Kalpa Publications in Computing

Volume 22, 2025, Pages 1102–1112

Proceedings of The Sixth International Conference on Civil and Building Engineering Informatics

Cybersecurity-Aware Decentralized Machine Learning Framework for Construction Equipment Motion Recognition Using Blockchain

Chengliang Zheng[1], Xingyu Tao[2*], Jiarui Lin[3], Moumita Das[4], Wenchi Shou[5], Jack C.P. Cheng[6]

[1] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan, China.

[2] Department of Civil and Environmental Engineering, The Hong Kong University of Science and Technology, Hong Kong, SAR.

[3] Department of Civil Engineering, Tsinghua University, Beijing, China.

[4] Department of Civil and Environmental Engineering, The Hong Kong University of Science and Technology, Hong Kong, SAR.

[5] School of Engineering, Design & Built Environment, Western Sydney University, Sydney, Australia.

[6] Department of Civil and Environmental Engineering, The Hong Kong University of Science and Technology, Hong Kong, SAR.

chengliang@ust.hk, xtaoab@connect.ust.hk, lin611@tsinghua.edu.cn, moumitadas@ust.hk, W.Shou@westernsydney.edu.au, cejcheng@ust.hk

Abstract

Artificial intelligence (AI) is playing an increasing role in the construction industry to enhance productivity, reduce safety accidents, and optimize collaboration efficiency. However, attacks on AI systems also introduce cybersecurity threats that could lead to severe consequences, such as equipment damage, financial loss, operational downtime, safety accidents, and potential loss of life. Motivated by the construction industry's limited efforts to defend against AI cybersecurity vulnerabilities—a result of a lack of awareness and IT resources—this paper aims to propose a cybersecurity-aware decentralized machine learning (CADML) framework to protect the life cycle cybersecurity of machine learning (ML) models leveraging blockchain. First, the workflow of the CADML framework will be introduced to illustrate the logic of blockchain-ML integration. Second, a new blockchain smart contract algorithm, ML-embed smart contract (MLSC), will be developed to train and apply AI in a decentralized manner. The primary innovation framework extends current "partially" blockchain-ML integration methods to enable the ML's "lifecycle" (from raw data storage, training, implementation, to model update) to operate in a decentralized and

I. Hkust, J. Cheng and Y. Yantao (eds.), ICCBEI 2025 (Kalpa Publications in Computing, vol. 22), pp. 1102–1112

secure blockchain environment. The framework is tested to recognize construction equipment motions. Results show that (1) the ML model could be successfully trained and implemented within a blockchain and (2) the ML performance (accuracy, precision, and recall) is acceptable.

1 Introduction

Artificial intelligence (AI) (e.g., machine learning (ML)) is transforming the construction sector, which is benefiting AI applications from areas like on-site safety management (Baker, Hallowell, & Tixier, 2020), schedule management (Pan & Zhang, 2021), supply chain optimization (Baduge et al., 2022), and the control of construction robotics and drones (Bademosi & Issa Raja, 2021). However, most AI models in this sector rely on centralized servers controlled by certain project members or third-party vendors for training and implementation, which introduces severe cybersecurity risks (Yazdinejad, Dehghantanha, Parizi, Srivastava, & Karimipour, 2023). These vulnerabilities include the potential for AI model manipulation—where attackers might alter training data or model parameters—and single-point failures that could compromise entire systems. An example of such a manipulation is a tape attack, where small pieces of tape are strategically placed on signs in a way that causes an AI-driven construction vehicle to misread the sign, leading to potential accidents or misrouting (Bansal et al., 2023). Moreover, the opaque nature of AI decision-making processes makes it difficult to detect when a system has been compromised or is repeating errors, thereby increasing the demand for explainable AI.

Integrating blockchain technology with AI systems presents a promising solution to the cybersecurity vulnerabilities inherent in centralized AI architectures (Han, Shiwakoti, Jarvis, Mordi, & Botchie, 2023). Blockchain is a decentralized digital ledger that records transactions across multiple computers in such a way that the registered transactions cannot be altered retroactively (Tao, Das, Liu, & Cheng, 2021). This technology is known for its robust security features, which include immutability, transparency, and the elimination of a single point of failure, making it highly resistant to tampering and cyber-attacks (Xu et al., 2023). Successful blockchain implementations in the construction industry include automating payments and enforcing contract terms, reducing disputes and delays (Hamledari & Fischer, 2021). Blockchain also improves supply chain management and collaborations by ensuring the traceability and quality of materials from origin to installation (Tao et al., 2023). Additionally, integration with IoT devices allows for real-time infrastructure monitoring, ensuring compliance and facilitating proactive maintenance (L. Wu, Lu, & Chen, 2023). By leveraging blockchain, AI systems in construction can also achieve enhanced security in several ways. First, blockchain can provide a secure platform for sharing AI training data and AI models among multiple stakeholders, reducing the risk of data tampering by ensuring that data alterations are traceable and transparent (Salah, Rehman, Nizamuddin, & Al-Fuqaha, 2019). Additionally, blockchain's decentralized nature prevents single-point failures, as the AI system's operational data and decisions are recorded on a blockchain distributed across many nodes (Adel, Elhakeem, & Marzouk, 2022).

Existing research primarily examines blockchain and AI separately, with most studies still theoretical. There has been limited exploration into integration solutions within construction. H. Wu, Li, Luo, and Jiang (2023) tried to improve quality traceability on construction sites using blockchain and computer vision, though only image hashes were stored on-chain, with the AI model and raw data kept off-chain. Similarly, Adel et al. (2022) introduced a decentralized AI system that leverages blockchain technology to calculate construction costs. The study demonstrated that the blockchain safeguarded the integrity and authenticity of the AI models. Moreover, it ensured that all predictions were synchronized across the blockchain, creating a transparent and auditable environment for

implementation (Yang et al., 2022). However, the model's training occurred off-chain, indicating only partial integration. This is because current AI-blockchain integrations rely on smart contracts, a blockchain element that can self-execute agreements with predefined rules and conditions written in code (Lu et al., 2021). In the context of construction, smart contracts support basic functions like information exchange, payment processes, and version management (Ciotta, Mariniello, Asprone, Botta, & Manfredi, 2021). However, integrating computationally demanding construction AI algorithms, such as machine learning or deep learning, poses challenges due to the limited computational capacity of smart contracts, arising from their decentralized setup and consensus mechanisms (Singh et al., 2020). Developing smart contracts that accommodate complex AI algorithms is technically demanding.

Thus, this paper aims to answer how to protect the lifecycle cybersecurity of construction AI in a decentralized blockchain network. Therefore, this paper proposes a Cybersecurity-Aware Decentralized Machine Learning (CADML) framework to enhance cybersecurity across the lifecycle of machine learning (ML) models. Initially, it will introduce the CADML framework's workflow to demonstrate the integration logic between blockchain and ML. Subsequently, a novel blockchain smart contract algorithm will be designed for decentralized training and AI application. This framework advances beyond current partial integrations by facilitating the complete lifecycle of ML models—from data storage and model training to implementation and updates—within a secure, decentralized blockchain environment. The framework's efficacy is tested by recognizing construction equipment movements.

2 Cybersecurity-Aware Decentralized Machine Learning (CADML) Framework

2.1 Workflow of the CADML Framework

Figure 1 shows the workflow of the CADML framework. Figure 1 (a) shows the CADML architecture, in which the raw data are securely placed in the blockchain database, and the smart contract hold the ML algorithm. The training and implementation are operated within the smart contract so that all authorized project members can maintain the lifecycle security of AI.

The detailed ML workflow in the smart contract is shown in Figure (b) with six steps: (1) Data Acquisition and Preprocessing: Sensor-generated data is continuously transmitted to a processing platform at regular intervals, known as time windows (TW). This data is preprocessed to reduce noise, lower dimensionality, and filter irrelevant information. It is then stored on the blockchain to guarantee its immutability. (2) AI Model Training: Smart contracts access the training data stored on the blockchain and perform security checks before formatting the data to suit model training requirements. If the AI model is actively being trained, it uses this data to update itself from version n to version n+1. (3) Model State Evaluation: Post training, the updated model and key metrics, such as accuracy, are reviewed by a controller to determine if the model is ready for deployment. It transitions from the "training" to the "application" phase if it meets the required accuracy. (4) Model Application: When new data, such as excavator poses, is received, it undergoes security checks and formatting by smart contracts before being fed into the AI model. (5) Continuous Model Monitoring: Smart contracts continuously monitor the model's performance during application. Changes in the site conditions or sensor alterations that affect data characteristics may degrade the model's effectiveness, necessitating a return to the training phase if the pose recognition accuracy falls below acceptable levels. (6) Result Documentation: If the model remains accurate and functional, the application results, including model hash, timestamp, and recognition outcomes (e.g., excavator poses), are recorded on the blockchain for transparency and traceability.

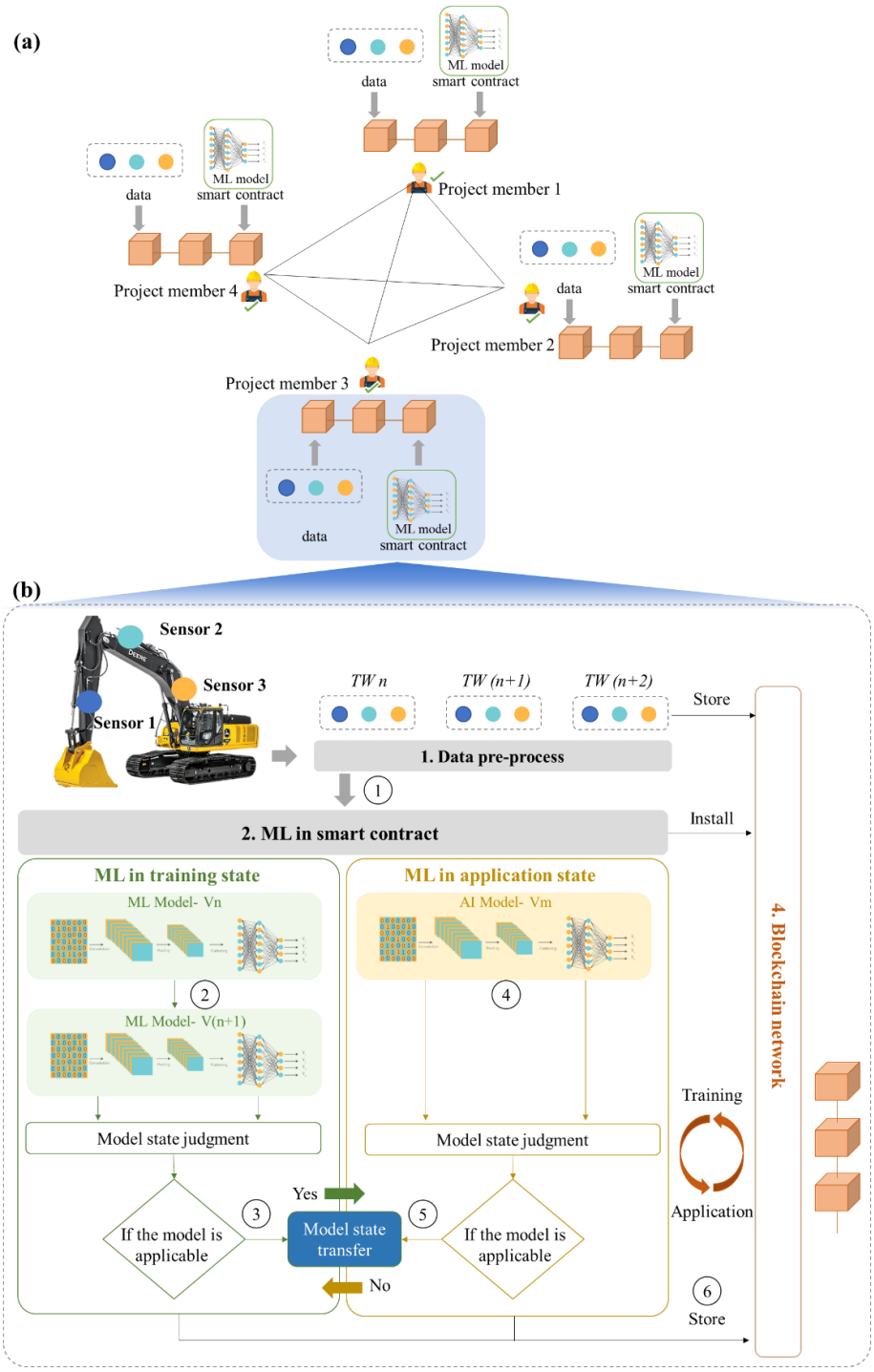

Figure 1: CADML framework

2.2 ML-embed Smart Contract (MLSC) Algorithm

Figure 1 shows the MLESC algorithm. Unlike existing smart that can only process simple computing, the MLSC includes kernel and user spaces. The kernel space supports developers with essential frameworks and common algorithms for AI model development, integrating two key AI/ML frameworks: Massive Online Analysis (MOA) (Li & Zhou, 2018) and Waikato Environment for Knowledge Analysis (WEKA) (Daw & Basak, 2020). MOA processes large data streams for real-time analysis, while WEKA offers robust data processing and model conversion tools. The user space in smart contracts is designated for training and utilizing AI models, structured into six essential layers: (1) Security Check Layer, which ensures data integrity by hashing to block tampered data, (2) Data Adaptation Layer, tasked with modifying data to suit specific algorithm requirements, (3) Algorithm Model Layer, the central component where training and application codes reside, (4) Feedback Layer, which communicates model state information either externally or to the Controller Layer, (5) Output Layer, which logs model data onto the blockchain, and (6) Controller Layer, which switches the AI model between training and application phases. These layers collectively facilitate AI's secure and efficient operation within smart contracts.

In construction pose recognition, sensor data is initially processed by the MLSC's Security Check Layer. The data then moves to the Data Adaptation Layer, where it's converted from string to Instance type, aligning with model requirements. The algorithm model layer uses this data for training or pose classification, which the controller layer controls. Model performance metrics like accuracy are relayed to project managers via the Feedback Layer in real-time. Finally, essential data and results are recorded on the blockchain by the Output Layer. The source code is available at https://github.com/iEricZHENG/BlockchainAI (Zheng et al., 2024).

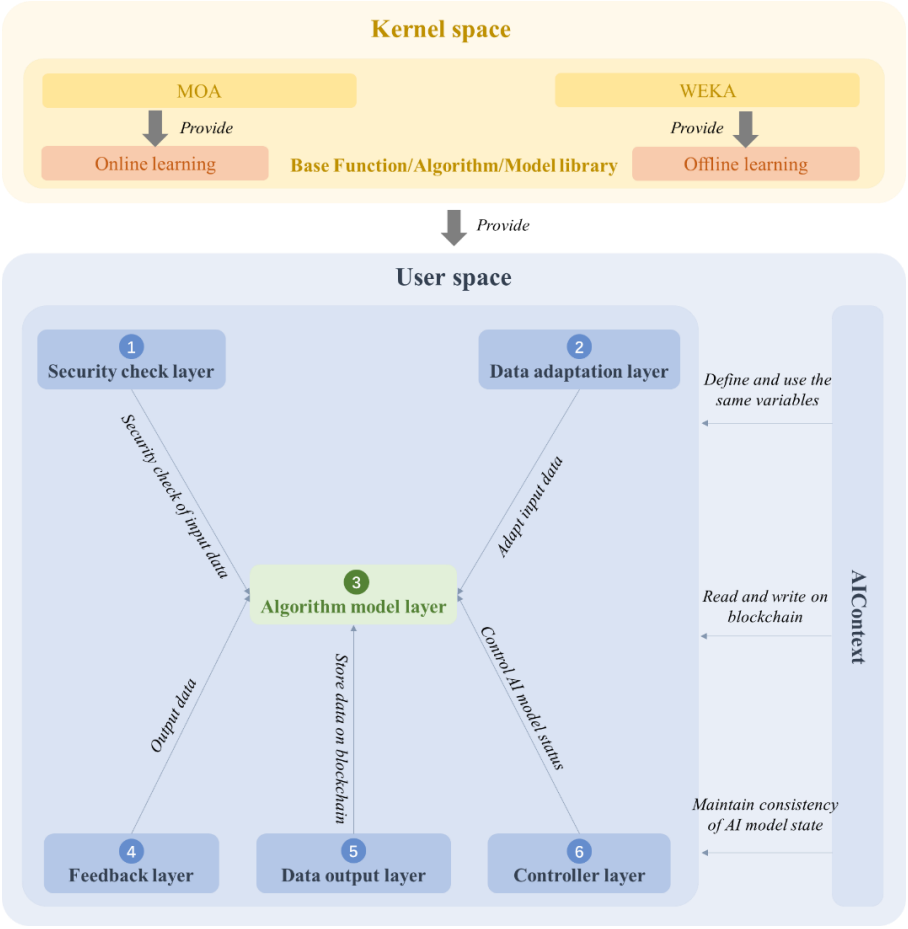

Figure 2: MLSC algorithm

3 Results

3.1 Validation Preparation

This paper validates the CADML framework by recognizing the motion of an excavator, followed by the validation environment and preparation.

Blockchain platform. Hyperledger Fabric (HF) was selected for the CADML framework because of its strong privacy protections, customizable development features, and proven feasibility in construction scenarios (Androulaki et al., 2018). The blockchain experiment utilizes HF version 2.3.0 with two organizations.

Data collection. The inertial measurement unit (IMU), consisting of an accelerometer and a gyroscope, was used in this experiment to track the spatial movements of independent components for excavators. The time-series data collected by the sensors includes acceleration and angular rate.

Machine learning selection. ROSE (Robust Online Self-Adjusting Ensemble) (Cano & Krawczyk, 2022) is a dynamic ensemble learning algorithm suitable for classifying tasks in data stream environments like excavator pose recognition. It effectively handles changing, imbalanced data and concept drift, adapting continuously to new inputs. This robustness addresses class imbalance, drift, and noise, ensuring high accuracy in real-time applications.

3.2 Results of CADML Framework Validation

Figure 3 (a) is the sensor installation. IMU sensors were affixed to the boom, arm, bucket, and cabin of the equipment. The appropriateness and effectiveness of the sensor placement and type were confirmed by Tang et al. (2023). Figure 3 (b) illustrates the training outcomes of the Machine Learning-Enabled Smart Contract (MLES). Specifically, Fig. 8(a) details the iterations of algorithm training recorded on the blockchain, while Fig. 8(b) displays a training record for version 2.0.0 of the ML algorithm. This record includes three components: (1) ML hash, where the blockchain calculates and logs the hash value to ensure each algorithm version is verifiable and secure. (2) Input data, documenting all raw training data, such as IMU sensor readings for x, y, and z-axis accelerations, along with the corresponding excavator posture. Three poses are identified: "0" for stationary, "1" for engine vibrations, and "2" for boom motion. (3) Timestamp, marking the completion of each training session, which helps in assessing the training efficiency of the ML algorithm. Figure 3 (c) demonstrates that the MLSC algorithm effectively identifies the excavator's boom motion, classified as state "2."

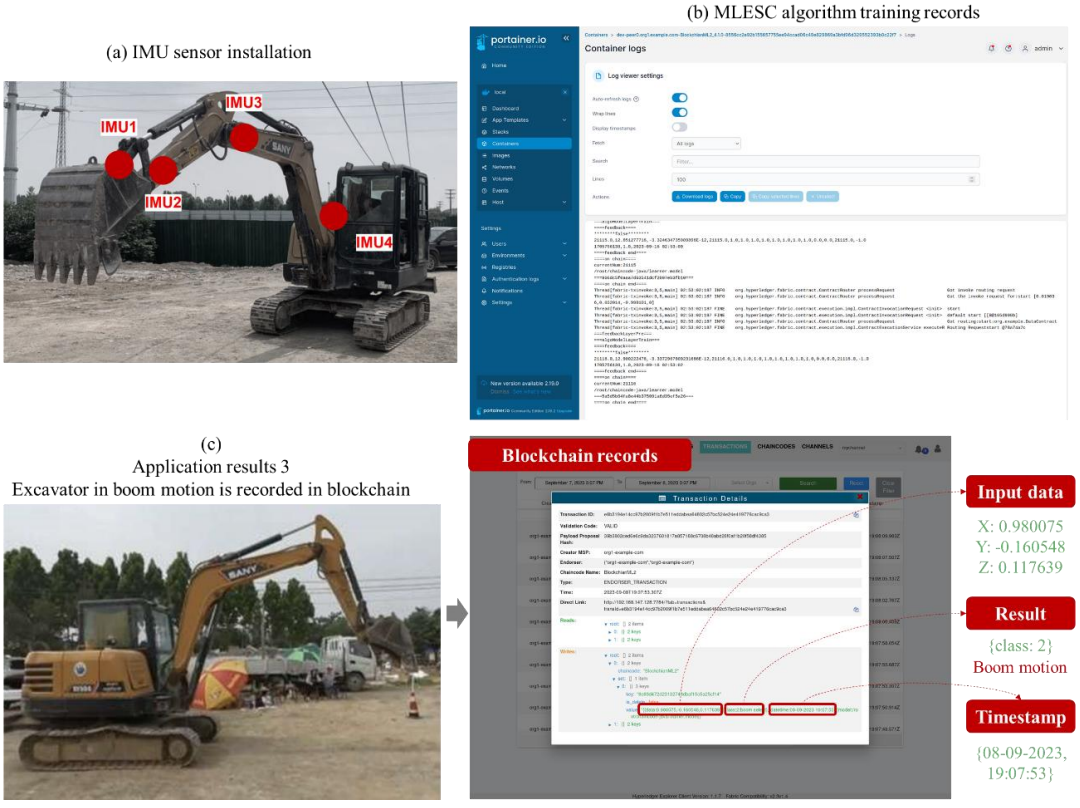

Figure 3: The CADML framework is successfully validated in recognizing excavator motion

This study evaluates the excavator pose recognition model using accuracy, precision, and recall. Accuracy, a common metric for classification models, measures the likelihood that the model accurately identifies the excavator's state. However, its utility diminishes with imbalanced sample classes, potentially skewing the perceived effectiveness of the model. This issue arises when one class predominates, causing the model to excel at recognizing that specific pose but falter with others. Hence, precision and recall are also employed to provide a more rounded assessment. Precision represents the ratio of correctly identified positive predictions (e.g., truly stationary excavators classified as stationary), minimizing the risk of false positives. Meanwhile, recall quantifies the correct positive predictions against all actual positives, which is crucial for ensuring the model reliably detects stationary states without misclassifying them. Together, these metrics offer a comprehensive view of the model's performance, addressing both its strengths and limitations in differentiating excavator poses.

Figure 4 displays the performance of the three metrics, starting from zero and rising with the increase in training data. As the data approaches 3,000 entries, accuracy achieves approximately 95%, precision hits around 94%, and recall reaches about 96%, after which each metric stabilizes. According to (Slaton, Hernandez, & Akhavian, 2020; Tang, Luo, Chen, Wong, & Cheng, 2022), the acceptable thresholds for machine pose recognition are set at 85% for average accuracy, 88% for precision, and 87.6% for recall. Given these benchmarks in our results, which exceed these thresholds, are deemed satisfactory.

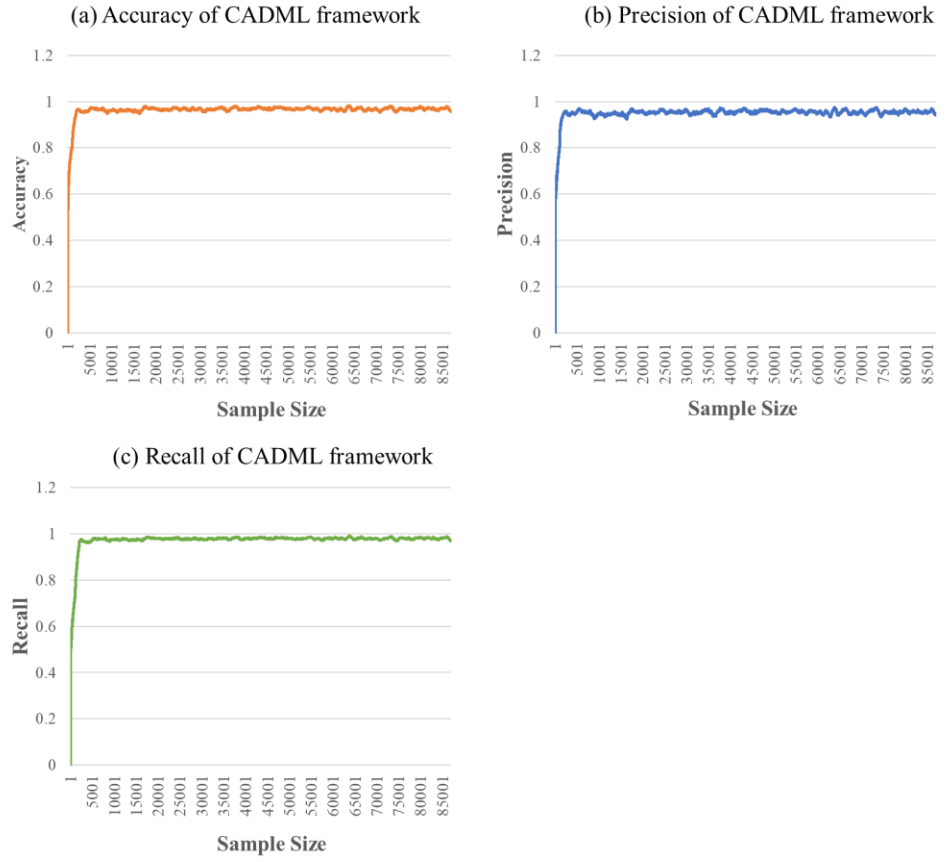

Figure 4: Computing performance of the CADML framework

4 Conclusion

Integrating AI technologies in the construction industry brings cybersecurity concerns such as data tampering, opacity in AI operations, and vulnerabilities from centralized control points. Although some initial studies have converged blockchain technology, a decentralized database technology that secures data immutability, traceability, and robustness, with AI, they only guaranteed "partial" security, as they stored part of AI data (e.g., raw data or trained AI models) to blockchain. This paper advances existing works and introduces a cybersecurity-aware decentralized machine learning (CADML) framework to bolster the "lifecycle" cybersecurity of AI data in construction by leveraging blockchain's. Two research objectives have been achieved. First, the mechanism of how an AI model is trained and implemented within a decentralized blockchain is illustrated via a CADML framework workflow. Second, an MLSC algorithm is developed within the framework to enable lifecycle AI model management. The framework is successfully validated in the scenarios of excavator motion recognition. Moreover, computing performance, including accuracy, precision, and recall, is acceptable. This CADML framework addresses the cybersecurity challenges faced by construction AI and enhances the robustness and reliability of AI applications in project management contexts, opening the door to encourage more stakeholders to contribute AI data and computing sources.

This work is an initial exploration of combining construction AI with blockchain. Two limitations still exist. The first challenge is slower AI training speeds due to blockchain's processing limitations, which hinders timely deployment. Future research could optimize blockchain architectures or develop efficient consensus algorithms to quicken AI training while maintaining security. Additionally, the complexity of configuring blockchain systems poses a barrier to widespread adoption. Simplifying blockchain interfaces and increasing educational efforts to boost blockchain comprehension among construction professionals could mitigate this issue.

References

Adel, K., Elhakeem, A., & Marzouk, M. (2022). Decentralizing construction AI applications using blockchain technology. *Expert Systems with Applications, 194*, 116548. doi:https://doi.org/10.1016/j.eswa.2022.116548

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., . . . Yellick, J. (2018). *Hyperledger fabric: A distributed operating system for permissioned blockchains.* Paper presented at the The 13th EuroSys Conference, Porto, Portugal.

Bademosi, F., & Issa Raja, R. A. (2021). Factors Influencing Adoption and Integration of Construction Robotics and Automation Technology in the US. *Journal of Construction Engineering and Management, 147*(8), 04021075. doi:https://doi.org/10.1061/(ASCE)CO.1943-7862.0002103

Baduge, S. K., Thilakarathna, S., Perera, J. S., Arashpour, M., Sharafi, P., Teodosio, B., . . . Mendis, P. (2022). Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications. *Automation in Construction, 141*, 104440. doi:https://doi.org/10.1016/j.autcon.2022.104440

Baker, H., Hallowell, M. R., & Tixier, A. J. P. (2020). AI-based prediction of independent construction safety outcomes from universal attributes. *Automation in Construction, 118*, 103146. doi:https://doi.org/10.1016/j.autcon.2020.103146

Bansal, V., Bhardwaj, A., Singh, J., Verma, D., Tiwari, M., & Siddi, S. (2023, 12-13 May 2023). *Using Artificial Intelligence to Integrate Machine Learning, Fuzzy Logic, and The IOT as A Cybersecurity System.* Paper presented at the 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE).

Cano, A., & Krawczyk, B. (2022). ROSE: robust online self-adjusting ensemble for continual learning on imbalanced drifting data streams. *Machine Learning, 111*(7), 2561-2599. doi:https://doi.org/10.1007/s10994-022-06168-x

Ciotta, V., Mariniello, G., Asprone, D., Botta, A., & Manfredi, G. (2021). Integration of blockchains and smart contracts into construction information flows: Proof-of-concept. *Automation in Construction, 132*, 103925. doi:https://doi.org/10.1016/j.autcon.2021.103925

Daw, S., & Basak, R. (2020, 11-13 March 2020). *Machine Learning Applications Using Waikato Environment for Knowledge Analysis.* Paper presented at the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC).

Hamledari, H., & Fischer, M. (2021). Construction payment automation using blockchain-enabled smart contracts and robotic reality capture technologies. *Automation in Construction, 132*, 103926. doi:https://doi.org/10.1016/j.autcon.2021.103926

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems, 48*, 100598. doi:https://doi.org/10.1016/j.accinf.2022.100598

Li, C., & Zhou, H. (2018). Enhancing the Efficiency of Massive Online Learning by Integrating Intelligent Analysis into MOOCs with an Application to Education of Sustainability. *10*(2), 468.

Lu, W., Li, X., Xue, F., Zhao, R., Wu, L., & Yeh, A. G. O. (2021). Exploring smart construction objects as blockchain oracles in construction supply chain management. *Automation in Construction, 129*, 103816. doi:https://doi.org/10.1016/j.autcon.2021.103816

Pan, Y., & Zhang, L. (2021). Roles of artificial intelligence in construction engineering and management: A critical review and future trends. *Automation in Construction, 122*, 103517. doi:https://doi.org/10.1016/j.autcon.2020.103517

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and Open Research Challenges. *IEEE Access, 7*, 10127-10149. doi:https://doi.org/10.1109/ACCESS.2018.2890507

Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., & Ra, I.-H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society, 63*, 102364. doi:https://doi.org/10.1016/j.scs.2020.102364

Slaton, T., Hernandez, C., & Akhavian, R. (2020). Construction activity recognition with convolutional recurrent networks. *Automation in Construction, 113*, 103138. doi:https://doi.org/10.1016/j.autcon.2020.103138

Tang, J., Luo, H., Chen, W., Wong, P. K.-Y., & Cheng, J. C. P. (2022). IMU-based full-body pose estimation for construction machines using kinematics modeling. *Automation in Construction, 138*, 104217. doi:https://doi.org/10.1016/j.autcon.2022.104217

Tang, J., Wang, M., Luo, H., Wong, P. K.-Y., Zhang, X., Chen, W., & Cheng, J. C. J. A. i. C. (2023). Full-body pose estimation for excavators based on data fusion of multiple onboard sensors. *147*, 104694.

Tao, X., Das, M., Liu, Y., & Cheng, J. C. P. (2021). Distributed common data environment using blockchain and Interplanetary File System for secure BIM-based collaborative design. *Automation in Construction, 130*, 103851. doi:https://doi.org/10.1016/j.autcon.2021.103851

Tao, X., Das, M., Zheng, C., Liu, Y., Wong, P. K.-Y., Xu, Y., . . . Cheng, J. C. P. (2023). Enhancing BIM security in emergency construction projects using lightweight blockchain-as-a-service. *Automation in Construction, 150*, 104846. doi:https://doi.org/10.1016/j.autcon.2023.104846

Wu, H., Li, H., Luo, X., & Jiang, S. (2023). Blockchain-Based Onsite Activity Management for Smart Construction Process Quality Traceability. *IEEE Internet of Things Journal, 10*(24), 21554-21565. doi:https://doi.org/10.1109/JIOT.2023.3300076

Wu, L., Lu, W., & Chen, C. (2023). Resolving power imbalances in construction payment using blockchain smart contracts. *Engineering, Construction and Architectural Management*(ahead-of-print). doi:https://doi.org/10.1108/ECAM-03-2023-0194

Xu, Y., Tao, X., Das, M., Kwok, H. H. L., Liu, H., Wang, G., & Cheng, J. C. P. (2023). Suitability analysis of consensus protocols for blockchain-based applications in the construction industry. *Automation in Construction, 145*, 104638. doi:https://doi.org/10.1016/j.autcon.2022.104638

Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., & Zheng, Z. (2022). Fusing Blockchain and AI With Metaverse: A Survey. *IEEE Open Journal of the Computer Society, 3*, 122-136. doi:https://doi.org/10.1109/OJCS.2022.3188249

Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023). Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. *Computers in Industry, 144*, 103801. doi:https://doi.org/10.1016/j.compind.2022.103801

Zheng, C., Tao, X., Dong, L., Zukaib, U., Tang, J., Zhou, H., . . . Shen, Z. (2024). Decentralized artificial intelligence in construction using blockchain. *Automation in Construction, 166*, 105669. doi:https://doi.org/10.1016/j.autcon.2024.105669