Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.048133

ARTICLE

Trusted Certified Auditor Using Cryptography for Secure Data Outsourcing and Privacy Preservation in Fog-Enabled VANETs

Nagaraju Pacharla and K. Srinivasa Reddy*

School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, 522237, India

*Corresponding Author: K. Srinivasa Reddy. Email: srinivasareddy.k@vitap.ac.in

Received: 28 November 2023 Accepted: 22 March 2024 Published: 15 May 2024

ABSTRACT

With the recent technological developments, massive vehicular ad hoc networks (VANETs) have been established, enabling numerous vehicles and their respective Road Side Unit (RSU) components to communicate with one another. The best way to enhance traffic flow for vehicles and traffic management departments is to share the data they receive. There needs to be more protection for the VANET systems. An effective and safe method of outsourcing is suggested, which reduces computation costs by achieving data security using a homomorphic mapping based on the conjugate operation of matrices. This research proposes a VANET-based data outsourcing system to fix the issues. To keep data outsourcing secure, the suggested model takes cryptography models into account. Fog will keep the generated keys for the purpose of vehicle authentication. For controlling and overseeing the outsourced data while preserving privacy, the suggested approach considers the Trusted Certified Auditor (TCA). Using the secret key, TCA can identify the genuine identity of VANETs when harmful messages are detected. The proposed model develops a TCA-based unique static vehicle labeling system using cryptography (TCA-USVLC) for secure data outsourcing and privacy preservation in VANETs. The proposed model calculates the trust of vehicles in 16 ms for an average of 180 vehicles and achieves 98.6% accuracy for data encryption to provide security. The proposed model achieved 98.5% accuracy in data outsourcing and 98.6% accuracy in privacy preservation in fog-enabled VANETs. Elliptical curve cryptography models can be applied in the future for better encryption and decryption rates with lightweight cryptography operations.

KEYWORDS

Vehicular ad-hoc networks; data outsourcing; privacy preservation; cryptography; keys; trusted certified auditors; data security

1 Introduction

For numerous reasons, including increased communication efficiency and decreased traffic accidents, the VANET is an essential part of the intelligent transportation network. The nodes that make up a VANET are split between an Onboard Unit (OBU) [1] installed in vehicles and an RSU positioned at the side of the road. Comfortable and secure services can be achieved between vehicles and infrastructure and via broadcast via the OBU. When it comes to secure communication, however, the VANET has significant obstacles due to its open network environment and changing network

topology [2]. Authentication of vehicles ensures the veracity of each communication node, which is a necessary first step towards establishing secure communication between vehicles [3]. For this reason, vehicle authentication is crucial in the VANET. However, there are still obstacles to building a safe and efficient authentication system between the vehicles and the RSU and ensuring that users' privacy is preserved while authentication is taking place [4]. Thus, there is an enormous demand for the development of efficient and safe anonymous authentication schemes [5].

Researchers have proposed a plethora of authentication techniques for VANET to address this problem [6]. To make sure everything was secure, most of these approaches used anonymous authentication. Furthermore, to evade tracking attempts, vehicles must regularly alter their aliases. To safeguard the privacy of vehicles' data, existing systems can validate their identities before allowing them to communicate with other legitimate vehicles or RSUs in the VANET [7]. Efficient authentication may be challenging to achieve due to a large Certificate Revocation List (CRL) and an unexpected rise in authentication requests [8]. During this period, enemy vehicles can strike the VANET at any moment. Broadcasting the CRL to other vehicles will also expose private information about the revoked vehicles, since the legal vehicles know all the aliases used by them [9]. Given the inefficiency of authentication and the cost issues created by CRL, related researchers have suggested various efficient techniques of authentication using the Hash Message Authentication Code (HMAC) [10]. The HMAC safeguards messages transmitted by authorized vehicles or RSUs against potential attackers who might modify their content. Furthermore, to protect the performance of the VANET system, the Trusted Authority (TA) can revoke the anonymity of any malicious vehicle and notify other vehicles about it [11]. Therefore, the revocation process is considered vital to the VANET community's integrity preservation efforts.

To guarantee the security of vehicle-to-vehicle communication, the problem of vehicle authentication has long been a focus of study in the field of privacy protection in VANETs. However, employing the identity in the verification process can easily lead to a breach of the vehicles' personal information [12]. As a result, most currently available privacy-protection methods rely on anonymous authentication and the need for direct interaction between vehicles and the TA. However, congestion on the network can occur if there are too many vehicles. When the TA or the car performs an update on the anonymity, it can compromise real-time performance and expose the system's master key [13]. In addition to its tremendous benefits, fog computing also presents great security and privacy problems. Location awareness, customization, accessibility at the moment, mobility, and scalability are just a few of the advantages. Fog makes it feasible to aggregate, filter, and analyze data at the network's periphery, which improvesQuality of Service (QoS) [14]. Gathering data, storage, and transmission are all handled by fog devices, while fog nodes link everything up to the cloud. The fog layer, placed in the heart of a three-layer design, is vital to the safety of the overall system, while its security capability extends to all stages [15].

Encryption and other security measures ensure that sensitive information about the sender and receiver remains hidden while data is transmitted anonymously [16]. A security system's entry point is its authentication services, which verify the identities of users [17]. Cloud data centre's, along with edge devices like sensors and smartphones, fog devices like gateways and small servers, and base stations, are also frequent fog computing authentication entities [18]. Before sending the information to the fog server, it must be encrypted using either asymmetric or symmetric encryption [19]. A secure key exchange is a necessary component of authentication for providing maximum protection. The suggested method uses a time-based decryption mechanism and a two-fold verification process to ensure the data is secure before transferring the cipher text to the user in the fog. The data's owner sets both the decryption timer and user authentication. Fig. 1 shows the Fog Computing Model.

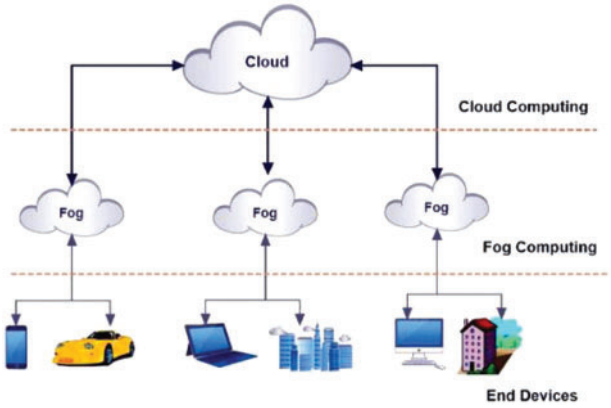

Figure 1: Fog Computing Model

The suggested model considers the VANET auditor node with the best transmission rate. To detect malicious activity in the network and keep monitoring all nodes, the auditor node measures their transmission rates and performance. The suggested model generates key pairs used for outsourcing data encryption. To prevent requests from being sent again, each node will be assigned a label [20]. The auditor node issues keys to the nodes that label the vehicles. Security issues plaguing VANETs include authentication, privacy, integrity, non-repudiation, pseudonymity, mobility, confirmation of data and location, access control [21], key management difficulties, and mobility. Fog computing is vulnerable to security breaches caused by the proliferation of devices connected to fog nodes through different gateways [22]. Any data saved in that fog node might possibly be accessible by any hacker using the device's unique IP address [23]. The unpredictable topology of VANETs is a result of the high speeds of vehicles, making it difficult for researchers to develop a protocol that can adequately handle this topology.

The location, velocity, and heading of a vehicle are all part of a vehicular message, making privacy a major concern in VANETs. Due to the sensitive nature of the information contained in these messages, secrecy is of the utmost importance [24]. Abuse of the service and malicious attacks on the drivers are two possible outcomes of a flawed security mechanism. A privacy-preserving authentication technique and a lightweight trust model for large data analytics were developed to address the security issues plaguing VANET [25]. Due to their superior processing capability, fog nodes, rather than RSUs, are deployed along the roadside in the proposed strategy for node and message authentication [26]. Including fog nodes in a VANET's security architecture can improve the network's capacity for both communication and computing. The proposed model considers TCA for managing and monitoring the outsourced data while maintaining privacy. When malicious messages are discovered, TCA can use the secret key to determine the identity of VANETS. The proposed model develops a TCA-USVLC for secure data outsourcing and privacy preservation in VANETS.

The manuscript is arranged in 5 sections. The manuscript is arranged in five sections. The introduction section discusses the uses and issues of VANETs and the need to use cryptography models in fog-enabled VANETs. The privacy preservation and data outsourcing requirements are discussed in Section 1. Section 2 provides a brief survey of traditional cryptography, privacy preservation, and data outsourcing models. Section 3 discusses the proposed model. This proposed model discusses the selection of auditor vehicles for monitoring the VANET, trust calculation of vehicles, and vehicle labeling process. The key generation process, encryption for data outsourcing, and privacy preservation

model are discussed clearly. Section 4 provides the results of the proposed model that are compared to the traditional models. Section 5 provides the conclusion of the research.

2 Literature Survey

Many security risks arise for VANET due to the key abuse problems involving users and attribute authorities (AAs). Guo et al. [1] suggested an accountable attribute-based data-sharing system that utilizes blockchain technology (AT-DS-VAHN) to address the problems. By utilizing the consortium blockchain that AAs maintains, the author accomplished distributed key storage and distribution for AAs key misuse. Each AA generates its own unique set of attribute keys, and the blockchain keeps track of how those keys are distributed. It is possible to identify and punish AAs for their critical abusive behavior thanks to the immutability of blockchain technology.

If customers are If customers are experiencing data island effects and are struggling to make do with restricted resources, outsourcing their cloud computing could be a good solution. Outsourcing user data and model training tasks, however, carries substantial privacy disclosure risks owing to worries about cloud server trust. Bi et al. [2] introduced a PriKPM approach that uses additive secret sharing (ASS). In PriKPM, two collaboration servers receive data samples that have been randomly divided into two parts and sent to them offline. To find out where and how many cluster centers there are, the author devised a safe initialization approach. After safely calculating the mixed distance between the cluster centers and samples, both servers then carry out the cluster update and sample partitioning activities.

An answer to the problem of terminals limited computational capability in the face of data explosions is cloud computing, which can be included in the Space-Air-Ground Integrated Internet of Things (SAGIIoT). Simultaneously, cloud data security is an important point of emphasis. Improving privacy preservation is made easier with secure outsourcing computing. The immense practicality of K-means clustering has made K-means computing outsourcing a prominent area of interest for researchers in both academia and business. Homotopic encryption, which is the foundation of most K-means clustering outsourcing efforts, is computationally expensive since it solves mathematical riddles. Also, developing a verification algorithm using homomorphic encryption has an intolerably high computational cost. Zhao et al. [3] developed a sparse matrix transformation-based K-means clustering outsourced program to solve these problems; this algorithm can efficiently verify the cloud's deceitful behaviour.

The Internet of Vehicles (IoV), a subset of VANET, is currently in development as a crucial means of inter-vehicle communication. However, with IoV, some traffic messages are often associated with personally identifying details. As a result, protecting people's anonymity when using IoV vehicles is a challenge. However, the genuine identities of the vehicles involved cannot be ascertained if the privacy of the vehicles' data is adequately safeguarded in IoV, as the transferred messages will have no connection to the vehicles' details. Then it will cause many more issues with IoV security. Also, fog computing provides enhanced computing services to end users by integrating diverse, dispersed computing resources into edge networks. Gu et al. [4] created a decentralized tracked privacy-preserving technique for vehicular identification in fog computing-based IoV that makes use of a network of fog servers to ascertain a vehicle's identity and most likely route based on the information gathered. To conceal and reveal the identity of a vehicle, the author uses a secret sharing technique in conjunction with data from a certificate authority. The author devised a vote system to select a reliable fog server capable of re-creating the polynomial via the secret sharing scheme and therefore establishing the identity of a vehicle and its corresponding trajectory.

Increases in both traffic efficiency and driver safety can be attributed in large part to the rise of VANETs. However, there are privacy and security concerns with wireless in-car communication. Zhong et al. [5] presented an elliptic curve cryptography-based CPPA system with minimal overhead in which the vehicle generates its own pseudonym and public/private key pair. In the proposed technique, two hash chains are used to generate the vehicle's pseudonym, allowing for a significant reduction in storage overhead while maintaining backward security. Researchers have proposed fog-based vehicular networks (FVNs) to improve vehicular network communication and service. Security and privacy in the network must be guaranteed before large-scale FVNs may be developed. Considering this, Zhang et al. [6] proposed a lightweight security protocol based on self-certified public key cryptography to encourage effective FVN authentication. The fact that this protocol allows for batch verification greatly improves the system's authentication efficiency. This protocol has been shown to be secure enough for use in vehicle networks and to be immune to the most frequent attacks.

By gathering and organizing sensor data in a sliding window fashion, Kong et al. [7] presented a continuous data-gathering strategy for predictive maintenance in vehicular fog that protects user privacy and is independently verifiable. The suggested method uses a truncated-geometric methodology and the homomorphicPavillier cryptosystem to safeguard the privacy of each piece of sensory input. In addition to continuously monitoring newly gathered vehicle sensory data, the suggested system aggregates and authenticates the reported sensory data in a time-series sliding window.

When talking about data collection, analysis, and insight delivery in a network, the term edge intelligence is being used more and more frequently. This refers to the use of a variety of cutting-edge intelligent technologies performed close to the location where the data was obtained. Attribute-based encryption (AbE) can overcome this difficulty, but its decryption performance is low because it requires a great deal of time-consuming modular exponential operations, bilinear pair operations, and serial computation. As a result, it is inadequate to meet the needs of edge-based intelligent IoV in terms of response time. Considering this issue, Feng et al. [8] suggested the use of an AbE model for edge-intelligent IoV that makes use of outsourced parallel decryption, dubbed AbEM-POD. A generic Spark and MapReduce-based outsourced decryption technique for AbE is included. This technique is adaptable to edge-based intelligent IoV and works with any AbE scheme that uses a tree-based access mechanism. In addition to allowing for parallel outsourced decryption, the suggested architecture ensures that any ABE technique maintains the same level of security. Three typical ABE schemes are used in this research to demonstrate the effectiveness and simplicity of the proposed AbEM-POD.

When it comes to cloud-based centralized management, cyberattacks often lead to privacy breaches. Nevertheless, prior studies have paid scant attention to the privacy issues linked to electric vehicle charging. To charge EVs in a decentralized and data-protected manner, Li et al. [9] suggested a solution that uses fog and blockchain technology. This strategy makes use of fog computing to bring low-latency computing to consumers in proximity. Fog computing networks allow for the delivery of geo-targeted, tailored services by fog computing nodes (FCNs). Furthermore, a blockchain consortium's modular structure is offered. A distributed and trustworthy data storage network is created by the implementation of blockchain technology on the distributed FCNs. Mutual authentication, smart contracts, and blockchain-based storage can ensure security and anonymity during the billing process.

The goal of improving vehicle network communication and service has led researchers to propose fog-based vehicular networks (FVNs). Before developing large-scale FVNs, it is necessary to ensure network-wide security and privacy. Zhang et al. [10] presented a simple security system based on self-certified public key cryptography to support efficient FVN authentication considering this. Without requiring the TA, the protocol enables online authentication between the vehicle and the fog node. The

car can also change its pseudonym and login password on the go, saving the user the trouble of having to go through the TA's tedious interaction procedures. This protocol also permits batch verification, which considerably improves the system's authentication efficiency. It has been demonstrated that this protocol is secure enough to be utilized in car networks, and it is resistant to the most common types of assaults.

A significant pull is required for a vehicular crowd-sensing data collection paradigm due to the large quantity of cars on the route. This leads to problems with user privacy leaks, as incentive mechanisms play a significant role in the development of crowdsensing techniques. To lessen the likelihood of personal information being leaked during the rollout of incentives, Sun et al. [11] suggested a fog computing-based crowd sensing architecture adapted for vehicle crowd sensing, complete with privacy-preserving techniques for data reporting, reward issues, and trust management.

3 Proposed Model

The concept of fog computing has recently gained traction in the realm of Internet of Things (IoT) implementations. As a result of its supremacy in service provisioning, the edge cloud has emerged as a viable option for IoT networks. Since lightweight devices outsource not only their data but also their computation, the data outsourcing scheme of IoT devices necessitates privacy protection computation verification [27]. Existing methods primarily address operations over encrypted data but do not concurrently enable computation verification. In this paper, a data outsourcing scheme built on top of an encrypted database system that is both linear-computable and query-efficient is proposed. Fog computing involves placing a proxy server or network node between the cloud and individual IoT gadgets. To meet the demands of networks with heavy traffic and applications that are sensitive to latency [28]. Fog computing has emerged as an alternative to the more conventional cloud computing model. With a shorter distance to travel and a more evenly distributed load of traffic between the cloud and IoT devices, the service that these devices receive may be significantly more reliable [29]. Traditionally, data has been sent from an edge node to a central server for processing, which has increased network latency and decreased available bandwidth [30]. VANET is an open, self-organized network, making security and privacy major considerations [31].

In the proposed model, initially, node/vehicle information is considered and processed, and a unique identity for each vehicle is allocated for easy identification and communication with vehicles. Once all the vehicles are registered and their information is processed, a vehicle called an auditor vehicle is selected that monitors all the remaining vehicles in the VANET. The auditor vehicle is selected based on the vehicle/node performance, distance, and range of transmission. The vehicle that has high data transmission capabilities, a high range of transmission, minimum energy consumption, and a low loss rate is considered, and this node will monitor the entire vehicle in the network [32]. The auditor node will then calculate the trust levels of each registered vehicle in the network. The proposed model generates and maintains key sets that contain three keys in a set for secure data transmissions. The proposed model generated three keys in a set of 128 bits each. The proposed model considers the RSA model as the base and generates the key sets. The RSA model generates 2 keys in a set, but the proposed model generates 3 keys in a set, and these keys can also be used for one-time purposes. This increases the security level of the model. The key labelling is performed with one of the keys in the key set that can be used only once. The vehicle labelling is performed with the keys. The remaining keys are used for encryption and the usage of data on the network.

The auditor node keeps track of the trust factor for every vehicle and computes the performance of every node. Labelling was assigned as '1' for all trusted vehicles and '0' for all non-trusted vehicles according to the suggested model. When it comes to key sharing and communication, only trusted cars will be considered. The existence of hostile nodes is acknowledged as a major obstacle and a security risk in VANET. An egocentric node is a legitimate vehicle node that propagates misinformation around the network on purpose. Attackers and self-centred nodes can be better dealt with a suitable and efficient security model. To safeguard users' privacy, this research developed a trust model and an authentication method for both nodes and communications. While message authentication was designed to preserve the confidentiality of communications, the suggested node authentication safeguards the validity of vehicle nodes. A labelled node is one that has passed authentication. To ensure that only nodes with the appropriate labels can participate in data encryption, vehicles are labelled that become authorized using the key in the key set and nodes with trustworthy values. An experience-based trust model can be used to deal with selfish nodes. To ensure the confidentiality of each vehicle, a distinct pseudo-identification was assigned to it throughout the mapping process. This was mostly due to the reduced latency and greater throughput brought forth by fog computing. Because of the centralized nature of the cloud's data storage and processing, it is susceptible to hacking from outside sources. The proposed model framework is represented in Fig. 2.

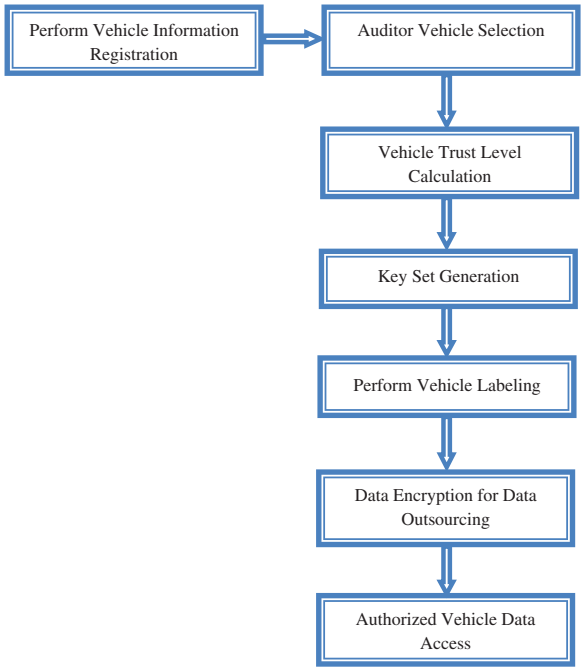

Figure 2: Proposed model framework

The proposed model considers TCA for managing and monitoring the outsourced data while maintaining privacy. When malicious messages are discovered, TCA can use the secret key to determine the identity of VANETS. The proposed model develops a TCA-USVLC for secure data outsourcing and privacy preservation in VANETS.

Initially, consider the vehicle list as Vset {V1, V2, . . . , Vn}. Each vehicle in the network will be registered with vehicle information, and after registration, each vehicle will be assigned a unique identity. The vehicle registration is performed as

$$InstTime\,[M] = \sum_{v=1}^{M} getCurrentTime\,(v) + getDate(v) \tag{1}$$

$$R1 = \sum_{v=1}^{M} getPrime\,(v) + Rand(v) \tag{2}$$

$$R2 = \sum_{v=1}^{M} getVal(v)\,\{v > getPrime(v) \tag{3}$$

$$VReg\,[M] = \sum_{v=1}^{M} getPhyAddr\,(v) + InstTime\,(v) + R1 + R2 + Th \tag{4}$$

Here Th is the threshold value, getCurrentTime() is used to extract the current time during registration, getDate() is used to extract the current time during registration, getPrime() is used to consider a prime number, the Rand() function considers a random value, and getPhyAddr() is used to know the physical address of a node for the calculation of a logical unique identity for each vehicle. Th is the threshold value considered.

Each vehicle, after successful registration, selects a vehicle node as the auditor vehicle node that is used to monitor the entire VANET. The auditor vehicle for monitoring is selected based on the vehicle's data transmission rate, vehicle distance, vehicle loss levels, and vehicle range. These factors are selected, and the vehicle that has the best range is considered the auditor vehicle that is selected as

$$Vdist\,[M] = \sum_{v=1}^{M} \sqrt{(X2 - X1)^2 + (Y2 - Y1)^2} \tag{5}$$

$$VTR\,[M] = \sum_{v=1}^{M} \frac{\mu(v)}{\omega}\,\{\mu(v-1) \rightarrow \mu(v) \tag{6}$$

$$Vloss\,[M] = \sum_{v=1}^{M} \frac{VTR\,(v) - \omega}{M} \tag{7}$$

$$AUVeh\,[M] = \sum_{v=1}^{M} \begin{array}{c} \min\,(Vdist\,(v, v+1)\,\forall VReg) + \max\,(VTR\,(v)) + \min\,(Vloss\,(v)) \\ \{AUVeh(v) \leftarrow VReg\,(v) \end{array} \tag{8}$$

Here X1, Y1 are the coordinate positions of vehicle 1 and X2, Y2 are the coordinate positions of vehicle v2, μ is the packets received by vehicle v, and ω is the total generated packets in the VANET.

The proposed model considers the trust level of each level based on the auditor's vehicle monitoring feedback. The trust level of each vehicle is important for identifying malicious actions in the network. The trust level calculation is performed as follows:

$$VTrust\,[M] = \prod_{v=1}^{M} \max(\delta(v, v+1)\forall VReg) + \min\,(Vdist\,(v, v+1)) + \max(VTR\,(v))$$

$$\begin{cases} VTrust\,(v) \leftarrow 1\ if\ ((\forall VReg \leftarrow \max\,(\delta) + \min\,(Vloss) + \max(VTR) \\ VTrust\,(v) \leftarrow 0\ Otherwise \end{cases} \tag{9}$$

Here δ is the range of the vehicle that it can communicate with. A node with a minimum loss and maximum trusted rate is considered a trusted vehicle that can be involved in VANET for communication.

The proposed model generates a key set that contains multiple keys for vehicle authentication, labelling, and secure data outsourcing. The cryptography model-based key generation is used for enhancing the security levels in the VANET, and the operation is performed as

$$Temp1\,[M] = \sum_{v=1}^{M} getVal(v) \tag{10}$$

$$Temp2\,[M] = \sum_{v=1}^{M} getPrime\,(v)\,\{\forall Temp2\,(v) > Temp1\,(v) \tag{11}$$

$$Flag\,[M] = \sum_{v=1}^{M} getRand(v)\,\{\forall Flag\,(v) < Temp2\,(v)\,and\,Flag\,(v) > Temp1(v) \tag{12}$$

$$Mkey\,[M] = \sum_{v=1}^{M} \frac{Temp1\,(v) + Temp2(v)}{Flag(v)} \tag{13}$$

$$Rkey\,[M] = \sum_{v=1}^{M} \frac{Mkey(v)}{Flag(v)} + Temp1\,(v) \ll 2 \tag{14}$$

$$LKey\,[M] = \sum_{v=1}^{M} \frac{Flag\,(v) + Temp2(v)}{Mkey(v)} \gg 2 \tag{15}$$

$$KeyL\,[M] = \sum_{v=1}^{M} RKey\,(v) \oplus Lkey\,(v) + Temp2\,(v) + \frac{Lkey(v)}{Rkey(v)} \tag{16}$$

$$KeyM\,[M] = \sum_{v=1}^{M} Lkey\,(v) \oplus Temp2\,(v) + Rkey\,(v) + \frac{Mkey(v)}{Flag(v)} \tag{17}$$

$$KeyR\,[M] = \sum_{v=1}^{M} Mkey\,(v) \oplus Flag\,(v) + \frac{Temp2(v)}{Temp1(v)} + \frac{(Lkey\,(v) \oplus Mkey\,(v))}{(Rkey\,(v) \oplus Flag\,(v))} \tag{18}$$

$$KeySet\,[M] = \sum_{v=1}^{M} \{KeyL\,(v) : KeyM\,(v) : KeyR\,(v)\} \tag{19}$$

The vehicle labeling is performed to utilize the vehicles for communication. The vehicle labeling is performed using the key set, and transmission is allowed only in the labeled vehicles. The process of labeling is performed as

$$VLabel\,[M] = \sum_{v=1}^{M} AUveh\,(v) + KeyL\,(v) + \frac{\max(VTrust\,(v))}{VReg(v)} \tag{20}$$

The data encryption is performed on the data that can be outsourced in the fog environment. The data that is maintained in a fog environment needs to be secured, and unauthorized access needs to be avoided. Data encryption is performed for the vehicles to securely outsource the data to the fog. The authorized users can gain access and decrypt the data. Privacy preservation is maintained as the proposed model performs strict authentication and access. The process of encryption and decryption is performed as

$$Vmsg\,[M] = \sum_{v=1}^{M} getMsg\,(v) + VReg\,(v) + VTrust(v) \tag{21}$$

$$ITmsg = \sum_{v=1}^{M} Vmsg^{KeyM(v)} modKeyR(v) \tag{22}$$

$$CTmsg = \sum_{v=1}^{M} ITmsg + Mkey\,(v) + Rkey(v) \tag{23}$$

$$Enmsg = \sum_{v=1}^{M} CTmsg^{KeyR(v)} modKeym(v) \tag{24}$$

The process of decryption is performed on authenticated node as

$$Nmsg = \sum_{v=1}^{M} Enmsg^{KeyM(v)} modKeyR(v) \tag{25}$$

$$Gmsg = \sum_{v=1}^{M} Nmsg - MKey\,(v) - Rkey(v) \tag{26}$$

$$Demsg = \sum_{v=1}^{M} Gmsg^{KeyR(v)} modKeyM(v) \tag{27}$$

Algorithm 1: TCA-USVLC

{
Input: Vehicles List {Vlist}
Output: Encrypted and Decrypted Messages
Step 1: Initially register all the vehicles available in the VANET list and maintain all information. Perform registration of all vehicles that are represented as nodes using Eq. (4).
Step 2: Perform the selection of an auditor node in the network that is used to monitor the remaining nodes in the network. The auditor node is selected based on performance, distance, and transmission rate. The auditor node selection is done using Eq. (8).
Step 3: The trust level of each node is calculated by the auditor node, and this trust factor is used to identify the internal behavior and properties of each node in VANET. The trust level calculation is done using Eq. (9).
Step 4: The key generation process is initiated, and the key set contains two keys as a pair. Key set generation involves the generation of public and private keys. The key generation process is performed using Eqs. (17) and (18).
Step 5: Each vehicle is allocated a key pair for secure data transmission and maintaining privacy. The vehicle allocated with keys is labeled. The vehicle labeling is performed using Eq. (20).
Step 6: The key pairs are used by the trusted nodes, and the encryption is performed for outsourcing the data. Any node that receives the encrypted data will decrypt the data for accessing the contents. The encryption and decryption processes are performed using Eqs. (24) and (27).
}

4 Results

VANETs are the wave of the future when it comes to connected cars and smarter highways. Services provided by VANETs include, but are not limited to, enhanced road safety, warning messages, increased comfort, and information sharing via vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. By exchanging safety messages with other vehicles and the infrastructure, drivers may better anticipate and avoid potential dangers and traffic jams. The rising numbers of vehicles, traffic accidents, and fatalities make the use of VANET to enhance road safety an absolute necessity.

Combining the best features of fog computing with those of vehicular cloud computing, a new paradigm in vehicular ad hoc networks has emerged: Fog-based VANETs. Fog-based VANET-based real-time navigation methods can boost the scheme's performance. In this research, we present a fog-based VANET-based vehicular spatial crowdsourcing navigation technique that is both secure and

privacy-preserving. Using real-time traffic data collected by automobiles in their coverage zones, fog nodes collectively determine the best route after crowdsourcing tasks are generated and released. The crowdsourcing vehicle, meanwhile, stands to gain a fair payment for its efforts. This experiment makes use of a Windows 10 PC with an AMD R7 4800 H CPU and 16 GB of RAM. The proposed model is implemented in Python and executed in Google Colab. Users can use Google Colab's GPUs and TPUs, among other powerful processing resources. This allows for the efficient and rapid training and execution of sophisticated security models. The programming language used in this implementation is Python, which is dynamic and high-level. The emphasis is on making the code easy to read and understand. Python is an efficient, versatile, and user-friendly computer language. A lively community of libraries is also present for Python. Many different types of network organizations utilize it. Since it is compatible with many different programming paradigms, Memory management is also handled automatically.

Using wireless networks, vehicles in a VANET can exchange information about traffic and road conditions. Reduced traffic incidents and congestion can be achieved by the exchange of this information. But because some cars may deliberately deceive others, it brings up major safety concerns. Consequently, spotting and correcting false information is crucial. They may lose some of their privacy if they must share information with other vehicles. An automobile also must handle similar issues while processing the data it has received and collected from other vehicles. One way to mitigate the communication and computing load on vehicles while still protecting their privacy is to upload the collected traffic data to the cloud, where the required computation can be run, and then communicate the results to the vehicles. The alternative method may not work, though, because traffic data is time-sensitive.

In intelligent traffic systems, VANETs have become increasingly widespread in recent years. Important aspects of VANET architecture are decentralized networking, quick topology changes, and autonomy. Research into the improvement of transportation systems that can save lives has piqued the interest of both academics and businesses in VANET and its applications for road safety. When it comes to privacy and security in VANETs, the biggest obstacle is message broadcasting in open-access systems like VANETs. There have been numerous suggestions for research into the privacy and security of VANETs. But none of them have taken unobservability and other broad privacy considerations into account. Our proposed privacy-preserving communication scheme (VPPCS) is based on VANETs and aims to solve these problems while also satisfying the needs for contextual and content privacy. Prior to their implementation, VANETs must address a few security issues. VANET is an essential component of an intelligent transportation system (ITS) since it ensures a safe trip by several secure services and applications. Before implementing them, make sure they address privacy and security concerns. This will ensure that VANET communication is secure and that authentication is both efficient and secure. When dealing with complex communication situations, it is important to keep users' privacy in mind.

Researchers have a hard time designing a protocol that can effectively manage inconsistent network topology in VANETs due to the unpredictable nature of the network topology caused by the fast speeds of vehicles. There are unique obstacles to face in every setting. For instance, the primary concern in a sparse network, such as fog-based VANET networks, is the relatively low vehicle density. Even in densely populated areas, network delays might be quite substantial due to factors like poor penetration ratios and low activity during the night.

To ensure the confidentiality of outsourced data, the proposed model takes cryptographic models into account; the keys generated are then stored in the fog for use in authenticating vehicles. If any malicious messages are discovered, the TCA can use the secret key to determine the real identity of

VANETS. The proposed model develops a TCA-USVLC for secure data outsourcing and privacy preservation in VANETS. The proposed model is compared with the traditional AbE with Parallel Outsourced Decryption for Edge Intelligent IoV (AbE-POD), Privacy-Preserving Charging Scheme for Electric Vehicles Using Blockchain and Fog Computing (PPCS), and Secure Data Transmission Mechanism for IoV Considering Privacy Protection in Fog Computing Environment (SDT-IoV-PP). The proposed model, when compared to the traditional model, performs better in privacy preservation and data outsourcing.

The vehicles that are forming a VANET must register the information with the network administrator for further correspondence. The vehicles will be provided with a digital identity that is used for vehicle recognition and to consider only authorized vehicles. The vehicle information registration time levels in milliseconds of the proposed and existing models are shown in Table 1 and Fig. 3.

Table 1: Vehicle information registration time levels in milliseconds

Vehicles considered in VANET	Models considered			
	TCA-USVLC model	AbE-POD model	PPCS model	SDT-IoV-PP model
30	11.0	12.5	13.0	15.4
60	11.2	12.8	14.0	15.8
90	11.5	13.0	15.0	16.0
120	11.6	13.2	16.0	16.3
150	11.8	13.5	17.0	16.7
180	12.0	14.0	18.0	17.0

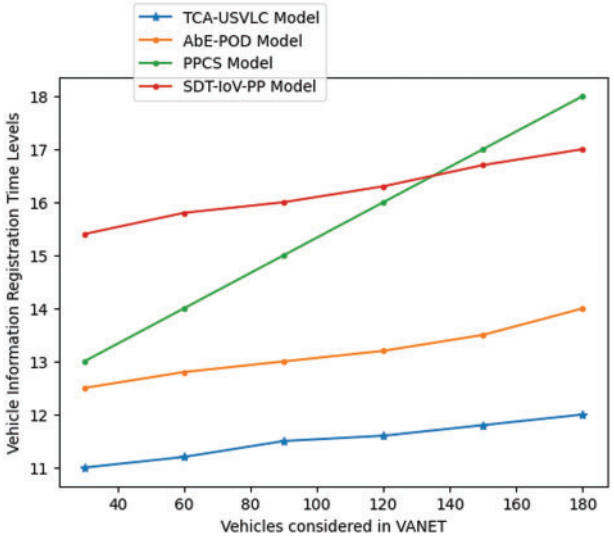

Figure 3: Vehicle information registration time levels in milliseconds

The registered vehicles have a digital identity that is used to recognize authorized vehicles in the VANET. An auditor vehicle selection is performed that monitors the transmission of all vehicles in the VANET to avoid unauthorized access and also to avoid attacks in the VANET. The vehicle with the best transmission rate and the lowest loss rate will be considered an auditor vehicle. Table 2 and Fig. 4 represent the auditor vehicle selection accuracy levels in percentage of the proposed and existing models.

Table 2: Auditor vehicle selection accuracy levels in percentage

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
30	97.7	93.4	93.5	92.8
60	97.9	93.8	94.0	93.0
90	98.0	94.0	94.5	93.2
120	98.2	94.2	95.0	93.4
150	98.4	94.6	95.5	93.7
180	98.5	95.0	96.0	94.0

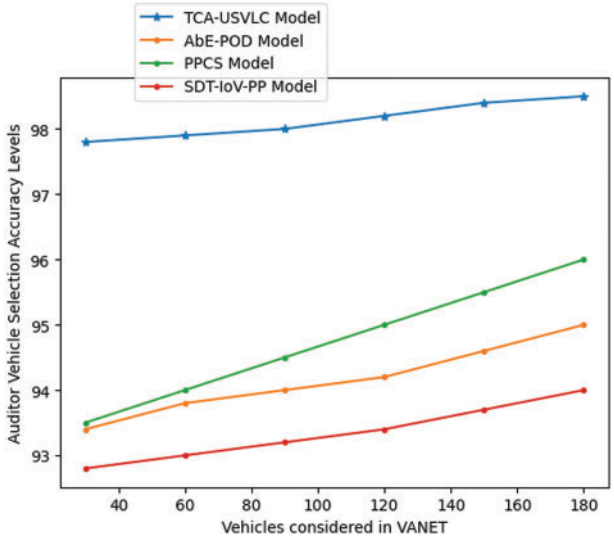

Figure 4: Auditor vehicle selection accuracy levels in percentage

The trust factors of the vehicles registered in the network are calculated by the auditor, who considers the vehicles transmissions and loss levels and privacy preservation levels. The vehicle trust factor is helpful in identifying vehicles causing malicious actions in the network. The vehicle trust calculation time levels in milliseconds of the existing and proposed models are shown in Table 3 and Fig. 5.

Table 3: Vehicle trust calculation time levels in milliseconds

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
30	15.0	16.4	21.7	19.6
60	15.2	16.7	22.0	20.0
90	15.4	17.2	22.1	20.2
120	15.7	17.5	22.4	20.6
150	15.8	17.8	22.7	20.9
180	16.0	18.0	23.0	21.0

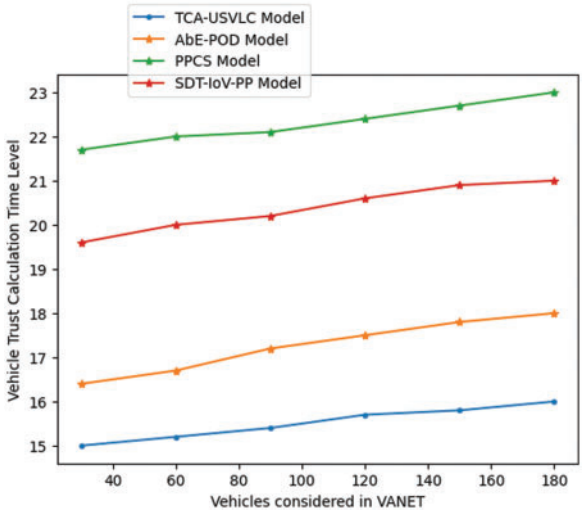

Figure 5: Vehicle trust calculation time level in milliseconds

Cryptography models are used to provide better security levels to the network and to the outsourcing data in the VANET. The proposed model generates key sets for vehicle authentication, vehicle labeling, data outsourcing, and privacy preservation. The key sets generated are used for vehicle labeling and for encryption and decryption of data. The key set generation accuracy levels in percentage of the proposed and existing models are represented in Table 4 and Fig. 6.

Table 4: Key set generation accuracy levels in percentage

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
30	97.5	93.5	95.0	91.0
60	97.7	93.7	95.2	91.1

(Continued)

Table 4 (continued)

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
90	97.9	93.9	95.4	91.4
120	98.0	94.0	95.5	91.6
150	98.1	94.2	95.8	91.8
180	98.3	94.5	96.0	92.0

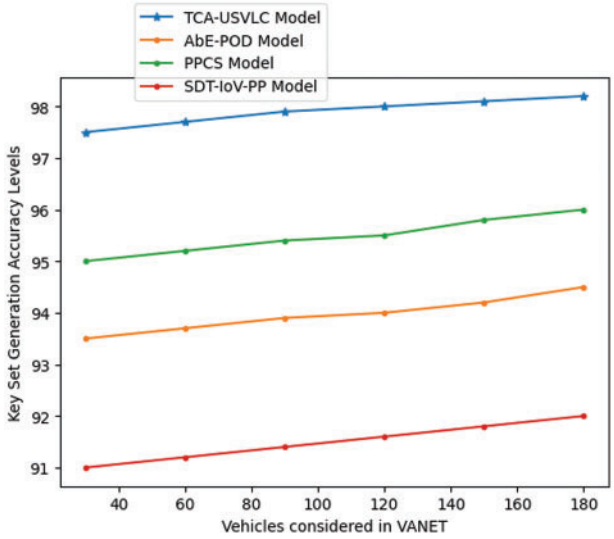

Figure 6: Key set generation accuracy levels in percentage

The trusted vehicles provide a key from the key set to the auditor node to complete the labeling process in the VANET. The vehicle labeling is used to consider only authenticated and trusted vehicles for transmissions. Labelled vehicles are only allowed for data transmission, maintaining security. The vehicle labeling time levels in milliseconds of the traditional and proposed models are shown in Table 5 and Fig. 7.

Table 5: Vehicle labeling time levels in milliseconds

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
30	14.0	17.0	15.0	17.7
60	14.2	17.1	15.3	18.0
90	14.3	17.2	15.5	18.2

(Continued)

Table 5 (continued)

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
120	14.5	17.5	15.6	18.5
150	14.7	17.7	15.8	18.7
180	15.0	18.0	16.0	19.0

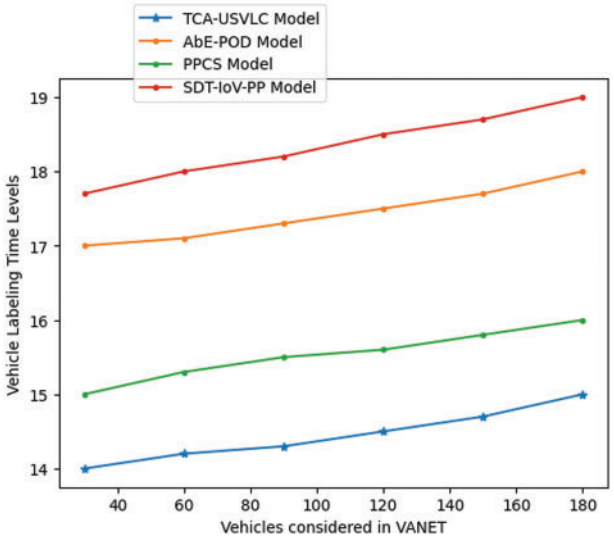

Figure 7: Vehicle labeling time levels in milliseconds

Data encryption refers to the action of encoding data in the VANET during data outsourcing. The plaintext form of the information is changed into the cipher text form throughout this procedure. Only approved-label vehicles would be able to convert cipher text back into plaintext and gain access to the original data. Table 6 and Fig. 8 represent the data encryption accuracy levels in percentage of the proposed and existing models.

Table 6: Data encryption accuracy levels in percentage

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
30	97.9	94.0	91.8	93.3
60	98.0	94.3	92.0	93.6
90	98.1	94.8	92.3	93.8
120	98.3	95.0	92.5	94.0

(Continued)

Table 6 (continued)

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
150	98.4	95.5	92.6	94.3
180	98.6	96.0	93.0	94.5

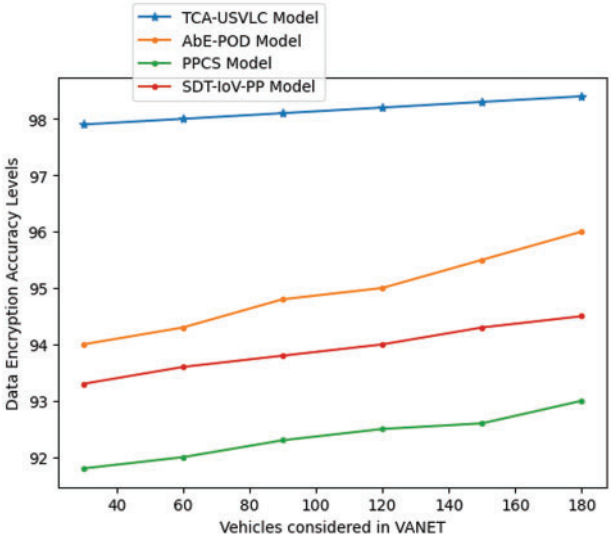

Figure 8: Data encryption accuracy levels in percentage

Data outsourcing is to transmit the data to the other vehicles managed by the Fog model so that vehicles can get traffic or accident-related information. The proposed model performs encryption on the data that will be outsourced to avoid attackers stealing the data. The data outsourcing accuracy levels in percentage of the proposed and existing models are shown in Table 7 and Fig. 9.

Table 7: Data outsourcing accuracy levels in percentage

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
30	97.8	93.6	95.0	91.7
60	98.0	93.8	95.2	92.0
90	98.1	94.1	95.3	92.3
120	98.2	94.3	95.5	92.6

(Continued)

Table 7 (continued)

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
150	98.4	94.6	95.7	92.8
180	98.5	95.0	96.0	93.0

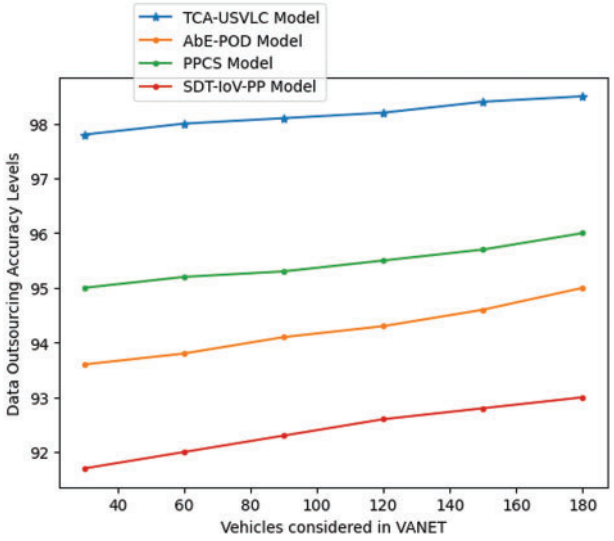

Figure 9: Data outsourcing accuracy levels in percentage

While VANET auditors can keep data-driven systems running smoothly with privacy-preserving technologies, vehicles can keep their personally identifiable information safe from other vehicles in the VANETs. When implemented on a distributed network, the suggested approach makes vehicle authentication much easier to achieve. The suggested technique protects vehicle personal information while still allowing for secure and transparent vehicle authentication on VANETs. Table 8 and Fig. 10 represent the privacy preservation accuracy levelsin percentage of the proposed and existing models.

Table 8: Privacy preservation accuracy levels in percentage

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
30	97.9	93.5	92.7	91.2
60	98.0	94.0	93.0	91.3
90	98.1	94.5	93.2	91.5
120	98.3	95.0	93.5	91.7

(Continued)

Table 8 (continued)

Vehicles considered in VANET	Models considered			
	TCA-USVLC model (%)	AbE-POD model (%)	PPCS model (%)	SDT-IoV-PP model (%)
150	98.4	95.5	93.7	91.8
180	98.6	96.0	94.0	92.0

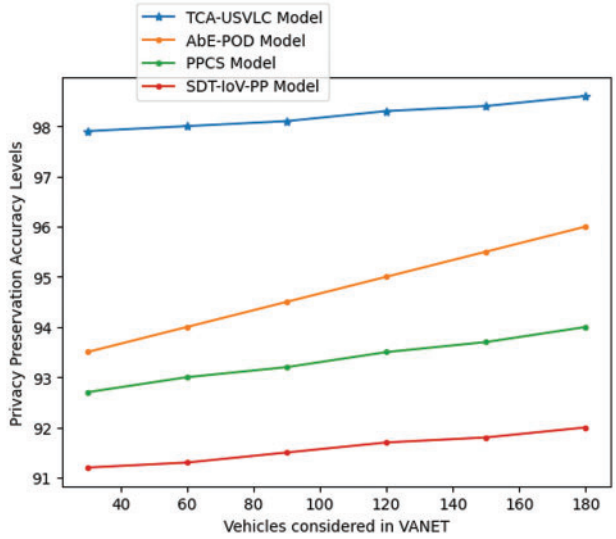

Figure 10: Privacy preservation accuracy levels in percentage

The proposed model evaluation metrics in percentages are indicated in Table 9 and are compared with the traditional models. The results show that the proposed model's performance is higher than that of traditional models, and the error rate of the model is also very low.

Table 9: Evaluation metrics in percentage

Evaluation metrics	Precision (%)	Recall (%)	F1 score (%)	Sensitivity (%)	Specificity (%)
TCA-USVLC model	98.2	96.7	97.4	93.2	94.6
AbE-POD model	93.7	93.1	93.9	90.6	92.1
PPCS Model	91.6	90.5	94.2	89.6	90.5
SDT-IoV-PP model	90.8	91.4	94.2	90.2	89.6

5 Conclusion

The use of VANETs is developing and expanding rapidly, but it still faces significant obstacles that must be overcome before it can be widely adopted. Fog computing Fog computing was created to address these issues by providing low-latency processing and storage services at the periphery of networks. As an expansion of cloud computing, fog computing brings data processing, storage, and sharing closer to end users, eliminating network bottlenecks. But if the computational resources provided by the edge devices are unreliable, data security and privacy could be compromised. A TCA-USVLC is proposed in this research for secure data outsourcing and privacy preservation in VANETS. The authenticity of the vehicle node was verified with this method using auditor labelling before any data sharing could begin. Performance, distance, and transmission rate are the three criteria used to choose the auditor node. The auditor node determines the trust level of every node in VANET and uses this trust factor to determine the internal behaviour and attributes of every node. A key set consisting of a pair of keys is generated once the process is started. Making new public and private keys is part of creating a key set. To facilitate identification, the vehicles that have been assigned key pairs will be labelled. To encrypt data for outsourcing purposes, trusted nodes use key pairs; subsequently, any node that gets the encrypted data can decode it and access its contents. The proposed model calculates the trust of vehicles in 16 ms for an average of 180 vehicles and achieves 98.6% accuracy for data encryption to provide security. The proposed model achieved 98.5% accuracy in data outsourcing and 98.6% accuracy in privacy preservation in fog-enabled VANETs. Establishing a strong system of sender authentication and offering a means to keep the user's location secret are the two main challenges in relation to enabling secure communication in VANETs. It is challenging to develop a protocol that can effectively manage inconsistent network topology in VANETs due to the unpredictable nature of the network topology caused by the fast speeds of vehicles, and it is also challenging to maintain the number of keys for vehicle authentication if more vehicles join the network.

- In the future, elliptic curve cryptography models can be integrated with available models to lower the transmission and processing costs associated with authenticating messages. The varied key size generations models also need to be designed to enhance security levels, avoid attacks in the VANETs, and handle more vehicles joining the network.

Acknowledgement: We acknowledge VIT-AP University for its support in providing the necessary resources to carry out the proposed work.

Funding Statement: The authors received no specific funding for this research.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Nagaraju Pacharla; data collection: Nagaraju Pacharla; analysis and interpretation of results: Nagaraju Pacharla, Srinivasa Reddy K; draft manuscript preparation: Nagaraju Pacharla, Srinivasa Reddy K; supervision and result analysis: Srinivasa Reddy K. All authors reviewed the results and approved the final version.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Z. Guo, G. Wang, Y. Li, J. Ni, R. Du and M. Wang, "Accountable attribute-based data-sharing scheme based on Blockchain for vehicular Ad Hoc Network," *IEEE Internet Things J*, vol. 10, no. 8, pp. 7011–7026, Apr. 15, 2023. doi: 10.1109/JIOT.2022.3228550.

[2] R. Bi, D. Guo, Y. Zhang, R. Huang, L. Lin and J. Xiong, "Outsourced and privacy-preserving collaborative k-prototype clustering for mixed data via additive secret sharing," *IEEE Internet Things J*, vol. 10, no. 18, pp. 15810–15821, Sep. 15, 2023. doi: 10.1109/JIOT.2023.3266028.

[3] W. Zhao *et al.*, "Privacy-preserving outsourcing of K-means clustering for cloud-device collaborative computing in space-air-ground integrated IoT," *IEEE Internet Things J*, vol. 10, no. 23, pp. 20396–20407, Dec. 1, 2023. doi: 10.1109/JIOT.2023.3288012.

[4] K. Gu, K. Wang, X. Li, and W. Jia, "Multi-fogs-based traceable privacy-preserving scheme for vehicular identity in internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 12544–12561, Aug. 2022. doi: 10.1109/TITS.2021.3115171.

[5] H. Zhong, L. Chen, J. Cui, J. Zhang, I. Bolodurina and L. Liu, "Secure and lightweight conditional privacy-preserving authentication for fog-based vehicular ad hoc networks," *IEEE Internet Things J*, vol. 9, no. 11, pp. 8485–8497, Jun. 01, 2022. doi: 10.1109/JIOT.2021.3116039.

[6] X. Zhang, H. Zhong, J. Cui, I. Bolodurina, and L. Liu, "LBVP: A lightweight batch verification protocol for fog-based vehicular networks using self-certified public key cryptography," *IEEE Trans. Vehicular Technol.*, vol. 71, no. 5, pp. 5519–5533, May, 2022. doi: 10.1109/TVT.2022.3157960.

[7] Q. Kong, R. Lu, F. Yin, and S. Cui, "Privacy-preserving continuous data collection for predictive maintenance in vehicular fog-cloud," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5060–5070, Aug. 2021. doi: 10.1109/TITS.2020.3011931.

[8] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV," *IEEE Trans. Vehicular Technol.*, vol. 69, no. 11, pp. 13784–13795, Nov. 2020. doi: 10.1109/TVT.2020.3027568.

[9] H. Li, D. Han, and M. Tang, "A privacy-preserving charging scheme for electric vehicles using Blockchain and fog computing," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3189–3200, Sep. 2021. doi: 10.1109/JSYST.2020.3009447.

[10] W. Zhang and G. Li, "An efficient and secure data transmission mechanism for internet of vehicles considering privacy protection in fog computing environment," *IEEE Access*, vol. 8, pp. 64461–64474, 2020. doi: 10.1109/ACCESS.2020.2983994.

[11] G. Sun, S. Sun, H. Yu, and M. Guizani, "Toward incentivizing fog-based privacy-preserving mobile crowdsensing in the internet of vehicles," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4128–4142, May, 2020. doi: 10.1109/JIOT.2019.2951410.

[12] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, "FBIA: A fog-based identity authentication scheme for privacy preservation in internet of vehicles," *IEEE Trans. Vehicular Technol.*, vol. 69, no. 5, pp. 5403–5415, May 2020. doi: 10.1109/TVT.2020.2977829.

[13] X. Liu, W. Chen, Y. Xia, and C. Yang, "SE-VFC: Secure and efficient outsourcing computing in vehicular fog computing," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 3389–3399, Sep. 2021. doi: 10.1109/TNSM.2021.3080138.

[14] H. Sami, A. Mourad, and W. El-Hajj, "Vehicular-OBUs-as-on-demand-fogs: Resource and context aware deployment of containerized micro-services," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 778–790, Apr. 2020. doi: 10.1109/TNET.2020.2973800.

[15] M. A. Hoque and R. Hasan, "Towards an analysis of the architecture, security, and privacy issues in vehicular fog computing," in *2019 SoutheastCon*, Huntsville, AL, USA, 2019, pp. 1–8. doi: 10.1109/SoutheastCon42311.2019.9020476.

[16] K. Liu, K. Xiao, P. Dai, V. C. S. Lee, S. Guo and J. Cao, "Fog computing empowered data dissemination in software defined heterogeneous VANETs," *IEEE Trans. Mob. Comput.*, vol. 20, no. 11, pp. 3181–3193, Nov. 01, 2021. doi: 10.1109/TMC.2020.2997460.

[17] C. Zhu *et al.*, "Folo: Latency and quality optimized task allocation in vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4150–4161, Jun. 2019. doi: 10.1109/JIOT.2018.2875520.

[18] S. S. Lee and S. Lee, "Resource allocation for vehicular fog computing using reinforcement learning combined with heuristic information," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10450–10464, Oct. 2020. doi: 10.1109/JIOT.2020.2996213.

[19] Z. Zhou, H. Liao, X. Zhao, B. Ai, and M. Guizani, "Reliable task offloading for vehicular fog computing under information asymmetry and information uncertainty," *IEEE Trans. Vehicular Technol.*, vol. 68, no. 9, pp. 8322–8335, Sep. 2019. doi: 10.1109/TVT.2019.2926732.

[20] H. Du, S. Leng, F. Wu, X. Chen, and S. Mao, "A new vehicular fog computing architecture for cooperative sensing of autonomous driving," *IEEE Access*, vol. 8, pp. 10997–11006, 2020. doi: 10.1109/ACCESS.2020.2964029.

[21] Y. Wang, C. Xu, Z. Zhou, H. Pervaiz, and S. Mumtaz, "Contract-based resource allocation for low-latency vehicular fog computing," in *2018 IEEE 29th Annu. Int. Symp. Personal, Indoor Mobile Radio Commun. (PIMRC)*, Bologna, Italy, 2018, pp. 812–816. doi: 10.1109/PIMRC.2018.8580843.

[22] Z. Wei, J. Li, X. Wang, and C. Z. Gao, "A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing," *IEEE Access*, vol. 7, pp. 62785–62793, 2019. doi: 10.1109/ACCESS.2019.2915794.

[23] C. Lai, Q. Li, H. Zhou, and D. Zheng, "SRSP: A secure and reliable smart parking scheme with dual privacy preservation," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10619–10630, Jul. 1, 2021. doi: 10.1109/JIOT.2020.3048177.

[24] K. Liu, X. Xu, M. Chen, B. Liu, L. Wu and V. C. S. Lee, "A hierarchical architecture for the future internet of vehicles," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 41–47, Jul. 2019. doi: 10.1109/MCOM.2019.1800772.

[25] A. Thakur and R. Malekian, "Fog computing for detecting vehicular congestion, an internet of vehicles based approach: A review," *IEEE Intell. Transp. Syst. Mag.*, vol. 11, no. 2, pp. 8–16, 2019. doi: 10.1109/MITS.2019.2903551.

[26] Y. Zhang, R. Wang, M. S. Hossain, M. F. Alhamid, and M. Guizani, "Heterogeneous information network-based content caching in the internet of vehicles," *IEEE Trans. Vehicular Technol.*, vol. 68, no. 10, pp. 10216–10226, Oct. 2019. doi: 10.1109/TVT.2019.2936792.

[27] B. Qin and D. Zheng, "Generic approach to outsource the decryption of attribute-based encryption in cloud computing," *IEEE Access*, vol. 7, pp. 42331–42342, 2019. doi: 10.1109/ACCESS.2019.2907364.

[28] M. Abbasi, M. Yaghoobikia, M. Rafiee, A. Jolfaei, and M. R. Khosravi, "Efficient resource management and workload allocation in fog-cloud computing paradigm in IoT using learning classifier systems," *Comput. Commun.*, vol. 153, pp. 217–228, 2020. doi: 10.1016/j.comcom.2020.02.017.

[29] S. Ghane, A. Jolfaei, L. Kulik, K. Ramamohanarao, and D. Puthal, "Preserving privacy in the internet of connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5018–5027, Aug. 2021. doi: 10.1109/TITS.2020.2964410.

[30] Y. Wu, J. Wu, L. Chen, G. Zhou, and J. Yan, "Fog computing model and efficient algorithms for directional vehicle mobility in vehicular network," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2599–2614, May 2021. doi: 10.1109/TITS.2020.2971343.

[31] K. Kaur, S. Garg, G. Kaddoum, E. Bou-Harb, and K. K. R. Choo, "A big data-enabled consolidated framework for energy efficient software defined data centers in IoT setups," *IEEE Trans. Ind. Inform.*, vol. 16, no. 4, pp. 2687–2697, Apr. 2020. doi: 10.1109/TII.2019.2939573.

[32] K. Gu, N. Wu, B. Yin, and W. Jia, "Secure data query framework for cloud and fog computing," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 332–345, Mar. 2020. doi: 10.1109/TNSM.2019.2941869.