


Please cite the Published Version

Awais, Muhammad, Saeed, Yousaf, Ali, Abid, Jabbar, Sohail, Ahmad, Awais, Alkhrijah, Yazeed, Raza, Umar  and Saleem, Yasir (2024) Deep learning based enhanced secure emergency video streaming approach by leveraging blockchain technology for Vehicular AdHoc 5G Networks. Journal of Cloud Computing: Advances, Systems and Applications, 13 (1). 130 ISSN 2192-113X

DOI: <https://doi.org/10.1186/s13677-024-00665-1>

Publisher: Springer

Version: Published Version

Downloaded from: <https://e-space.mmu.ac.uk/635370/>

Usage rights:  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

Additional Information: This is an open access article which first appeared in Journal of Cloud Computing: Advances, Systems and Applications

Data Access Statement: The datasets used and/or analysed during the current study are available from the corresponding author upon reasonable request.

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

RESEARCH

Open Access



Deep learning based enhanced secure emergency video streaming approach by leveraging blockchain technology for Vehicular AdHoc 5G Networks

Muhammad Awais¹, Yousaf Saeed¹, Abid Ali^{2,3}, Sohail Jabbar^{4*}, Awais Ahmad⁵, Yazeed Alkhrijah⁶, Umar Raza⁷ and Yasir Saleem²

Abstract

VANET is a category of MANET that aims to provide wireless communication. It increases the safety of roads and passengers. Millions of people lose their precious lives in accidents yearly, millions are injured, and others incur disability daily. Emergency vehicles need clear roads to reach their destination faster to save lives. Video streaming can be more effective as compared to textual messages and warnings. To address this issue, we proposed a methodology to use visual sensors, cameras, and OBU to record emergency videos. Initially, the frames are detected. After re-recording, the frames detection algorithm detects the specific event from the video frames. Blockchain encrypts an emergency or specific event using hashing algorithms in the second layer of our proposed framework. In the third layer of the proposed methodology, encrypted video is broadcast with the help of 5G wireless technology to the connected nodes in the VANET. The dataset used in this research comprises up to 72 video sequences averaging about 120 seconds per video. All videos have different traffic conditions and vehicles. The ResNet-50 model is used for the feature extraction process of extracted frames. The model is trained using Tensorflow and Keras deep learning models. The Elbow method finds the optimal K number for the K Means model. This data is split into training and testing. 70% is reserved for training the support vector machine (SVM) model and test datasets, while 30%. 98% accuracy is achieved with 98% precision and 99% recall as results for the proposed methodology.

Keywords Vehicular ad-hoc network, Blockchain adaptation layer, Communication security, Emergency video streaming, Deep learning

*Correspondence:

Sohail Jabbar
sjjabbar@imamu.edu.sa

¹ Department of Information Technology, The University of Haripur,
Haripur, Punjab, Pakistan

² Department of Computer Science, University of Engineering
and Technology Lahore, Lahore, Punjab, Pakistan

³ Department of Computer Science, GANK(S) DC KTS, Haripur, Pakistan

⁴ Computer Science Department, College of Computer and Information
Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU),
Riyadh 11432, Saudi Arabia

⁵ Information Systems Department, College of Computer and Information
Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU),
Riyadh 11432, Saudi Arabia

⁶ College of Engineering, Imam Mohammad Ibn Saud Islamic University
(IMSIU), Riyadh 11432, Saudi Arabia

⁷ School of Engineering, Faculty of science and Engineering, Manchester
Metropolitan University (MMU), Manchester, UK



© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Introduction

Thousands of vehicles running on the roads daily, in which millions of passengers travel to reach their offices, schools, universities, factories, hospitals, and other workplaces. Traffic in big cities is increasing day by day [1]. Road accidents have become a common incident today. Thousands of people die daily in road accidents due to human error, and hundreds of passengers suffer from average or fatal injuries. Populated cities have a traffic jam problem, generating many other issues that severely affect health. The most common issues are the loss of precious time in traffic and the tremendous fuel, which ultimately increases CO₂ emission [2]. The vehicular ad-hoc network aims to reduce the number of accident cases, improve users' safety, and improve passenger comfort. Almost 70% of the errors can be avoided if the driver is warned at least a few seconds before the incident. Road safety can be improved by decreasing traffic crashes. Traffic crashes result in congestion, which has become problematic and time wastage, especially in the bigger cities. Due to traffic congestion, total loss is over \$124 billion [3]. The main objective of VANET is to improve traffic safety by broadcasting real-time information to drivers. Textual communication among vehicles is not always trustworthy. We need to take rapid action in many emergencies like accidents, traffic jams, and poor road conditions. In this Section, we introduce our research, video streaming, emergency surveillance, and blockchain technology. This section concerns motivation, problem statement, research question, research contribution, and thesis outline [4]. Vehicular networks will be as prevalent in the future as smartphones are now. Vehicles will come with a variety of sensors, some level of computational power, and can communicate with other vehicles and, if any, the infrastructure that is currently in place. They'll be able to gather data, develop it, and disseminate it. Intelligent Transport Systems (ITS) will be made practicable as a result. Video streaming is one of the applications for VANETs. A wide range of VANET applications include travel information, contextual advertising, digital entertainment, video on demand, and others about security issues, such as emergency video calls, etc., connected to video streaming. Real-time information will be used and delivered via vehicular networks with video streaming services for safety and practical purposes. Video streaming in real-time will significantly improve the quality of the user's experience because it will give them more visibility into their surroundings, the state of the traffic, the ability to use applications like emergency video calls, etc. This poses a significant challenge for VANETs [5]. It is a hostile environment for any data transmission, particularly video transmission (many packet losses, mobility of the nodes, etc.). As a result,

researchers have concentrated on enhancing and optimizing video communication. Unfortunately, it has not been simple to assess video transmission performance. Video streaming strengthens the VANET by increasing the coherence of emergency response in the event of an accident or other incident and by broadcasting real-time video from the scene of an accident to the adjacent vehicles. Several obstacles must be overcome to disclose higher-quality films to moving vehicles, including the network's dynamic architecture and high mobility. The Doppler Effect, attenuation, packet loss, quickly changing network topology, and many other issues can occur in VANETs [6]. Additionally, the daily operation of the video streaming process requires enormous resources. These two underlying assumptions make it clear that video streaming over VANETs is a demanding operation that must be accomplished. Therefore, to guarantee the lowest possible Quality of Experience (QoE), further research is needed on the constraints of video Streaming over VANETs and the error resilience measures that must be used [7]. The primary goal of this study is to increase the trust mechanism between V2V and V2I communication by broadcasting video streaming of emergency conditions to all the connected vehicles. We used a 5G network to broadcast and receive video streaming data. Blockchain technology has been used widely for data security in many fields. We used Blockchain for the security of video-streamed data to maintain its privacy.

VANET and its components

VANET emerged from MANET, having a wide range of implementations in making transportation systems smart and intelligent. It can transform the traveling and driving abilities of people. VANET vehicles can broadcast emergency messages and road conditions via V2V and V2I communication. ITS was implemented using VANET. All the significant traffic alarming messages like traffic jams, obstacle detection, and road accidents are broadcasted by VANET to avoid terrible traffic situations by notifying the drivers. VANET infrastructure is formed using roadside units (RSU) and onboard units (OBU) inside the vehicle. RSU is a computational device located on the sides of a road that provides connectivity support to moving vehicles [8]. The roadside unit's (RSU) significant responsibility is to provide an internet connection to onboard units (OBU) and safety applications and extend the communication domain. All the warning and alert messages are forwarded and received by a vehicle connected to OBU. There are three main VANET parts. These are the Application Unit (AU), Onboard Unit (OBU), and Roadside Unit (RSU) [9]. The application unit is a device installed within the car and uses the

OBU's communication capabilities to communicate with the applications the user provides. Road Side Unit devices are fixed on the sides of the road or improved to a certain point, like parking areas. Roadside units are static or fitted devices beside the highways to link and support these devices for specific access and scenario-based communication infrastructure. Every vehicle has a unit that is the hardware used for communication and other purposes. OBU offers connectivity so various RSUs, other communication devices, and other life elements can exchange information. The transceiver and other devices are linked and offer improved communication information [10].

Background

5G in VANET

5G is fifth fifth-generation cellular network. The growth of vehicle ad hoc networks (VANETs) will be considerably aided by the fifth generation (5G) mobile communication technology, which has increased capacity and data rate, ultra-low device-to-device (D2D) latency, and extensive device connectivity [11]. It is the latest global wireless network after 1G, 2G, 3G, and 4G networks. It is designed to virtually connect everything, like machines, devices, and objects. 5G aims to deliver higher data speeds, high bandwidth, ultra-low latency, higher network capacity, and excellent reliability [12]. It is designed to provide higher connectivity which was never available before. 5G is used across significant connected services: enhanced mobile broadband, mission-critical communications, and the Internet of Things. 5G is meant to make our smartphones better. This innovative mobile technology can provide uniform experiences like virtual and augmented reality with faster data rates, low latency, and reduced cost per bit. The combination of 5G networks with vehicular ad-hoc network results in intelligent transportation, improved safety services, and entertainment services in the vehicle, so as a result, a group of connected devices (vehicles, mobile phones, control devices, and other communication devices/sensors) will get advantage from un-loading of network data on unlicensed bands [13]. There is a rapid increase in the global Internet of vehicles, increasing its value in the coming years. VANET plays a crucial role in the development of ITS, as communication of vehicles with each other. This research proposed a model for integrating 5G and Blockchain to manage VANET.

VANET video streaming for vehicles and emergency surveillance

Video streaming is one of the data that needs to be securely handled through VANET. Video streaming data consisted of important emergency messages and driver video briefings for road conditions. Video Streaming

Data Consisted of Road Conditions, accidental conditions, congested traffic, Military and Govt. messages. High-quality video streaming over VANET is one of the most popular on-road entertainment applications for passengers. Still, video streaming of road conditions is also essential in VANET to avoid any terrible situation. Real-time video streaming has been designed to improve both traffic efficiency and road safety [14]. By adding video streaming features in VANET, it improves existing vehicular networking infrastructure and applications and also encourages a variety of other features to strengthen, like accurate time traffic condition monitoring, vehicle crossing assistance, and multimedia data delivery between connected vehicles [15]. Safety and non-safety-related applications are supported by VANET that need the transmission of emergency safety and periodic beacon messages. Imagine vehicles moving on motorways on two different lanes [16]. If there is an accident in lane 1, vehicles near that place will record the accident video and broadcast it to the VANET with the warning message to change lane.

Security of emergency video sharing

Blockchain technology is a collection of records connected, strongly resistant to alteration, and protected by cryptography. A hacker cannot alter data in the Blockchain because every customer has a copy of the ledger, and complex algorithms encrypt the data within the block. There are two keys for every user: private and public keys [17]. We can assume the public key is an address that everybody knows, like our email address and the private key is like a different address that only the user knows about, like our email password. A blockchain can record information about crypto-currency transactions, trustworthy message dissemination in vehicular ad-hoc networks, and smart contracts without third-party interference. Conventional data can also store such type of information, but the Blockchain is decentralized, and it is its uniqueness. Instead of being sustained in one location only, by a centralized administrator, for example, think of an Excel spreadsheet or a bank database. Multiple computers hold identical copies of a blockchain spread across a network. These individual computers are referred to as nodes [18].

In real-world VANET settings, the communication between V2V and V2R links occurs in wireless communication in an open environment. Due to the danger that hostile parties could intercept or counterfeit the sent vehicular information, there are serious security and privacy implications. Secrets shared by users and important keying information may be illegally disclosed to opponents [19]. This could compromise the VANET system as a whole. In this situation, appropriate security

preservation and privacy protection procedures must be implemented in VANETs. Academics and businesses are paying close attention to pertinent studies on secure VANET transmission. Mutual authentication occurs between the vehicle and roadside unit, followed by a session essential distribution process for vehicles verified in various schemes using different safe methodologies and cryptographic approaches. The RSU intends to distribute group key sharing to nearby cars. As a result, the V2V and V2R communication channels are both supported by the universal group communication channel. In other words, the group channel exchanges data between the nearest vehicles and transfers data from the vehicle to the central server. Both. The high mobility feature of the group key may be modified or changed at any time. We utilize blockchain technology to secure VANET video streaming data to maintain its integrity [20].

Studies on blockchain technology have so far received a lot of attention. Blockchain can be used in various Internet of Things scenarios because of having clear advantages in decentralized data exchange. The capacity of blockchain technology to secure automotive data across a tamper-proof decentralized ledger has recently been the subject of several initiatives. The Bitcoin cryptocurrency is based on the emerging decentralized and distributed computing paradigm known as Blockchain, which can offer security and accountability in peer-to-peer networks. It might occasionally support the issues related to privacy alongside cryptographic improvements [21]. Numerous attempts have been made to apply a blockchain-based VANET application because, since Bitcoin introduced it, of advanced beyond cryptocurrencies to carry the deployment of more general-purpose distributed applications in various fields. Currently, there are four types of blockchain networks: consortium blockchains, hybrid blockchains, public blockchains, and private blockchains. These have been used in a variety of communication scenarios. The consortium blockchains, in particular, have a great potential for adoption in V2V group communications since they assign the pre-selected user group to construct decentralized paradigms for collaborative data exchange. All legal vehicles can dynamically manage and store the records of a shared group membership. To preserve conditional privacy, it is essential to note that historical group communicating records can be verified and tracked [22].

Machine learning to control emergency video streaming

The machine learning mechanism comprised of three main parts which are;

- A Decision Process: Generally, predictions or classifications are made using machine learning algorithms.

The algorithm will approximate a given pattern used in the data input, which may be labeled or unlabeled.

- The error function measures the accuracy of the model's prediction. It can compare examples to gauge the algorithm's correctness if examples are already known.
- Optimization of models: Weights are changing to reduce differences between the known example and the estimated model if there is a more accurate match in the training set of data points. The algorithm will repeat this "evaluate and optimize" procedure, with weights being updated automatically until a predetermined level of accuracy is reached.

In VANETS, textual communication between V2V and V2I cannot be trustful by some other vehicles in the network all the time. Video streaming in VANETS will be more innocent. Emergency services like ambulances, fire brigades, and military convey need clear roads to reach their destination faster. We will use video streaming in VANETS by implementing it with Blockchain and 5G to deliver video packets to nearby vehicles to clear their way. VANET is one of the most demanding environments for intelligent vehicles. Today's modern data management and communication are easily possible through the VANET. The VANET provides support for multimedia data. Inside the multimedia data, video streaming is also one of the demanding needs for VANET handling. Content management and content delivery for video streaming is one of the most challenging features of the VANET [23]. The proposed mechanism helps the VANET efficiently deliver video-streamed data. Based on the research problem, some identified research questions need to be addressed.

1. How can video streaming be handled during V2V and V2I in a VANET environment?
2. How does Blockchain help to secure the VANET streaming data to maintain the integrity of data?
3. How to detect events from the video messages through proper video frame transformation?

Research contributions

This underlying work has the following major contributions in the research domain.

- This research improves the emergency video streaming data communication in VANET by integrating 5G and Blockchain. It provides secure content management of video-streamed data in the VANET environment.

- It contributes to the Emergency services like ambulances, fire brigades, and military conveys that need clear routes to reach their destination faster. The Vehicles in VANET broadcast emergency messages with live evidence, so if a vehicle does not respond according to the situation, it will suffer plenty from the network.
- This research contributes to detecting specific events from the video messages through the aligned video frame transformation.

Paper organization

Background section reviews the literature work. We have illustrated the key components and workings of our proposed solution in **Literature survey** section. This section has four components that are supported by the related algorithms at appropriate places. In **Proposed model** section, the secure video encoding section, we use blockchain to secure the video for blockchain. Furthermore, in this section, we implement the detection events from the video messages through proper video frame transformation through a 5G network. In **Proposed model** section, we present the Secured video encoding method, that we followed, and is further divided into eight subsections. In this section, we handle vehicular communication using V2V and V2I communication architecture. In this section, we further provide video streaming. This section's presentation is supported by the related algorithms and necessary illustrations. Performance evaluation is done in **Secure video encoding** section followed by conclusion and future directions in the subsequent section.

Literature survey

There are various applications of Real-time video broadcasting over VANETs: live transmission of emergency video, video streaming between vehicles, and many other domains [24]. Video streaming in VANETs focused on real-time video streaming, emergency services, bandwidth allocation, storage optimization, and video packet scheduling. There is a comparison of literature on video streaming models over VANETs. Video streaming in VANETs is considered a future research direction. Different use cases of video streaming, like pedestrian crossing assistance, overtaking scenarios, and video communication for entertainment, are discussed [25]. For drivers, other services can be used by applying real-time video transmission over VANET: conference calls, games, video-on-demand, and others.

Privacy and security issues in VANET

A blockchain-based security framework has been developed to analyze the privacy and security issues in 5G-VANET to support vehicle IOT services. It brings additional cloud-based video reporting and vehicle message trust management. The results of simulations demonstrate that fraudulent vehicle messages can be easily spotted. They designed a trust management system by utilizing Blockchain. Regular elections are conducted using two consensus mechanisms: proof of work and proof of stake. The privacy of legitimate vehicles is protected by eliminating malicious nodes. A semi-centralized video and road status trust management system is created and simulated based on centralized authentication and blockchain distribution trust management. Kestrel, a cloud-based video gathering and analysis system, leverages low-cost visual characteristics to extract attributes [26]. Each vehicle is registered through the vehicle registration algorithm. Every vehicle in the VANET has a 5G SIM (subscriber identification module). A unique ID and the SIM number identify each vehicle. Dnum is used to represent the device number. When a new vehicle (Vm) joins the system, it will not be available until the operator has confirmed its Vm device number. Its ID matches and none of them can be changed. A unique symmetric key SKE is randomly generated for the registration procedure by Vm. When the vehicle is registered, during the drive, the VM uses its visual sensor camera installed on OBU to record video files of the road conditions and estimate their message digest. This practice is repeated as a term every minute. Recorded video is encrypted using the symmetric key, and then it is broadcast after verification of the public key certificate of the vehicle. A vehicle must post important messages to other adjacent or nearby vehicles, such as its driving operations and the conditions of the road, in addition to reporting video records about itself. As part of the message delivery process, vehicles evaluate the trustworthiness of the road condition and rank it. It is possible to provide a score of +1 or -1. The Road Side Unit (RSU) receives messages, verifies the message's origin, and then organizes the information about the state of the road into categories based on where it is about the road area. The reliability of the scoring will decline if the scoring vehicle is located distant from the broadcasting vehicle. Thus, this score is considered reliable if the trust value is more than 0.5. The primary performance metric is message detection accuracy (MDA), which is stated in Eq. 1.

$$MDA = \frac{(TP + TN)}{(TP + FN + FP + TN)} \quad (1)$$

Here, MDA is Message Detection Accuracy, TP is confirmed positive, TN is true negative, FN is false negative, and FP is a false positive value.

L. Xie et al. [27] consider the 200 to 500-vehicle range to analyze the network performance. Vehicles considered are uniformly distributed and have speeds in different directions, approximately 110km/h. Vehicle to network (V2N) communication range is set at 100 m, while vehicle to vehicle (V2V) communication range is set at 50 m. The hash algorithm utilized in the Blockchain is SHA-256. To determine whether the network can support the video report service, three video encryption algorithms-AES/CBC (256-bit key), Two fish/CTR (256-bit key), and Serpent/CTR (256-bit key)-were examined for their time overhead. Blockchain produces better outcomes for the detection of rogue vehicles. The network will experience increased traffic if the message rate of each car rises since more messages must be transmitted, and more transactions must be broadcast. A rate of at least one per minute can ensure the message's efficacy in real-time. The transmission delay is accepted if the message rate is 10 per minute. This is because of the high bandwidth of 5G in VANET. The range of time overhead for encryption of video is about 20 milliseconds to 160 milliseconds. Theoretical and experimental results show the framework efficiency, which enhanced the detection of malicious nodes.

All the above research papers contribute to improving video streaming in VANETs. Different simulation tools were used to implement their concepts. All the researchers work on various communication modes. One of them produces a protocol enabling efficient real-time video delivery with quality of experience awareness and better video quality in VANETs. Another focuses on how real-time video streaming can be supported with IEEE 802.11p, LTE, and LTE Direct networks. Some of them contribute to improving video delivery performance, reducing frame loss increasing packet delivery ratio, and enhancing peak signal-to-noise ratio and video quality. In addition to these, It also works for reducing the impact of interference, maximizing the effecting transmission rates, improving stress as well as traffic flow, achieving continuous video delivery, and enhancing the performance of multimedia services.

The integration of deep learning and blockchain technology into vehicular ad hoc networks (VANETs) for secure emergency video streaming in 5G environments is a burgeoning area of research. VANETs play a critical role in facilitating communication among vehicles and infrastructure, particularly in emergency scenarios where real-time video streaming is vital for situational awareness. Deep learning techniques have shown promise in

enhancing video processing tasks such as object detection, classification, and tracking, thereby improving the efficiency and accuracy of video streaming in VANETs (Zhang et al., 2020). By leveraging deep learning algorithms, vehicles can better analyze video data and make informed decisions during emergencies. Moreover, the integration of blockchain technology adds an extra layer of security and trust to the communication process in VANETs. Blockchain ensures data integrity, confidentiality, and accountability by decentralizing control and providing tamper-resistant data storage [22]. This decentralized nature of blockchain ensures that emergency video streams are securely transmitted and stored, reducing the risk of data manipulation or unauthorized access. Research by [28] demonstrates the potential of combining deep learning and blockchain in VANETs for secure emergency communication. Their proposed approach employs deep learning algorithms for real-time video analysis and blockchain for secure data transmission and storage. By utilizing blockchain's distributed ledger technology, the integrity and authenticity of emergency video streams are preserved, enhancing the overall reliability and trustworthiness of the communication system. The integration of deep learning and blockchain technology holds great promise for enhancing the security and efficiency of emergency video streaming in VANETs. Future research in this area should focus on optimizing the performance of deep learning models for resource-constrained vehicular environments and further exploring the potential applications of blockchain in ensuring the integrity and security of emergency communication systems.

The integration of deep learning and blockchain technology has garnered significant attention in recent years, particularly in the context of enhancing secure emergency video streaming within Vehicular AdHoc 5G Networks (VANETs). Authors in [29] explored the application of deep learning techniques, specifically Farneback Optical Flow, in VANETs to improve the accuracy of emergency video streaming, achieving a commendable 91% accuracy. Authors in [30] extended this research by implementing convolutional neural networks (CNNs) for video analysis within VANETs, achieving an 85% accuracy rate. [31] further advanced the field by utilizing CNNs and achieving a notable accuracy rate of 95.21% in emergency video classification tasks. Masood et al. [32] contributed to this area by employing deep learning methodologies, achieving a competitive accuracy rate of 92% in emergency video streaming. [33] took a different approach by combining ResNet and SVM algorithms, achieving an impressive accuracy rate

of 94.14% in VANETs. [34] continued to explore the effectiveness of CNNs in VANET environments, reporting a promising accuracy rate of 92.38% in their study. In response to the growing demand for secure emergency video streaming in VANETs, researchers have begun to leverage blockchain technology. The proposed methodology by the authors introduces a novel approach that integrates ResNet-50 and SVM algorithms, leveraging blockchain technology for enhanced security measures. The methodology achieves a remarkable accuracy rate of 98%, surpassing previous studies in the field. Additionally, the incorporation of blockchain ensures data integrity, transparency, and decentralized control, mitigating potential security risks within the VANET ecosystem [35]. This approach addresses critical challenges in VANETs, such as ensuring the authenticity and reliability of emergency video streams, thereby enhancing overall safety and security in vehicular communication networks. The contributions of the proposed research are significant, offering a comprehensive solution that combines advanced deep learning techniques with blockchain technology to address the complexities of emergency video streaming in VANETs [36]. By achieving a high level of accuracy and ensuring data security through blockchain integration, the proposed methodology sets a new standard for secure communication and emergency response systems in vehicular networks. Future research in this area may focus on further optimizing the integration of deep learning and blockchain, exploring additional use cases, and evaluating the scalability and efficiency of the proposed approach in real-world VANET deployments [16].

Proposed model

The strategy proposed in this study is a secure emergency video streaming approach in VANETs through a 5G network. The fundamental objective of this study is to address the video streaming advantages of VANETs compared to traditional textual warnings. Video streaming in vehicular ad-hoc networks is a challenging task, certainly when we want only that part of video frames where the actual emergency event occurred. VANETs are uninviting networks due to wireless transmission and relatively high speed between the nodes. Many problems arise, like attenuation, Doppler Effect, packet losses, and quickly varying network topologies. Moreover, video streaming is a highly resource-demanding task. In our proposed methodology, visual sensors and cameras inside onboard units will record the video of real-time road conditions and emergency events. After recording the video, the first layer, the frames conversion layer, will convert the whole tape into frames. The frames detection algorithm will detect the specific event from the video frames. Then in the second layer of our proposed

framework, the Blockchain will encrypt the emergency or particular event using specific hashing algorithms. In the third layer of the suggested methodology, encrypted video is then broadcasted with the help of 5G wireless technology to the connected nodes in the vehicular ad-hoc network. In the next section, we will explain all three layers in detail.

Video recording procedure

The camera is placed on the OBU of each vehicle, so wherever the article goes, it records the video of the entire path travelled with them. It will record all the significant events like emergency recording, road conditions, and traffic scenarios. The footage is recorded continuously and is saved to vehicle memory after every two minutes. The recorded video file will be in the vehicle memory for the next phase.

Convolutional frames

When the video is recorded and saved in the vehicle memory, the next aim of our research is to convert that video file into video frames. We want only that part of the recorded video containing special events like accidents, poor road conditions, ambulance on the way, fire brigade or army conveys, etc. Cameras placed on OBU will record and save the video file after every two minutes. We are interested only in detecting and broadcasting only emergency-related video frames. So we will use the frames detection algorithm to get only desired emergency-related video frames and discard the unnecessary data. The frames conversion layer is responsible for detecting emergency events. This process consists of four phases.

Preprocessing

In preprocessing, we will extract desired critical frames from the recorded video. For this purpose, firstly, changing scene videos are broken down into smaller video clips. Then from every smaller video clip, frames are extracted. The same is presented in Algorithm 1.

Algorithm 1 *FRAME EXTRACTION*

INPUT: INPUT VIDEO

```

1: procedure FRAMES (input)
2: video_Object ← cv2.VideoCapture (input)
3: temp_cont ← 0
4: get frame ← 1
5: while getframe == 1 do
6: getframe, image ← video_Object.read ()
7: cv2.imwrite ("frame%d.jpg"%temp_cont, image)
8: temp_cont ← temp_cont + 1
9: end while
10: end procedure

```

Finally, desired emergency eventual frames are removed from these frames for further processing. Frames are individual pictures in a sequence of images.

Feature selection

After the preprocessing phase, feature extraction is performed to detect emergencies, accidents, poor road conditions, and stormy weather that can cause massive damage to other nodes in the VANET environment. So, accurate feature extraction is essential (Algorithm 3). We will deploy the deep learning architecture ResNet50 for this purpose. ResNet stands for Residual Network and is a particular type of neural network introduced in 2015. ResNet50 architecture will be initiated and initialized with the already trained model on Image Net.

Algorithm 2 RESNET50 FEATURE EXTRACTION

INPUT: DESIRED FRAMES
OUTPUT: RESNET50 EXTRACTED FRAMES
 1: Transfer_learning_model=Resnet 50
 2: target_size=224,224,3
 3: Preprocess_frames=img_preprocess (input)
 4: Transform_frames= Preprocess_frames into grayscale
 5: convert_to_array=img_to_arr (Transform_frames) convert image to array
 6: pre_trained model. Predict () extract features from input frames
 7: X = [] list of features
 8: Save(X)
 9: End

Secure video encoding

In this portion, we will discuss different components and working of proposed models and their details. The process starts with the input data in the form of videos and ends with the classification results of the support vector machine algorithm. The proposed method begins with feeding input videos to the proposed system. After that, the video change is identified using a standard Python library called Pyscene Detect. It is a command-line utility and Python library that scans a video for scene transitions and cuts. PySceneDetect works with external tools to intelligently break the video into separate pieces when using the split-video command. A stats file, a frame-by-frame evaluation of a video, can also be created to assist in choosing the best threshold levels or other analysis techniques for a specific video. PySceneDetect employs two primary detection techniques: detect-threshold, which compares every frame to the predetermined black level and is beneficial for identifying cuts and fades to/from black, and detect-content, which compares each frame and looking for changes in content, helpful in detecting fast cuts between video scenes, although it slower to process of detection. Every model offers a few marginally various parameters that are used according to the nature of the problem. Below are the steps that provide secure video encoding.

- Apply robust encryption algorithms to encode video data, ensuring confidentiality.

- Attach digital signatures to verify the authenticity of video streams, preventing tampering.
- Utilize blockchain technology for decentralized authentication and data validation.
- Implement access control protocols to restrict video access to authorized entities only.
- Employ secure transmission protocols (e.g., HTTPS) to safeguard video data during transmission.
- Embed unique identifiers or watermarks in video streams for traceability and copyright protection.
- Introduce multi-factor authentication mechanisms for enhanced user verification.
- Store encoded video data in secure repositories with access controls and backup mechanisms.
- Conduct regular security audits to identify and address vulnerabilities in the encoding process.
- Ensure compliance with industry-standard security protocols and regulations to maintain data integrity and privacy.

Algorithm 3 DESIRED FRAME EXTRACTION

1: Proc HISTOGRAM DIFF (Img i, Img j)
 2: Transform i and j into grayscale
 3: Calculate the histogram (Hi and Hj) for images i and j
 4: Find variation between histogram Hi and Hj
 5: Find the sum of differences "DS."
 6: if $DS \geq$ Threshold value
 7: Return i as Desired Frame
 8: end if
 9: end procedure

After the Scene detection, video frames are extracted using the OpenCV module, as illustrated in Fig. 1. A Python package called OpenCV makes it possible to carry out image analysis and computer vision tasks. It offers diverse applications like tracking, face recognition, object detection, etc. For desired frame extraction, three methods were used (Algorithm 2). These methods include histogram, object detection, and Difference estimation. These techniques are applied to extract more relevant frames from the videos removed by the PyScene detect library. The steps for this process are listed below

- The first file video is loaded by using cv2.VideoCapture()
- Then read video frames by using cv2.VideoCapture.read()
- Apply Difference Estimation, Histogram difference, and object detection
- Then write each frame by using cv2.imwrite()
- Release the Video Capture object by using cv2.VideoCapture.release()
- Finally, Exit the window and then destroy all the windows using cv2.destroyAllWindows()

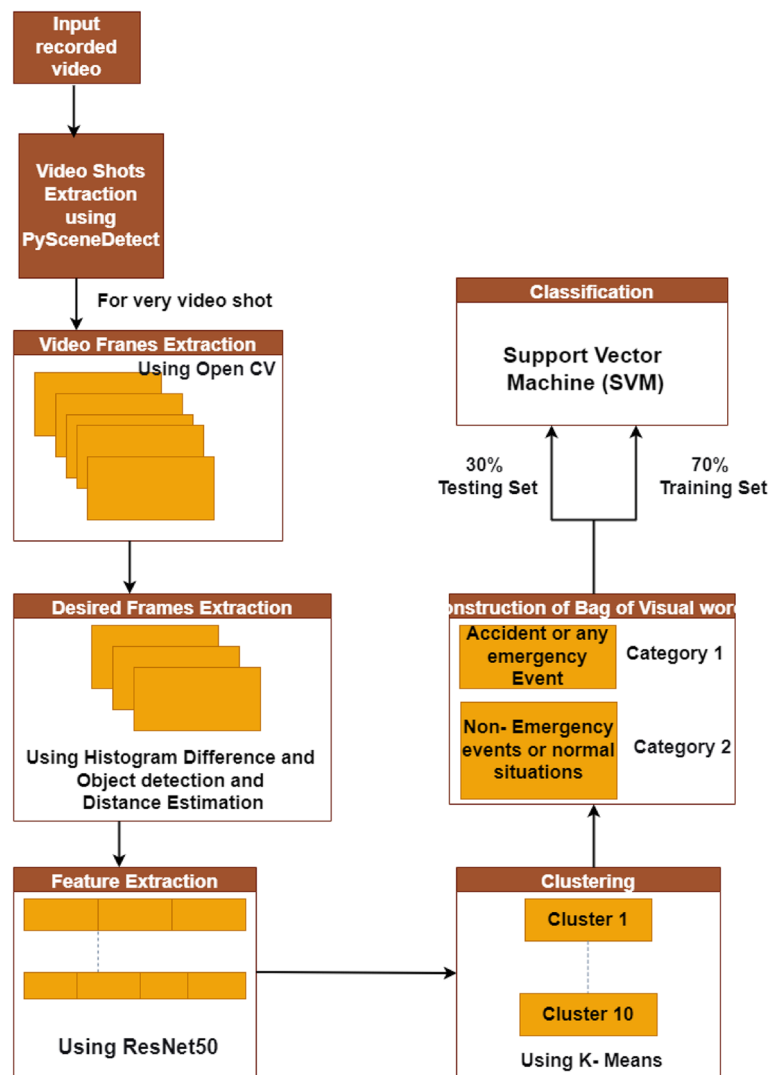


Fig. 1 Schematic Diagram of the Proposed Work

After the successful extraction of frames, deep learning is applied for feature extraction of extracted frames. We used the ResNet50 model for this purpose. Kaiming et al. present a study in 2015 in which they introduce the deep residual learning technique to do better image processing tasks. ResNet is a convolutional neural network (CNN) variant with 50 layers. It is widely used for image processing and computer vision tasks. The 50-layer convolutional neural network ResNet-50 contains 48 convolution layers, one MaxPool layer, and one average pool layer. Neural networks that use layers to build networks are residual neural network models. For the implementation of ResNet-50, we used Tensorflow and Kear’s frameworks.

Clustering

Unsupervised machine learning techniques like clustering are used. It is the method in which we can draw references from datasets comprising the input data without any labeled responses. Specifically, it is used to find meaningful structure, explanatory underlying processes, and generative features. Clustering is the process of dividing the population or data points into various groups such that data points in similar groups are more similar to those in the same group and dissimilar to the data points in different groups. Clustering is a collection of objects based on similarities and dissimilarities among them. In our proposed system, the clustering phase will make a Bag of Visual Words (BOVW) from the features extracted from the videos.

We deploy K-means clustering for the purpose mentioned above.

K-means clustering is the most straightforward unsupervised learning technique in which k refers to groups based on their characteristics. It needs unlabeled data to train. K-means clustering can gradually learn how to cluster the unlabelled data points into groups by analyzing the mean distance of input points (Algorithm 4).

Algorithm 4 K-MEANS CLUSTERING

```

1: Select Number of Clusters= $K$ 
2: Input= $X$ [features]
3: Randomly set the centroids= $c_1, c_2, c_3, \dots, c_k$ 
4: Repeat steps 4 and 5 until convergence
5: for each data point  $x_i$ : Find the nearest centroid ( $c_1, c_2, \dots, c_k$ ) Assign data points to cluster
6: for every cluster  $i = 1$  to  $j$  new_centroid = mean of cluster's data points
7: End

```

Bag of visual words construction

We will apply k-means clustering to get BOVW. We will make 5 to 10 clusters for every video. After this, each cluster's centroid is included in a vector to get the final version of BOVW. This process will be carried out for all the data sets. The data set is split into 70% for training data and 30% for testing it.

After the selection of the dataset for training and testing the classification in machine learning is performed which refers to the predictive modelling problem where a specific label is predicted for the provided input data. For example, given data is to check whether email is a scam. In our proposed system, we will use classification for correctly classifying the data from video to detect emergency events. It will try to determine whether the emergency-related event occurs in its nearby environment in VANETs. A support Vector Machine (SVM) classifier is used for this work.

SVM is a supervised machine learning model that utilizes classification and regression algorithms. The idea of a support vector machine is straightforward. This algorithm generates a line that separates the data into classes (Algorithm 5). SVM will classify the recorded video data into emergency events, if any, from the extracted frames. When we get the emergency-related frames, we will use them for the next phase, securing all that data via Blockchain, as shown in Fig. 2.

Algorithm 5 SVM CLASSIFICATION

```

1: Import Sklearn
2: Class SVM [features, Labels]
3: Preprocess ← (features, Labels)
4: Encoding ← (Labels)
5: Data,  $splitting = X_{train}, X_{test}, train_y, test_y, train, est, split(features, Labels, testsize = 0.3)$ 6 : def model :
7: Model ← SVC ( ) initialize the model 8: Compile ← SVC. Compile ( )
9: Fit Model ← SVC.fit ( $x_{train}, y_{train}$ ) Fitting the model
10: Predict ← SVC.predict ( $X_{test}$ ) Prediction
END Class

```

The algorithm starts by taking a video sequence as input, and then extracts frames using OpenCV. Each frame undergoes preprocessing for consistency. Pre-trained RESNET50 is used to extract features from frames, stored in NumPy arrays. These features enable deep learning tasks like classification or clustering, enhancing secure emergency video streaming in Vehicular AdHoc 5G Networks. Algorithm 6, provides the frames extraction through the RESNET50.

Algorithm 6 Frames Extraction through the RESNET50

```

1: Input a video sequence.
2: Extract frames from the video using OpenCV.
3: Preprocess each frame to ensure consistency and compatibility.
4: Utilize the pre-trained RESNET50 model to extract features from each frame.
5: Extracted features are then stored in NumPy arrays for further analysis and processing.
6: These features serve as inputs for subsequent deep learning tasks, such as classification or clustering.
7: The process ensures efficient utilization of RESNET50's capabilities for frame-level feature extraction, contributing to the enhanced secure emergency video streaming approach in Vehicular AdHoc 5G Networks. END Class

```

Blockchain adaptation layer

When the desired video frames are detected, they are extracted using machine learning techniques. After extraction, the video file is encrypted using a video encryption algorithm. Blockchain is used for the privacy and immutability of video data. In the proposed methodology, blockchain technology is harnessed to bolster the security of emergency video streaming in Vehicular AdHoc 5G Networks (VANETs). Through blockchain integration, each video stream transaction is cryptographically secured and recorded across multiple nodes in a decentralized ledger. This ensures the integrity and transparency of the data, mitigating risks of tampering or unauthorized access. Moreover, smart contracts can be employed to automate and enforce security protocols, such as access control and data validation, further enhancing the security framework. The decentralized nature of blockchain eliminates single points of failure and vulnerabilities, providing robust protection against malicious attacks. To illustrate, consider a pictorial representation where each video stream transaction is represented as a block in a chain, with cryptographic hashes linking them together. Each node in the VANET network maintains a copy of the blockchain, ensuring redundancy and reliability. Smart contracts govern access rights and validate incoming data streams, ensuring only authorized entities can access and transmit emergency video feeds. Overall, blockchain technology acts as a foundational layer of security, bolstering the resilience and trustworthiness of emergency video streaming in VANETs.

Blockchain is used for the security of sensitive video data. The integration of deep learning and blockchain technology into vehicular ad hoc networks (VANETs) for secure emergency video streaming in 5G environments

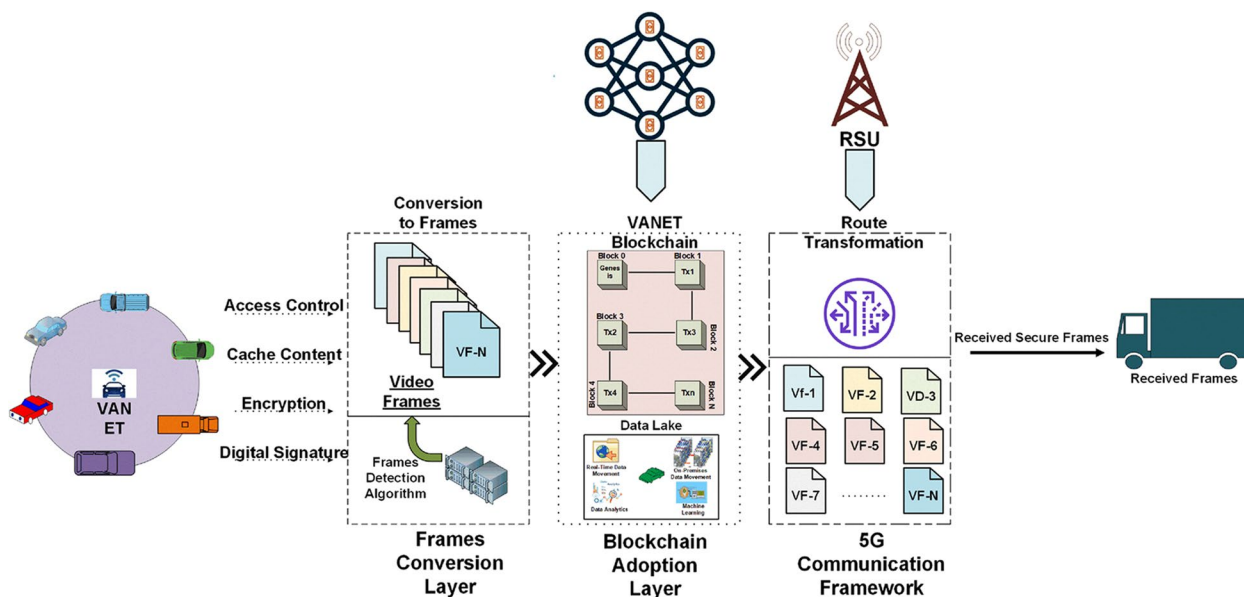


Fig. 2 Block Diagram of Proposed Model

is a burgeoning area of research. VANETs play a critical role in facilitating communication among vehicles and infrastructure, particularly in emergency scenarios where real-time video streaming is vital for situational awareness. Deep learning techniques have shown promise in enhancing video processing tasks such as object detection, classification, and tracking, thereby improving the efficiency and accuracy of video streaming in VANETs (Zhang et al., 2020). By leveraging deep learning algorithms, vehicles can better analyze video data and make informed decisions during emergencies.

The proposed scheme integrating deep learning and blockchain technology presents a sophisticated solution for ensuring secure emergency video streaming within Vehicular AdHoc 5G Networks (VANETs). At its core, deep learning algorithms are utilized to enhance the security measures of the system, enabling robust identification and mitigation of potential threats. This integration allows for the real-time analysis of video streams, facilitating prompt decision-making in emergency scenarios. Leveraging blockchain technology further fortifies the security framework by establishing a decentralized and immutable ledger for transaction verification and data integrity maintenance. Through blockchain, each transaction within the network is cryptographically secured and recorded across multiple nodes, ensuring transparency and preventing unauthorized tampering. The decentralized nature of blockchain also enhances reliability, as there is no single point of failure vulnerable to malicious attacks. Additionally,

smart contracts can be employed to automate certain processes, such as access control and resource allocation, streamlining operations within the network. Illustratively, consider a scenario where a vehicle encounters an emergency, such as an accident. The deep learning algorithms swiftly detect the anomaly and trigger the emergency video streaming protocol. Simultaneously, blockchain technology verifies the legitimacy of the request, ensuring that only authorized entities can access the video feed. As the video stream is transmitted across the VANET, each node in the network securely records the transaction on the blockchain, maintaining an immutable audit trail. Consequently, emergency responders receive real-time, authenticated video footage, enabling them to assess the situation accurately and initiate timely interventions. This symbiotic integration of deep learning and blockchain technologies establishes a robust and resilient framework for secure emergency video streaming in VANETs, fostering safer and more efficient communication within the network.

5G communication framework

Now the video is ready to be broadcast to the vehicular ad-hoc network. Video data needs more powerful wireless technology to transmit data faster. We use 5G technology to promote the video data to all the connected vehicles and RSU. We are adopting 5G technology because of its peak data speeds, massive network capacity, low latency, and increased availability. All the connected vehicles will receive video messages. After

receiving the emergency alerts with video streams, vehicles will respond accordingly.

Inside the vehicle, OBU has a sensory module with visual sensors installed. Optical sensors will perform real-time monitoring of road conditions via video. There is also a checking unit to check whether the visual sensors are working correctly or not. If the visual sensors are not working properly, OBU will be informed. Video files are saved continuously in the vehicle's memory. The detection unit will detect the specific event frames from the video using machine learning algorithms. When the frames are detected, then these video frames are extracted from the full video. After extraction, video frames are secured using Blockchain technology to avoid alterations in the video data. When the video frames are secured, they are transmitted to the vehicular ad-hoc network using 5G technology. Figure 3 illustrates the flowchart of the proposed work.

Performance evaluation

All the experiments related to the proposed model are used to secure the video transmission through 5 G-enabled messages of the vehicular nodes. Blockchain distributed ledger is applied to store secure data through 5G communication architecture. Moreover, deep learning algorithms and machine learning classify accidental and non-accidental situations in any VANET environment. In this section, the evaluation of the discussed framework is discussed.

System implementation

A system used for simulation purposes is corei7 7th generation with 16GB RAM, 512GB SSD, and 4GB Nvidia GPU. The tools used for simulation purposes are Anaconda and Python 3.9. Various libraries were used during the simulation, including TensorFlow, Keras, PyScene Detect, Sklearn, OpenCV, Pandas, and Numpy [37].

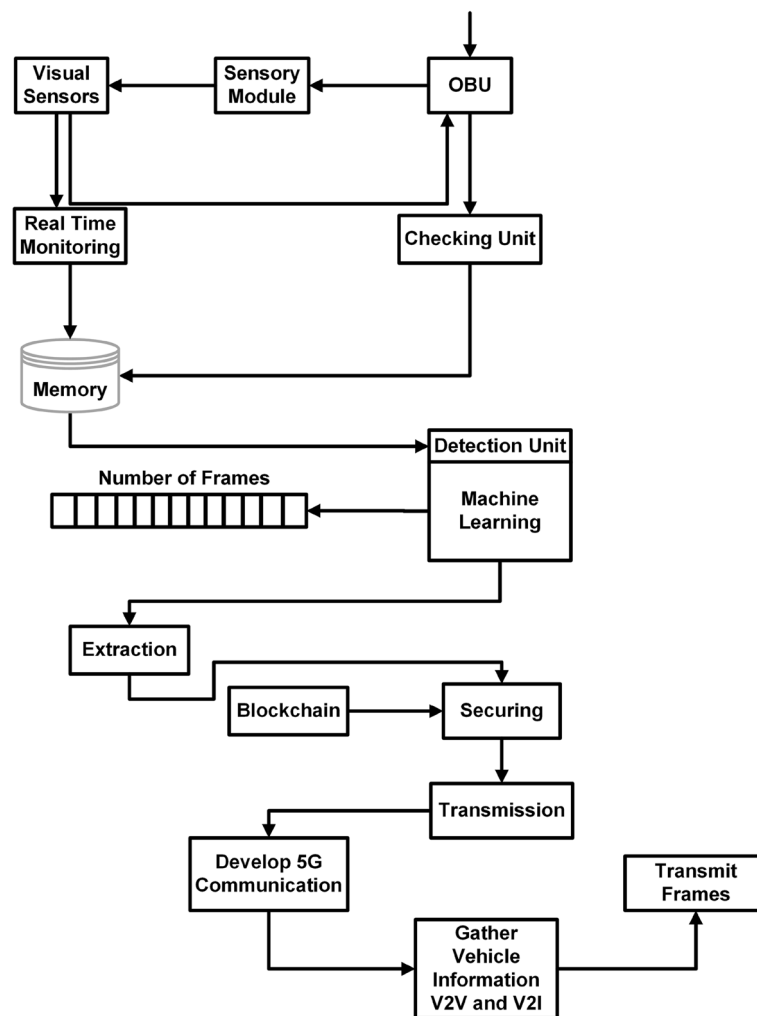


Fig. 3 Flow of Proposed Work

The dataset consists of upto 72 video sequences averaging about 120 seconds per video. All videos have different traffic conditions and vehicles. These videos have all significant events like emergency recordings, road conditions, and traffic scenarios. The data is stored in .mp4 format. The dataset is created from two standard datasets, i.e., the VRiV dataset and OPV2V Dataset. Both datasets and papers with code platforms are available online on Kaggle.

The VRiV dataset and OPV2V dataset serve as fundamental components in the research endeavor titled “Deep Learning Based Enhanced Secure Emergency Video Streaming Approach by Leveraging Blockchain Technology for Vehicular AdHoc 5G Networks.” The VRiV dataset, sourced from Kaggle, and the OPV2V dataset, obtained from Paperswithcode, are selected due to their comprehensive coverage of vehicular video data, encompassing various scenarios relevant to emergencies. These datasets provide a diverse range of video clips capturing incidents and non-incidents in vehicular environments,

essential for training and testing deep learning models. Their integrated form offers a more robust and representative dataset, enhancing the accuracy and reliability of the proposed approach in addressing emergency video streaming challenges within Vehicular AdHoc 5G Networks.

VANET scenario is created to understand the importance of this environment. There are mainly three types of communication used in VANET, which are V2V, V2I, and I2I, as shown in Fig. 4. The accident of two cars is demonstrated in the scenario connected in VANET, and the live visuals have been recorded by the nearby vehicles and communicated with the connected vehicles and the roadside units. When video streaming of this incident received by nearby vehicles, they can alter their routes to avoid traffic jams. An ambulance service near this incident location can approach this location much earlier to rescue the victims.

In the VANET scenario, a simulated environment is constructed to simulate and understand the dynamics and

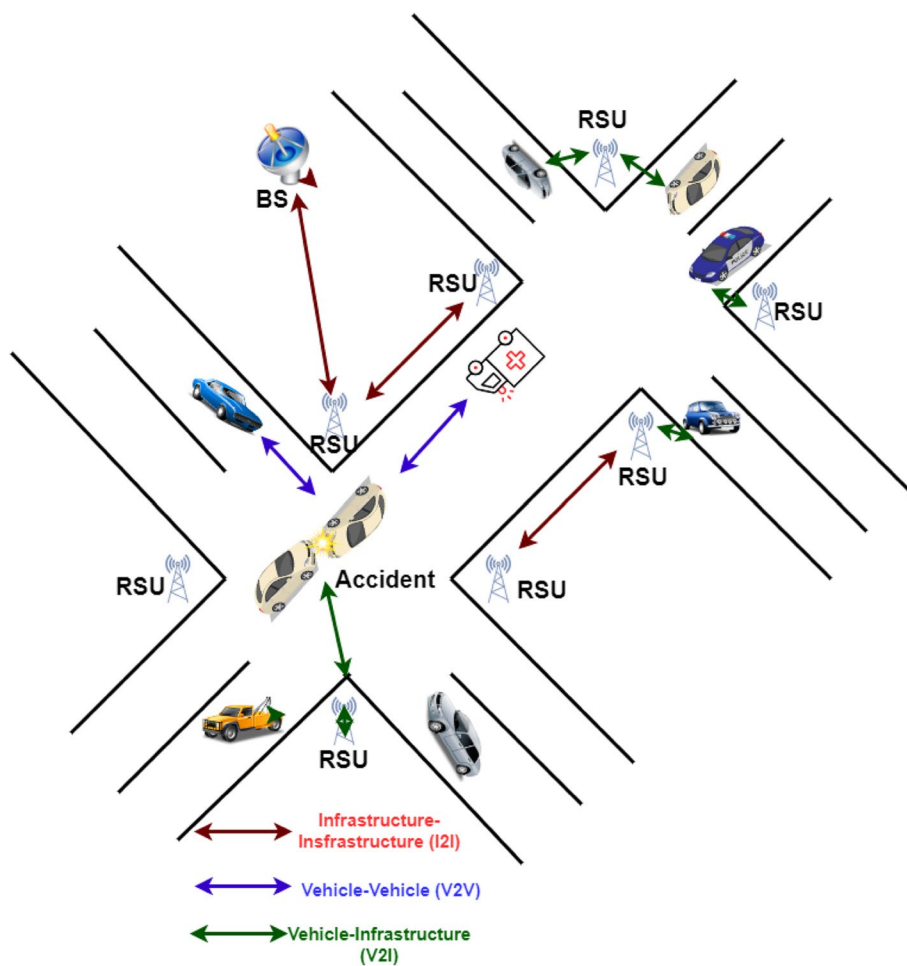


Fig. 4 VANET and Proposed VANET Architecture Development

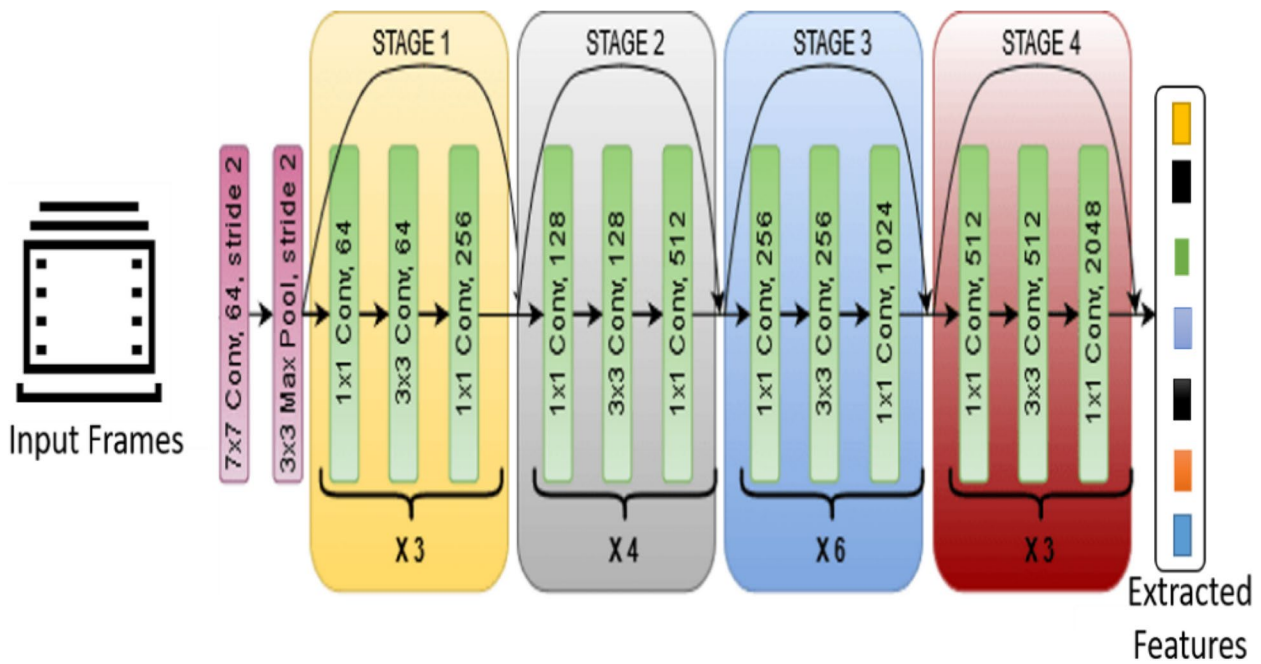


Fig. 5 Feature Extraction Mechanism

significance of Vehicular AdHoc Networks (VANETs). VANETs encompass three primary modes of communication: Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communication, as depicted in Fig. 4. Within this

scenario, an accident involving two vehicles is portrayed, serving as a real-world example of VANET communication in action. During the accident, live visual footage is recorded by nearby vehicles and transmitted to other connected vehicles and roadside units through V2V

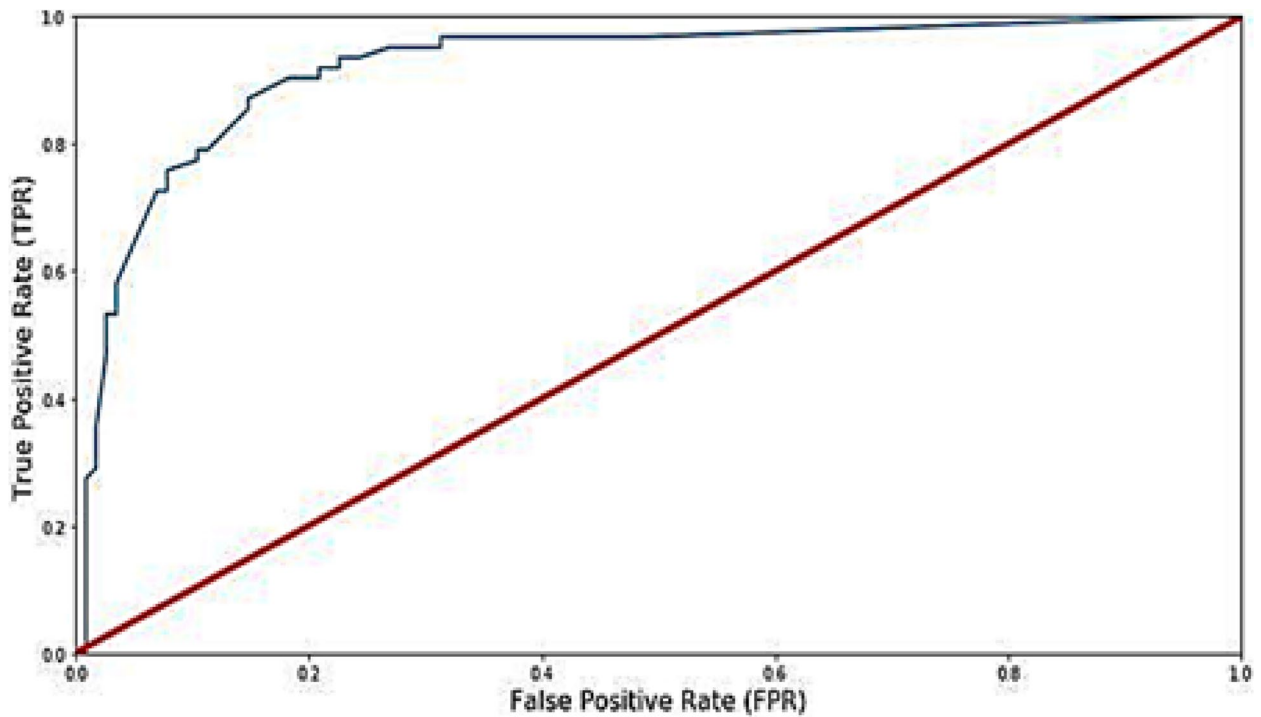


Fig. 6 Represents the AUC curve for ResNet-50

and V2I communication channels. This real-time video streaming enables surrounding vehicles to perceive the incident and make informed decisions promptly. For instance, vehicles receiving the video stream can adjust their routes to avoid potential traffic congestion caused by the accident, thus enhancing overall traffic management efficiency. Moreover, the prompt dissemination of video footage allows emergency response services, such as ambulance units, to swiftly respond to the incident location. With access to live visuals, ambulance services can accurately assess the situation and navigate to the accident site expediently, potentially saving crucial time in rescuing and providing medical aid to the victims. This scenario vividly illustrates the practical utility and benefits of VANETs in enhancing road safety, traffic management, and emergency response. By leveraging the connectivity and information-sharing capabilities of VANETs, stakeholders can collaborate in real-time to mitigate the impact of accidents, streamline traffic flow, and expedite emergency response efforts, ultimately contributing to safer and more efficient transportation systems. The PyScenedetect library is used to scan videos for scene transitions. PyScenedetect is a Python library designed specifically for detecting scene changes in videos. It offers functionalities to automatically identify cuts, fades, and other scene transitions, providing valuable insights into the structure of the video content. Moreover, an important aspect of the PyScenedetect library is its ability to cut the video into pieces based on detected scene transitions. This process, known as scene splitting or segmentation, is essential for breaking down the video into smaller segments corresponding to different scenes or events. By accurately identifying scene transitions and cutting the video accordingly, PyScenedetect enables efficient processing and analysis of video data, particularly in applications such as emergency video streaming in Vehicular AdHoc 5G Networks. Therefore, the authors leveraged PyScenedetect not only to detect scene transitions within videos but also to segment the videos into manageable pieces, facilitating subsequent analysis and processing tasks. This integration of PyScenedetect played a crucial role in the overall methodology proposed by the authors for enhancing secure emergency video streaming in Vehicular AdHoc 5G Networks.

Model training

This section will discuss the model training procedure and simulation results.

ResNET-50: The ResNet-50 deep learning model is used for the feature extraction process of extracted frames. The model is trained using Tensorflow and Keras deep learning models. We Load pre-trained ResNet50 without fully connected layers and use it

as a feature extractor. Then frames are prepared, features extracted, and these features are in NumPy arrays. These features are used for clustering purposes. We used the reliable and widely used unsupervised machine learning approach, K-means clustering, to cluster features. The process of feature extraction is shown in Fig. 5.

The ResNet-50 model achieves handsome results in the feature extraction of frames. Figure 6 presents the AUC curve of the Resnet-50 model. The feature extraction is done with an AUC score of 92%, as illustrated in Fig. 6.

K-mean clustering

The k-means model is among the most basic and often used unsupervised machine learning methods. Unsupervised algorithms typically conclude datasets utilizing input vectors

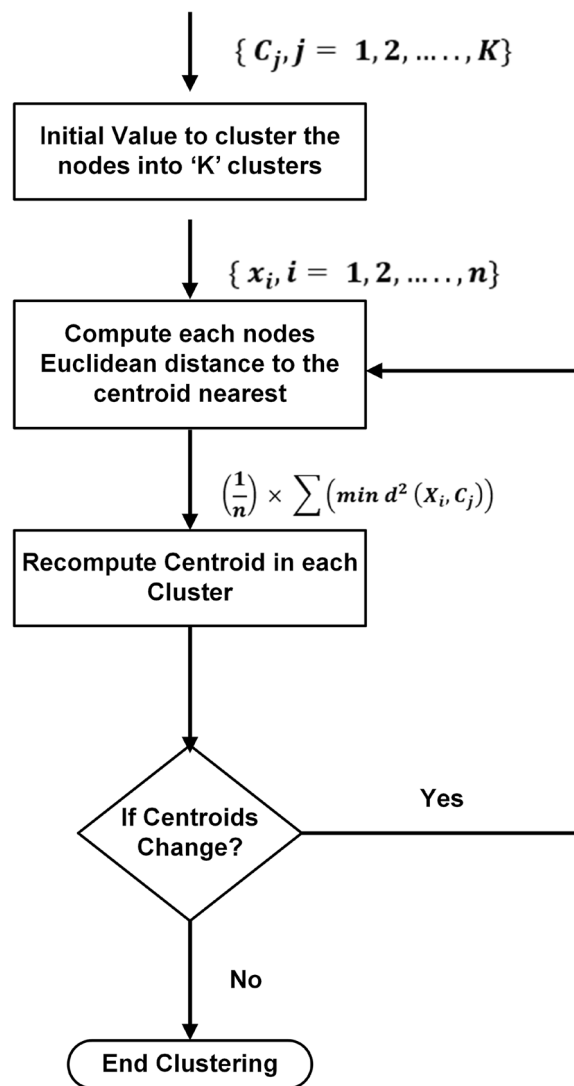


Fig. 7 Process flow of K-means for the proposed problem

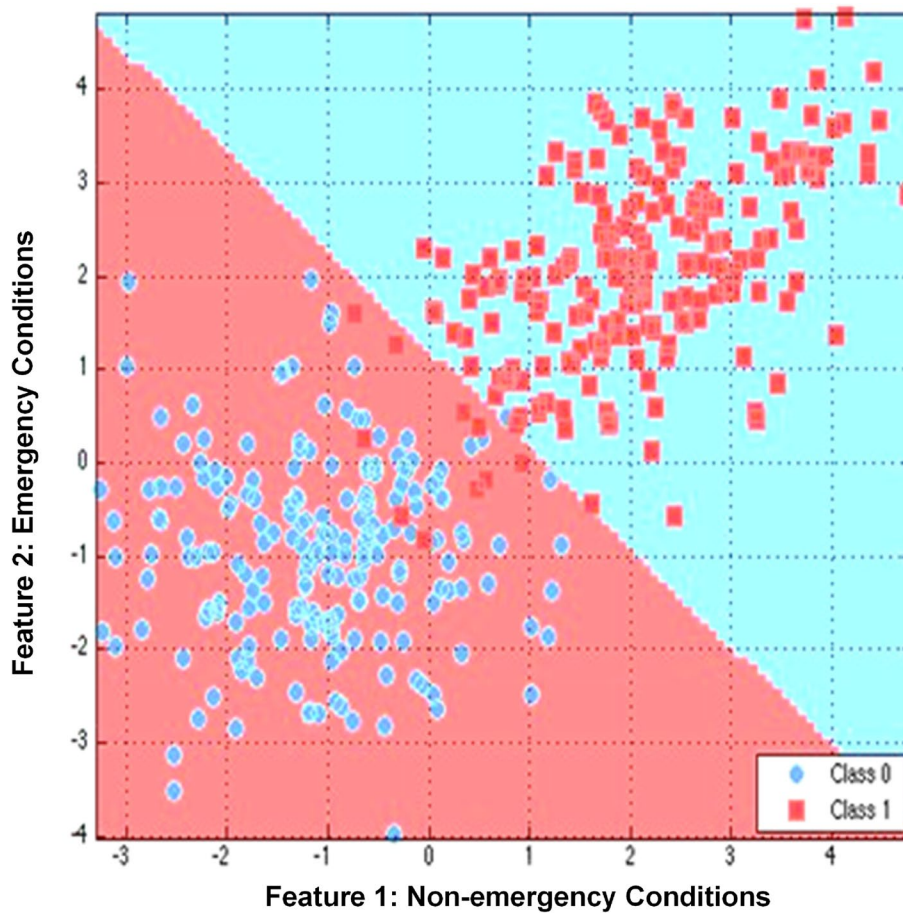


Fig. 8 K Means Clustering Results

without considering predetermined or labeled outputs. Finding underlying patterns by combining comparable data points is K-means’ primary goal. K-means searches the input data for a predetermined number (k) of clusters to accomplish this goal. A cluster is a group of data items combined

due to their shared characteristics. We used the scikit learn library for the implementation of the k-means model. We used the Elbow method to find the optimal K number for the K Means model. We used the yellow-brick library to construct a basic elbow technique and determine how many clusters to employ in our K Means algorithm. The model is trained and then tested on the features extracted by the ResNet-50 model. Figure 7 illustrates the flow of K-means.

After the clustering, the data is split into two clusters. These clusters have two categories of data. The first cluster contains the data of normal or non-emergency conditions represented by class 0, while the second includes the

Table 1 Default parameters of the SVM Model

Parameter	Value
C	1.0
class_weight	None
cache_size	200
decision_function_shape	‘over’
Gamma	‘auto_deprecated’
Kernel	‘rbf’
probability	False
coef0	0.0
Shrinking	True
Degree	3
Verbose	False

Table 2 Classification report of the SVM model

Parameters	Precision	Recall
0	0.84	0.85
1	0.69	0.67
Accuracy	Precision	Recall
Macro Average	0.76	0.76
Weighted Average	0.79	0.79

Table 3 Default parameters of the SVM Model

Recall
<pre> params = { 'gamma': [0.1,0.01,0,0.001,0.0001], 'C': [0.1,10,1000], 'kernel': ['rbf'] } </pre>

Table 4 Classification report of Optimized model

	Precision	Recall	F1-Score	Support
0	0.98	0.99	0.99	18743
1	0.99	0.97	0.98	12409
Accuracy			0.98	31152
Macro Average	0.98	0.98	0.98	31152
Weighted Average	0.98	0.98	0.98	31152

emergency conditions data represented by class 1. This data is split into train and test datasets using the sklearn library in Python. 70% data is reserved for training the support vector machine (SVM) model, while 30% is used for testing. The output of the K-means model is data that has two categories. These categories have data on emergency and non-emergency conditions of an autonomous vehicle. The clustering results of the K-means model are shown in Fig. 8.

Support vector machine (SVM)

Support vector machine (SVM) is a machine learning algorithm for classification, regression, and outlier

detection. It is a sophisticated machine-learning model. An SVM classifier designs a model that allocates fresh data points to one of the specified categories. As a result, it may be thought of as a non-probabilistic binary classification model. It is trained on training data using the RBF kernel of the SVM model. The RBF kernel function calculates the similarity or distance between two points, X1 and X2. This kernel can be expressed mathematically, as in Eq. 1. Where,

- Represents the variance and our hyperparameter.
- The Euclidean distance between two points - (L2-norm) is $\|X1 - X2\|$.

After successfully training the SVM model, this model is tested on a test dataset using various classification metrics. These metrics include accuracy, precision, recall, F1-score, ROC, etc. The SVM model was first trained on default parameters and achieved 79% accuracy. The default parameters of the SVM model are shown in Table 1. The classification report of the first model is illustrated in Table 2.

As illustrated in Table 1, the SVM model with default parameters achieved 79% accuracy with 84% and 69% precision for both classes. After that, we used a grid search technique to optimize the SVM model. We used various values of “C” and gamma with the RBF kernel. The importance of the given parameters is illustrated in Table 3.

Using the above values of gamma, C, kernel, and other parameters with default values, the model achieved 98% accuracy with 98% precision and 99% recall value. Table 4

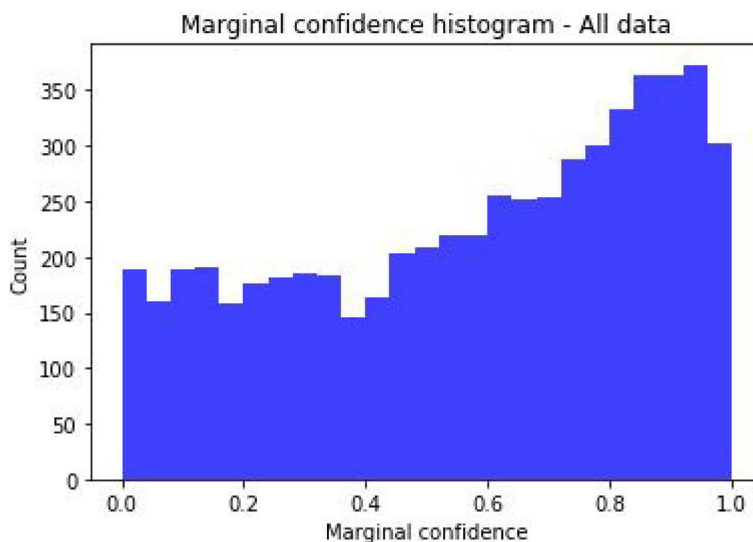


Fig. 9 Marginal Confidence on complete data

illustrates the classification report of the optimized model. For checking the optimized model’s predicted values, we also find the marginal confidence of data using the histogram. Figure 9 presents the borderline spirit of the optimized model on data on both categories.

The model is also evaluated by using a confusion matrix. It is a method for summarizing the performance of classification algorithms. If our dataset has more than two classes or an uneven number of observations in each class, classification accuracy alone might be deceiving. Calculating a confusion matrix can help us determine what our trained model is making suitable and what kinds of mistakes it makes (Fig. 10). A confusion matrix is illustrated in Fig. 12. The predicted label chart has two boxes, white and blue, where data in the blue box are corrected while data in the white box are correct. We have obtained 97 % accuracy using the optimized model.

The predictive matrix and confusion matrix serve as critical tools in evaluating the performance of

classification algorithms, particularly when applied to datasets like the VRiV and OPV2V datasets. The predictive matrix, also known as the confusion matrix, provides a comprehensive summary of the model’s classification performance. It aids in understanding how well the trained algorithm distinguishes between different classes within the dataset. By examining the confusion matrix, we can assess the accuracy of the model’s predictions and identify any misclassifications or errors. In the context of the provided explanation, the confusion matrix assists in discerning the accuracy of the optimized model applied to the datasets. It consists of a chart with two boxes, white and blue, representing correct and incorrect predictions, respectively. This matrix allows for a deeper understanding of the model’s behavior by highlighting where it excels and where it falters in classification tasks. With an achieved accuracy of 97%, as mentioned, the confusion matrix provides valuable insights into the model’s performance beyond a simple accuracy metric,

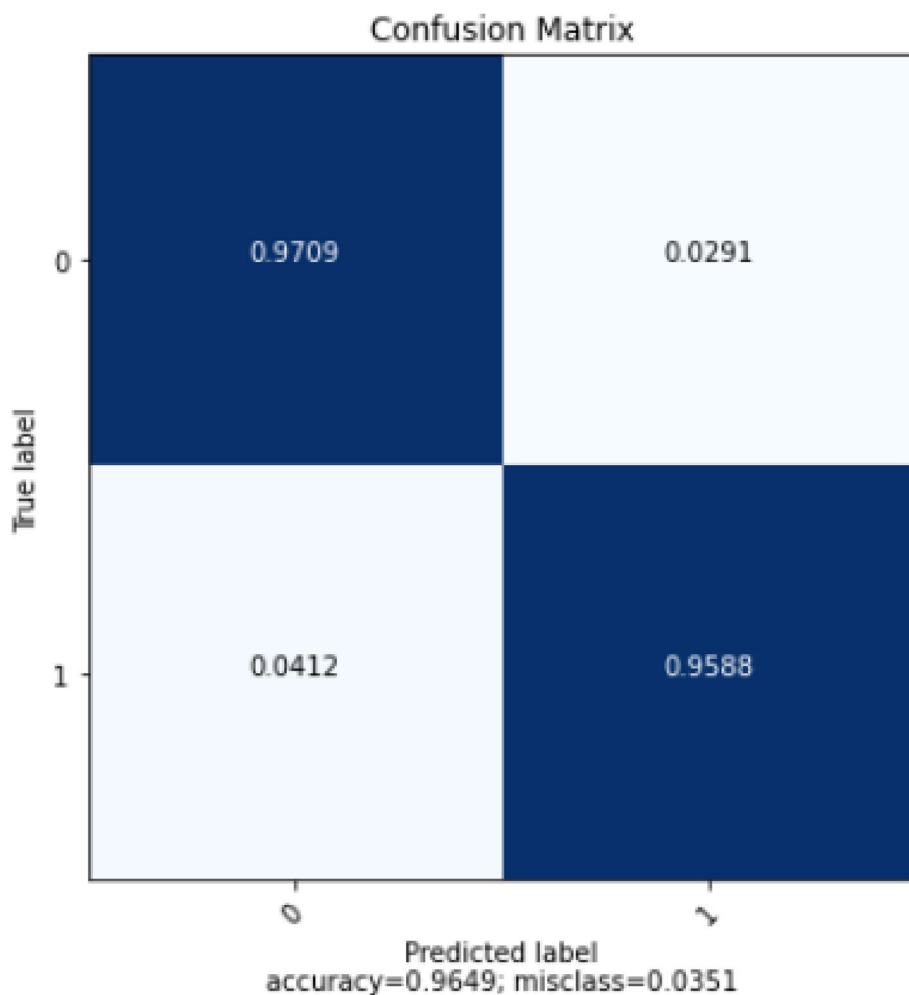


Fig. 10 Predicted Matrix for Optimized SVM Model

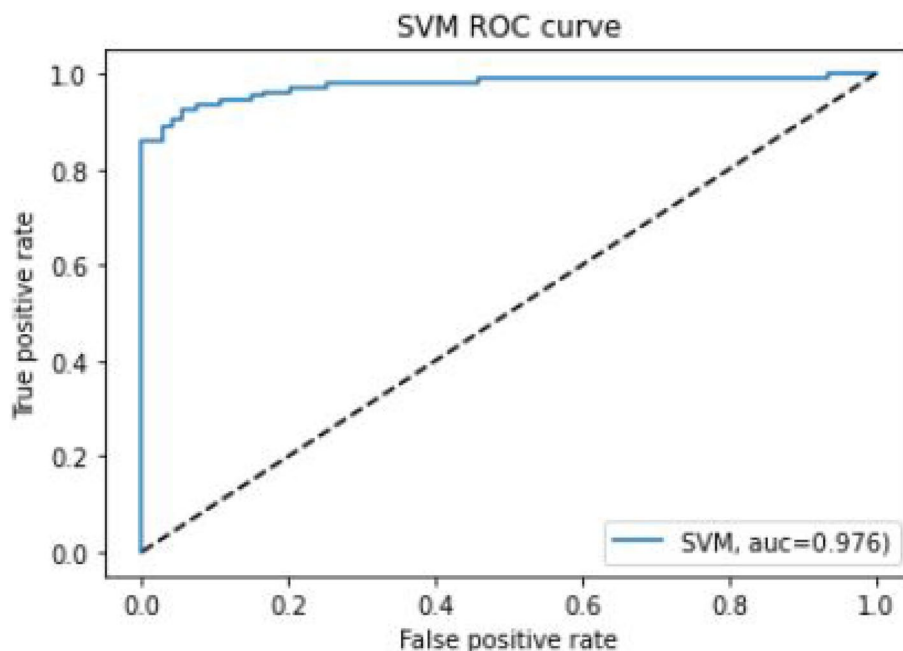


Fig. 11 SVM ROC Curve

Table 5 Result Comparison of literature work and proposed work

Methodologies	Algorithms	Accuracy
Shareef S.M et al. [39]	CNN	85%
Yadav D.K et al. [42]	Deep learning	92%
Ghosh S et al. [43]	CNN	92.38%
Maaloul B et al. [38]	Farneback Optical flow	91%
Agrawal K.A et al. [41]	ResNet and SVM	94.14%
Santhi SK et al. [40]	CNN	95.21%
Proposed Method	ResNet-50 and SVM	98%

ensuring a more nuanced evaluation of its efficacy in handling the given datasets.

ROC curve is a receiver operating characteristic curve that displays how well a classification model performs across all categorization levels. Two parameters are shown which are True Positive and False Positive Rate. Figure 11 presents the ROC curve of the optimized SVM model. We achieved 98% SVM accuracy.

Table 5 compares the literature results and our research work and their accuracy. The graph in Fig. 12 depicts the accuracy rates achieved by various methodologies and algorithms in a classification task. Each methodology is represented by a different color, and the corresponding accuracy score is shown on the y-axis. From the accompanying table, we observe a range of algorithms employed by different researchers, including Farneback

Optical Flow, CNN, Deep Learning, RestNet, and SVM. Notably, the proposed methodology combines RestNet-50 and SVM for classification tasks and achieves an impressive accuracy rate of 98%. Statistical observations reveal a notable variance in accuracy across the methodologies. For instance, Maaloul B et al. [38] utilizing Farneback Optical flow achieved an accuracy of 91%, while Shareef S.M. et al. [39] employing CNN reached 85%. Conversely, Santhi SK et al. [40] and Agrawal K.A. et al. [41] reported higher accuracies of 95.21% and 94.14%, respectively, with their CNN and RestNet-SVM combinations. The proposed methodology outperforms all others with a remarkable accuracy of 98%. This graph and accompanying table highlight the importance of selecting appropriate algorithms and methodologies for classification tasks. The significant variation in accuracy underscores the need for careful consideration of the underlying techniques and frameworks when designing and implementing classification models. Additionally, the superior performance of the proposed methodology indicates its potential for practical applications requiring high-accuracy classification.

Conclusion and future directions

Conclusion

This study undertook a comprehensive examination of video streaming challenges within VANET environments, emphasizing the selective transmission of meaningful video frames amidst V2V and V2I communication.

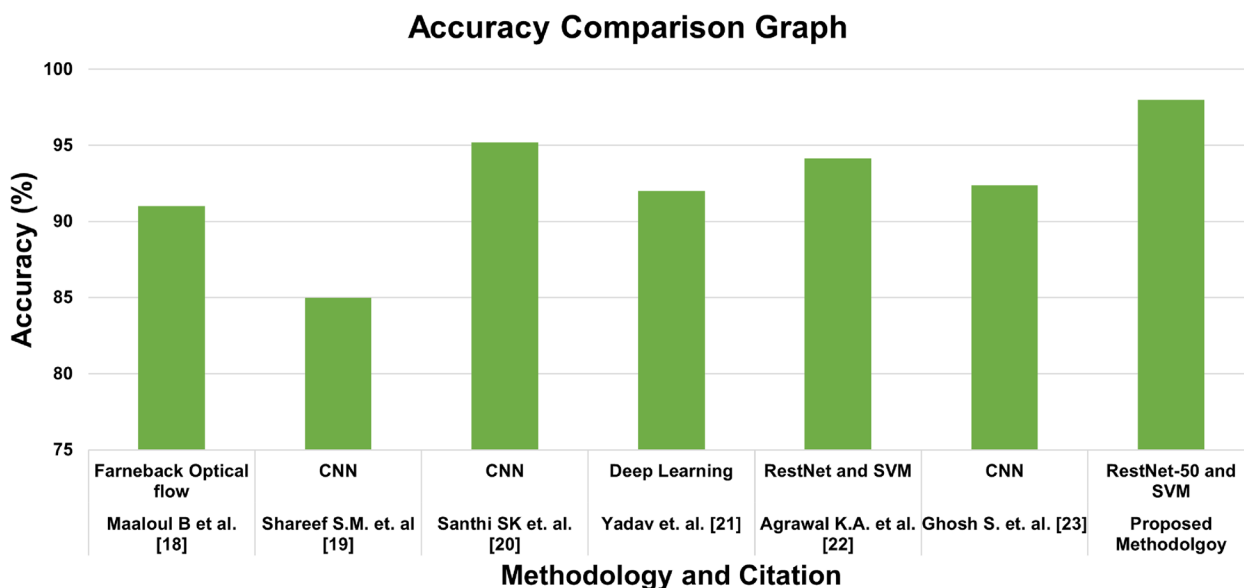


Fig. 12 Comparison between Proposed Scheme and State-of-the-Art Work

Leveraging a blend of algorithms, including Sklearn for machine learning analysis, PyScenedetect for scene transition detection, and OpenCV for video frame extraction, the research focused on accurately classifying frames as accident or non-accident scenarios. Dataset amalgamation from VRiV and OPV2V facilitated robust experimentation, with a 70% training and 30% testing split. Notably, feature extraction employing ResNet-50, coupled with TensorFlow and Keras models, enabled effective data representation. K-means clustering further streamlined the process, distinguishing between regular and emergency clusters. The subsequent SVM training, employing the RBF kernel, initially yielded 79% accuracy, later optimized to a remarkable 98% accuracy, with corresponding precision and recall rates of 98% and 99%, respectively. In addition to model performance, marginal confidence analysis and confusion matrix evaluation were conducted, crucial for discerning model efficacy beyond raw accuracy metrics. The obtained 97% accuracy from the confusion matrix underscores the model’s robustness in classification tasks. The demonstrated advancements surpass previous research endeavors in VANET video streaming, solidifying the proposed methodology’s efficacy and offering promising avenues for future research in vehicular communication systems.

Future directions

In the future, researchers can work on other parameters related to video streaming, new video streaming solutions, and improved applications that can enhance road safety in VANET. In the future, various deep-learning

approaches can be used to maximize the accuracy of accident frame extraction and rapidly broadcast the required data to all vehicles in the VANET environment. The number of vehicles in VANET sending and receiving videos is increasing rapidly, so the VANET environment needs to be more secure and requires extra bandwidth. Quality of service and video broadcasting are also the leading research gaps that must be filled. Expanding the proposed scheme beyond VANETs, potential applications include surveillance systems, disaster management, and remote health-care. Socio-economic benefits include improved public safety, reduced response times, and enhanced accessibility to emergency services, contributing to overall societal well-being and economic productivity. Further research should explore these diverse application scenarios to maximize societal impact.

Acknowledgements

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-RG23157).

Authors’ contributions

Conceptualization, M.A. and S.J.; methodology, S.J. and Ab.A.; software, A.A. and M.A.; validation, Q.A. and A.A.; formal analysis, S.K. and U.R.; investigation, Y.A.; resources, U.R., Y.S.; data curation, M.A.; writing-original draft preparation, S.J., A.A. and Ab.A.; writing—review and editing, U.R., Y.A.; visualization, A.A. and Y.A.; supervision, S.J.; project administration, A.A. and Y.S.; funding acquisition, S.J. All authors have read and agreed to the published version of the manuscript.”

Availability of data and materials

The datasets used and/or analysed during the current study are available from the corresponding author upon reasonable request.

Declarations

Competing interests

The authors declare no competing interests.

Received: 3 February 2024 Accepted: 3 May 2024

Published online: 15 August 2024

References

- Yu S, Zhao C, Song L, Li Y, Du Y (2023) Understanding traffic bottlenecks of long freeway tunnels based on a novel location-dependent lighting-related car-following model. *Tunn Undergr Space Technol* 136:105098
- Cunha B, Brito C, Araújo G, Sousa R, Soares A, Silva FA (2021) Smart traffic control in vehicle ad-hoc networks: a systematic literature review. *Int J Wireless Inf Networks* 28(3):362–384
- Al Najada H, Mahgoub I (2016) Big vehicular traffic data mining: Towards accident and congestion prevention. In: 2016 International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, pp 256–261
- Chen J, Wang Q, Cheng HH, Peng W, Xu W (2022) A review of vision-based traffic semantic understanding in its. *IEEE Trans Intell Transp Syst*. <https://ieeexplore.ieee.org/document/10122471>
- Chen J, Xu M, Xu W, Li D, Peng W, Xu H (2023) A flow feedback traffic prediction based on visual quantified features. *IEEE Trans Intell Transp Syst*. <https://ieeexplore.ieee.org/document/9999027?denied=>
- Ahmed A, Jabbar S, Iqbal MM, Ibrar M, Erbad A, Song H (2022) An efficient hierarchical mobile ipv6 group-based bu scheme for mobile nodes in iot network. *IEEE Internet Things J* 10(10):8684–8695
- Chen J, Wang Q, Peng W, Xu H, Li X, Xu W (2022) Disparity-based multi-scale fusion network for transportation detection. *IEEE Trans Intell Transp Syst* 23(10):18855–18863
- Habib MA, Ahmad M, Jabbar S, Khalid S, Chaudhry J, Saleem K, Rodrigues JJ, Khalil MS (2019) Security and privacy based access control model for internet of connected vehicles. *Futur Gener Comput Syst* 97:687–696
- Fang Z, Wang J, Liang J, Yan Y, Pi D, Zhang H, Yin G (2023) Authority allocation strategy for shared steering control considering human-machine mutual trust level. *IEEE Trans Intell Veh*. <https://ieeexplore.ieee.org/document/10197516>
- Akbar H, Iqbal MM, Ali A, Parveen A, Samee NA, Alohal MA, Muthanna MSA (2023) Detecting rotational symmetry in polar domain based on sift. *IEEE Access*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10143638>
- ul Hassan M, Al-Awady AA, Ali A (2024) Ann-based intelligent secure routing protocol in vehicular ad hoc networks (vanets) using enhanced aodv. *Sensors* 24(3):818
- Balen J, Tomasic B, Semialjac K, Varga H (2022) Survey on using 5g technology in vanets. In: 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO). IEEE, pp 442–448
- Shahzad M, Antoniou J (2019) Quality of user experience in 5g-vanet. In: 2019 IEEE 24th international workshop on computer aided modeling and design of communication links and networks (camad). IEEE, pp 1–6
- Zhang X, Wang Y, Yuan X, Shen Y, Lu Z, Wang Z (2022) Adaptive dynamic surface control with disturbance observers for battery/supercapacitor-based hybrid energy sources in electric vehicles. *IEEE Trans Transp Electrification*. <https://ieeexplore.ieee.org/document/9840409>
- Lopes R, Luis M, Sargento S (2021) Real-time video frame differentiation in multihomed vanets. *Wirel Netw* 27:2559–2575
- Ali A, Iqbal MM, Jabbar S, Asghar MN, Raza U, Al-Turjman F (2022) Vablock: A blockchain-based secure communication in v2v network using icn network support technology. *Microprocess Microsyst* 93:104569. <https://doi.org/10.1016/j.micpro.2022.104569>
- Cao K, Wang B, Ding H, Lv L, Tian J, Hu H, Gong F (2021) Achieving reliable and secure communications in wireless-powered noma systems. *IEEE Trans Veh Technol* 70(2):1978–1983
- Zhang S (2023) Paraviewweb architecture method of power security emergency drill platform based on vr technology. *Multimedia Tools Appl* 83(3):6447–6467. <https://doi.org/10.1007/s11042-023-15934-5>
- Dai X, Xiao Z, Jiang H, Chen H, Min G, Dustdar S, Cao J (2022) A learning-based approach for vehicle-to-vehicle computation offloading. *IEEE Inter-net Things J* 10(8):7244–7258
- Khan H, Samarakoon S, Bennis M (2020) Enhancing video streaming in vehicular networks via resource slicing. *IEEE Trans Veh Technol* 69(4):3513–3522
- Habib MA, Ahmad M, Jabbar S, Ahmed SH, Rodrigues JJ (2018) Speeding up the internet of things: Leaiot: A lightweight encryption algorithm toward low-latency communication for the internet of things. *IEEE Consum Electron Mag* 7(6):31–37. <https://doi.org/10.1109/mce.2018.2851722>
- Sun L, Liang J, Zhang C, Wu D, Zhang Y (2023) Meta-transfer metric learning for time series classification in 6g-supported intelligent transportation systems. *IEEE Trans Intell Transp Syst*. <https://ieeexplore.ieee.org/document/10061349>
- Burhanuddin LA, Liu X, Deng Y, Challita U, Zahemszky A (2022) Qoe optimization for live video streaming in uav-to-uav communications via deep reinforcement learning. *IEEE Trans Veh Technol* 71(5):5358–5370. <https://doi.org/10.1109/tvt.2022.3152146>
- Quadros C, Santos A, Gerla M, Cerqueira E (2016) Qoe-driven dissemination of real-time videos over vehicular networks. *Comput Commun* 91:133–147
- Alaya B, Khan R, Moulahi T, Khediri SE (2021) Study on qos management for video streaming in vehicular ad hoc network (vanet). *Wirel Pers Commun* 118:2175–2207
- Roy D, Chatterjee M, Pasilio E (2018) Video quality assessment for inter-vehicular streaming with ieee 802.11 p, lte, and lte direct networks over fading channels. *Comput Commun* 118:69–80
- Xie L, Ding Y, Yang H, Wang X (2019) Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets. *IEEE Access* 7:56656–56666
- Zhang X, Deng H, Xiong Z, Liu Y, Rao Y, Lyu Y, Li Y, Hou D, Li Y (2024) Secure routing strategy based on attribute-based trust access control in social-aware networks. *J Signal Process Syst* 1–16. <https://ui.adsabs.harvard.edu/abs/2024JSPSy.tmp....4Z/abstract>
- Wu Z, Zhu H, He L, Zhao Q, Shi J, Wu W (2023) Real-time stereo matching with high accuracy via spatial attention-guided upsampling. *Appl Intell* 53(20):24253–24274
- Jiang Z, Xu C (2023) Disrupting the technology innovation efficiency of manufacturing enterprises through digital technology promotion: An evidence of 5g technology construction in china. *IEEE Trans Eng Manag*. <https://ieeexplore.ieee.org/document/10094227?denied=>
- Bashir RR, Saeed Y, Ali A, Algarni AD, Muthanna A, Hijjawi M, Alsbou T (2024) 2cap: A novel curve crash avoidance protocol to handle curve crashes in vehicular ad-hoc network. *IEEE*. Accessed 3 Jan 2024
- Masood S, Saeed Y, Ali A, Jamil H, Samee NA, Alamro H, Muthanna MSA, Khakimov A (2023) Detecting and preventing false nodes and messages in vehicular ad-hoc networking (vanet). *IEEE Access*
- Sohail R, Saeed Y, Ali A, Alkanhel R, Jamil H, Muthanna A, Akbar H (2023) A machine learning-based intelligent vehicular system (ivs) for driver's diabetes monitoring in vehicular ad-hoc networks (vanets). *Appl Sci* 13(5):3326
- Sohail H, Hassan Mu, Elmagzoub M, Rajab A, Rajab K, Ahmed A, Shaikh A, Ali A, Jamil H (2023) Bbsf: Blockchain-based secure weather forecasting information through routing protocol in vanet. *Sensors* 23(11):5259
- Rashid K, Saeed Y, Ali A, Jamil F, Alkanhel R, Muthanna A (2023) An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (vanets). *Sensors* 23(5):2594
- Nazar K, Saeed Y, Ali A, Algarni AD, Soliman NF, Ateya AA, Muthanna MSA, Jamil F (2022) Towards intelligent zone-based content pre-caching approach in vanet for congestion control. *Sensors* 22(23):9157
- Alkanhel R, Ali A, Jamil F, Nawaz M, Mehmood F, Muthanna A (2022) Intelligent transmission control for efficient operations in sdn. *Comput Mater Continua* 71(2). <https://www.techscience.com/cmcc/v71n2/45768>
- Maaloul B, Taleb-Ahmed A, Niar S, Harb N, Valderrama C (2017) Adaptive video-based algorithm for accident detection on highways. In: 2017 12th IEEE International Symposium on Industrial Embedded Systems (SIES). IEEE, pp 1–6. <https://www.iasj.net/iasj/article/198385>
- Shareef SM, Ali AM, et al (2020) Optimized frame detection technique in vehicle accident using deep learning. *Zanco J Pure Appl Sci* 32(4). *IEEE*
- Santhi SK (2023) Accident detection using convolutional neural networks. *J Emerg Technol Innov Res* 10(4):646–649. *IEEE*

41. Agrawal AK, Agarwal K, Choudhary J, Bhattacharya A, Tangudu S, Makhija N, Rajitha B (2020) Automatic traffic accident detection system using resnet and svm. In: 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN). IEEE, pp 71–76
42. Yadav DK, Anjum I, et al (2020) Accident detection using deep learning. In: 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). IEEE, pp 232–235
43. Ghosh S, Sunny SJ, Roney R (2019) Accident detection using convolutional neural networks. In: 2019 international conference on data science and communication (IconDSC). IEEE, pp 1–6

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.