVCb, QSJb) validity of l.

23. encrypt (QVCb, QSJb), use TLF

24: else

25: Fails

26: end if

27. NOP forward Encrypted (QVCb, QSJb to Wb.

28.Jb decrypt data encrypted with OFQ (QVCb, QSJb).

29. Jb acquires QVCb and QSJb.

30: A valid registration

Algorithm 2 Road Condition Report

Input:

Jb’s public-key certificate Qdfsub

Jb’s public key QVCb

Jb’s private key QSJb

Output:

Road video VidS

Road condition tag

1.while minute++ do

2. Jb do and

3.Vidk.a create a video file.

4.Record placeb and sign placeb with QSJb

5. Record the tagl.b and sign tagl.b with QSJb

6: Hash (Vidl.b)

7.encryt Vidl.b, Hash(Vidl.b) with UFQ as En(Vidl.b, Hash(Vidl.b)).

8:Sign En(Vidl.b, Hash(Vidl.b)) with QSJb.

9. Distribute signed placeb, tagl.b, En(Vidl.b, Hash(Vidml.b)) together with Qbfsub.

10: end while

11: for time = 0;; time++do

12: Node Xd receives message

13: end for

14. if X ← Other Vehicles then

15: Verify the signature's validity

16: if pass then

17: forward it

18.else

19:fails

20: end if

21: end if

22: if X ← RSUs then

23: Check the validity of signature

24. if pass then

25. Upload it to the gNBs

26: else

27: Fails

28: end if

29: end if

30. gNBs uploads the updated data

Each vehicle goes at a different speed since one communication equals one transaction.

It is crucial to choose a temporary center node, also known as the miner, to disseminate its message and reach a consensus because it is difficult to rule out the potential of fraudulent messages or malicious nodes. Elections are held periodically in each RSU to choose the miner in charge of creating new network blocks. In this system, proof-of-work and proof-of-stake voting are both used to elect miners. This strategy has been created and is now being used. The nonce, bits, prior hash, and date must all be present in the data that makes up the block header of each RSU-generated block, as illustrated in Figure 3. To do this, the nonce value is iteratively changed during the proof-of-work election process until the first x bits of the hash output are precisely 0. This enables the proof-of-work election method to produce the intended results. Bits are the absolute minimum for a proof-of-work hash. For a miner to effectively complete proof-of-work, the block header's data must have a calculated hash value less than the network's hash threshold. The formula below has been suggested as a component of the miner election process: The RSU count is r, and the RSU hash threshold is br. Its hashing algorithm is defined as follows:

$$\text{hash}(\text{prehash}, \text{bits}, \text{timestamp}) \leq \text{Mr}$$

The proposed system can be used with many hashing algorithms, including the well-known SHA-256 approach. The hash threshold is calculated using the SHA-256 method using the formula $Br = 2\ 256{-}x - 1$, where Br meets the requirement that the first x-bit must exactly be 0. With the nonce in mind, each RSU node calculates the block header's hash value and updates its nonce value often. If the estimated hash value of the RSU is lower than the allowed hash barrier, then it is eligible for miner selection and block publication.

B. TRUST MANAGEMENT FOR PARTICULAR MESSAGES

1) THE COLLECTION OF INFORMATION RELATED TO TRAFFIC

Automobiles assess the accuracy of the road condition tags during the message transmission process and give each one a score depending on it. A score can only have one of two potential values: +1 or -1. Consider the following scenario: the automobile Ia sends a message, which Ib receives. In addition to retrieving the traffic tags tagn.k, and place from the message, Vn verifies Jb. Jc is unable to understand Vido and J's specifics. It only examines tagm's dependability. The credibility of level j is evaluated using Jb. The tag is given an extra point when and the road condition specified by tagn.b line up. If Jb believes the road

condition indicated by tagn.k is false, a value of -1 is applied to the tag. Then Ib informs the neighboring RSU of its location, the rating it assigned to tagl.b, and its public key certificate Pcertn,k. Ib completes the transaction. The notation

{Kcertn,k , Si(IDm, IDn, markm,j,p, placen)}.

may be used when communicating this information. After the RSU has verified the message's origin, the information about the condition of the road at time j is categorized as

"Aj,1, Aj,2, Aj,3,... Aj,p"

depending on where the road segment is located. While "p" denotes the section number, "Aj,p" denotes the road condition of section L at time j. The information is then sent via the RSU to the intended recipient. Aj, components include the following: p's According to vehicle Ia, the numbers

ak.l1 ak.l2 ak.l3 …..ak.lm describe the traffic conditions on road segment p at time j.

Every time but time j, the message distribution is the same.

2) TRUST VALUE COMPUTATION

The scores sent by forwarding vehicles to RSU are identified as "Aj,1, Aj,2 , Aj,3 Aj,p" where p is the number of the road segment. The representation of the road conditions in section p at time k is " A1,bc,d A2,bc,d,A3,bc,d …..An,bc,d" Cars that are physically closer to the location where the tag was generated are more likely to earn reliable ratings since not all scores in set Sj,p are equally reliable. As a result, the reliability rating of a vehicle may be determined using the equation below: Where PM is the vehicle's road segment and S J, P N, M is the trust score

The letters V and PN designate the video forwarding vehicle's route. In the formula, o j, p n, m stands for the trust value, and Ia, |Pm −Pn| is a rate-modifying parameter that measures the distance between two vehicles

Weighted aggregation can be used to improve the trust value's dependability if the attacker does not control most vehicles. The following definition of the trust value of the road condition at section p was sent by Ia at time

Only in the event when aj.pi.m and oj.pi.m are both equal to zero can the formula be used to calculate aj.pi.m, and oj.pi.m. This is because I stands for the vehicle capturing the video, and oj.pi.m stands for the confidence value of the road situation at section p as communicated by Ia at time j.

The precision of scoring declines as the distance between the scoring vehicle and the broadcast address of the tag increases. Therefore, it is considered trustworthy when s j,p n, trust m's value exceeds 0.5. Any scores with a trust level less than or equal to 50% are ignored. Since o j,p i,l > 0.5 and s j,p i,l 6 = 0, the trust value of score aj.pi.m for the road state of section p at time j is computed as follows: aj.pi.m oj.pi.m. We use l to represent the number of vehicles broadcasting the road condition at the same road section as section p and at the same time as section j since many vehicles may be broadcasting the road condition of section p at time j. The RSU tries to add both the computed trust values and the pertinent road conditions to the blockchain when r is the number of the RSU in charge of gathering road conditions and calculating trust values. Less trustworthy tags are those with lower ratings. RSU regularly sends TA the identification numbers of cars with a high percentage of false positives and monitors the identity numbers of vehicles with fake license plates.

Based on the value of x and the particular RSU, the hash threshold of some RSUs may change. This method uses proof-of-stake to assess how difficult it is for an RSU to be chosen as a miner and produce a new block.

The overall trustworthiness of RSU for vehicles is represented by x in the following equation. If a variable parameter is greater than 0, x is equal to int(e (Ft Gr e))(7). Formula (3) also used the value to determine the time between the generation of new blocks. Our data indicate that it needs to be 100. Ab is the mean of the trust scores determined by RSUr. To reflect the change in Gr, decreasing the value of x causes Ab to increase. It follows that the likelihood that an RSU will be chosen as the miner and add a new block to the blockchain increases with the hash threshold because an increase in the hash threshold is connected to a drop in x. Using the following formula, gr is calculated:

where oj.pi.m is the trust value RSUr generated for Aj.pi.m. If RSUr obtains more precise and reliable road traffic data, it will have a better chance of winning the race for miners. The trust metrics used by Set Or are based on a range of historical and geographical contexts. The Set Or components that RSUr is currently holding will be deleted as soon as it is chosen as a miner and its block is broadcast to the blockchain. To address the concern that RSUs with older blocks may monopolize voting rights and prevent a small number of RSUs with older blocks from holding the right to be elected as a miner for a prolonged length of time, Formula (6) introduces a value adjustment function Ft. The purpose of this feature is to prevent the election of a few RSUs as miners for an extended period of time.

The following is the definition of the function

$$F_t = \begin{cases} 1 \ (t < t1) \\ 1 - \beta t \ (t1 < t < 2t1) \\ 0 \ (\text{if } Ft > 0 \text{ and } t = 2t1) \end{cases} \quad (1)$$

Where t1 is the typical length of time required for a successful miner election to take place during a given period and t is the amount of time since the last time RSUr was used to delete items from Set Or. Ft always = 1 when t is less than t1 when t is less than t1. The value of Ft decreases when t rises over t1 but falls below 2t1. The symbol represents a coefficient greater than zero and regulates the rate at which Ft is reduced. When it gets close to 0, Ft's value will stop decreasing any further. You can choose between an Ft range of 0 and 1. The collection Or's contents will be deleted during this procedure, and t will be reset to 0 to start the timing method over from scratch. After t has been raised to 2t1, if Ft is still greater than 0, the Set Or entries are cleared, and t is returned to 0. Because of this, the timing will start over. Another RSU validates the nonce value when it receives a block from an elected miner by executing a validation check. Each blockchain then posts the block. The blockchain will divide if an RSU receives multiple valid blocks at once. Due to the distributed consensus mechanism used by blockchains, only the longest fork that has been accepted by most of us will remain after a certain time.

3) VEHICLE CREDIBILITY EVALUATION

In an accident, the cloud server's data can be used to recover the video and reconstruct the exact course of events. On 5G networks, SIM numbers are the only way to be watched. The Department of Motor Vehicles is aware of the license plate numbers, but they won't be made public. This suggests that a reliable third party will be needed in addition to a blockchain base. If the report phase is completed on time, videos can also be used to balance traffic. The transportation management center can then analyze overall traffic volume and divert stopped vehicles to less crowded lanes.

Before uploading a message to the blockchain, an RSU can use [20] to assess its trust in the messages delivered by nearby cars. Using all of the data in the blocks, the trustworthiness of a vehicle may be assessed, and the vehicle may be rewarded or penalized as a result. Each individual is often in charge of analyzing and comprehending the signals sent by a small group of linked or nearby autos. However, everyone can agree on anything because of the immutable data in the blocks necessary to confirm the blockchain. All ratings and information about the associated cars can be stored in the blocks. Finding messages is much simpler as a result.

$$MDA = (TP + TN)/(TP + FN + FP + TN) \quad (2)$$

TP represents the total number of authorized messages. The TN estimates the number of fraudulent communications. The value FN represents the number of genuine communications mistakenly believed to be fraudulent. In contrast, the value FP represents the number of fraudulent messages mistakenly believed to be genuine. A higher MDA denotes a better capacity to judge the truthfulness of a message.

V. EXPERIMENTAL RESULTS AND ANALYSIS

A. EXPERIMENT CONFIGURATIONS

To execute the simulation, we make use of OMNeT++ 4.5 [22, 23] and the crypto++ library 5.6.2 [24]. A laptop with an Intel Core i7 processor, 16 GB of RAM, and a GeForce 920 M graphics card is used to administer all numerical tests. The measurement of the transportation area is 1,000 by 1,000 meters. RSUs offer the same service as 802.11p 10Mbps APs. The bandwidth of the gNBs is set to 1 Gbps. We assigned the numbers 30 and 25 to RSUs and gNBs, assuming they were dispersed uniformly across the region. We expect anywhere between 200 and 500 cars on the network at any given time. In addition, traffic is moving at 110 km/h in all directions and is evenly distributed. V2N communication has a 100 m range, but V2V communication has a 50 m range.

SHA-256 is used as the hash algorithm in the blockchain, i.e., hashed result = dhash(input) = SHA256(SHA256(input)). The temporal overhead of the video encryption methods AES/CBC (256-bit key), Twofish/CTR (256-bit key), and Serpent/CTR (256-bit key) is examined in this experiment (256-bit key). This is done to determine whether the network can sustain the video report service. The efficiency of individual and collective detection in the blockchain-based architecture is evaluated. To show that the blockchain-based framework can be utilized in the 5G-VANET and is scalable, we evaluate the amount of time needed for blockchain transactions to be relayed at different message rates and vehicle counts.

B. Assessment of quantitative findings

The amount of time needed to process a blockchain block is shown in Figure 4. We employ a straightforward yet time-consuming method to get blocks from blockchain miners. The relationship between processing time and block count

Vehicle-to-vehicle communication is possible when there aren't many rogue nodes. Blockchain-based detection performs 5% to 15% better than individual detection when the percentage of harmful objects is close to 5%. The relationship between the number of malicious nodes and the success of detection is shown in Figure 5.

As more messages are transmitted by each node, as seen in FIGURE 6, the network has to do more work. Notifications alone won't be enough; there will also need to be a growing number of transactions publicized. We expect the system to run in real-time if at least one message is sent every minute. Less than 50 milliseconds pass quickly during transmission, even with 10 messages per minute (no more than 50ms). The bandwidth restrictions of the 5G VANET are mostly to blame for this. FIGURE 7 shows that, depending on the encryption algorithm and the video size, the time needed to encrypt a video might vary from 20 to 160 milliseconds. The video size and encryption time frequently reduce as the frequency of the video report phase rises. In the proposed scenario, the video report occurs for 10 minutes per automobile. The high-definition movie is only a few minutes long, but its size is sufficient for reliable encryption.

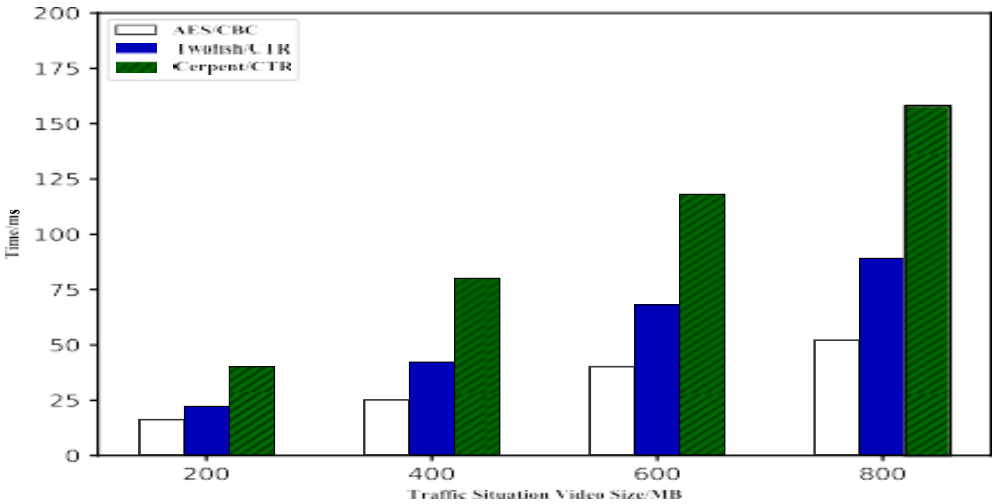

FIGURE 4. Video encryption time overhead.

This suggests that encrypted video can fulfill the need for real-time effectiveness.

C. SAFETY ANALYSIS

1) PROTECTION OF USER PRIVACY AND SECURITY

The SIM number assigned to an automobile is specific to that vehicle and cannot be changed. The operator checks to ensure the SIM number isn't changed before permitting a car to connect to the Internet. The vehicle won't be able to connect to the Internet if the SIM number and device number do not match. Vehicles send videos to a server connected to the operator's network. The operator cannot immediately access the contents of the videos since they are encrypted. Examining the license plate number is the only way to identify the kind of vehicle. Only an anonymous approach will let AT save private key data. The owner's identity is not made known to AT by the car's SIM number. The link between a vehicle's SIM number and license plate number is only kept at the MNO. This makes hiding the vehicle's genuine identification simple. The recipient may confirm both the legitimacy of the videos and the sender's identity thanks to the sender's digital signature. An attacker can be stopped from submitting a fake film by aiming for a real car. The receiver can check the videos' integrity by computing their hash functions. The uploaded videos won't be changed if you carry on in this way.

2) ANALYSIS OF MALICIOUS VEHICLES

Depending on the route data that a vehicle transmits, other vehicles in the system will evaluate the tags that the vehicle conveys. These tags will be rated negatively rather than favorably by other vehicles. If they are broadcast by a malevolent vehicle or one that has been hacked and is disseminating false information regarding road conditions, they will be regarded as unreliable. For instance, RSU might give AT the vehicle's SIM number if it turns out over time that the data provided by the vehicle Ia is unreliable. The MNO will be given the car's registration details if AT receives numerous reports from RSUs claiming the same vehicle is suspicious. The MNO searches the database for the actual names of malicious vehicles and adds them to a temporary blacklist to stop them from joining the car network. Operators and the police will be informed of serious infractions and will take action.

3) MALICIOUS SCORING

The trustworthiness of the broadcasted road conditions is unaffected if a tag is purposely scored, such as by giving a low score to a trustworthy tag and a high score to a non-trustworthy tag. Several vehicles will report on the condition of the same section of the road over a predetermined period. The same road conditions will receive the same safety rating from several vehicles. As a result, the ratings provided by a single car have little impact on how accurately the road quality is assessed. An enemy needs to win the majority of the ratings to reduce the credibility of traffic broadcasts. An unreasonably high price like that will deter attackers. As a result, you may trust that the tag scoring results are correct.

4) RSU BEING ATTACKED AND COMPROMISED

An RSU will attempt to implant phony trust evaluation values into the blockchain if it is assaulted during the miner election. Even then, other RSUs will scrutinize the bogus RSU's digital certificates and prevent it from being able to add blocks to the blockchain, even if it were to win the election. The MNO and AT won't be able to punish the vehicles if an RSU sends legitimate cars to them disguised as malevolent ones. A vehicle is only deemed unreliable when several RSUs report it at once. Like an attacker can only access a certain number of resources at once, several RSUs cannot be attacked at once. As a result, legitimate vehicles won't be impacted.

VI. Conclusion

This paper presents a decentralized security architecture for the Internet of Things (IoT) in 5G-VANETs with SDN support. OBUs, RSUs, and gNBs are active nodes in the vehicle system, and together they form a P2P network that looks after the blockchain. The blockchain records all messages and their sources, and the cars communicate in real time about the state of the roads. The provenance of the communication is verified using the immutability of blockchain technology. Real-time video report service installation improves the existing design. The movies are encrypted and checked against pertinent messages before being uploaded to cloud servers. We provide a blockchain-based framework for system-wide trust management if

adversarial nodes claim messages are faked or altered. Our method, which is substantially more effective at identifying malicious nodes, is supported by theoretical and empirical data. It can be implemented widely, according to an analysis of the extra work needed for video encryption and the transmission of texts and movies.

REFERENCES

1. R. A. Uzcategui, A. J. D. Sucre, and G. Acosta-Marum, ''Wave: A tutorial,'' IEEE Commun. Mag., vol. 47, no. 5, pp. 126–133, May 2009.
2. G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, ''LTE for vehicular networking: A survey,'' IEEE Commun. Mag., vol. 51, no. 5, pp. 148–157, May 2013.
3. D. Soldani and A. Manzalini, ''Horizon 2020 and beyond: On the 5G operating system for a true digital society,'' IEEE Veh. Technol. Mag., vol. 10, no. 1, pp. 32–42, Mar. 2015.
4. C. Wu, Z. Liu, T. Yoshinaga, Y. Ji, and D. Zhang, ''Spatial intelligence toward trustworthy vehicular IoT,'' IEEE Commun. Mag., vol. 56, no. 10, pp. 22–27, Oct. 2018.
5. M. Kim, J. Lim, H. Yu, K. Kim, Y. Kim, and S. Lee, ''ViewMap: Sharing private in-vehicle dashcam videos,'' in Proc. 14th USENIX Symp. Netw. Syst. Design Implement. (NSDI), 2017, pp. 163–176.
6. M. H. Eiza, Q. Ni, and Q. Shi, ''Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks,'' IEEE Trans. Veh. Technol., vol. 65, no. 10, pp. 7868–7881, Oct. 2016.
7. T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah, and B. Chen, ''SIGMM: A novel machine learning algorithm for spammer identification in indus- trial mobile cloud computing,'' IEEE Trans. Ind. Informat., vol. 15, no. 4, pp. 2349–2359, Apr. 2018.
8. W. He, G. Yan, and L. D. Xu, ''Developing vehicular data cloud ser- vices in the IoT environment,'' IEEE Trans. Ind. Inform., vol. 10, no. 2, pp. 1587–1595, May 2014.
9. T. Zhang, A. Chowdhery, P. Bahl, K. Jamieson, and S. Banerjee, ''The design and implementation of a wireless video surveillance system,'' in Proc. 21st Annu. Int. Conf. Mobile Comput. Netw., 2015, pp. 426–438.
10. H. Qiu et al., ''Kestrel: Video analytics for augmented multi-camera vehi- cle tracking,'' in Proc. IEEE/ACM 3rd Int. Conf. Internet-of-Things Design Implement. (IoTDI), Apr. 2018, pp. 48–59.
11. T. Qiu, R. Qiao, and D. Wu, ''EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things,'' IEEE Trans. Mobile Comput., vol. 17, no. 1, pp. 72–84, Jan. 2018.
12. Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, ''Blockchain- based decentralized trust management in vehicular networks,'' IEEE Inter- net Things J., to be published.
13. R. Rivest, The MD5 Message-Digest Algorithm, document RFC 1321, 1992.
14. A. Varga, ''Using the OMNeT discrete event simulation system in education,'' IEEE Trans. Educ., vol. 42, no. 4, p. 11, Nov. 1999.
15. C. Sommer, R. German, and F. Dressler, ''Bidirectionally coupled network and road traffic simulation for improved IVC analysis,'' IEEE Trans. Mobile Comput., vol. 10, no. 1, pp. 3–15, Jan. 2010.
16. Vijayalakshmi A, Vidyavathy Balraj (2017), 'Optical, thermal, laser damage threshold, dielectric studies and z-scan technique of novel semiorganic NLO material: sodium boro succinate (NaBS)', U.P.B. Scientific Bulletin- Series B, vol. 79, issue 1, pp. 221-232.
17. Vijayalakshmi A, Vidyavathy Balraj, Determination of basic solid state parameters and characterization of optical, dielectric and fluorescence properties of Calcium Boro Lactate(CaBL) , Journal of chemical society, Pakistan. Vol. 38 Issue 6, pp. 1092-1097.
18. Vijayalakshmi A, Vidyavathy Balraj, G. Vinitha, (2016),"Crystal structure, growth and nonlinear optical studies of Isonicotinamide p-nitrophenol: A new organic crystal for optical limiting applications", Journal of crystal growth, 448 pp.82-88. doi: https://doi.org/10.1016/j.jcrysgro.2016.05.002
19. Vijayalakshmi A, Vidyavathy Balraj , Vinitha G. , (2016) "Structure and characterization of a new organic crystal for optical limiting applications, isonicotinamide bis-p-aminobenzoic acid", Ukranian J. Phys. Opt., Volume 17, Issue 3.pp. 98-104.
20. Vijayalakshmi A, Vidyavathy, B, Peramaiyan, G & Vinitha, G (2017), 'Synthesis, growth, structural and optical studies of a new organic three dimensional framework: 4-(aminocarbonyl) pyridine 4 (aminocarbonyl) pyridinium hydrogen L-malate, Journal of Solid State Chemistry, vol. 246, pp. 237-244. doi: https://doi.org/10.1016/j.jssc.2016.11.025
21. Vijayalakshmi A, Vidyavathy Balraj , B. Gunasekaran, Abdul Razack Ibrahim, Synthesis, Structural, Optical, Thermal and LDT Characterization of Novel Semi-Organic Non-Linear Optical Material: Calcium Borolactate, Asian Journal of Chemistry; Vol. 28, No. 12 (2016).
22. Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., ... & Hamdi, M. (2022). A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography. Computers and Electrical Engineering, 102, 108205.
23. Gupta, S., Iyer, S., Agarwal, G., Manoharan, P., Algarni, A. D., Aldehim, G., & Raahemifar, K. (2022). Efficient Prioritization and Processor Selection Schemes for HEFT Algorithm: A Makespan Optimizer for Task Scheduling in Cloud Environment. Electronics, 11(16), 2557.
24. Balyan, A. K., Ahuja, S., Lilhore, U. K., Sharma, S. K., Manoharan, P., Algarni, A. D., ... & Raahemifar, K. (2022). A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method. Sensors, 22(16), 5986.
25. Poongodi, M., Bourouis, S., Ahmed, A. N., Vijayaragavan, M., Venkatesan, K. G. S., Alhakami, W., & Hamdi, M. (2022). A Novel Secured Multi-Access Edge Computing based VANET with Neuro fuzzy systems based Blockchain Framework. Computer Communications.
26. Manoharan, P., Walia, R., Iwendi, C., Ahanger, T. A., Suganthi, S. T., Kamruzzaman, M. M., ... & Hamdi, M. (2022). SVM-based generative adverserial networks for federated learning and edge computing attack model and outpoising. Expert Systems, e13072.
27. Ramesh, T. R., Lilhore, U. K., Poongodi, M., Simaiya, S., Kaur, A., & Hamdi, M. (2022). PREDICTIVE ANALYSIS OF HEART DISEASES WITH MACHINE LEARNING APPROACHES. Malaysian Journal of Computer Science, 132-148.
28. Poongodi, M., Malviya, M., Hamdi, M., Vijayakumar, V., Mohammed, M. A., Rauf, H. T., & Al-Dhlan, K. A. (2022). 5G based Blockchain network for authentic and ethical keyword search engine. IET Commun., 16(5), 442-448.
29. Poongodi, M., Malviya, M., Kumar, C., Hamdi, M., Vijayakumar, V., Nebhen, J., & Alyamani, H. (2022). New York City taxi trip duration prediction using MLP and XGBoost. International Journal of System Assurance Engineering and Management, 13(1), 16-27.
30. Poongodi, M., Hamdi, M., & Wang, H. (2022). Image and audio caps: automated captioning of background sounds and images using deep learning. Multimedia Systems, 1-9.
31. Poongodi, M., Hamdi, M., Gao, J., & Rauf, H. T. (2021, December). A Novel Security Mechanism of 6G for IMD using Authentication and Key Agreement Scheme. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.
32. Ramesh, T. R., Vijayaragavan, M., Poongodi, M., Hamdi, M., Wang, H., & Bourouis, S. (2022). Peer-to-peer trust management in intelligent transportation system: An Aumann's agreement theorem based approach. ICT Express.

33. Hamdi, M., Bourouis, S., Rastislav, K., & Mohmed, F. (2022). Evaluation of Neuro Image for the Diagnosis of Alzhimer's Disease Using Deep Learning Neural Network. Frontiers in Public Health, 35.
34. Poongodi, M., Hamdi, M., Malviya, M., Sharma, A., Dhiman, G., & Vimal, S. (2022). Diagnosis and combating COVID-19 using wearable Oura smart ring with deep learning methods. Personal and ubiquitous computing, 26(1), 25-35.
35. Sahoo, S. K., Mudligiriyappa, N., Algethami, A. A., Manoharan, P., Hamdi, M., & Raahemifar, K. (2022). Intelligent Trust-Based Utility and Reusability Model: Enhanced Security Using Unmanned Aerial Vehicles on Sensor Nodes. Applied Sciences, 12(3), 1317.
36. Muniyappan, A., Sundarappan, B., Manoharan, P., Hamdi, M., Raahemifar, K., Bourouis, S., & Varadarajan, V. (2022). Stability and numerical solutions of second wave mathematical modeling on covid-19 and omicron outbreak strategy of pandemic: Analytical and error analysis of approximate series solutions by using hpm. Mathematics, 10(3), 343.
37. Rawal, B. S., Manogaran, G., & Poongodi, M. (2022). Implementing and Leveraging Blockchain Programming.
38. Bourouis, S., Band, S. S., Mosavi, A., Agrawal, S., & Hamdi, M. (2022). Meta-Heuristic Algorithm-Tuned Neural Network for Breast Cancer Diagnosis Using Ultrasound Images. Frontiers in Oncology, 12, 834028.
39. Lilhore, U. K., Poongodi, M., Kaur, A., Simaiya, S., Algarni, A. D., Elmannai, H., ... & Hamdi, M. (2022). Hybrid Model for Detection of Cervical Cancer Using Causal Analysis and Machine Learning Techniques. Computational and Mathematical Methods in Medicine, 2022.
40. Lilhore, U. K., Khalaf, O. I., Simaiya, S., Tavera Romero, C. A., Abdulsahib, G. M., & Kumar, D. (2022). A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks. International Journal of Distributed Sensor Networks, 18(9), 15501329221117118.
41. Sekar, S., Solayappan, A., Srimathi, J., Raja, S., Durga, S., Manoharan, P., ... & Tunze, G. B. (2022). Autonomous Transaction Model for E-Commerce Management Using Blockchain Technology. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-14.
42. Singh, D. K. S., Nithya, N., Rahunathan, L., Sanghavi, P., Vaghela, R. S., Manoharan, P., ... & Tunze, G. B. (2022). Social Network Analysis for Precise Friend Suggestion for Twitter by Associating Multiple Networks Using ML. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-11.
43. Balasubramaniam, K., Vidhya, S., Jayapandian, N., Ramya, K., Poongodi, M., Hamdi, M., & Tunze, G. B. (2022). Social Network User Profiling With Multilayer Semantic Modeling Using Ego Network. International Journal of Information Technology and Web Engineering (IJITWE), 17(1), 1-14.
44. Dhiman, P., Kukreja, V., Manoharan, P., Kaur, A., Kamruzzaman, M. M., Dhaou, I. B., & Iwendi, C. (2022). A Novel Deep Learning Model for Detection of Severity Level of the Disease in Citrus Fruits. Electronics, 11(3), 495.
45. Dhanaraj, R. K., Ramakrishnan, V., Poongodi, M., Krishnasamy, L., Hamdi, M., Kotecha, K., & Vijayakumar, V. (2021). Random Forest Bagging and X-Means Clustered Antipattern Detection from SQL Query Log for Accessing Secure Mobile Data. Wireless Communications and Mobile Computing, 2021.
46. Maurya, S., Joseph, S., Asokan, A., Algethami, A. A., Hamdi, M., & Rauf, H. T. (2021). Federated transfer learning for authentication and privacy preservation using novel supportive twin delayed DDPG (S-TD3) algorithm for IIoT. Sensors, 21(23), 7793.
47. Poongodi, M., Nguyen, T. N., Hamdi, M., & Cengiz, K. (2021). Global cryptocurrency trend prediction using social media. Information Processing & Management, 58(6), 102708.
48. Poongodi, M., Sharma, A., Hamdi, M., Maode, M., & Chilamkurti, N. (2021). Smart healthcare in smart cities: wireless patient monitoring system using IoT. The Journal of Supercomputing, 77(11), 12230-12255.
49. Rawal, B. S., Manogaran, G., & Hamdi, M. (2021). Multi-Tier Stack of Block Chain with Proxy Re-Encryption Method Scheme on the Internet of Things Platform. ACM Transactions on Internet Technology (TOIT), 22(2), 1-20.
50. Poongodi, M., Nguyen, T. N., Hamdi, M., & Cengiz, K. (2021). A measurement approach using smart-IoT based architecture for detecting the COVID-19. Neural Processing Letters, 1-15.
51. Poongodi, M., Malviya, M., Hamdi, M., Rauf, H. T., Kadry, S., & Thinnukool, O. (2021). The recent technologies to curb the second-wave of COVID-19 pandemic. Ieee Access, 9, 97906-97928.
52. Rawal, B. S., Manogaran, G., Singh, R., Poongodi, M., & Hamdi, M. (2021, June). Network augmentation by dynamically splitting the switching function in SDN. In 2021 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-6). IEEE. Poongodi, M., Hamdi, M., Gao, J., & Rauf, H. T. (2021, December). A Novel Security Mechanism of 6G for IMD using Authentication and Key Agreement Scheme. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.
53. Poongodi, M., Hamdi, M., Vijayakumar, V., Rawal, B. S., & Maode, M. (2020, September). An effective electronic waste management solution based on blockchain smart contract in 5G communities. In 2020 IEEE 3rd 5G World Forum (5GWF) (pp. 1-6). IEEE.
54. Poongodi, M., Sharma, A., Vijayakumar, V., Bhardwaj, V., Sharma, A. P., Iqbal, R., & Kumar, R. (2020). Prediction of the price of Ethereum blockchain cryptocurrency in an industrial finance system. Computers & Electrical Engineering, 81, 106527.
55. Poongodi, M., Hamdi, M., Varadarajan, V., Rawal, B. S., & Maode, M. (2020, July). Building an authentic and ethical keyword search by applying decentralised (Blockchain) verification. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 746-753). IEEE.
56. Poongodi, M., Vijayakumar, V., & Chilamkurti, N. (2020). Bitcoin price prediction using ARIMA model. International Journal of Internet Technology and Secured Transactions, 10(4), 396-406.
57. Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M., & Ma, M. (2019). Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics. IEEE Access, 7, 158481-158491.
58. Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS detection mechanism using trust-based evaluation system in VANET. IEEE Access, 7, 183532-183544.
59. Poongodi, M., Vijayakumar, V., Ramanathan, L., Gao, X. Z., Bhardwaj, V., & Agarwal, T. (2019). Chat-bot-based natural language interface for blogs and information networks. International Journal of Web Based Communities, 15(2), 178-195.
60. Poongodi, M., Vijayakumar, V., Rawal, B., Bhardwaj, V., Agarwal, T., Jain, A., ... & Sriram, V. P. (2019). Recommendation model based on trust relations & user credibility. Journal of Intelligent & Fuzzy Systems, 36(5), 4057-4064.
61. Jeyachandran, A., & Poongodi, M. (2018). Securing Cloud information with the use of Bastion Algorithm to enhance Confiden-tiality and Protection. Int. J. Pure Appl. Math, 118, 223-245.
62. Poongodi, M., Al-Shaikhli, I. F., & Vijayakumar, V. (2017). The probabilistic approach of energy utility and reusability model with enhanced security from the compromised nodes through wireless energy transfer in WSN. Int. J. Pure Appl. Math, 116(22), 233-250.
63. Poongodi, M., & Bose, S. (2015). Stochastic model: reCAPTCHA controller based co-variance matrix analysis on frequency distribution using trust evaluation and re-eval by Aumann agreement theorem against DDoS attack in MANET. Cluster Computing, 18(4), 1549-1559.
64. Poongodi, M., & Bose, S. (2015). A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET. Arabian Journal for Science and Engineering, 40(12), 3583-3594.
65. Poongodi, M., & Bose, S. (2015). The COLLID based intrusion detection system for detection against DDOS attacks using trust evaluation. Adv. Nat. Appl. Sci, 9(6), 574-580.
66. Poongodi, M., & Bose, S. (2015). Detection and Prevention system towards the truth of convergence on decision using Aumann agreement theorem.

Procedia Computer Science, 50, 244-251.
67. Poongodi, M., Bose, S., & Ganeshkumar, N. (2015). The effective intrusion detection system using optimal feature selection algorithm. International Journal of Enterprise Network Management, 6(4), 263-274.
68. Poongodi, M., & Bose, S. (2014). A firegroup mechanism to provide intrusion detection and prevention system against DDoS attack in collaborative clustered networks. International Journal of Information Security and Privacy (IJISP), 8(2), 1-18.
69. Poongodi, M., & Bose, S. (2013, December). Design of Intrusion Detection and Prevention System (IDPS) using DGSOTFC in collaborative protection networks. In 2013 Fifth International Conference on Advanced Computing (ICoAC) (pp. 172-178). IEEE.
70. Pandithurai, O., Poongodi, M., Kumar, S. P., & Krishnan, C. G. (2011, December). A method to support multi-tenant as a service. In 2011 Third International Conference on Advanced Computing (pp. 157-162). IEEE.
71. Lahari, P. L., Bharathi, M., & Shirur, Y. J. (2020, June). An efficient truncated mac using approximate adders for image and video processing applications. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184) (pp. 1039-1043). IEEE.
72. Bharathi, M., Shirur, Y. J. M., & Lahari, P. L. (2020, July). Performance evaluation of Distributed Arithmetic based MAC Structures for DSP Applications. In 2020 7th International Conference on Smart Structures and Systems (ICSSS) (pp. 1-5). IEEE.
73. Bharathi, M., & Shirur, Y. J. M. (2021). Power-Efficient Modulo Multiply and Accumulate Unit Using Distributed Arithmetic. Design Engineering, 3548-3556.
74. Lahari, P. L., Bharathi, M., & Shirur, Y. J. M. (2019). A Review on Distributed Arithmetic and Offset Binary Coding. i-Manager's Journal on Digital Signal Processing, 7(3), 27.
75. Bharathi, M., & Shirur, Y. J. M. (2021). Floating-Point Multiply and Accumulate Unit Core using Distributed Arithmetic for DSP Applications. Turkish Journal of Computer and Mathematics Education, 12(11), 4730-4738.
76. Bharathi, M., & Shirur, Y. J. M. (2021). Vlsi Implementation Of Multiply And Accumulate Unit Using Offset Binary Coding Distributed Arithmetic. Turkish Journal of Computer and Mathematics Education, 12(11), 4739-4749.
77. Sivapriya, N., & Mohandas, R. (2022). Analysis on Essential Challenges and Attacks on MANET Security Appraisal. JOURNAL OF ALGEBRAIC STATISTICS, 13(3), 2578-2589.
78. Sivapriya, N., & Mohandas, R. (2022). Optimal Route Selection for Mobile Ad-hoc Networks based on Cluster Head Selection and Energy Efficient Multicast Routing Protocol. JOURNAL OF ALGEBRAIC STATISTICS, 13(2), 595-607.
79. Sivapriya, N., & Ravi, D. T. (2018). QoS Routing Protocols in MANET: A Survey. International Journal of Pure and Applied Mathematics, 119(12), 16573-16579.
80. Sivapriya, N., & Ravi, T. N. Efficient Fuzzy-based Multi-constraint Multicast Routing With Multi-criteria Enhanced Optimal Capacity-Delay Tradeoff.
81. Sivapriya, N., & Ravi, T. N. (2019, May). Efficient Fuzzy-Based Multi-constraint Multicasting with Fault Tolerance Routing Mechanism. In International Conference on Computer Networks and Inventive Communication Technologies (pp. 475-484). Springer, Cham.
82. Haribabu, S., Cheepu, M., Tammineni, L., Gurasala, N. K., Devuri, V., & Kantumuchu, V. C. (2018). Dissimilar Friction Welding of AISI 304 Austenitic Stainless Steel and AISI D3 Tool Steel: Mechanical Properties and Microstructural Characterization. Advances in Materials and Metallurgy, 271–281. https://doi.org/10.1007/978-981-13-1780-4_27
83. Shiva, A., Cheepu, M., Kantumuchu, V. C., Ravi Kumar, K., Venkateswarlu, D., Srinivas, B., & Jerome, S. (2018). Microstructure Characterization of Al-TiC Surface Composite Fabricated by Friction Stir Processing. IOP Conference Series: Materials Science and Engineering, 330, 012060. https://doi.org/10.1088/1757-899x/330/1/012060
84. Haribabu, S., Cheepu, M., Devuri, V., & Kantumuchu, V. C. (2019). Optimization of Welding Parameters for Friction Welding of 304 Stainless Steel to D3Tool Steel Using Response Surface Methodology. Techno-Societal 2018, 427–437. https://doi.org/10.1007/978-3-030-16962-6_44
85. Sarila, V. K., Koneru, H. P., Pathapalli, V. R., Cheepu, M., & Kantumuchu, V. C. (2022). Wear and Microstructural Characteristics of Colmonoy-4 and Stellite-6 Additive Layer Deposits on En19 Steel by Laser Cladding. Transactions of the Indian Institute of Metals. https://doi.org/10.1007/s12666-022-02769-1
86. Kavitha, Ch., Geetha Malini, P. S., Charan Kantumuchu, V., Manoj Kumar, N., Verma, A., & Boopathi, S. (2022). An experimental study on the hardness and wear rate of carbonitride coated stainless steel. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2022.09.524
87. Cheepu, M., & Kantumuchu, V. C. (2022). Numerical Simulations of the Effect of Heat Input on Microstructural Growth for MIG-Based Wire Arc Additive Manufacturing of Inconel 718. Transactions of the Indian Institute of Metals. https://doi.org/10.1007/s12666-022-02749-5
88. Sarila, V. K., Moinuddin, S. Q., Cheepu, M., Rajendran, H., & Kantumuchu, V. C. (2022). Characterization of Microstructural Anisotropy in 17–4 PH Stainless Steel Fabricated by DMLS Additive Manufacturing and Laser Shot Peening. Transactions of the Indian Institute of Metals. https://doi.org/10.1007/s12666-022-02742-y
89. Sarila, V., Koneru, H. P., Cheepu, M., Chigilipalli, B. K., Kantumuchu, V. C., & Shanmugam, M. (2022). Microstructural and Mechanical Properties of AZ31B to AA6061 Dissimilar Joints Fabricated by Refill Friction Stir Spot Welding. Journal of Manufacturing and Materials Processing, 6(5), 95. https://doi.org/10.3390/jmmp6050095
90. Kantumuchu, V. C., & Cheepu, M. M. (2022). The Influence of Friction Time on the Joint Interface and Mechanical Properties in Dissimilar Friction Welds. Journal of Metallic Material Research, 5(1). https://doi.org/10.30564/jmmr.v5i1.4209
91. Kantumuchu, V. (2020, July). More than meets the eye: The hidden benefits of flowcharts. Quality Progress, 53(7), 56.
92. Webber, J., Mehbodniya, A., Teng, R., Arafa, A., & Alwakeel, A. (2021). Finger-Gesture Recognition for Visible Light Communication Systems Using Machine Learning. Applied Sciences, 11(24), 11582.
93. Webber, J., Mehbodniya, A., Arafa, A., & Alwakeel, A. (2022). Improved Human Activity Recognition Using Majority Combining of Reduced-Complexity Sensor Branch Classifiers. Electronics, 11(3), 392.
94. Bukhari, S. N. H., Jain, A., Haq, E., Mehbodniya, A., & Webber, J. (2022). Machine learning techniques for the prediction of B-cell and T-cell epitopes as potential vaccine targets with a specific focus on SARS-CoV-2 pathogen: A review. Pathogens, 11(2), 146.
95. Mehbodniya, A., Webber, J. L., Rani, R., Ahmad, S. S., Wattar, I., Ali, L., & Nuagah, S. J. (2022). Energy-Aware Routing Protocol with Fuzzy Logic in Industrial Internet of Things with Blockchain Technology. Wireless Communications and Mobile Computing, 2022.
96. Mehbodniya, A., Kumar, P., Changqing, X., Webber, J. L., Mamodiya, U., Halifa, A., & Srinivasulu, C. (2022). Hybrid Optimization Approach for Energy Control in Electric Vehicle Controller for Regulation of Three-Phase Induction Motors. Mathematical Problems in Engineering, 2022.
97. Bukhari, S. N. H., Webber, J., & Mehbodniya, A. (2022). Decision tree based ensemble machine learning model for the prediction of Zika virus T-cell epitopes as potential vaccine candidates. Scientific Reports, 12(1), 1-11.
98. Khaliq, A. A., Anjum, A., Ajmal, A. B., Webber, J. L., Mehbodniya, A., & Khan, S. (2022). A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve c Cryptography and Local Differential Privacy. IEEE Access.