Construction of an AI-Driven Privacy Protection Framework for Traffic Big Data: A Perspective Based on the Fusion of Multimodal Image Recognition and Federated Learning

Xiang Gong, Qiaoqiao Wang, Dehan Kong, Yingyu Cheng, Jiaye Ma
Hebei University of Environmental Engineering, Department of Information Engineering, Qinhuangdao 066102, Hebei, China
Corresponding author: Xiang Gong (e-mail: hebueegx@126.com)

ABSTRACT The rapid development of intelligent transportation systems has generated massive volumes of heterogeneous traffic data, creating significant challenges for privacy protection and secure data utilization. To overcome the limitations of centralized storage architectures and single privacy-preserving approaches, this study proposes an AI-driven privacy protection framework based on the integration of multimodal image recognition and federated learning. A hierarchical multimodal feature extraction architecture is first developed to process heterogeneous visual and traffic data efficiently. Federated learning is then employed to enable distributed collaborative model training while preventing raw data exposure. To further enhance privacy protection, differential privacy mechanisms and dynamic parameter aggregation strategies are incorporated to resist inference attacks and improve model robustness. Experimental analysis demonstrates that the proposed framework effectively balances privacy preservation and model performance while supporting large-scale distributed data processing. The proposed methodology provides a practical solution for secure intelligent transportation systems and offers valuable references for distributed sensing networks, wireless communication infrastructures, and secure information transmission environments.

INDEX TERMS traffic big data, federated learning, privacy protection, wireless communication networks, secure information transmission

I. INTRODUCTION

DRIVEN by the wave of smart city construction, intelligent transportation systems and advanced engineering for smart infrastructure have become essential components for improving the efficient operation of cities. This synergy integrates data-driven traffic management with high-performance industrial materials and embedded fiber sensors, ensuring that both the urban mobility network and the physical fabric of modern architecture are digitally interconnected and structurally resilient. Hundreds of millions of IoT sensors, high-definition cameras, and vehicle terminals emit petabytes of data every day, which will create a vast, modal-rich, and high-value-density transportation big data system. This data not only contains the biometrics and the identity of the person (number of license plate information, facial information, etc.) but also the information of deep-seated privacy of the person (information of vehicle trajectories and preferences of driving behaviors). Data breaches or misuse to one would be a serious threat to personal safety or even public safety. Traditional techniques for privacy protection, such as data anonymization, desensitization, or access control may be questionable when there is a complex correlation and inference attacks. Traffic data, in particular, is multi-source and heterogeneous, and it is difficult for privacy protection technology to solve the unstructured characteristic of video images and the time sensitivity of trajectory data at the same time. Furthermore, centralized data storage and processing models not only create single points of failure risks but also result in excessive concentration of data control with added significance of the misuse of data.

In recent years, the development of federated learning has offered a revolutionary way to destroy “data silos” without compromising data privacy. By training the models locally and uploading only encrypted model parameters, federated learning fundamentally avoids the possible risk of raw data leakage. Meanwhile, the advancements in multimodal image recognition technology have made it possible to extract

high dimensional features from heterogeneous visual data. However, how to solve the convergence challenges of non-independent and identically distributed data to ensure model performance, and how to solve the problem of efficiently aggregating parameters in the low-latency traffic scenarios, are pressing technical challenges that need to be solved.

This paper proposes a privacy protection framework of traffic big data based on multimodal image recognition and federated learning. This framework resolves the privacy protection challenges inherent in the concurrent processing of multi-source heterogeneous data from intelligent transportation and engineering through technological integration and innovation. By securing the data streams of both urban mobility and automated manufacturing, it provides the theoretical support and practical reference necessary for constructing a safe, reliable, and efficient environment for material science research and smart infrastructure.

II. RELATED WORK

Currently, research on data privacy protection is undergoing a profound paradigm shift from "peripheral defense" to "source embedding" and from "centralized aggregation" to "distributed collaboration". YANG [1] explored the necessity of applying privacy protection technology on social media platforms to address the challenges of data abuse and unauthorized access. Ji et al. [2] advocated embedding privacy protection mechanisms from the source of data and at the moment of generation, which is a more fundamental and effective paradigm for IoT data security. Huang et al. [3] proposed a personalized federated transfer learning method. This method allows a predictive model to be trained collaboratively using data from multiple heterogeneous clients while protecting data privacy, and to adapt to the personalized characteristics of different clients through transfer learning technology. Yuan et al. [4] successfully protected data privacy while achieving effective domain adaptation, providing a new approach for utilizing multi-source data under privacy constraints. Jiang and Lv [5] combined zero-knowledge proof and blockchain technology to construct a distributed vehicle network data privacy protection scheme.

Privacy is easily leaked during the sharing and use of personal data, and centralized storage and management models have single point of failure and data abuse risks. Liang et al. [6] effectively enhanced the security, transparency and controllability of personal data during the sharing and use process, and reduced the dependence on a single centralized institution. Sultana and Srinivas [7] used visual cryptography to decompose secret images into multiple meaningless shared images. Liu et al. [8] used the decentralized, tamper-proof and traceable characteristics of blockchain to encrypt and store logistics data and manage permissions, ensuring that only authorized parties can access specific data. The scheme constructed by Hong and Sun [9] provides a safer and more reliable data search service for intelligent systems, while protecting data privacy and solving the trust problem of the authenticity of search results. Ni et al. [10] broke the scenario limitation and effectively utilized multi-source data while protecting data privacy. Existing methods mostly focus on single data modalities or specific application scenarios, which are difficult to cope with the needs of concurrent processing of massive, multi-source, heterogeneous data (such as surveillance video, trajectory data, vehicle network signaling) in the transportation field. Furthermore, how to construct a privacy protection framework that can withstand complex attacks and meet real-time requirements in a highly dynamic, low-latency traffic environment remains a challenge for current research. This paper aims to explore a new technological integration path to provide theoretical reference and practical solutions for overcoming the aforementioned limitations.

III. METHODS

A. FEATURE EXTRACTION AND PREPROCESSING OF MULTIMODAL TRAFFIC DATA

In intelligent transportation scenarios, raw data typically exists in multiple modalities, including visual images from roadside cameras, trajectory sequences from vehicle-mounted GPS devices, and traffic signaling from inductive loops or radar. To achieve efficient collaborative training in the subsequent federated learning framework, it is necessary to first perform unified representation and preprocessing of heterogeneous data. For visual modal data, this paper adopts a lightweight convolutional neural network architecture for feature extraction. Considering the limited computing resources of roadside devices, MobileNetV3 is chosen as the basic feature extraction network to reduce computational overhead while ensuring high recognition accuracy. Specifically, for each frame of monitoring image, denoising and size normalization are first performed, uniformly adjusting it to an input size of 224×224 pixels. Subsequently, multi-level features of the image are extracted through the depthwise separable convolutional layers of MobileNetV3, including visual semantic information such as vehicle type, body color, license plate area, and occupant information. For trajectory modal data, this paper uses a long short-term memory network for modeling. Trajectory data is usually a sequence of timestamps and includes attributes such as latitude and longitude coordinates, instantaneous speed, and direction of travel. The temporal dependencies of vehicle driving are captured by LSTM network, and the implicit features of the trajectory, such as driving behavior patterns and path preferences, are extracted. For vehicle network signaling data, multilayer perceptron is used for feature encoding, and the event type, signal strength, base station switching information, etc. contained in the signaling are converted into fixed-dimensional feature vectors [11]. To achieve deep fusion of multimodal features, this paper designs a feature fusion layer based on an attention mechanism. This layer first maps visual features, trajectory features, and signal features to the same dimension through three independent linear transformations, thus aligning the scale of each modality. Next, a learnable query vector is

introduced to calculate the importance score of each modality feature: the mapped modality feature is then multiplied by the query vector to obtain an unnormalized attention score. These scores are then softmax normalized to obtain the attention weight for each modality; the sum of these weights is 1, intuitively reflecting the relative contribution of each modality to the current task. Finally, the original visual, trajectory, and signal feature vectors are multiplied by their corresponding attention weights and concatenated sequentially into a unified joint feature vector. This design allows the model to dynamically adjust the fusion ratio of each modality based on the characteristics of the input data. For example, higher weights are given to visual features when the image is clear, while trajectory and signal data may be relied upon more at night or in severe weather, thus achieving adaptive and interpretable multimodal fusion and providing a high-quality data foundation for subsequent privacy-preserving distributed training.

B. DISTRIBUTED PRIVACY-PRESERVING TRAINING MECHANISM BASED ON FEDERATED LEARNING

After the local multimodal feature extraction is finished, this paper proposes a federated learning framework to meet the privacy protection requirement of "data usable but not visible." Unlike traditional centralized training, compared with the federated learning framework, each traffic node (such as intersection edge computing units and regional traffic data centers) only use local data to train the model, and only upload encrypted gradient or model parameter to the central server. The federated learning architecture designed in this paper contains three main components: multiple local clients (per the various traffic data collection nodes), an aggregation server, and a trusted execution environment (if needed). At the start of each round of communication, the aggregation server sends the current global model to selected clients. Each client uses local multimodal data for training the received model and the number of training rounds is 5 epochs and batch size is 32. After local training the client uploads the updated model parameters to the aggregation server. To prevent attackers from inferring the original data through inverse gradients, this paper proposes a differential privacy perturbation mechanism before the client uploads the data. In particular, random noise that follows the Laplace distribution is added to the gradients calculated, which makes it impossible for an attacker to correctly suss out whether or not a particular sample is contained in the training set. This local differential privacy mechanism offers strong privacy guarantees from a mathematical point of view; even if the model parameters are acquired by the server or a third party, the privacy information for the individual cannot be revived. Furthermore, to address potential privacy breaches during server-side dynamic parameter aggregation, this paper introduces a secure aggregation protocol: before the client uploads parameters, a secret sharing technique is used to encrypt parameter updates, ensuring that the aggregation server can only decrypt and aggregate after collecting a sufficient number of encrypted updates, thus preventing the server from spying on individual client updates before aggregation. Simultaneously, gradient pruning is combined with this technique to limit the impact of a single sample on parameter updates, further reducing the sensitivity to differential privacy and enhancing defense against inference attacks. To solve the problem of communication efficiency in federated learning, in this paper, we use gradient sparse learning technology, that is, gradient updates are only sent when the top k% of update absolute value, and the rest is set to zero, and local accumulation until the threshold, and then sent. This does reduce the communication overhead significantly, and is suitable for those situations with limited network bandwidth, such as traffic scenarios. After receiving the encrypted gradients from each client, the aggregation server does weighted aggregation by a federated averaging algorithm. During aggregation, the weight of the volume of local data for each client is taken into account; the client with a larger amount of data contributes more to the construction of the global model. The model is aggregated and updated globally and used for the next iteration until either the model converges or after a preset number of communication rounds.

C. DYNAMIC PARAMETER AGGREGATION AND ADAPTIVE SECURITY STRATEGY

In heterogeneous traffic environments, the distribution of the data of different nodes often has many differences. For example, the traffic flow patterns of intersections in the city center and suburban roads are different and the image quality of the sun and rainy days are different [12-13]. This non-independent and identically distributed characteristic may cause a slow convergence or even a divergence of global model in federated learning. To cope with this, a dynamic parameter aggregation strategy is proposed in this paper based on the data quality awareness. This strategy an evaluation module is introduced in the server side to evaluate the quality of the uploaded model updates from the client's side in multiple dimensions. Evaluation metrics include magnitude of loss reduction in the local validation set, norm of gradient update and the computational latency of the client. Clients with higher qualities scores get higher aggregation weights for the aggregation of global, hence guiding the model to a better direction for optimization. For clients that have abnormal gradient updates owing to the poor quality of the data collected or malicious attacks, the aggregation server implements weight reduction or isolation processing to improve the robustness of the framework. Meanwhile, considering the real-time requirements of traffic scenarios, this paper designs a resource-adaptive security policy switching mechanism. The core objective of this mechanism is to always meet a preset minimum privacy protection budget ($\epsilon_{\min}$). Under this premise, real-time requirements are met by optimizing computational and communication resources. When the system detects network congestion or excessive computational burden, it

does not reduce the strength of privacy protection. Instead, it reduces the amount of communication data by adjusting gradient sparsity (e.g., sending the top-5% instead of the top-10%) or using more efficient model compression techniques, thus prioritizing system response speed while adhering to the bottom line of privacy protection. The logic of this mechanism is: data sensitivity is high during peak periods, therefore a high level of privacy protection (i.e., a small ϵ value) must be maintained; while real-time requirements are met by sacrificing some non-core communication efficiency. Through this design, the framework constructed in this paper can achieve stable, efficient, and adaptive distributed model training while strictly ensuring the lower limit of privacy protection.

IV. RESULTS AND DISCUSSION

A. EXPERIMENTAL SETUP AND DATASET CONSTRUCTION

To verify the effectiveness of the proposed privacy protection framework, we conducted experiments in a real-world traffic big data environment. The dataset consists of three parts: image data from the publicly available traffic monitoring dataset UA-DETRAC, comprising 20,000 video frames covering different lighting conditions, weather conditions, and traffic densities; and vehicle-to-everything (V2X) signal data generated according to the V2X communication standard, including interaction events between vehicles and roadside units. All data was divided into 50 non-independent, identically distributed clients based on geographical region, with each client containing different modal data combinations. The experiments were implemented using the PyTorch framework, with the server configured with an Intel Xeon Gold processor and an Nvidia A100 graphics card.

B. MULTIMODAL FUSION AND PRIVACY PROTECTION PERFORMANCE ANALYSIS

The experiments initially compared the performance of the framework on two tasks, namely vehicle classification and traffic flow prediction. The vehicle classification task was to recognize vehicle brand, type, and color in photos in images and the traffic flow prediction task was to predict the average speed of road segments over the next 15 minutes based on historical trajectories and signaling data. Table 1 demonstrates that the proposed fusion framework was able to achieve state-of-the-art performance on both tasks. The mean absolute error of traffic flow prediction was reduced to 4.21, which showed that the fusion of multimodal feature data could better compensate for the information missing of single modalities, and the federated mechanism ensured the availability of data. The introduction of differential privacy noise had some effect on the model performance, but through careful control of the noise budget, it is still possible to guarantee the average accuracy of 94.8% when ϵ=2.0, indicating that there is a trade-off between the privacy guarantee and model performance.

TABLE 1. Performance comparison of different methods on multimodal traffic tasks.

method	Vehicle classification accuracy rate (%)	Traffic flow forecast MAE (km/h)	Privacy protection strength (ϵ)
Centralized training (no privacy)	97.5	3.89	Unprotected
Local training (without federation)	89.2	6.12	Data localization
Federal Average (FedAvg)	92.6	5.08	Parameter Upload
Framework of this paper (ϵ=5.0)	96.1	4.35	5.0
Framework of this paper (ϵ=2.0)	94.8	4.21	2.0

Analysis result of Table 1 indicates that under the strict privacy protection(=2.0), the vehicle classification accuracy of the proposed framework is less than 2.7 percentage points of ideal centralized training without privacy protection which is in an acceptable range for the practical application. The traffic flow prediction error is 4.21km/h, which is superior to the traditional federated averaging algorithm and pure local training algorithm, indicating that multimodal information plays a complementary gain effect on the perception of the traffic situations. While enhancing the privacy protection strength does cause some performance degradation in the model, the degree is slow and does not cause drastic model degradation, which reflects the robustness degree of the model to noise addition.

C. EVALUATION OF COMMUNICATION EFFICIENCY AND CONVERGENCE SPEED

Communication overhead is crucial to assess the practicality of federated learning frameworks. This paper measures the amount of communication data and the communication round number that different methods need to achieve the same model accuracy. As shown in Table 2, after introducing gradient sparsity techniques, our framework communication data volume per round is only 1.8 MB which approximately 62.3% lower than traditional federated averaging algorithm. For the target accuracy, the number of communication rounds is 28, or 15 fewer than used by the federated averaging algorithm, and 9 fewer than the framework without sparsity. This is attributed to the dynamic parameter aggregation strategy being an effective way of filtering for high quality gradients, thereby accelerating

the model convergence process. The reduction in the cost of communication is significant for deployment on edge computing nodes with limited bandwidth because it can significantly reduce network congestion and transmission latency.

TABLE 2. Comparison of communication overhead and convergence rounds for different methods

method	Single-round communication data volume (MB)	Number of rounds required to achieve target accuracy	Total communication data volume (MB)
Federal Average (FedAvg)	4.8	43	206.4
Federal average + sparsity	2.3	37	85.1
This paper's framework (without sparsity)	4.8	29	139.2
This article's framework (full mechanism)	1.8	28	50.4

Analysis of the results in Table 2 shows that the total communication data volume of the proposed framework is only 50.4 MB. This means that under the same network bandwidth conditions, the proposed framework can support more concurrent client participation or provide more frequent iteration cycles for model updates. The reduction in convergence rounds also means a reduction in local computing power consumption on the client side, which is particularly beneficial for edge devices that rely on battery power. Although gradient sparsity loses some gradient information, combined with the dynamic aggregation strategy, it actually promotes convergence by reducing noise interference, demonstrating the synergistic effect of the combination of technological innovations.

D. VERIFICATION OF PRIVACY PROTECTION STRENGTH AND ATTACK RESISTANCE

To verify the privacy protection effectiveness of the framework, this paper simulates two typical attack scenarios: membership inference attacks and model inversion attacks. Membership inference attacks aim to determine whether a specific sample participated in model training, while model inversion attacks attempt to reconstruct the original image from the gradients. The experimental control groups include unprotected federated learning, differential privacy with added noise, and the complete framework proposed in this paper. As shown in Table 3, under membership inference attacks, the attack success rate of the proposed framework is only 52.3%, indicating that the differential privacy mechanism effectively obfuscates sample existence. Under model inversion attacks, the structural similarity index of the proposed framework is only 0.18, far lower than the 0.67 of the unprotected framework, indicating that attackers cannot reconstruct identifiable image content from the gradients. The introduced adaptive security mechanism dynamically enhances the noise level as the attack intensity increases, further improving the defense effect.

TABLE 3. Comparison of attack defense effectiveness under different privacy protection mechanisms

Protection mechanism	Members infer attack success rate (%)	Model Reverse Attack SSIM	Average response time (ms)
Unprotected Federal Learning	87.6	0.67	124
Differential privacy only (fixed ϵ)	54.2	0.21	156
Gradient sparsity only	79.3	0.58	112
This article's framework (adaptive)	52.3	0.18	138

Analysis of the results in Table 3 shows that the proposed framework effectively defends against both types of attacks while maintaining an average response time of 138 milliseconds, meeting the needs of most real-time traffic applications. Compared to fixed differential privacy mechanisms, the adaptive mechanism optimizes response time while maintaining a high level of privacy protection because it addresses the load by optimizing communication rather than reducing the privacy budget. The significant decrease in attack success rate and reconstructed image quality demonstrates that the framework integrating multimodal feature extraction and federated differential privacy can form a defense-in-depth system, preventing attackers from effectively extracting individual privacy even if they intercept the transmitted model parameters. Notably, an SSIM value of 0.18 indicates that the reconstructed image has almost no visual similarity to the original image, and sensitive information such as license plates and faces in the image is no longer recognizable. To further investigate the risk of feature-level privacy breaches, additional analysis was conducted: a classifier was trained based on reconstructed images (SSIM=0.18) to identify the macro-categories (color, model) of vehicles. The results showed that the classifier's accuracy was only 31.2% (close to 30% of random guessing), significantly lower than the 99.1% accuracy achieved when trained on the original images. This

indicates that despite the low SSIM value, attackers cannot effectively infer meaningful category features from severely distorted reconstructed images, thus protecting privacy at both the visual and semantic levels.

V. CONCLUSION

This paper addresses the urgent need for privacy protection of multimodal big data in intelligent transportation and engineering, proposing a privacy-preserving framework that integrates multimodal image recognition of both traffic patterns and material science microscopic structures through federated learning. By securing the data streams of urban mobility alongside high-precision manufacturing parameters, the framework ensures a robust and confidential environment for the collaborative development of smart industrial infrastructure. This framework unifies the representation of heterogeneous traffic data through a hierarchical multimodal feature extraction module; introduces a federated learning mechanism to achieve distributed collaborative training, ensuring that the original data does not leave the local machine; combines differential privacy noise injection and gradient sparsity techniques to optimize communication efficiency while protecting privacy; and further proposes dynamic parameter aggregation and adaptive security strategies to effectively address non-independent and identically distributed data and real-time requirements. Experimental results show that the proposed framework achieves an average accuracy of 94.8% in typical traffic tasks such as vehicle classification and traffic flow prediction, reduces communication overhead by more than 62%, and demonstrates strong resistance to member inference and model reverse engineering attacks, achieving a good balance between privacy protection and system performance. The theoretical contribution of this research lies in exploring the technical integration path of multimodal perception and distributed privacy protection; its practical value lies in providing a feasible solution for the compliant circulation and secure utilization of traffic big data. Future work will focus on cross-domain migration capabilities in more complex traffic scenarios alongside high-precision engineering environments, integrating blockchain technology to achieve trusted auditing of the aggregation process for both vehicular data and material science parameters.This convergence further enhances the framework's practicality and robustness, ensuring secure data governance across the digital infrastructures of intelligent transportation and automated manufacturing.

AUTHOR CONTRIBUTIONS

Conceptualization –Xiang Gong, Qiaoqiao Wang, Dehan Kong, Yingyu Cheng and Jiaye Ma; methodology – Xiang Gong, Dehan Kong, Yingyu Cheng and Jiaye Ma; investigation – Xiang Gong, Qiaoqiao Wang, Dehan Kong, Yingyu Cheng and Jiaye Ma; writing-original draft preparation – Xiang Gong, Qiaoqiao Wang, Dehan Kong, Yingyu Cheng and Jiaye Ma. All authors have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

FUNDING

This research was supported by, 1. Funded by Science Research Project of Hebei Education Department (BJK 2023119) 2. Funded by Scientific Research of Hebei University of Environmental Engineering (XJXM-QN-2025006)

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

[1] D. YANG, "Application of Data Privacy Protection Technology in Social Media Platforms," JOURNAL OF COMPUTER SCIENCE, vol. 2, no. 2, pp. 53-56, 2025, doi: 10.54097/wzrb4w15.

[2] X. Ji, W. Zhu, S. Xiao, et al., "Sensor-based IoT data privacy protection," Nature Reviews Electrical Engineering, vol. 1, no. 7, pp. 427-428, 2024, doi: 10.1038/s44287-024-00073-2.

[3] G. Huang C, H. Li, W. Peng, et al., "Personalized federated transfer learning for cycle-life prediction of lithium-ion batteries in heterogeneous clients with data privacy protection," IEEE Internet of Things Journal, vol. 11, no. 22, pp. 36895-36906, 2024, doi: 10.1109/JIOT.2024.3433460.

[4] L. Yuan, M. Erdt, R. Li, et al., "Data privacy protection domain adaptation by roughing and finishing stage," The Visual Computer, vol. 40, no. 2, pp. 471-488, 2024, doi: 10.1007/s00371-023-02794-1.

[5] W. Jiang and X. Lv, "A distributed internet of vehicles data privacy protection method based on zero-knowledge proof and blockchain," IEEE Transactions on Vehicular Technology, vol. 73, no. 5, pp. 6332-6345, 2023, doi: 10.1109/TVT.2023.3345272.

[6] W. Liang, Y. Yang, C. Yang, et al., "PDPChain: A consortium blockchain-based privacy protection scheme for personal data," IEEE Transactions on Reliability, vol. 72, no. 2, pp. 586-598, 2022, doi: 10.1109/TR.2022.3190932.

[7] M. Sultana N and K. Srinivas, "Data privacy protection in cloud computing using visual cryptography," Multimedia Tools and Applications, vol. 84, no. 21, pp. 23577-23597, 2025, doi: 10.1007/s11042-024-19963-6.

[8] J. Liu, J. Zhao, H. Huang, et al., "A novel logistics data privacy protection method based on blockchain," Multimedia Tools and Applications, vol. 81, no. 17, pp. 23867-23887, 2022, doi: 10.1007/s11042-022-12836-w.

[9] H. Hong and Z. Sun, "Constructing conditional PKEET with verification mechanism for data privacy protection in intelligent systems: H," Hong, Z. Sun. The Journal of Supercomputing, vol. 79, no. 13, pp. 15004-15022, 2023, doi: 10.1007/s11227-023-05253-9.

[10] R. Ni, Y. Lu, B. Yang, et al., "A federated pedestrian trajectory prediction model with data privacy protection," Complex & Intelligent Systems, vol. 10, no. 2, pp. 1787-1799, 2024, doi: 10.1007/s40747-023-01239-5.

[11] W. Fang, J. Zhang, X. Lin, et al., "A study on data privacy protection in power battery SOH prediction based on federated learning," Ionics, vol. 31, no. 10, pp. 10579-10595, 2025, doi: 10.1007/s11581-025-06606-5.

[12] C. Yudiana T, D. Rosadi S, and S. Priowirjanto E, "The urgency of doxing on social media regulation and the implementation of right to be forgotten on related content for the optimization of data privacy protection in Indonesia," Padjadjaran Jurnal Ilmu Hukum (Journal of Law), vol. 9, no. 1, pp. 24-45, 2022, doi: 10.22304/pjih.v9n1.a2.

[13] H. Huang, S. Sun, D. Wang, et al., "Data privacy protection diagnostic algorithm for industrial robot joint harmonic reducers based on swarm learning," IEEE/ASME Transactions on Mechatronics, vol. 30, no. 6, pp. 6268-6277, 2025, doi: 10.1109/TMECH.2025.3528212.