Privacy-Preserving Machine Learning Using Consortium Blockchain in Vehicular Social Networks

Amna Arak Radeini Asal and Shaimaa Jabbr Ali
Department of Arabic, College of Education for Women, University of Anbar, 31001 Ramadi, Iraq
amn21w5005@uoanbar.edu.iq, shaimaaja@uoanbar.edu.iq

Keywords: Vehicular Social Networks (VSNs), Privacy-Preserving Machine Learning, Consortium Blockchain, Threshold Paillier Cryptosystem, Support Vector Machine (SVM).

Abstract: It presents both opportunities for intelligent transportation systems and challenges for ensuring privacy during the data analysis process that VSNs (Vehicular Social Networks) generate. Our paper proposes a threshold Paillier cryptosystem and consortium blockchain for training Support Vector Machines (SVMs) on vertically partitioned datasets. Traditional approaches that rely on trusted third parties are insecure compared to blockchain-based collaboration. Most computations are performed locally and intermediate values are only shared if they are encrypted. This ensures high levels of privacy and efficiency. This model (PP-SVM) offers classification accuracy comparable to standard SVMs, resulting in privacy-preserving learning environments in virtual social networks. As a result of this approach, sensitive user data is effectively protected, and a robust sense of trust among network members is fostered. In addition to ensuring data integrity, consortium blockchain technology promotes collaborative learning by leveraging its inherently decentralized nature, facilitating secure interactions and shared decision-making processes. With the rapid evolution and increasing adoption of vehicular social networks, preserving user privacy has become increasingly crucial, demanding scalable and reliable security mechanisms.

1 INTRODUCTION

Vehicular Social Networks (VSNs) are a significant advancement in intelligent transportation systems, enabling vehicle-to-vehicle and infrastructure-to-network data exchange. As a result of these networks, traffic management, safety, and user experience can be improved [1]. A critical challenge remains, however: securing sensitive data and enabling collaborative, decentralized decision-making while protecting privacy. The increasing amount of real-time, location-based, and personal data being shared in VSNs makes privacy preservation essential. Blockchain-based machine learning (ML) is one promising solution for addressing privacy concerns while allowing intelligent data processing. In particular, consortium blockchains provide a secure and transparent platform for managing data and facilitating collaborative learning, as they are permissioned blockchains where trusted parties collaborate. A similar setup would allow vehicles to contribute data for training machine learning models without exposing their sensitive information to others.

Several scenarios have benefited from cloud and edge computing, including mobile social networks (VSNs) [2], [3]. VSNs can be optimized in terms of safety, convenience, amenity, and entertainment with the use of efficient methods [4], [5]. The application of machine learning and deep learning has captured the interest of researchers across a wide range of disciplines [6], [7]. Data analysis of VSNs is gradually advancing with the application of related technologies, including machine learning and deep learning. In many scenarios, support vector machines (SVMs) are frequently used due to their efficiency and robustness. Negative communication conditions can be detected using SVM, for example.VSNs collect data from multiple sources, including vehicle manufacturers, vehicle management agencies, and social networking application developers [8], [9].

Data sources differ between these entities, so their attributes are different. A VSN rarely has a comprehensive training dataset due to the limited number of sources available. Vehicle network service platforms control the majority of vehicle location and mobility trace attributes, and social network applications may control user preferences. As you

might expect, the performance of SVM classifiers is determined by datasets [10]. A VSN application trains SVM classifiers by combining datasets with sufficient attributes before reaching a more efficient model. An alternative approach is to segment the merged dataset vertically based on the datasets owned by the entities. SVM training presents several serious security challenges, however. VSNs contain extensive private information (e.g., vehicle location, user preferences), so companies are prohibited from using and sharing this information across borders due to constantly enacted regulations. VSN data, however, contain high-value information that makes data providers hesitant to share their original data. The value of shared data is lost if a privacy-preserving mechanism is not in place. Several security challenges are associated with intelligent and connected vehicles [9], [11], [12]. Data sharing between entities is also a problem that should be well-researched.

2 LITERATURE REVIEW

Several methods of machine learning have been investigated that preserve privacy, including linear regression, SVMs, naive Bayes classifiers, and logic regressions. In recent years, deep learning [13] has also gained attention. The author [14] trains a linear regression classifier using a hybrid approach based on vertically partitioned datasets. Two parties compute using garbled circuits in this protocol. Two parties require a crypto service provider, and multiple parties require an evaluator and crypto service provider simultaneously.

In [15], the author developed an algorithm using heteromorphic encryption, and Yao garbled circuits were separated. Crypto service providers and evaluators are essential for realizing the algorithm [16]. Several machine learning algorithms, such as linear regression, logistic regression, and neural networks, are supported [17], [18]. With the use of two-party computation, data is collected from data providers, and a model is trained securely. Neither server can work simultaneously with the other. An author [19] developed a framework using three servers to train linear regression models, logistic regression models, and neural networks.

2.1 Machine Learning in Vehicular Social Networks (VSNs)

Vehicular social networks (VSNs) are adopting machine learning (ML) techniques for a variety of applications [20]. Transport and communication can be enhanced through these techniques by leveraging data collected from vehicles and their surroundings. Intelligent and adaptive services can be provided by VSNs with ML algorithms, addressing the increasing demands of modern transportation systems. A growing volume of vehicle data necessitates machine learning to extract valuable insights and optimize network performance. As a consequence of these applications, road safety is enhanced, vehicular services are improved, and intelligent transportation systems are promoted [21]. With ML algorithms, drivers can be warned of potential hazards in real time and reduce the risk of accidents by predicting potential hazards. Additionally, machine learning helps optimize traffic flow through the dynamic adjustment of traffic signals and efficient routing of vehicles, which in turn reduces congestion and increases travel time. Additionally, the use of machine learning in VSNs facilitates customized services, such as navigation and entertainment options, which enhances the driving experience.

2.2 Blockchain Technology in Vehicular Social Networks

VSNs can benefit from blockchain technology in terms of security and efficiency [22]. As a result of its inherent properties, such as immutability and transparency, blockchains are ideally suited to address the security and efficiency challenges facing VSNs. In addition to ensuring data integrity and authenticity, blockchain enables VSNs to streamline data sharing and access control processes. Secure transactions are enhanced by blockchain's decentralization, anonymity, and trust properties. By eliminating a central authority, the network will be less prone to failures and will become more resilient. In addition to protecting participants' identities, anonymity also prevents tracking and profiling by unauthorized parties. Participants in the blockchain network benefit from the tamper-proof and verifiable properties of blockchain, resulting in a high level of trust. Combined, these features improve VSN security and efficiency.

3 PROPOSED METHODOLOGY

3.1 SVM Overview

SVM is explained first by describing the notation. When a prime superscript is applied to a vector, it converts it to a row vector. A matrix containing two

vectors x and y is denoted by the scalar product. $x'y$, and a matrix containing $||x||$ 2-norm is called x. Taking an n-dimensional input space and using $m * n$ matrix a to represent m data points. Data points A are labelled +1 or -1 using a $m * n$ diagonal matrix D. x_i is represented by the class label D_{ii} or d_i in short. In mathematics, e denotes a column vector of ones of any dimension. A matrix with arbitrary dimensions is called an identity matrix.

Here is an example of a linear binary classification task. This problem can be solved with SVM by identifying the separating hyperplane $(w \cdot x = \gamma)$ that maximizes the margin between the hyperplane and the closest data points. When a boundary is located at a different distance from each support vector, we use the "soft" margin. A "hard" margin is expressed as $\frac{1}{||w||}$, as illustrated below. Following is a primal program that combines the standard SVM solution with the objective of maximizing margin while minimizing error [23], [24]:

$$\min_{w,y} \frac{1}{2} w'w + ve'y, \quad (1)$$

$$s.t.\, D(Aw - ey) + y \geq e \; and \; y \geq 0\,. \quad (2)$$

The method minimizes both the margin and error (w' and $e'y$). SVM allows soft margins or error by including the slack variable y in constraint (2). As the objective function (1) minimizes the slack or error, it will be larger than zero if the point lies within the margins. This parameter (a user parameter) balances the margin size with the error. With the help of this optimization problem, we will be able to calculate the vector of weights w and the bias b. As soon as w and y are calculated, we can identify the class of a new data object x using $f(x) = w'x - \gamma$, where $f(x) > 0$ indicates a positive class, otherwise a negative class.

3.2 Threshold Cryptosystems of Paillier

Typically, threshold cryptosystems have two components:

1) the public key is distributed, and the secret key is shared;
2) the secret key is decrypted and signed based on the shared representation.

When there should be no knowledge of the secret key of an individual, threshold schemes are vital. We have previously proposed threshold RSA encryption and decryption [20], DSS encryption and decryption [20] and Paillier in multiparty settings [19].

We have previously proposed threshold RSA encryption and decryption systems [25], SS encryption and decryption [26], DSS [26] and Paillier in multiparty settings. There are some cases (e.g., ElGamal) where multiparty techniques can easily be applied to two-party settings. However, there is still no solution to the problem of anti-malicious two-party threshold Paillier encryption.

3.3 System Model

According to Figure 1, a system such as ours is composed of three components: DD, DP, and BSP (Blockchain Service Platform).

Data Device. Sensors, mobile devices, and other data-generating devices are examples of this. Using these devices, valuable data can be collected and analyzed.

Data Provider: It is the responsibility of data providers to generate, collect, store, and analyze data from a variety of sources. The equipment and methods used by these participants resulted in varying data sets. As far as attributes are concerned, these diverse data sets complement one another. The participants in this collaborative machine-learning effort also serve as model trainers and provide data. This paper's scheme involves participants performing most training tasks locally.

Blockchain Service Platform. This platform uses blockchain technology. The BSP provides participants with a transparent platform for sharing data, allowing them access to all the data stored there. Moreover, the BSP protects data records from unauthorized alteration by maintaining their integrity. Additionally, it provides robust security measures that prevent data from leaving the participants' domain from being accessed. Participants and BSPs communicate using encrypted communications to ensure data confidentiality and prevent leakage.

Threat Model. A single role is assigned to the data provider in our scheme. In the security model, we view participants as honest but curious, implying that while they are curious about others' data, they will abide by the rules. In addition, as participants interact with the BSP extensively, potential threats during this interaction process are also considered.

3.4 The Construction of Secure SVM

3.4.1 Overview of Secure SVM Training with IoT Data

SVM models are trained using data collected from multiple IoT data providers in this method. A provider of IoT data preprocesses IoT data instances,

encrypts them locally with their private keys, and generates transactions to record them on a blockchain. In the global ledger, encrypted data can be accessed by data analysts who are training the SVM model. Interaction with each data provider is a necessary part of the training process.

3.4.2 Blockchain-Based Encryption of Data Sharing

Our blockchain transaction structure enables the storage of encrypted IoT data. Inputs and outputs are the two main fields of a transaction. There are three fields in the input form: the data provider's address, the type of IoT device, and the encrypted data. Output fields include the data analyst's address, encrypted data, and IoT device type. Address fields contain 32-byte hash values. Using the homomorphic encryption Paillier, the encrypted data was generated. The Bitcoin blockchain stores encrypted data instances that are 128 bytes long, assuming the private key is 128 bytes long. IoT device type segments are 4 bytes long.

3.5 Building Blocks

Gradient Descent. It is possible to optimize the parameters of an SVM using several methods. Sequential minimum optimization algorithms (SMO) and gradient descent algorithms (GD) are examples of these algorithms. It is a method for optimizing biquadratic SVM programs. Also, linear SVM and sparse data are well handled. There are many comparisons, dots, and divisions involved in SMO, which makes it complex. As a result of applying SMO cryptographically, there is a great deal of cost associated with computing and communication. Based on GD, SVM optimization is a simple and efficient algorithm that involves only a few comparisons and multiplications of vectors. For this reason, we selected GD as the optimization algorithm for optimizing SVM model parameters.

In the GD method, the primary SVM is converted into an empirical loss minimization problem by using a penalty factor.

$$\min_{w,b} \frac{1}{2}\left|\left|w\right|\right|^2 + C\sum_{i=1}^{m} L(w,b,(x_i,y_i)). \quad (3)$$

In this equation, the hinge-loss function appears on the right side

$$C\sum_{i=1}^{m} L\big(w,b,(x_i,y_i)\big) = C\sum_{i=1}^{m} \max\{0,1-y_i(wx_i-b)\}. \quad (4)$$

In most cases, $\frac{1}{m}$ is the misclassification penalty, and C is the penalty.

GD consists of the following forms:

$$x_{n+1} = x_n - \lambda\Delta Grad(x_n). \quad (5)$$

Secure Polynomial Multiplication. A secure addition can be described as a homomorphic addition based on Paillier's homomorphic property

$$\big[[m_1+m_2]\big] = \big[[m_1]\big] * \big[[m_2]\big](modN^2). \quad (6)$$

As an example of secure subtraction, consider the following:

$$\big[[m_1-m_2]\big] = \big[[m_1]\big] * \big[[m_2]\big]^{-1}(modN^2). \quad (7)$$

The modular multiplicative inverse is $\big[[m]\big]^{-1}$, which performs the operation

$$\big[[m]\big] * [m]]\text{^} - 1\ mod\ N^2 = 1. \quad (8)$$

Functions can be used to compute $\big[[m]\big]^{-1}$

$$\phi(N), \big[[m]\big]^{-1} = \big[[m]\big]^{\phi(N)-1}. \quad (9)$$

The manipulation of ciphertext can be used to obtain polynomial multiplication,

$$\big[[am_1+bm_2]\big] = \Big[[m_1^b]\Big]\,(modN^2). \quad (10)$$

During the training model, the calculated median value must be shared between all three participants. A threshold homomorphic encryption scheme is used as the solution to protect the shared data, ensuring its security and ensuring gradient calculation accuracy. As a basis for judging the manner in which the gradients should be updated, we construct equations (11), (12), and (7) using additive homomorphic encryption.

$$\big[[a]\big] = \left[\left[\sum_{i=1}^{n} a^i\right]\right] = \prod_{i=1}^{n}\Big[[a^i]\Big], \quad (11)$$

$$\big[[r_2]\big] = \left[\left[\sum_{i=1}^{n} r_2^i\right]\right] = \prod_{i=1}^{n}\Big[[r_2^i]\Big], \quad (12)$$

$$[[ar_1+r_2]] = [[ar_1]][[r_2]] = [[\prod_{i=1}^{r_1}[[a]][[r_2]] = [[a]]^{r_1}[[r_2]]. \quad (13)$$

This solution determined the gradient update method by comparing the encoded calculation result with the constant 1.

3.6 Data Sharing on BSP and Security Analysis

The BSP simplifies point-to-point communications by securely computing intermediate values. On-chain data is managed, and smart contracts execute queries. During the iteration process, every participant uploads data twice: once for calculating the intermediate values (IVs) and once for calculating the decrypted values (DVs).

3.7 The Format of IVs

Iteration Round. Data exchange round, managed by smart contracts, during collaborative model training.

DP ID: At the time of data upload, the data owner is automatically identified.

Training Intermediate Value. When training the model, the encrypted state's intermediate value is used. The encrypted state sums each participant's values and compares them to 1. This comparison uses three cryptographic parameters:

- r1: Comparative integer that is unencrypted.
- r2: For comparison, a positive integer is encrypted.
- r3: A positive integer that has not been encrypted is used for comparison.

3.8 Random Positive Integer

In the next iteration, the data instances will be determined by a random generator for each participant.

3.9 The Format of DVs

Iteration Round. Identifies the round of data exchange, similar to IVs.

DP ID. Provides information about who owns the data.

Decrypted Value. Decrypting the result based on each participant's private key allows participants to obtain the final decryption result collectively.

4 RESULT ANALYSIS AND DISCUSSION

Figures 1 and 2 illustrates the PP-SVM's classification accuracy, showing no observable performance degradation compared to the standard SVM. In spite of the threshold Paillier encryption, the encryption and decryption processes maintain computational precision, ensuring that the classifier remains effective.

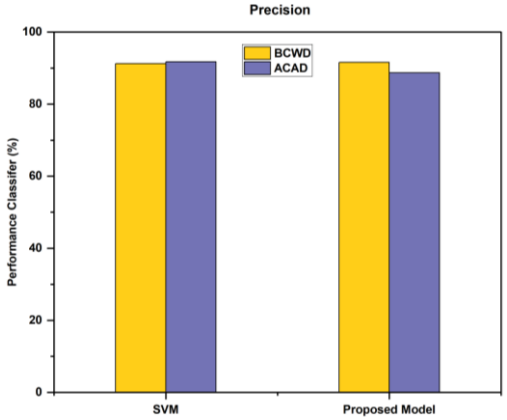

Figure 1: Performance of classifier accuracy.

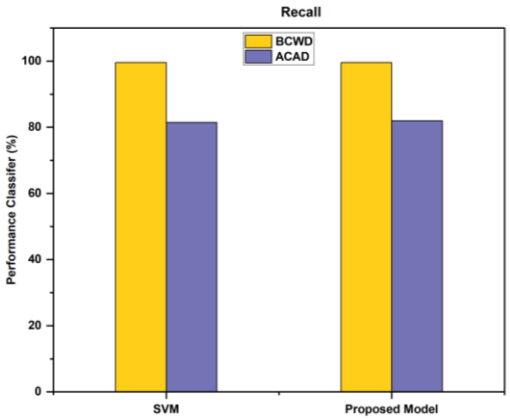

Figure 2: Recall comparison of SVM and PP-SVM on BCWD and ACAD.

In Figure 2, both the standard SVM and PP-SVM models are compared using BCWD and ACAD datasets. There is little difference in recall scores between the two models, which indicates that PP-SVM is not affected by the privacy-preserving mechanism. Data privacy is protected while maintaining effectiveness in the proposed model.

In this study, the standard SVM model is compared with the proposed PP-SVM model on two datasets: BCWD and ACAD. BCWD dataset has two yellow bars, one representing performance on the ACAD dataset and one representing performance on the BCWD dataset. Only slight differences occur in accuracy between the two models across the datasets. The proposed privacy-preserving PP-SVM model performs as well as a standard SVM without sacrificing performance, proving its efficiency in secure data processing.

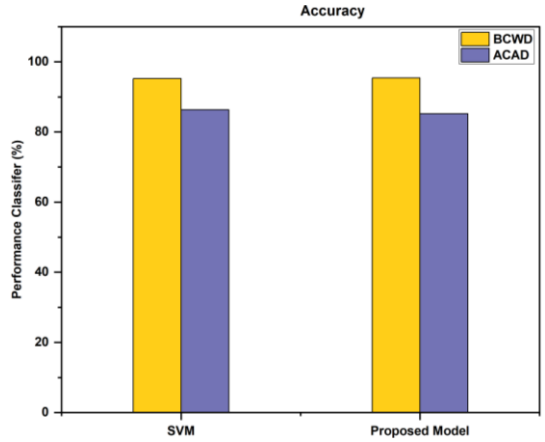

Figure 3: Accuracy with different numbers of VDPs.

Both datasets are represented in Figure 4. In general, the time spent in computation remains relatively low, with communications overhead taking up the majority of the time. Communication time remains elevated even as the training phase is completed quickly. Data sharing on consortium blockchains is often delayed due to consensus mechanisms among participating nodes, which require unavoidable delays.

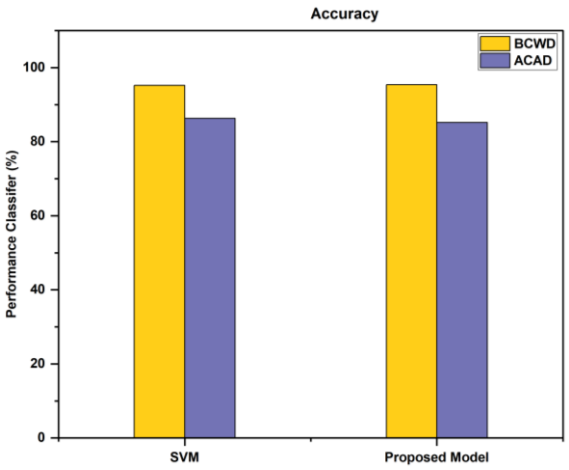

Figure 4: Performance of classifier efficiency.

5 CONCLUSIONS

SVM classifiers can be trained in VSNs using a privacy-preserving technique based on consortium blockchains and threshold Paillier encryption. As a result of the proposed model, data providers will no longer have to depend on trusted third parties to train accurate classifiers, thereby significantly enhancing user autonomy, reducing privacy risks, and effectively safeguarding data confidentiality. This novel system strategically minimizes communication overheads and costs while ensuring high computing precision by encrypting only intermediate computation values, subsequently optimizing them through gradient descent algorithms. A thorough evaluation of the PP-SVM model demonstrates that its classification accuracy is consistently comparable to traditional SVM methods, and confirms its robustness and adaptability under diverse operational configurations and settings. Furthermore, consortium blockchain technology enhances data sharing processes by improving transparency, enforcing stringent security protocols, and maintaining strong access control mechanisms. Consequently, this framework represents a practical, scalable, and robust solution for securing machine learning processes in decentralized networks where privacy preservation and secure collaboration are critical.

REFERENCES

[1] N. Hussain, P. Rani, N. Kumar, and M. G. Chaudhary, “A deep comprehensive research architecture, characteristics, challenges, issues, and benefits of routing protocol for vehicular ad-hoc networks,” Int. J. Distrib. Syst. Technol. (IJDST), vol. 13, no. 8, pp. 1–23, 2022.

[2] N. Cheng et al., “Big data driven vehicular networks,” IEEE Netw., vol. 32, no. 6, pp. 160–167, 2018.

[3] Y. Zhang et al., “BDS: a centralized near-optimal overlay network for inter-datacenter data replication,” in Proc. 13th EuroSys Conf., Porto, Portugal: ACM, Apr. 2018, pp. 1–14, doi: 10.1145/3190508.3190519.

[4] A. M. Vegni and V. Loscri, “A Survey on Vehicular Social Networks,” IEEE Commun. Surv. Tutor., vol. 17, no. 4, pp. 2397–2419, 2015, doi: 10.1109/COMST.2015.2453481.

[5] N. Hussain and P. Rani, “Comparative studied based on attack resilient and efficient protocol with intrusion detection system based on deep neural network for vehicular system security,” in Distributed Artificial Intelligence, CRC Press, 2020, pp. 217–236.

[6] N. Kato et al., “The Deep Learning Vision for Heterogeneous Network Traffic Control: Proposal, Challenges, and Future Perspective,” IEEE Wirel. Commun., vol. 24, no. 3, pp. 146–153, Jun. 2017, doi: 10.1109/MWC.2016.1600317WC.

[7] G. Xu, H. Li, S. Liu, K. Yang, and X. Lin, “VerifyNet: Secure and verifiable federated learning,” IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 911–926, 2019.

[8] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Security and Privacy (S&P), 2000, pp. 44–55. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/848445/

[9] R. Bost, R. A. Popa, S. Tu, and S. Goldwasser, "Machine Learning Classification over Encrypted Data," in Proc. 2015 Network and Distributed System Security Symp., San Diego, CA: Internet Society, 2015, doi: 10.14722/ndss.2015.23241.

[10] G. Ansari, P. Rani, and V. Kumar, "A novel technique of mixed gas identification based on the group method of data handling (GMDH) on time-dependent MOX gas sensor data," in Proc. Int. Conf. Recent Trends in Computing (ICRTC 2022), Springer, 2023, pp. 641–654.

[11] Y. Li, Q. Luo, J. Liu, H. Guo, and N. Kato, "TSP Security in Intelligent and Connected Vehicles: Challenges and Solutions," IEEE Wirel. Commun., vol. 26, no. 3, pp. 125–131, Jun. 2019, doi: 10.1109/MWC.2019.1800289.

[12] A. Singh et al., "Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication," IEEE Trans. Consum. Electron., vol. 70, no. 2, pp. 4898–4907, May 2024, doi: 10.1109/TCE.2024.3351221.

[13] R. Shokri and V. Shmatikov, "Privacy-Preserving Deep Learning," in Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur., Denver, CO, USA: ACM, Oct. 2015, pp. 1310–1321, doi: 10.1145/2810103.2813687.

[14] A. Gascón et al., "Secure linear regression on vertically partitioned datasets," IACR Cryptol. EPrint Arch., vol. 2016, p. 892, 2016.

[15] V. Nikolaenko, U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, and N. Taft, "Privacy-Preserving Ridge Regression on Hundreds of Millions of Records," in Proc. IEEE Symp. Security and Privacy (S&P), Berkeley, CA: IEEE, May 2013, pp. 334–348, doi: 10.1109/SP.2013.30.

[16] P. Rani and R. Sharma, "An experimental study of IEEE 802.11n devices for vehicular networks with various propagation loss models," in Proc. Int. Conf. Signal Processing and Integrated Networks, Springer, 2022, pp. 125–135.

[17] P. Mohassel and Y. Zhang, "SecureML: A System for Scalable Privacy-Preserving Machine Learning," in Proc. IEEE Symp. Security and Privacy (SP), San Jose, CA, USA: IEEE, May 2017, pp. 19–38, doi: 10.1109/SP.2017.12.

[18] P. Rani and R. Sharma, "Intelligent transportation system for internet of vehicles based vehicular networks for smart cities," Comput. Electr. Eng., vol. 105, p. 108543, 2023.

[19] P. Mohassel and P. Rindal, "ABY3: A Mixed Protocol Framework for Machine Learning," in Proc. 2018 ACM SIGSAC Conf. Comput. Commun. Secur., Toronto, Canada: ACM, Oct. 2018, pp. 35–52, doi: 10.1145/3243734.3243760.

[20] M. Shen, J. Zhang, L. Zhu, K. Xu, and X. Tang, "Secure SVM Training Over Vertically-Partitioned Datasets Using Consortium Blockchain for Vehicular Social Networks," IEEE Trans. Veh. Technol., vol. 69, no. 6, pp. 5773–5783, Jun. 2020, doi: 10.1109/TVT.2019.2957425.

[21] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and Efficient Data Sharing Among Vehicles Based on Consortium Blockchain," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 8857–8867, Jul. 2022, doi: 10.1109/TITS.2021.3086976.

[22] H. Shen, J. Zhou, Z. Cao, X. Dong, and K.-K. R. Choo, "Blockchain-Based Lightweight Certificate Authority for Efficient Privacy-Preserving Location-Based Service in Vehicular Social Networks," IEEE Internet Things J., vol. 7, no. 7, pp. 6610–6622, Jul. 2020, doi: 10.1109/JIOT.2020.2974874.

[23] H. H. S. Office for Civil Rights, "Standards for privacy of individually identifiable health information. Final rule," Fed. Regist., vol. 67, no. 157, pp. 53181–53273, 2002.

[24] V. Vapnik and V. Vapnik, Statistical Learning Theory. New York: Wiley, 1998.

[25] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems," in Advances in Cryptology – EUROCRYPT '99, J. Stern, Ed., Lecture Notes in Computer Science, vol. 1592. Berlin, Heidelberg: Springer, 1999, pp. 295–310, doi: 10.1007/3-540-48910-X_21.

[26] C. Hazay, G. L. Mikkelsen, T. Rabin, and T. Toft, "Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting," in Topics in Cryptology – CT-RSA 2012, O. Dunkelman, Ed., Lecture Notes in Computer Science, vol. 7178. Berlin, Heidelberg: Springer, 2012, pp. 313–331, doi: 10.1007/978-3-642-27954-6_20.