Department: Head

Secure and Privacy Aware Data Sharing Approach for Smart Electric Vehicles

Debashis Das, Pushpita Chaterjee and Uttam Ghosh
Meharry Medical College

Benjamin Blakely
Argonne National Laboratory

***Abstract*—The integration of smart electric vehicles (SEVs) into smart cities marks a significant step toward creating efficient, sustainable, and connected urban spaces. However, secure and private data sharing is a major challenge as SEVs connect with smart city systems. The interaction between SEVs and consumer electronic devices (CEDs) raises serious concerns about data security and privacy. To address these challenges, this article presents how blockchain technology and federated learning (FL) can address these issues. The proposed approach provides a secure and privacy-aware framework for data exchange between SEVs and CEDs in smart cities. The experiment results demonstrate the effectiveness of the proposed framework for secure data sharing and maintaining system reliability in smart city environments. It also enables trust and promotes the widespread adoption of interconnected urban technologies.**

CONSUMER ELECTRONICS DEVICES(CEDS) like smart home devices, wearables, and IoT sensors serve an essential function in the smart city ecosystem to collect and transmit data to enhance urban living. As urban environments increasingly adopt smart city technologies, smart electric vehicles (SEVs) with CEDs become an important aspect of this transformation [1]. Communication between SEVs and CEDs optimizes the smart city ecosystem. Meanwhile, CEDs interact with SEVs and other smart city infrastructure to contribute to a cohesive and responsive environment. These devices enable seamless communication and data exchange to facilitate real-time decision-making and optimize urban services. However, this interconnectedness introduces vulnerabilities, as shown in Fig. 1 that need to be addressed to protect user privacy and ensure data security during data sharing.

As smart cities continue to progress, SEVs bring together electric vehicles, smart grid technology, and advanced communication systems. These vehicles will generate voluminous data from location/speed to battery status/energy consumption, which may be used

Digital Object Identifier 10.1109/MCE.YYYY.Doi Number
Date of publication DD MM YYYY; date of current version DD MM YYYY

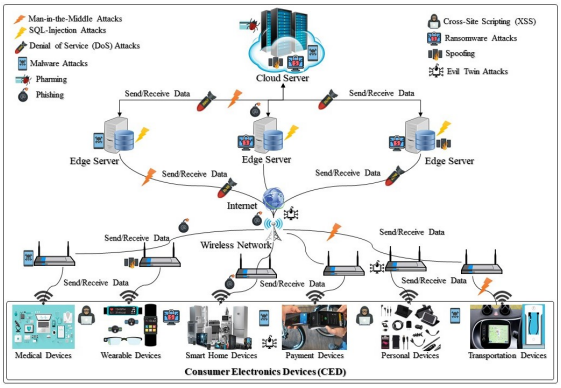


Figure 1: Possible attacks in CEDs.

for enhancing urban mobility and optimizing energy management to contribute to overall quality of life. The variety of devices and systems involved in smart city ecosystems come with different security protocols. This diversity can create security gaps and make it easier for attackers to exploit vulnerabilities. However, SEVs with CEDs in smart city infrastructure introduce several significant security challenges, such as data breaches, privacy concerns, and system reliability [2]. These may disrupt vehicle operations or steal sensitive information. To address these issues, it is essential to implement robust security measures and privacy-preserving techniques for SEVs. Without a unified framework, the current SEVs are highly vulnerable to cyber threats and leakage of personal information.

Therefore, we propose a secure and privacy-aware data-sharing approach for SEVs using blockchain and federated learning (FL). The proposed approach is designed for SEVs's communication without sharing its data using FL. A permissioned blockchain is considered to store and share data. Our approach uses blockchain's immutability and transparency to ensure data integrity and FL to allow decentralized model training to keep user data private. In addition, secure multi-party computation (MPC) and homomorphic encryption are integrated to maintain data confidentiality during processing. Furthermore, the proposed framework can build trust among users by assuring them that data sharing is secure and transparent so they can engage in smart city technologies without fear of losing personal information. It also ensures safer and more efficient ways of exchanging data in smart city ecosystems. Our approach will bridge the existing gap in data security and, therefore, create confidence for users to adopt SEVs and their associated technologies. It provides an innovative solution that addresses both privacy concerns and operational challenges in the deployment of CEDs. Furthermore, this study aims to achieve the following research objectives within the context of consumer-focused smart city infrastructure:

- We aim to implement FL to allow for privacy-preserving model training to ensure that sensitive data from SEVs remains decentralized and secure.
- We aim to develop a blockchain-based framework to secure FL models and data as well as prevent unauthorized access in SEV networks.
- We aim to discuss the integration of the proposed framework with existing smart city infrastructure and CEDs to assess how it can interact with different technologies and platforms.

PROPOSED METHODOLOGY

This section discusses the proposed framework as shown in Fig. 2 that includes SEVs, a blockchain network, and an FL server. SEVs participate in the FL process and interact with the blockchain for data sharing and smart contract execution.

Data Security Management in SEVs: In this approach, SEVs collect data that is initially stored locally on the SEV's onboard computer or edge device. Before data is transmitted, it is hashed using cryptographic algorithms to ensure that even a small change in the data would result in a completely different hash. Each blockchain transaction consists of a sender and receiver, transaction ID, timestamp, and digital signature [3]. The hashed data, along with metadata (such as timestamp, source, and any relevant identifiers), is packaged into a transaction and broadcast for verification. A block groups valid transactions, links to the previous block, and forms a chain of blocks known as a blockchain. Only authorized entities have access to

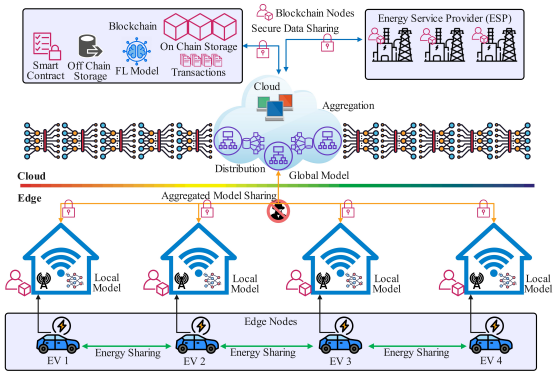


Figure 2: Proposed system model.

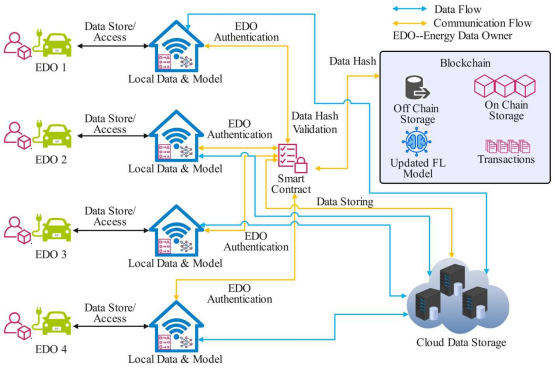


Figure 3: Proposed data sharing model.

view the data on the blockchain. These transactions are designed to ensure transparency, accountability, and security across distributed participants. Smart contracts deployed on the blockchain network automate transaction validation, data verification, and reward distribution for contributions. Vehicles submit local updates for aggregation as part of FL model updates, and access control ensures that only authorized participants can submit or query data.

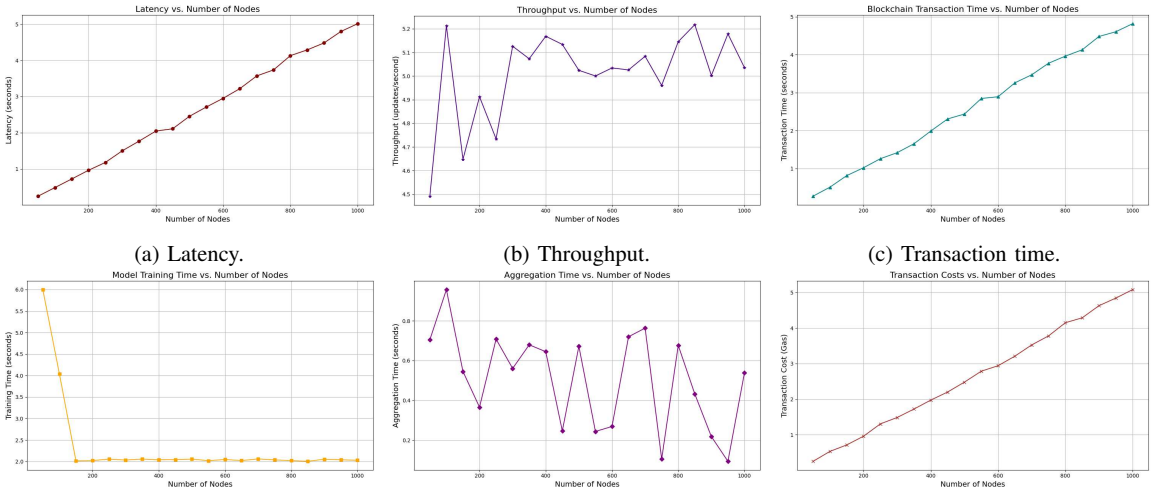
Data Privacy Management in SEVs: FL is a machine learning/deep learning approach where SEVs collaboratively train a model [4]. A global model is initialized and distributed to participating SEVs. Each SEV uses its local data to train the model. After local training, each SEV computes updates to the model (e.g., weight adjustments) based on its data. Therefore, a central server or aggregator receives the local model updates. The central server aggregates the updates using averaging or weighted aggregation from all participating SEVs to improve the global model. The SEVs receive the aggregated and updated global model back. Each SEV then continues training using this improved model, and the cycle repeats. Secure techniques, such as encryption or secure multi-party computation, can be used to ensure that model updates cannot be reverse-engineered to reveal sensitive data [5]. MPC is used to securely aggregate model updates or data from SEVs without compromising individual privacy. SEVs participate in an MPC protocol to compute the aggregated model securely by splitting inputs into random shares and distributing them among participating vehicles or nodes, as well as computing the global aggregate using these shares without reconstructing individual inputs.

Secure and Privacy-Aware Data Sharing in SEVs: Fig. 4 shows the detailed scenario for secure and privacy-aware data sharing. Blockchain records and verifies the model updates shared during the FL process. Each update is logged in a blockchain ledger to ensure its authenticity and protect against tampering or unauthorized modifications. This adds a layer of security to the FL process, which ensures that the global model improvements are based on legitimate updates [6]. The blockchain records each node's contribution, including the validation data, to pinpoint and isolate the origin of any discrepancies resulting from noisy data. This way, bad or noisy validation data won't affect the final model validation. However, any data sharing or model modification can be traced back through the blockchain to ensure transparency and adherence to privacy agreements. Together, they create a secure and efficient framework for managing and utilizing data in smart cities and SEV ecosystems. So, the proposed system makes sure that model validation is strong and safe in a blockchain environment that supports FL.

EXPERIMENT RESULTS AND ANALYSIS

We experimented to assess the proposed approach and its impact on system performance and scalability. First, we used Ethereum to handle and record transactions and to manage and aggregate model updates from FL participants. Ethereum is a widely adopted blockchain platform with a strong development community to execute smart contracts, which allows for the automation of energy trading transactions and other complex interactions within the smart grid. We implemented an FL setup using TensorFlow Federated for training models on simulated datasets. The dataset used in the experiment simulates vehicle data and contains information about used cars [7]. The experiment evaluates FL performance and scalability in a blockchain-integrated environment. The dataset is divided into multiple subsets, each representing a different participant in the FL setup. Therefore, we measured several performance metrics as shown in Fig. 4. Fig. 4a shows how the latency changes as the number of nodes in the FL system increases. As the number of nodes increases, the latency usually increases as well. Because more nodes must communicate and validate blockchain transactions, it takes longer. Fig. 4b illustrates how throughput changes with the number of nodes. Initially, as the number of nodes grows, the throughput might increase due to parallel processing.

This article has been accepted for publication in IEEE Consumer Electronics Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCE.2025.3529398



(a) Latency. (b) Throughput. (c) Transaction time.

(d) Model training time. (e) Aggregation time. (f) Transaction costs.

Figure 4: Performance analysis results.

Fig. 4c shows how the time required for blockchain transactions changes as the number of nodes increases. As more nodes participate in the blockchain, the transaction time typically increases because of the added complexity of maintaining consensus among a larger number of nodes. Fig. 4d tracks how long it takes to train the model on each node as the number of nodes increases. Initially, adding more nodes may result in a decrease in the training time per node, as each node possesses a smaller subset of data. Fig. 4e shows how the aggregate time changes with the number of nodes. Here, aggregation time usually decreases and increases with the number of nodes. Finally, Fig. 4f illustrates how the blockchain transaction costs change as the number of nodes grows. In most blockchain systems, the transaction cost increases as the number of nodes grows because more resources are required to validate and store transactions across the network. Table 1 compares data-sharing approaches using several techniques for SEVs based on several metrics [8]. The results indicate that this integrated framework can support real-time processing, secure data handling, and effective decision-making in SEV systems.

APPLICATION OF THE PROPOSED APPROACH

In a smart city, where SEVs are integral components of the energy ecosystem, efficient data management and real-time energy trading between SEVs and the grid are crucial for sustainability. The proposed approach provides several practical applications beyond our objectives. These applications include:

Energy Trading and Grid Optimization: The proposed framework enhances energy trading in a smart city with SEVs by enabling vehicles to communicate their energy needs and availability to the grid in real-time. This provides a decentralized, transparent, and tamper-proof system for negotiating energy prices to

Table 1: Comparison of data sharing approaches in SEVs.

Metrics	**CA**	**EC**	**DP**	**HE**	**BC**	**FL**	**Proposed**
Data Privacy	✖	✔	✔	✔	✖	✔	✔
Data Integrity	✖	✔	✔	✔	✔	✔	✔
Scalability	✖	✔	✔	✖	✔	✔	✔
Latency	✖	✔	✔	✖	✔	✔	✔
Single Point of Failure	✖	✔	✔	✔	✔	✔	✔
Real-time Processing	✖	✔	✖	✖	✔	✔	✔
Transparency and Auditability	✖	✖	✔	✔	✔	✖	✔
Secure Data Sharing	✖	✔	✔	✔	✔	✔	✔
Compliance with Regulations	✔	✔	✔	✔	✔	✔	✔

✔ *support;* ✖ *do not support; CA: Centralized Approach; EC: Edge Computing; DP: Differential Privacy; HE: Homomorphic Encryption; BC: Blockchain;*

distribute energy efficiently across the grid. The FL model can predict energy demand patterns based on driving behavior and location, and blockchain ensures the security and integrity of the data.

Vehicle-to-Grid (V2G) Integration: SEVs are essential in V2G systems, where vehicles can store and supply energy to the grid. SEVs can participate in real-time energy exchanges with grid infrastructure by deploying the proposed framework. It helps optimize energy flow and provides seamless integration between EVs and the grid.

Autonomous Energy Management in Smart Cities: The proposed framework also enables the autonomous management of energy resources within smart cities. Using the FL model, SEVs can independently make decisions regarding energy consumption based on local shared data, and blockchain guarantees that each decision is transparent, immutable, and auditable. This decentralized approach can help reduce grid congestion and minimize energy waste in urban areas.

Emergency Health Alerts for Pedestrians: For older adults and pedestrians walking along the roadside, SEVs can function as mobile health monitoring units. These vehicles can collect vital health data from wearable devices or sensors on pedestrians, including heart rate, oxygen levels, and other key signs. If any irregularities are detected, SEVs can immediately transmit this information to emergency responders or nearby healthcare facilities. This prompt action ensures that medical emergencies are addressed quickly and provides additional security for pedestrians, particularly older adults.

EVALUATION AND DISCUSSION

Benefits of the Proposed Approach

The proposed approach enhances the role of CEDs in smart cities by addressing critical concerns related to data security and privacy. As smart cities continue to evolve, this approach will provide secure and efficient operation of CEDs. We will discuss a few benefits below.

Data Confidentiality and Integrity: Data related to vehicle performance are securely recorded on the blockchain. Multiple nodes validate each transaction to prevent unauthorized tampering and ensure data integrity. In a closed blockchain with fewer participants, the risk of a 51% attack is indeed higher. The economic cost of acquiring 51% of the stake in a closed system is typically prohibitive. On the other hand, the proposed system can detect and mitigate data poisoning risks. All model updates are immutable and traceable for the identification of suspicious or malicious contributions. This traceability allows the system to pinpoint malicious updates and take corrective action. Each participating vehicle in the system is registered with a unique cryptographic identity, and its actions and updates are linked to a verifiable identity to make it difficult for malicious entities to create multiple fake identities (Sybil nodes) without being detected. Therefore, the creation of multiple Sybil identities necessitates a significant investment of resources to make it costly for attackers to flood the network with fake nodes.

Security and Privacy: The proposed approach aligns with current security and privacy regulations by ensuring compliance and enhancing user trust in smart city applications. It secures data sharing and adheres to principles of data integrity and transparency mandated by regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Meanwhile, FL supports the data minimization principle of GDPR by allowing CEDs to contribute to model training without sharing sensitive personal data. Overall, the proposed framework adheres to existing security and privacy regulations and lays a solid foundation for future compliance as regulations evolve to safeguard user data and increase trust in the deployment of CEDs within smart cities.

Scalability and Flexible Integration: Blockchain's decentralized nature scales effectively with increasing numbers of devices. Each device in a smart city contributes to the blockchain network. As the number of SEVs and other CEDs increases, the blockchain network scales to handle the growing volume of data. Therefore, the system remains efficient and responsive even with many interconnected devices. While full integration across all smart city components may require further development, our approach provides a flexible framework that can be adapted to specific use cases, such as SEVs and energy management systems. They can connect with city-wide traffic management systems, smart grids, and other services.

Secure Data Sharing and Privacy Protection: Smart contracts on the blockchain automate and enforce data-sharing agreements. These contracts define the rules for data access and usage so that only authorized parties can interact with the data. For example, a SEV could automatically grant data access

to a city traffic management system during congestion events while protecting data from unauthorized access. Instead of transmitting sensitive data, devices share only aggregated model updates with a central server, which updates the global model without compromising individual privacy. The proposed approach improves features such as autonomous driving and energy management and enables SEVs to learn from diverse data sources without exposing individual driver habits or location details.

User Acceptance in Smart City Integration: The proposed framework can incorporate user-friendly applications that simplify data management for users to monitor their energy consumption and transactions effortlessly. This ease of use encourages active participation in energy trading and smart grid interactions. Users are provided with transparency regarding how their data is collected, stored, and utilized and can track their energy transactions in real-time. This integration facilitates a smoother transition to smart city technologies and finally promotes user acceptance.

Limitations and Future Scope

While the proposed approach provides significant advancements, it also presents several limitations. The reliance on blockchain may introduce latency and computational overhead, especially in large-scale smart city environments with numerous CEDs.

High Computational and Communication Overhead: The proposed approach requires substantial computational power for training and validating models. This may strain the limited resources of SEVs and require additional infrastructure, such as edge computing, to offset the load. In the future, the development of optimized machine learning algorithms for resource-constrained devices will be more efficient in model training and validation directly on SEVs.

Latency Issues: SEVs require real-time data updates and quick decision-making for energy trading or grid balancing. Blockchain's transaction processing time, especially when combined with the FL's aggregation, could lead to delays for time-sensitive tasks like energy distribution and trading. Hybrid consensus mechanisms or layer-2 blockchain solutions can accelerate transaction speeds in the future.

Energy Consumption: The proposed work may require more energy consumption due to the real-time data sharing and model updates in smart city ecosystems, as it requires constant system availability and active node participation. Our future task will be focused on developing energy-efficient protocols to optimize resource usage and reduce the overall energy footprint of the system.

CONCLUSION

This study presents a secure and privacy-aware data-sharing approach for SEVs within smart city ecosystems. The proposed approach provides a significant advancement in the data sharing of SEVs and addresses key challenges like data tampering, privacy concerns, and noisy or malicious inputs. Blockchain's immutable ledger provides a secure platform for recording transactions, and FL minimizes data exposure on SEVs without centralizing sensitive information. The experimental results show that the proposed framework scales efficiently with increasing numbers of participants. The use of blockchain for managing and aggregating model updates has proven to be highly effective. Future research will focus on optimizing the aggregation process to support larger networks with low latency and energy.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation under award numbers 2219741 and 2401928. The submitted manuscript has also been created by UChicago Argonne, LLC, operator of Argonne National Laboratory. Argonne, a DOE Office of Science Laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the government.

REFERENCES

1. J. A. Sanguesa, V. Torres-Sanz, P. Garrido, F. J. Martinez, and J. M. Marquez-Barja, "A review on electric vehicles: Technologies and challenges," *Smart Cities*, vol. 4, no. 1, pp. 372–404, 2021.
2. F. Liao, E. Molin, and B. van Wee, "Consumer preferences for electric vehicles: a literature review," *Transport Reviews*, vol. 37, no. 3, pp. 252–275, 2017.
3. P. Kumar, R. Kumar, M. Aloqaily, and A. K. M. N. Islam, "Explainable ai and blockchain for metaverse: A security and privacy perspective," *IEEE Consumer Electronics Magazine*, vol. 13, no. 3, pp. 90–97, 2024.

4. D. Das, U. Ghosh, P. Chatterjee, and S. Shetty, "Advanced federated learning-empowered edge-cloud framework for school safety prediction and emergency alert system," in *2023 IEEE 12th International Conference on Cloud Networking (CloudNet)*, 2023, pp. 507–512.
5. P. Chatterjee, D. Das, and D. B. Rawat, "Federated learning empowered recommendation model for financial consumer services," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 2508–2516, 2024.
6. S. Banerjee, D. Das, P. Chatterjee, B. Blakely, and U. Ghosh, "A blockchain-enabled sustainable safety management framework for connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 6, pp. 5271–5281, 2024.
7. N. Birla, N. Verma, and N. Kushwaha, "Vehicle dataset contains information about used cars," 2022, accessed on August 6, 2024. [Online]. Available: https://www.kaggle.com/datasets/nehalbirla/vehicle-dataset-from-cardekho
8. A. Sadiq, M. U. Javed, R. Khalid, A. Almogren, M. Shafiq, and N. Javaid, "Blockchain based data and energy trading in internet of electric vehicles," *Ieee Access*, vol. 9, pp. 7000–7020, 2020.

Debashis Das is with the Department of Computer Science and Data Science at Meharry Medical College, Nashville, TN, USA. Email: debashis.das@ieee.org.

Pushpita Chatterjee is with the Department of Computer Science and Data Science at Meharry Medical College, Nashville, TN, USA. Email: pushpita.c@ieee.org.

Uttam Ghosh is with the Department of Computer Science and Data Science at Meharry Medical College, Nashville, TN, USA. Email: ghosh.uttam@ieee.org.

Benjamin Blakely is a Cybersecurity and Artificial Intelligence Researcher with the Argonne National Laboratory, leading the Applied Research Group, Strategic Security Sciences Division, Lemont, IL, USA. Email: bblakely@anl.gov.