Computers, Materials &
Continua

Tech Science Press

DOI: 10.32604/cmc.2024.059238

ARTICLE

A Support Vector Machine (SVM) Model for Privacy Recommending Data Processing Model (PRDPM) in Internet of Vehicles

Ali Alqarni*

Department of Computer Science and Artificial Intelligence, College of Computing and Information Technology,
University of Bisha, Bisha, 61922, Saudi Arabia

*Corresponding Author: Ali Alqarni. Email: aqrni@ub.edu.sa

Received: 01 October 2024 Accepted: 20 November 2024 Published: 03 January 2025

ABSTRACT

Open networks and heterogeneous services in the Internet of Vehicles (IoV) can lead to security and privacy challenges. One key requirement for such systems is the preservation of user privacy, ensuring a seamless experience in driving, navigation, and communication. These privacy needs are influenced by various factors, such as data collected at different intervals, trip durations, and user interactions. To address this, the paper proposes a Support Vector Machine (SVM) model designed to process large amounts of aggregated data and recommend privacy-preserving measures. The model analyzes data based on user demands and interactions with service providers or neighboring infrastructure. It aims to minimize privacy risks while ensuring service continuity and sustainability. The SVM model helps validate the system's reliability by creating a hyperplane that distinguishes between maximum and minimum privacy recommendations. The results demonstrate the effectiveness of the proposed SVM model in enhancing both privacy and service performance.

KEYWORDS

Support vector machine; big data; IoV; privacy-preserving

Glossary/Nomenclature/Abbreviations

IoV	Internet of vehicles
SVM	Support vector machines
VANET	Vehicular ad-hoc network
ML	Machine learning

1 Introduction

Big data is a technology that analyzes or identifies data from a large amount of heterogeneous data. Big data technology is widely used in various fields to improve the efficiency ratio of systems [1]. The Internet of Vehicles (IoV) faces various privacy and security issues that cause severe damage to the network. Big data-based privacy-preserving schemes are used in IoV that provide feasible privacy services to the users [2–4]. Big data-based technique identifies the key privacy issues which occurred during the authentication process. A vehicular ad-hoc network (VANET) is implemented in

Copyright © 2025 The Author. Published by Tech Science Press.
This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IoV which provides prominent services to the users [5]. Big data solves privacy issues that improve the performance range of the networks. The actual goal of big data in privacy issues is to increase the safety and security level of users from third-party members [6]. An authentication and key agreement (AKA) scheme is mostly used in IoV systems [7]. AKA scheme provides a secret key value to the users used during the authentication process. The secret key values contain important values that reduce the complexity of the authentication process [8]. The AKA scheme ensures the privacy and security level of user data from unauthorized persons in IoV networks. A privacy-preserving data-sharing scheme is also used in IoV [9]. The privacy-preserving scheme collects the data captured via vehicular sensors. The sensors produce optimal information for the authorization process that reduces the authentication error [10]. The privacy-preserving scheme improves the trustworthiness and feasibility level of IoV by providing optimal privacy services to the users. A blockchain (BC), based privacy-preserving policy is also used in IoV which preserves users' data from hackers. The BC-based policy is a distributed framework in IoV [11]. A filtering model is used in the policy which filters the privacy issues based on priorities and severity. The BC-based policy achieves high privacy that improves the performance range of IoV systems [12]. Machine learning (ML) algorithms are commonly used for detection and prediction processes. ML algorithm is used in IoV to identify the privacy issues which occurred in the systems [13]. A long short-term memory (LSTM) algorithm-based privacy framework is used for IoV. The LSTM model is mainly used to detect intrusion in IoV. The detected intrusion provides relevant data for privacy-preserving policies. The LSTM models increase the accuracy of intrusion detection which enhances the efficiency of privacy-preserving policies. The LSTM model improves the quality of experience (QoE) range of the systems [14,15]. A deep reinforcement learning (DRL) algorithm is also used in the privacy management process. The DRL algorithm uses a task offloading scheme that provides an effective architecture for IoV [16]. The DRL algorithm analyses the datasets which are relevant to privacy and security. The DRL-based privacy policy ensures the safety and security level of users in IoV [17]. A privacy-preserving-based secured framework (P2SF) for IoV provides an efficient enclosure technique for securing users' data from third-party members. The P2SF maximizes the performance range of the systems [18].

1.1 Motivation

This work is motivated by the growing need for privacy-preserving data processing inside the Internet of Vehicles (IoV) context, where substantial volumes of sensitive, diverse data are shared to provide connected and autonomous vehicle services. As IoV networks expand, the danger of privacy violation increases due to data sharing across diverse vehicle, edge, and cloud infrastructures. The research acknowledges the difficulty of maintaining user and vehicle privacy while providing real-time, responsive services essential for applications such as traffic management, safety warnings, and predictive maintenance. Conventional privacy-preserving models often encounter difficulties reconciling privacy with the requisite performance for Internet of Vehicles (IoV) systems, particularly under substantial data loads on congested networks. This work aims to address this gap by creating a scalable and effective privacy-preserving approach, the Privacy Recommending Data Processing approach (PRDPM), focusing on the adaptation to the dynamic data and security requirements specific to IoV contexts. The emphasis on enhancing Support Vector Machine (SVM) techniques inside PRDPM is to provide a resilient solution that maintains privacy while preserving performance, following the advancing framework of intelligent transportation systems. This study ultimately addresses the increasing need for secure, dependable, and privacy oriented IoV infrastructures, enhancing the safety and efficiency of transportation networks.

1.2 Contribution

Privacy-preserving in IoV requires dynamic mobility support and sustainable security implications across heterogeneous application demands. Based on the available data, the augmenting privacy demands are to be classified under differential security. This augmentation is satisfied by the limited methods proposed above such that the processing increases the complexity without instigating the recommendations. By considering this feature across various information exchange intervals, the proposed model is designed to mitigate the above issues.

The following are the contributions of this article:

- Proposes an SVM based Internet of Vehicles privacy recommended processing model to increase service sustainability under safe application environments.
- Using support vector classification to validate the privacy presence and sustainability enriches the recommendations throughout several service intervals.
- Validating the consistency of the suggested model by means of a comparison analysis conducted under several criteria and approaches connected to security and data handling.

The rest of the paper is prearranged as follows: Section 2 discusses the related works, Section 3 proposes the PRDPM model, Section 4 deliberates the results and discussion, and Section 5 concludes the research paper.

2 Related Work

For the IoV, Aman et al. have presented a scalable and privacy-preserving authentication system [19]. Offering IoV users efficient services is the key goal. Here we reduce the complexity ratio in the authentication process using physical unclonable functions. The suggested paradigm raises the IoV system security level. In another work, for location-based service (LBS) in IoVs, Huang et al. have put up a privacy-preserving scheme. Mostly, the LBS is utilized to give drivers the best services [20]. LBS finds the precise positions of the cars improving IoV performance. The suggested system optimizes IoV safety and privacy ranges. The other work by Benarous et al. has presented a concerted silence-based location privacy-preserving method (CSLPPS) [21]. Travelling unlinkable attacks are detected by the CSLPPS. The CSLPPS marks the cyber-attacks that reduce task performance delay. The scheme raises the authentication process's performance degree.

A privacy-preserving data scheduling in the incentive-driven vehicular network (VN) has been suggested by Xia et al. [22]. The real objective is to offer VN cars a suitable data scheduling method. Here efficient data security services are given to the users by means of an incentive structure. The scheduling guarantees the degree of security during the data transfer process. In another work, Liu et al. have built up a distributed and privacy-preserving reputation system for the social Internet of Vehicles (SIoV) [23]. From third-party members, the suggested system guarantees users' safety and privacy spectrum. The system investigates the privacy and attacks of the networks using Blockchain (BC) technologies. The suggested system raises SIoV's performance range and efficiency. While Atmaca et al. have put up a privacy-preserving way of planning [24]. This offers the users efficient routing schemes. Furthermore, included in the planned system are graph-based location-sharing mechanisms among the cars. The suggested system maximizes IoVs' spectrum of privacy efficacy. For IoV, Zhang et al. have presented a blockchain (BC) enabled data access approach based on attribute-based encryption [25]. Here the Roadside Unit (RSU) generates ideal data for regulations aimed at maintaining privacy. Here the BC is mostly utilized to find the latent characteristics of the encryption mechanism. The technique improves IoV systems' safety and privacy ratio. While Xing et al. have proposed SIoV a location entropy-based privacy protection (LEPPV) algorithm [26]. The major goal is to give the users appropriate location entropy elements. We find points of interest (POIs) that generate required data for the process of location entropy. The suggested method guarantees the systems' security and privacy degree. In another work, Benarous et al. presented a location privacy-preserving method for the Internet of Vehicles (CE-IoV) supported by clouds [27]. The suggested method maximizes CE-IoVs' level of competence and robustness. For IoV, Hu et al. presented a lightweight and safe privacy-preserving data aggregation (SLPDA) system [28]. The system encrypts the data used for authentication by means of masking technology. SLDPA points out the cyberattacks that happened during the authentication procedure. The presented SLPDA reduces the IoV authentication overload ratio. For vehicle clouds (VC), Hu et al. developed an effective privacy-preserving data query and dissemination technique (EPDQD) [29]. Relevant datasets available for the querying procedure come from the roadside unit (RSU). Effective codes for the authentication process are given by the planned EPDQD system. In another work, for the SIoV, Lai et al. built a trust-based privacy-preserving friend-matching system [30]. The system filters the required hostile cars using Bloom filters. The relevant datasets for the privacy-preserving process are examined using a theoretical analytical approach. The proposed system maximizes the accuracy in a matching process thereby improving SIoV's efficiency level. For vehicle ad-hoc networks (VANET), Ren et al. presented an effective distance-based privacy-preserving authentication (EDPPA) system [31]. For third-party users, the EDPPA optimizes the safety and security spectrum of users. The suggested EDPPA lowers the complexity and latency in the authentication procedure.

Privacy-preserving in IoV requires dynamic mobility support and sustainable security implications across heterogeneous application demands. Based on the available data, the augmenting privacy demands will be classified under differential security. This augmentation is satisfied by the limited methods proposed above such that the processing increases the complexity without instigating the recommendations. Considering this feature across various information exchange intervals, the proposed model mitigates the above issues. Hence, this paper proposes the Privacy Recommending Data Processing Model (PRDPM) for Internet Vehicles to improve service sustainability under secure application conditions.

Table 1 discusses the works related to the proposed model by referencing the techniques and their results.

Table 1: Related works with techniques and results

Work	Method	Key area	Technique used	Results	Limitations
Aman et al. [19]	Privacy-preserving and scalable authentication	Effective services to IoV users	Physical unclonable functions	Increases the security level	Limited scalability
Huang et al. [20]	A location-based service in IoVs	Optimization of services	LBS identifies the exact location of the vehicles	Maximizes the privacy and safety range of IoVs	Delays in real-time response
Benarous et al. [21]	Concerted silence-based location privacy-preserving scheme	Detection of unlinkable attacks	CSLPPS to minimizes the latency	Improved authentication process.	Limited to specific attack types; may miss others
Xia et al. [22]	Privacy-preserving data scheduling	An effective data scheduling algorithm for VN vehicles	Incentive mechanism	Improved the security level	High reliance on user participation for incentives

(Continued)

Table 1 (continued)

Work	Method	Key area	Technique used	Results	Limitations
Liu et al. [23]	Safety and privacy	Decentralized and privacy-preserving reputation	Blockchain technology	Increases the effectiveness and performance	High computational cost
Atmaca et al. [24]	A privacy-preserving route planning	It provides effective routing plans to the users	Graph-based location-sharing	Maximizes the privacy	Limited flexibility
Zhang et al. [25]	A blockchain enabled data access	Optimization of the data for privacy-preserving	Hidden attributes of the encryption process	Improves safety and privacy ratio	Increased computational load
Xing et al. [26]	Privacy protection	Location entropy-based privacy protection	Points of Interest (POI) are detected, producing necessary data.	Increases privacy and security level	May produce low accuracy in high-entropy areas
Benarous et al. [27]	Privacy-preserving	Location-based privacy-preserving	Method for Internet of Vehicles supported by clouds	Maximizes competence and robustness	Limited scalability
Hu et al. [28]	Privacy-preserving	Masking technology	Safe privacy-preserving data aggregation (SLPDA)	Reduces the IoV authentication overload ratio	High computational cost
Hu et al. [29]	Privacy-preserving	Effective privacy-preserving data query and dissemination technique (EPDQD)	Relevant datasets available for the querying procedure	Effective codes for the authentication process	Limited scalability
Lai et al. [30]	Privacy-preserving	Trust-based privacy-preserving friend-matching system	The system filters the required hostile cars using Bloom filters	Maximizes the accuracy in a matching process	High computational cost
Ren et al. [31]	Privacy-preserving authentication	An effective distance-based privacy-preserving authentication (EDPPA) system	For vehicle ad-hoc For third-party users, the EDPPA optimizes the safety and security spectrum of users	Minimizes the complexity and latency in the authentication procedure	High computational cost

3 SVM-Based Privacy Recommending Big Data Processing Model

Big data is the information that comprises a significant amount of data about the input provided by the user, which is then processed to achieve better results through the improvement of data collection. A support vector machine (SVM) is a regulated machine learning algorithm that accomplishes categorization or relapse processes by executing a boundary that separates data into two categories. Cloud services in this privacy-preserving process promote the flow of user data from the service providers and then based on this the support vector machine algorithm takes place through the internet, to the provider's requirements, and back. The IoV network necessitates the implementation of applications for neighbors and service providers. Based on the prior service response, two application demands have been identified: privacy and service response. To determine the existence and sustainability, these outputs are sent into the support vector machine algorithm. Cloud and IoT services also reveal similar persistence and longevity. The support vector algorithm consists of two planes which are the operation plane and the data plane. And for differentiation, the data plane and the operational plane, the hyperplane engendered. These distinguished application demands are used for the determination of the min-max privacy conclusions for existence and sustainability. The services are provided to the users according to the output of the support vector algorithm.

By segmenting sensitive information from non-sensitive data at the decision boundary of the support vector machine (SVM) model, hyperplane differentiation is an essential privacy safeguard in PRDPM. This method separates potentially sensitive information from ordinary data used for analysis in vehicular communications by establishing discrete hyperplanes that categorize data according to sensitivity levels. While less sensitive data may be accessed more readily for real-time applications, PRDPM processes highly sensitive data with greater privacy protections. Even while data flows constantly inside the IoV network, this differentiation layer limits the visibility of sensitive data across connection intervals, thus reducing privacy leakage. To improve privacy without sacrificing real-time processing, hyperplane differentiation allows quicker data segregation and prioritization. The SVM model efficiently sorts incoming data according to privacy needs and routes it accordingly, allowing real-time operations to analyze the most important data without latency. In dense IoV networks, this efficiency is especially useful because of the high speed of vehicle communication and the need for strong privacy protections and quick data access. To maintain high performance in congested IoV settings, PRDPM streamlines data processing by targeted categorization at the hyperplane level, balancing real-time processing demands with privacy protection.

The applications are demanded by the users through the IoV for the accomplishment of the service according to the requirements. These vehicles help in the enhancement of the safety of the information and the fastest response though. The service provider considers the demand of the users before processing the privacy-preserving procedure.

The application demand by the user is the foremost step in the service accomplishment operation and then the process is initiated based on the demand and it checks the authentication for further processes. The service response and the privacy of the previous response are the vital application demand the demand must be validated based on these characteristics. Then the support vector machine algorithm helps in determining the services for the users depending on the demands with the high privacy which helps in protecting the data from malfunctions. Depending on these application demands, further processes take place and then the services are provided for the users with high privacy preserving data. The following Eq. (1) shows how to get users to request an application demand through the IoV [2].

$$\left.\begin{array}{c}
\langle a,b\rangle\, x^{2} = \langle a^{x}, b^{x}\rangle\, x + \langle a^{x_1}, b^{x_2}\rangle\, x \\
\langle a,b\rangle\, x = \langle a^{x}, b^{x}\rangle\, x + \langle a^{x_1}, b^{x_2}\rangle\, x + 1\left(\langle a^{x}, b^{x_1}\rangle\, x - \langle a^{x_1}, b^{x}\rangle\, x\right) \\
a = a^{x} + x_1 a^{1} \\
b = b^{x} + x_1 b^{1} \\
x_1\langle a,b\rangle = \begin{bmatrix} x_1 a & x_1 b & \ldots & x_1 ab \\ x_1 a_1 & x_1 b_1 & \ldots & x_1\left(a_1 b_1\right) \\ \vdots & \vdots & \ddots & \vdots \\ x_n a_n & x_n b_n & \cdots & x_n(a_n b_n) \end{bmatrix}
\end{array}\right\}. \tag{1}$$

The *a* represents application demands generated by the users while *b* is represents the procedure of the IoV in this application, *x* is represent the classification of the demands *a*. Now the application demand is classified into two namely: service response and then the privacy. The service response is the one which checks whether the service is accomplished on time to the users or not. Based on the previous service production processes, the taken for the execution of the service is consolidated in this service response category in the application demand. By associating the service response from the previous processes, the further procedure takes place by preserving the privacy of the users' personation details. The process of service response in the application demand can be shown by the Eq. (2) below [2]:

$$\left.\begin{array}{c} \varphi_C\left(Z\right) = \varphi_C(a+b) \\ = \varphi_C(a,b) \\ = \varphi_{C_1}\left(a,b\right) + x\varphi_C(a+b) \\ \varphi_C\left(a+b\right) = x_1\left(\cdot\left(a,b\right)\right) \\ C = a + x_1 b \\ \left\langle \varphi_x\left(C\right), \varphi_{x_1}(C')\right\rangle x = \left\langle \varphi_C\left(a+b\right), \varphi_{x_1}(a',b')\right\rangle x \\ = \varphi_C\left((a',b')\cdot(a,b)\right) \end{array}\right\}. \tag{2}$$

The φ is the service response while C is represents previous processes, and Z is the response of the service in the previous process. Based on the service response and privacy, the substantiating process of the acquired demands takes place for the enhancement of the privacy-preserving operation. An Eq. (3) below shows how the user's authentication of the application is demanded by the application 2.

$$\left.\begin{array}{c} b_c^T\left(Z,Z'\right) = b_c^T(Z',Z) \\ b_c^x\left(Z,Z'\right) = b_c^x(Z',Z) \\ \sum_{n,x=1}^{n} C_n C_x b_c^T(Z_n, Z_x) = 0 \\ where, \\ n > 0, C_1 \ldots\ldots C_n \in C \\ Z_1 \ldots\ldots Z_n \in X \end{array}\right\}. \tag{3}$$

The T in Eq. (3) represents the authentication procedure. The procedure's privacy has now been validated in preparation for the next steps. The privacy production for the prior service execution is determined by the application requirements.

The authentication for privacy is led using registration to validated phases. First the session, the request relies on C for the existing vehicle whereas the new vehicles Z from any a. Therefore, the authentication process requires Z_1 to $Z_n \in X$ satisfaction for maximizing ψ. Those outcomes are associated with enhancements in the privacy-preserving process in the existing service production procedures. Based on the previous service response, the privacy level of the present method is validated in the application demands. Then this output is given as the input to the support vector machine algorithm to estimate the existence and sustainability. The process of determining the privacy of the previous response is explained by the following Eq. (4) given below [2]:

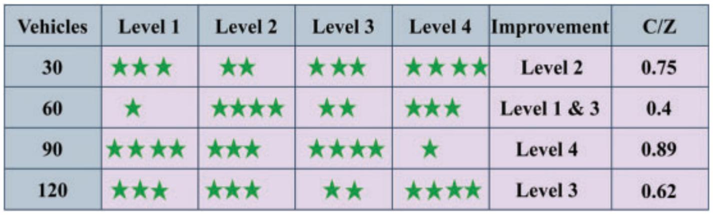
$$\left.\begin{array}{c} \sum_{n,x=1}^{n} Z_n Z_x b_c^T\left(x_n, x_c\right) = -\sum_{n,x=1}^{n} c_n c_x b_c^T\left(Z_n, Z_x\right) \\ = -\sum_{n,x=1}^{n} c_n c_x b_c^T\left(Z_x, Z_n\right) \\ \sum_{n,x=1}^{n} c_n c_x b_c^T\left(Z_n, Z_x\right) = 0 \end{array}\right\}, \tag{4}$$

where Z is represented as the privacy of the previous response of the service providers. The validation process takes place depending on the outcome of the service providers and the privacy of the previous response. Now based on the determined previous response, the present privacy level of the process is acquired then these outcomes are given to the algorithm for the determination of the planes fand the hyperplane boundary between the existence and the sustainability. The process of determining the present privacy level of the method based on the previous response is explained by the following Eq. (5)

given below [2]:

$$\left.\begin{array}{c} L_c^T = \left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix}\right) = \sum_{n=1} \left(b_c\left(Z, Z'\right)\right) \\ = \sum_{n=1}^{x} \left[\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \times \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix}\right] \\ Z = x + Ty \\ Z' = x' + Ty' \\ n > 0, b_1 \ldots\ldots b_n \in T \\ Z_1 \ldots\ldots Z_n \in X \end{array}\right\}, \tag{5}$$

where L is denoted as the present privacy level based on the previous service response. Then these outcomes are given as the input to the support vector machine algorithm for the determination of the existence and sustainability. The privacy level-based recommendations assessment for improvement is illustrated in Fig. 1.



Vehicles	Level 1	Level 2	Level 3	Level 4	Improvement	C/Z
30	★★★	★★	★★★	★★★★	Level 2	0.75
60	★	★★★★	★★	★★★	Level 1 & 3	0.4
90	★★★★	★★★	★★★★	★	Level 4	0.89
120	★★★	★★★	★★	★★★★	Level 3	0.62

Figure 1: Privacy level improvement

In the above representation, the 4 stars represent (verification, authentication, approval, and response), respectively. If the levels are exhibiting multiple variations, then improvements are high. This level determination is performed using ψ from C such that c/Z is to be high. If the variations are suppressed, then authentication is provided for frequency response and therefore the Z levels are improved. Considering the changes in the level the SVM classification is performed (Fig. 1). Here in this support vector algorithm, two planes take place, the data plane, and the operational plane. The conceptual big data is exploited from this part based on the information aggregated from multiple intervals, travel time, and the communication established between the vehicles. Initially the vehicle information occupies the fundamental role for introducing and verifying a vehicle before communication. Besides the communication related information, the privacy levels, and agreements form the second level of big data. The accumulated data contains both necessary and trivial utilization that is handled using support vectors. The hyperplane is the divider that differentiates the two planes from the boundary. The existence and sustainability are identified with the help of the support vector machines in the operational planes for further processes. The existence and the sustainability are the data planes where the operation plane is helping in making the decisions based on the data plane. The process of support vector machine in the identification and the authentication operation is explained by the following Eq. (6) given below:

$$\left.\begin{array}{c} W_c^T = \left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} a' \\ b' \end{pmatrix}\right) = \sum_{x=1}^{n} (XC\,(Z, Z') \\ \sum_{n,x=1}^{n} W_n W_x W_C(Z_n, Z_x) \geq 0 \\ \sum_{n,x=1}^{n} W_n W_x W_C\,(Z_n, Z_x) = \sum_{n,x=1}^{n} W_n W_x W_c^T(Z_n, Z_x) \\ T \sum_{n,x=1}^{n} W_n W_x W_c^x\,(x_n, x_T) = \sum_{n,x=1}^{n} W_n W_x W_c^x(x_n, x_T) \\ \sum_{n,x=1}^{n} Z_n W_x X_c^T(Z_n, Z_x) > 0 \\ \sum_{n,x=1}^{n} Z_n X_T C_n \left(\begin{pmatrix} a_n \\ b_n \end{pmatrix}, \begin{pmatrix} a_x \\ b_x \end{pmatrix}\right) \geq 0 \end{array}\right\}, \tag{6}$$

where W is denoted as the operation of the support vector machine algorithm in the identification procedure. The existence and sustainability are determined by using the support vector machine with the help of the outcome of the previous service response and then the privacy of the previous service response. Here the min-max recommendation is determined by validating the above-mentioned features in the operational plane. The recommendations are extracted from the characteristics of the support vector machine algorithm, and it is explained by the following Eq. (7) given below:

$$\left.\begin{array}{l} G = \frac{1}{2}||W||^2 + \frac{1}{2}||W||^2 + \frac{C}{X} \sum_{n=1}^{G} (x_1 x_2 + c_1 c_2) \\ = \sum_{n=1} \left[\hat{W}_n \begin{pmatrix} a_n \\ b_n \end{pmatrix}, W_x \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + \hat{X}_n \begin{pmatrix} a_n \\ b_n \end{pmatrix}, X_c \begin{pmatrix} a_c \\ b_c \end{pmatrix}\right] \\ = \sum_{x=1} \left[\hat{X}_n \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, X_c \begin{pmatrix} a_c \\ b_c \end{pmatrix} + \hat{W}_n \begin{pmatrix} a_n \\ b_n \end{pmatrix}, W_x \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}\right] \\ = \sum_{n=1} \left[b_n \begin{pmatrix} a_n \\ b_n \end{pmatrix} + Z_n \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} * Z_n \begin{pmatrix} a_n \\ b_n \end{pmatrix} + b_n \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}\right] \\ = \sum_{x=1}^{n} G\,(x_1, Z_1) + \sum_{n=1}^{x} C(y_1, Z_1) + \sum_{x=1}^{T} W(a_1, b_1) \end{array}\right\}, \tag{7}$$

where G is represented as the recommendations extracted from the vector machine algorithm. Now the existence and the sustainability are identified for the service accomplishment process without any lags and issues. The SVM operation of privacy existence verification is presented in Fig. 2.

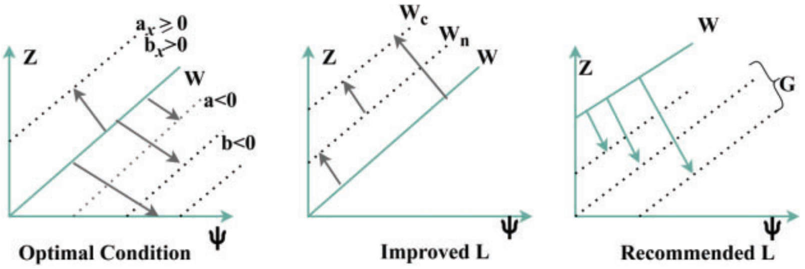


Figure 2: SVM process for privacy existence verification

The variations between W and (Z, ψ) for three outcomes: optimal, improved, and recommendation based. The $a_x, b_x \geq 0$ identifies the optimal condition for Z maximization from ψ. This condition is retained $\forall W_n$ toW_c indicating the L improvement. Any variation in W_n or W_c across W surpassing $a_x, b_x \geq 0$ is induced for a recommendation. In the recommendation for L, the G variation across $x_1 x_2$

and c_1, c_2 are validated such that ψ is less compared to the previous C. Therefore, the improvements are pursued in the recommended L as presented in Fig. 2. The existence is the one in the support vector machine, used in the estimation of the privacy whether it is in the data or not before executing the services to the users according to their requirements. The privacy level of the present data execution process is determined in this existence identification process. As mentioned earlier, the aggregated data is filtered for its non-trivial utilization based on control plane operations. The accumulated voluptuous data is split for its non-trivial validation for privacy check preventing anonymous communication. The major big data is filtered for the privacy related information; the existence of this data is the travel/communication time. In the consecutive interval, the privacy levels are validated for preventing sustainability failures. The process of determining the existence is explained by the following Eq. (8) given below:

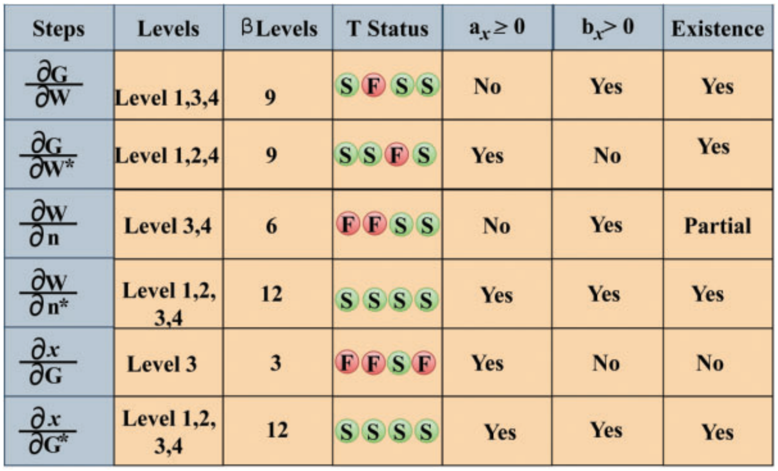
$$\left.\begin{aligned} \frac{\partial G}{\partial W} &= \frac{1}{2}W + \frac{1}{2}\sum\nolimits_{n=1} \alpha\varphi_c\left(Z_n\right) - \frac{1}{2}\sum\nolimits_{n=1}^{x} \varphi_c\left(a,b\right) \\ &= T\frac{1}{2}\sum\nolimits_{n=1}^{x} b_n\varphi_c\left(Z_n\right) + \frac{1}{2}\sum\nolimits_{x=1}^{n} \hat{b}_n\varphi_c\left(Z_n\right) \\ \frac{\partial G}{\partial W^*} &= \frac{1}{2} + \frac{1}{2}\sum\nolimits_{n=1} \beta\varphi_c\left(G_n\right) - \frac{1}{2}\sum\nolimits_{n=1}^{x} \varphi_c\left(x,y\right) \\ &= T\frac{1}{2}\sum\nolimits_{n=1}^{x} a_n\varphi_c\left(G_n\right) + \frac{1}{2}\sum\nolimits_{x=1}^{n} \hat{a}_n\varphi_c\left(x_n\right) \\ \frac{\partial G}{\partial x} &= \frac{1}{2}\sum\nolimits_{n=1} \frac{\partial G}{\partial W} + T\frac{1}{2}\sum\nolimits_{x=1} \frac{\partial G}{\partial W^*} \end{aligned}\right\}, \tag{8}$$

where α is denoted as the existence determination operation, β is represented as the checking of the privacy level in the existing method. Based on the existence and sustainability, the services are accomplished to the users depending on their requirements expressed in Eq. (9).

$$\left.\begin{aligned} \frac{\partial G}{\partial W} &= \frac{C}{N} = a_n - b_n \\ \frac{\partial G}{\partial W^*} &= \frac{C}{N} = \widehat{a_n} - b_n \\ \frac{\partial W}{\partial n} &= \frac{Z}{N} = b_n - x_n \\ \frac{\partial W}{\partial n^*} &= \frac{Z}{N} = \widehat{b_n} - x_n \\ \frac{\partial x}{\partial G} &= \frac{a}{N} = x_n - y_n \\ \frac{\partial x}{\partial G^*} &= \frac{a}{N} = \widehat{x_n} - y_n \end{aligned}\right\}. \tag{9}$$

This existence of privacy helps in the data's privacy preservation and then the outputs of the previous privacy of the service providers help in the enhancement of the privacy-preserving processes. The existence of privacy-preserving of the given data is explained by the equation mentioned above. The privacy existence for different levels is presented in Fig. 3.

Support vector machines (SVMs) can handle smaller, heterogeneous data samples with excellent classification accuracy, unlike deep learning methods that normally need massive datasets and substantial processing resources. Regarding IoV settings, this efficiency is valuable since real-time data processing is crucial, and deep learning models might cause delays or require more complicated gear to accomplish the same results. In addition, SVM provides more interpretability and transparency than deep learning models, which makes it simpler to include explicit privacy-preserving measures. Reaction times are essential for processing heterogeneous IoV data under rigorous privacy rules; SVM's emphasis on data separation via optimal hyperplane differentiation allows PRDPM to emphasize privacy without sacrificing response times. Compared to other deep learning approaches, SVM achieves a better mix of efficiency, interpretability, and accuracy, making it an ideal fit for the privacy-focused, resource-constrained environment of IoV.



Steps	Levels	β Levels	T Status	$a_x \geq 0$	$b_x > 0$	Existence
$\frac{\partial G}{\partial W}$	Level 1,3,4	9	S F S S	No	Yes	Yes
$\frac{\partial G}{\partial W^*}$	Level 1,2,4	9	S S F S	Yes	No	Yes
$\frac{\partial W}{\partial n}$	Level 3,4	6	F F S S	No	Yes	Partial
$\frac{\partial W}{\partial n^*}$	Level 1,2, 3,4	12	S S S S	Yes	Yes	Yes
$\frac{\partial x}{\partial G}$	Level 3	3	F F S F	Yes	No	No
$\frac{\partial x}{\partial G^*}$	Level 1,2, 3,4	12	S S S S	Yes	Yes	Yes

Figure 3: Privacy existence for different levels

The derivatives in Eq. (9) are used for handling privacy proposed levels based on β. The β operations are optimal for highly successful (S) T status. The possible conditions $a_x \geq 0$ and $b_x \geq 0$ based on the derivatives increases the existence of privacy. Therefore, the levels are computed from the available steps for improving the existence. Considering the swapping states of W and $\psi \forall Z$, the new T is determined. This forms the optimal c for the supporting Z with high L. The ceasing L is estimated from the $a_x < 0$ or $b_x < 0$ or both conditions for β improvements (Refer to Fig. 3). Now the sustainability is determined from the support vector machine to identify the prolonged time of the privacy in the data. Depending on this, the service is executed for the users, and improvements are happening in the privacy-preserving process. The existence and the sustainability are identified by the support vector machine and the data plane, and the operational planes are determined by the algorithm.

Indeed, federated learning approaches are useful for privacy protection and have proven successful in comparable IoV scenarios. These techniques enable decentralized data processing across numerous nodes without exchanging raw data. When it comes to IoV systems, with their complex and dense data flows, a more streamlined processing and quick reaction capability is required. This is why an SVM-based, cloud-oriented solution was chosen for PRDPM. The need for frequent model updates and synchronization and the substantial processing resources required by each node in federated learning might introduce delay and restrict its real-time usefulness in IoV systems. Critical in high-traffic IoV networks where split-second processing is required for operational efficiency and safety, PRDPM provides quick threat detection and unified privacy-preserving solutions by centralizing data analysis in a cloud-based architecture. By avoiding the latency issues that federated learning may bring, PRDPM can control privacy and performance better, which is especially important in IoV contexts.

4 Results and Discussion

The proposed model is validated using NS3 experiments that include an OpenSource map in SUMO. The simulation scenario includes a 3 km-long roadway with four crossings and two parallel routes. The vehicle density ranges from 10 to 120 at an average speed of 45 km/h. The vehicles are calibrated to communicate information at 15-min intervals for a maximum of 30 min within their 250-m communication range. With this simulation setup, the metrics of privacy leaks, service failure, privacy recommendations, recommendation time, and data processing rates are validated. The proposed model reduces service failure by distributing data processing across cloud-edge nodes, improving fault tolerance in a distributed IoV network. Recommendation time in our SVM model is improved by leveraging edge processing to deliver fast, localized privacy recommendations without requiring central data transmission. The proposed model's data processing rate is optimized by distributing computations, making it proportional to the combined processing rates of both edge and cloud nodes. The most critical metrics demonstrating our model's efficacy are service failure rate and recommendation time. Lower failure rates improve reliability and user trust, essential in IoV environments, while shorter recommendation times provide rapid responses, enhancing user experience. The collected data is validated using the WEKA 3.0 tool for validation. The levels of data filtering outlined in the preceding sections are achievable with this tool-based approach. This simulation setup validates parameters such as service failures, recommendation time, and data processing speeds. The proposed model uses benchmarks form from the results available in EPDQD [29], EDPPA [31], and PPDS [22] when comparing metrics. Such metrics are exploited in the discussion and proposed contributions above. This is slightly different from the previous metrics provided in the related works. However, these features are closely related to the actual metrics discussed in those works. The privacy, efficiency, and resilience-focused validation criteria allow our SVM model to provide privacy-preserving procedures in IoV contexts. The integrity of federated model updates is tested to ensure that only model parameters, and not raw data, are exchanged, which preserves decentralized privacy, and compliance with differential privacy metrics is maintained to prevent individual data from being reconstructed. To ensure data processing is efficient as IoV devices grow, measurements for scalability and latency are run across networks at the edge of the cloud. To ensure reliable performance in various environments, cross-validation tests compare the model's accuracy with different kinds of heterogeneous IoV data. Lastly, to ensure that the system's privacy-preserving policies will withstand the test of time, adaptive security audits are conducted regularly to identify and resolve new risks. These criteria strengthen our model by fixing major issues with competing privacy-preserving methods for IoV settings. Compared to other state-of-the-art approaches, PRDPM is more resilient thanks to these validation criteria, which provide ongoing, context-specific privacy guarantees designed for IoV contexts. In the ever-changing IoV environment, where data kinds, sources, and volumes may fluctuate greatly, PRDPM constantly adjusts by emphasizing sensitivity and accuracy. A component absent from many models is the ability to detect and reduce threats proactively; PRDPM's incorporation of privacy leak evaluations add to this strength. These updates work together to make PRDPM the most reliable and long-lasting IoV solution, protecting user privacy while keeping performance consistent across various real-world scenarios.

4.1 Service Failure

This process reduces the number of service failures by implementing the effective min-max recommendations derived from the sustainability determination process's results. The service accomplishment to the users based on their application demand is happening without the privacy leak and improvised preserving data process. If there is no effective privacy in the data, then a new privacy method is to be added in the process for the elimination of the treacherous transaction of the services to the users. This vitally avoids the failures of the services and enhances the privacy-preserving procedures of the data within the given period. The efficacious services are provided for the users with better privacy. The services are executed to the users from the cloud/IoT with efficacious decisions and min-max recommendations. Based on the services provided to the users, the sustainability is determined, and then based on the planes and hyperplane functions, the existence is also identified. The support vector helps in the estimation of the privacy period in the services which are provided to the users according to their application demand (Fig. 4). To be more precise, PRDPM's SVM efficiently distinguishes between sensitive and non-sensitive data, which greatly simplifies and speeds up privacy-preserving processing while minimizing the likelihood of service failures. In contrast to EPDQD and PPDS, which have greater failure rates due to their privacy methods' slowness, PRDPM consistently displays lower Service Failure Rate numbers. Service Failure Rate is the fraction of requests not completed because of processing delays or failures.

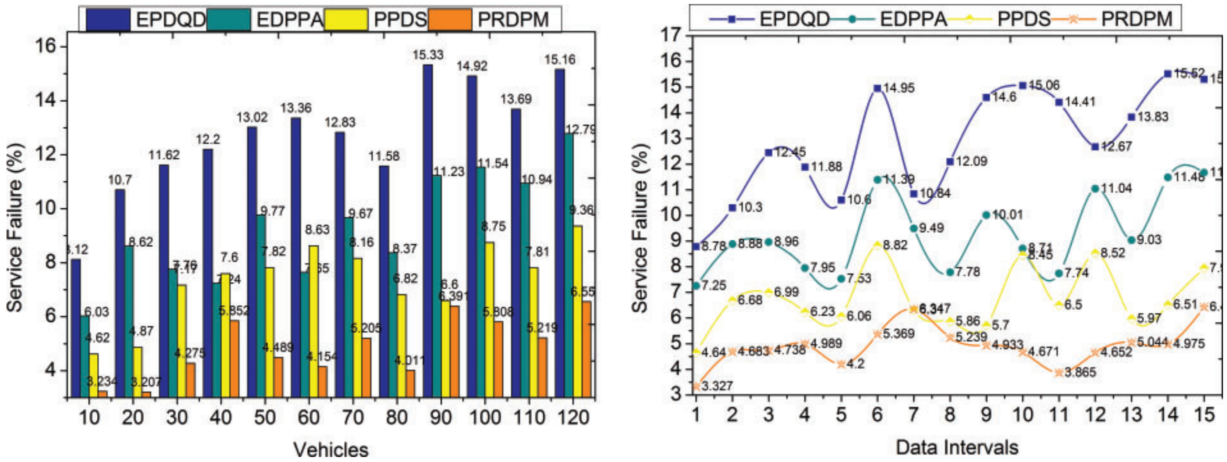


Figure 4: Service failure

4.2 *Recommendation Time*

The recommendation is completed in a shorter amount of time; therefore, privacy preservation is effective in achieving better outcomes for the services. Sustainability is determined from the support vector machine to identify the prolonged time of privacy in the data. Depending on this, the service is executed for the users, and improvements are happening in the privacy-preserving process. The two planes from the support vector machine decide the decision to enhance privacy or not. The data plane includes the existence and the sustainability where the privacy of the data is enhanced in the process and then the operational or control plane distributes the decisions based on the data plane. These decide if there is efficacious privacy represented in the service there are no issues and nothing to alter. If there is no effective privacy in the data, then a new privacy method is to be added in the process for the elimination of the treacherous transaction of the services to the users. Based on the sustainability and the operational plane outcome, the recommendations are provided within a shorter period (Fig. 5).

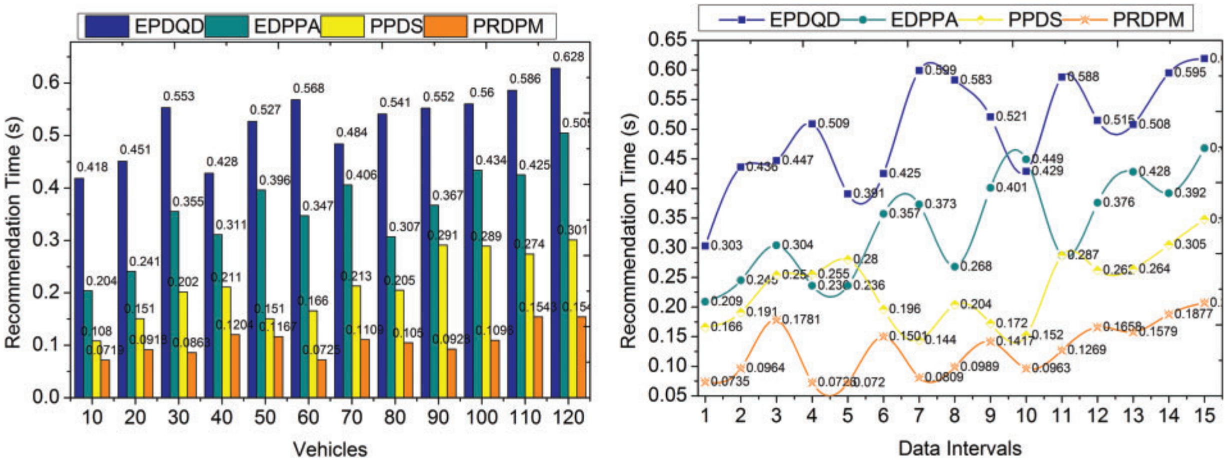


Figure 5: Recommendation time

4.3 Data Processing Rate

The rate of data processing is efficacious with the help of the support vector machine in the PRDPM approach. The internet of vehicles demands the application for the following the neighbor and the service providers. The service provider considers the demand of the users before processing the privacy-preserving procedure. The data extracted from the user is considered for the further data preserving process with high privacy. This also helps in the enhancement of the privacy of the data and processing rate of the data. These different application demands are used for the determination of the min-max privacy conclusions for existence and sustainability. The information from the different acquired time intervals is used for authenticating the pre-mentioned characteristics in the operational plane by distinguishing the hyperplane for min-max recommendations. By consolidating these characteristics, the data processing rate is efficacious with the aid of the support vector machine algorithm (Fig. 6). In the below Table 2, the comparative analysis summary with the improvements is presented. Through edge processing and localized data partitioning, PRDPM facilitates the processing of sensitive data nearer to its origin, hence diminishing the need for data transmission across networks, which concurrently reduces privacy threats and bolsters data security. This decentralized methodology corresponds with PRDPM's privacy-preserving protocols, enabling local management of sensitive data with targeted privacy safeguards and reducing susceptibility to centralized failures or breaches. Furthermore, decentralized processing in PRDPM enhances bandwidth efficiency and elevates real-time responsiveness since data pertinent to immediate vehicular encounters or environmental alterations is handled expeditiously at the edge. The ability to manage local data while ensuring strong privacy protections renders PRDPM especially appropriate for the decentralized and dynamic nature of IoV ecosystems.

PRDPM's cloud-based architecture greatly improves its capacity to manage real-time privacy concerns in IoV systems by consolidating data processing, analysis, and threat detection across linked cars and edge devices. Because the cloud constantly gathers data from many sources and uses SVM-based classification to identify sensitive data segments in real time, PRDPM can quickly detect and react to new privacy threats. Vehicles and IoT endpoints throughout the network can quickly adjust to any identified risks because of the cloud's centralized structure, which allows for instant upgrades to privacy-preserving protocols and speedy dissemination of threat notifications. Data privacy across varied and ever-changing IoV settings depends on this proactive threat-handling capacity.

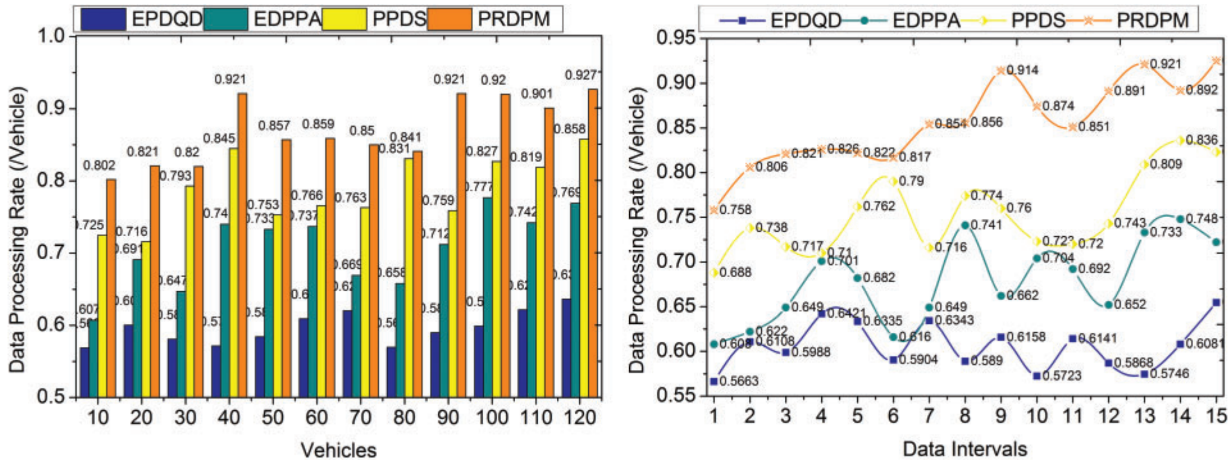


Figure 6: Data processing rate

Table 2: Comparative analysis summary

Metrics	EPDQD [29]	EDPPA [31]	PPDS [22]	PRDPM
		Vehicles		
Service failure (%)	15.16	12.79	9.36	6.556
Recommendation time (s)	0.628	0.505	0.301	0.1544
Data processing rate (/Vehicle)	0.6363	0.769	0.858	0.927
		Data Intervals		
Service failure (%)	15.31	11.67	7.94	6.428
Recommendation time (s)	0.619	0.468	0.348	0.2072
Data processing rate (/Vehicle)	0.6547	0.722	0.823	0.925

Adaptive machine learning methods, such as reinforcement learning, will be included in future upgrades so the model may self-adjust its privacy safeguards in response to changing threat patterns in IoV systems. Another area of interest is the integration of edge-level decentralized threat detection modules. This would enable local devices and vehicles to autonomously detect and counteract threats before transmitting their data to the cloud, improving reaction time and reducing latency. Further improvements in federated learning might allow the model to learn from dispersed data sources while protecting privacy. This would make it more adaptable and successful in handling privacy issues related to the IoT.

PRDPM improves privacy protection by lowering privacy leakage risks as data moves over the network using hyperplane differentiation inside its support vector machine model. This model classifies data depending on sensitivity. With the help of effective data partitioning and feature selection, which reduce computational overhead, it can handle the high-density data volumes in IoV systems, thanks to its scalability. For responsive Internet of Vehicles (IoV) applications like traffic management and vehicle-to-vehicle communications, PRDPM's caching and edge processing algorithms provide real-time data handling. In contrast to many deep learning models, which may be resource-intensive and complicated, this uses SVM, which adds interpretability and simplicity while enabling transparent privacy-preserving processes. Nevertheless, there are a few drawbacks to PRDPM. One is that SVM models may not be as flexible when dealing with complicated data patterns as deep learning algorithms. Another issue is that it might be difficult to fine-tune the SVM kernel to fit various IoVsituations, affecting its flexibility in handling multiple use cases.

In the context of IoV services, the suggested SVM model enhances the scalability and efficacy of current privacy-preserving approaches. Using a cloud-edge integration architecture, our model overcomes the challenges posed by the large amount and diversity of IoV data compared to conventional methods. This configuration enables cloud-based processing of massive amounts of data, with local processing handled by edge nodes; this reduces the need to transmit sensitive data, which improves privacy. The model can easily accommodate additional cars and data sources because of this distributed architecture, greatly enhancing scalability. The SVM model uses federated learning to enable decentralized model training, greatly improving its efficacy. The central model in an IoV architecture only needs model parameters, not raw data, so that each node may train autonomously on its data. Using this method may protect privacy and lessen the likelihood of data sharing. Federated learning guarantees the decentralization of sensitive IoV data while achieving high accuracy across many dynamic data sources. As a result, our SVM model succeeds where other privacy-preserving approaches have failed by providing strong privacy protection with high data value and efficient scalability.

5 Conclusions

In the validation method, support vector learning is employed. This classification method independently evaluates the aforementioned features to ensure reliable service across different intervals. Maximum classification accuracy is implied using the minimum privacy leak and maximum recommendation for security improvement. The proposed process is classified using the SVM hyperplane based on its movement across the min-max variations. The adjustments are linear throughout the vehicle's travel intervals for which the plane differentiation for sustainability and existence is validated. From the metric-based analysis, it is seen that the proposed model reduces service failures by 11.76%, and recommendation time by 11.28% while the data processing rate has increased by 17.26% for different vehicle densities. Similarly, the proposed model reduces service failures by 10.46%, and recommendation time by 9.45% while the data processing rate has increased by 19.18% for different data intervals.

Acknowledgement: The authors extend their appreciation to the Deanship of Graduate Studies and Scientific Research at University of Bisha for funding this research through the promising program under grant number (UB-Promising-33-1445).

Funding Statement: This study was supported by the Deanship of Graduate Studies and Scientific Research at University of Bisha for funding this research through the promising program under grant number (UB-Promising-33-1445).

Availability of Data and Materials: Data not available due to "Deanship of Graduate Studies and Scientific Research at University of Bisha" restrictions.

Ethics Approval: Not applicable.

Conflicts of Interest: The author declares no conflicts of interest to report regarding the present study.

References

[1] C. Xu, H. Wu, H. Liu, W. Gu, Y. Li and D. Cao, "Blockchain-oriented privacy protection of sensitive data in the internet of vehicles," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 2, pp. 1057–1067, Feb. 2023. doi: 10.1109/TIV.2022.3164657.

[2] A. Alqarni, "A privacy recommending data processing model for internet of vehicles (IoV) services," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 4, pp. 15729–15733, Aug. 2024. doi: 10.48084/etasr.7743.

[3] 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, 2021. doi: 10.1109/TITS.2020.3011931.

[4] M. A. Khan, A. S. Alluhaidan, A. Alharthi, A. Alqarni, and S. Tyagi, "Dynamic secure multi-access scheme for interaction in internet of vehicles," *IEEE Transact. Vehic. Technol.*, 2024. doi: 10.1109/TVT.2024.3453962.

[5] Y. Wu, L. Wu, and H. Cai, "Cloud-edge data encryption in the internet of vehicles using Zeckendorf representation," *J. Cloud Comput.*, vol. 12, no. 1, 2023, Art. no. 39. doi: 10.1186/s13677-023-00417-7.

[6] 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, 2021. doi: 10.1109/JSYST.2020.3009447.

[7] F. Wei, S. Zeadally, P. Vijayakumar, N. Kumar, and D. He, "An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3939–3951, 2021. doi: 10.1109/TITS.2020.2998775.

[8] 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, 2022. doi: 10.1109/TITS.2021.3115171.

[9] Y. Li *et al.*, "Privacy-preserving and real-time detection of vehicular congestion using multilayer perceptron approach for internet of vehicles," *IEEE Trans. Vehicular Technol.*, vol. 71, no. 12, pp. 12530–12542, 2022. doi: 10.1109/TVT.2022.3199407.

[10] N. Wang *et al.*, "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles," *Digit. Commun. Netw.*, vol. 10, no. 1, pp. 126–134, 2022. doi: 10.1016/j.dcan.2022.05.020.

[11] N. Liu, A. Nikitas, and S. Parkinson, "Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: A thematic analysis approach," *Transport. Res. Part F: Traffic Psychol. Behav.*, vol. 75, no. 4, pp. 66–86, 2020. doi: 10.1016/j.trf.2020.09.019.

[12] P. Zhao, G. Zhang, S. Wan, G. Liu, and T. Umer, "A survey of local differential privacy for securing internet of vehicles," *J. Supercomput.*, vol. 76, no. 11, pp. 8391–8412, 2019. doi: 10.1007/s11227-019-03104-0.

[13] M. Pang, L. Wang, and N. Fang, "A collaborative scheduling strategy for IoV computing resources considering location privacy protection in mobile edge computing environment," *J. Cloud Comput.*, vol. 9, no. 1, 2020. doi: 10.1186/s13677-020-00201-x.

[14] Y. Ren, X. Li, S. -F. Sun, X. Yuan, and X. Zhang, "Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks," *J. Inf. Secur. Appl.*, vol. 58, 2021, Art. no. 102698. doi: 10.1016/j.jisa.2020.102698.

[15] Y. Pu, T. Xiang, C. Hu, A. Alrawais, and H. Yan, "An efficient blockchain-based privacy preserving scheme for vehicular social networks," *Inf. Sci.*, vol. 540, no. 8, pp. 308–324, 2020. doi: 10.1016/j.ins.2020.05.087.

[16] J. Xiong, R. Bi, Y. Tian, X. Liu, and D. Wu, "Toward lightweight, privacy-preserving cooperative object classification for connected autonomous Vehicles," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2787–2801, 2022. doi: 10.1109/JIOT.2021.3093573.

[17] Z. Li *et al.*, "Towards efficient and privacy-preserving versatile task allocation for internet of vehicles," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 295–303, 2022. doi: 10.1109/OJCS.2022.3222363.

[18] P. Hu *et al.*, "Efficient location privacy-preserving range query scheme for vehicle sensing systems," *J. Syst. Archit.*, vol. 106, 2020, Art. no. 101714. doi: 10.1016/j.sysarc.2020.101714.

[19] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the Internet of vehicles," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1123–1139, 2021. doi: 10.1109/JIOT.2020.3010893.

[20] J. Huang, Y. Qian, and R. Q. Hu, "A privacy-preserving scheme for location-based services in the internet of vehicles," *J. Commun. Inf. Netw.*, vol. 6, no. 4, pp. 385–395, 2021. doi: 10.23919/JCIN.2021.9663103.

[21] L. Benarous, S. Bitam, and A. Mellouk, "CSLPPS: Concerted silence-based location privacy preserving scheme for internet of vehicles," *IEEE Trans. Vehicular Technol.*, vol. 70, no. 7, pp. 7153–7160, 2021. doi: 10.1109/TVT.2021.3088762.

[22] Y. Xia, T. Zhang, L. Wu, X. Zheng, and J. Jin, "Privacy-preserving data scheduling in incentive-driven vehicular network," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22669–22681, 2022. doi: 10.1109/JIOT.2022.3182542.

[23] Y. Liu *et al.*, "VRepChain: A decentralized and privacy-preserving reputation system for social internet of vehicles based on blockchain," *IEEE Trans. Vehicular Technol.*, vol. 71, no. 12, pp. 13242–13253, Dec. 2022. doi: 10.1109/TVT.2022.3198004.

[24] U. I. Atmaca, C. Maple, G. Epiphaniou, and M. Dianati, "A privacy-preserving route planning scheme for the internet of vehicles," *Ad Hoc Netw.*, vol. 123, 2021, Art. no. 102680. doi: 10.1016/j.adhoc.2021.102680.

[25] Y. Zhang, L. Zhang, Q. Wu, and Y. Mu, "Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9216–9227, 2022. doi: 10.1016/j.jksuci.2022.09.004.

[26] L. Xing *et al.*, "Location entropy-based privacy protection algorithm for Social Internet of Vehicles," *Wirel. Pers. Commun.*, vol. 130, no. 4, pp. 3009–3025, 2023. doi: 10.1007/s11277-023-10413-4.

[27] L. Benarous and B. Kadri, "Kadri Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vehicles," *Peer-to-Peer Netw. Appl.*, vol. 15, no. 1, pp. 461–472, 2021. doi: 10.1007/s12083-021-01233-z.

[28] P. Hu *et al.*, "A secure and lightweight privacy-preserving data aggregation scheme for Internet of Vehicles," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 3, pp. 1002–1013, 2020. doi: 10.1007/s12083-019-00849-6.

[29] P. Hu *et al.*, "An efficient privacy-preserving data query and dissemination scheme in Vehicular Cloud," *Pervasive Mob. Comput.*, vol. 65, 2020, Art. no. 101152. doi: 10.1016/j.pmcj.2020.101152.

[30] C. Lai, Y. Du, Q. Guo, and D. Zheng, "A trust-based privacy-preserving friend matching scheme in social internet of Vehicles," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 4, pp. 2011–2025, 2021. doi: 10.1007/s12083-021-01140-3.

[31] J. Ren, Y. Cheng, and S. Xu, "EDPPA: An efficient distance-based privacy preserving authentication protocol in VANET," *Peer-to-Peer Netw. Appl.*, vol. 15, no. 3, pp. 1385–1397, 2022. doi: 10.1007/s12083-022-01297-5.