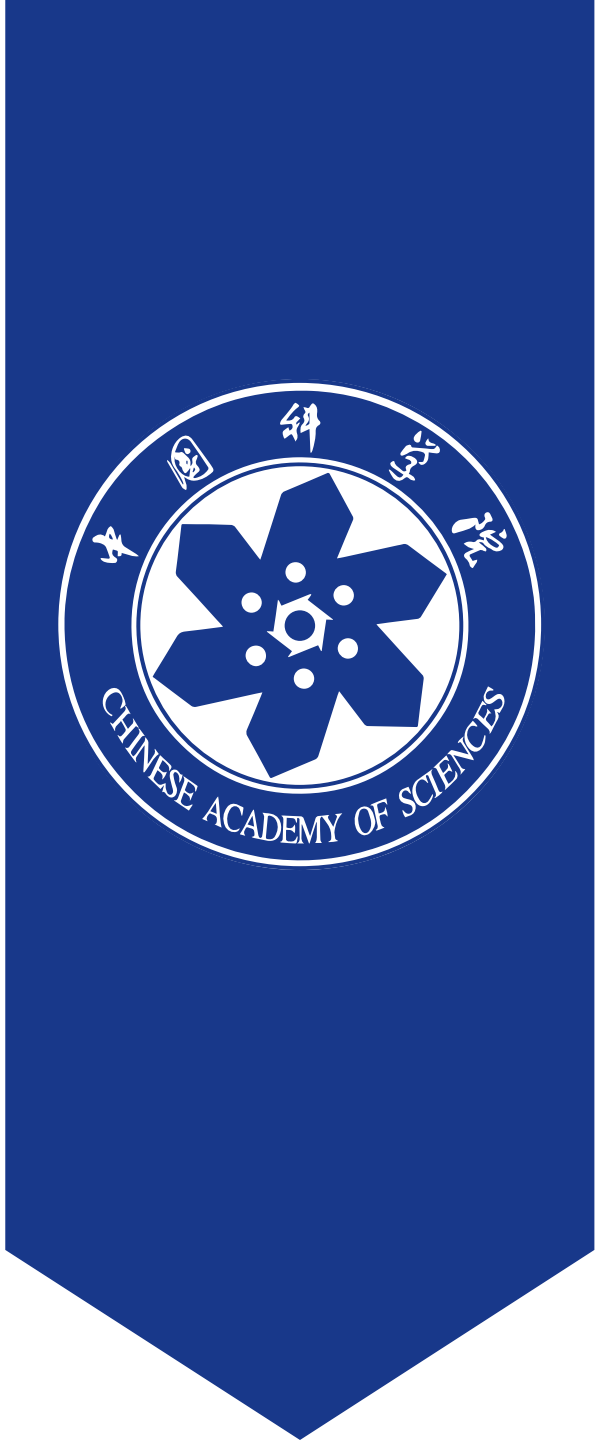


中国科学院上海微系统与信息技术研究所
Shanghai Institute of Microsystem and Information Technology Chinese Academy of Sciences

Deep Neural Network-based Intrusion Detection in Internet of Things: A State-of-the-art Review

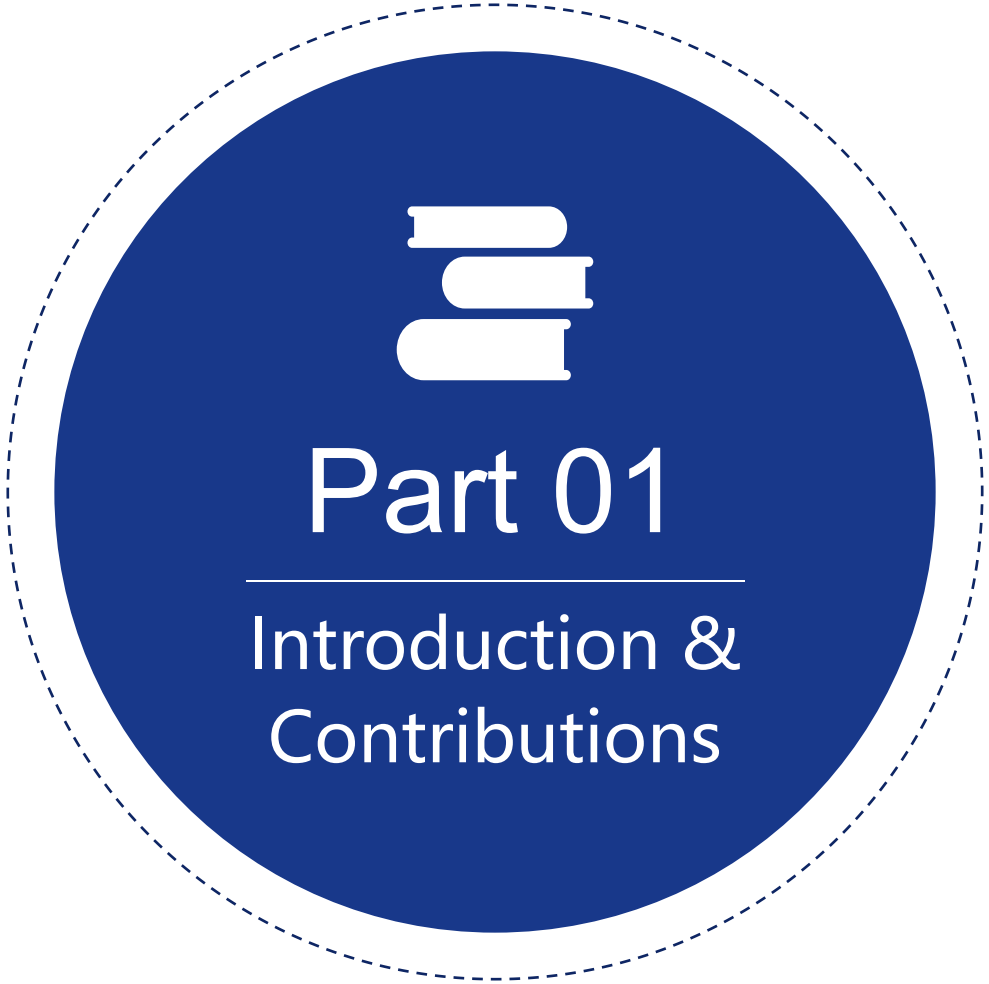
Oral Presentation For

2024 International Conference on Intelligent Computing

Zhiqi Li

Augst/7/2024

Contents



Part 01

Introduction & Contributions

Introduction

Using DNN-based IDS in IoT

Various security threats are faced by the Internet of Things (IoT).

Intrusion detection is employed as an effective method to mitigate these threats, encompassing Botnet, DDoS, and Scan at-tacks.

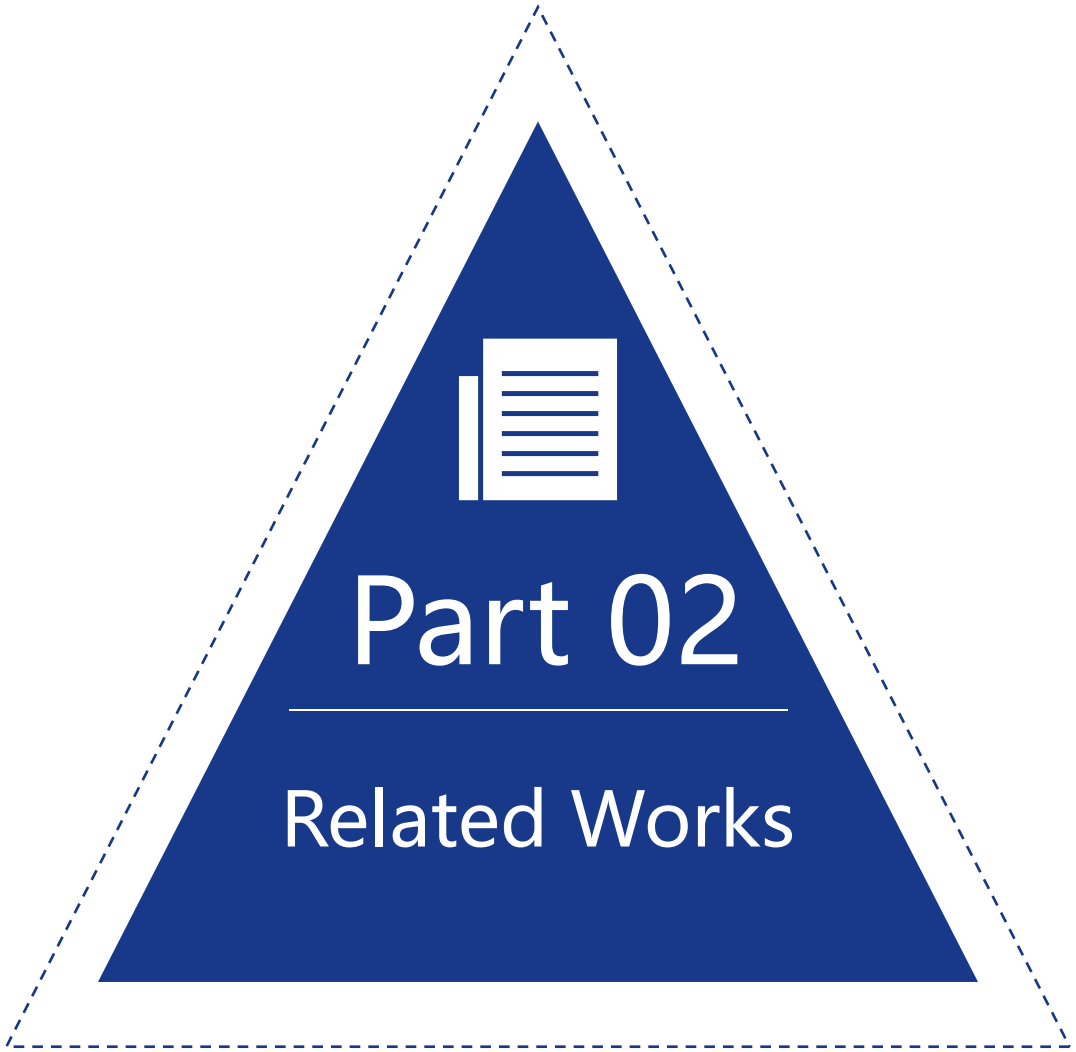
Due to the rapid development of machine learning technology in recent years, deep neural networks (DNNs) emerge as powerful models utilized to significantly enhance the accuracy performance of intrusion detection systems (IDSs) and to increase their adaptability to dynamic networks.

Contributions

1. Conducting a thorough analysis and comparison of advanced works related to trust evaluation using deep learning techniques in OSNs. Analyzing and comparing some advanced related works on intrusion detection in IoT with DNN.

2. Find that, in DDoS attacks, better performance is exhibited by network traffic-based systems. Additionally, higher accuracy is achieved by device behavior-based systems for internal threats and unknown types of attacks.

3. Analyzing challenges and open issues and suggesting some research directions.


Part 02
Related Works

Related Works

Network Traffic-based Intrusion Detection

It focuses on analyzing and monitoring data flows and communication patterns within the network to detect potential intrusion behaviors.
It emphasizes network characteristics such as the flow of network packets, protocol usage patterns, and the frequency and size of data packets.

Device Behavior-based Intrusion Detection

It concentrates on analyzing and monitoring the activities and behavioral patterns of individual devices (such as servers, endpoint devices, etc.) to detect potential intrusions.
It can monitor aspects such as device resource usage, file access patterns, user behaviors, and more.

Network Traffic-based Intrusion Detection

Scheme	Tech.	Dataset	Result	Advantage	Disadvantage
ADI *(L. Adi et al., 2022)*	DNN	DDoS dataset	A=99.99%.	Accuracy was significantly higher than KNN-based methods.	The results were influenced greatly by the learning rate and hidden layers.
VARMA *(P. Varma et al., 2023)*	EENN	CICDDoS 2018	A=97.89%, P=98.85%, R=99.97%.	High accuracy performance.	High computational overhead and time complexity.
ASWAD *(F. Aswad et al., 2023)*	RNN, LSTM	CICIDS2017	A=99.76%, P=98.90%.	Combining the advantages of three neural networks.	Lacking of a realistic testing platform results in unstable reliability.
YOUSUF *(O. Yousuf et al., 2022)*	RNN	NSL KDD	A=99.98%, P=99.9%, R=99.9%.	Excellent accuracy and throughput performance.	A limited number of DDoS attack could be effectively detected.
RED *(D. Reddy et al., 2021)*	DRNN	Synthetic	A=98.28%.	High accuracy and robustness.	High time complexity.
LATIF *(S. Latif et al., 2020)*	DRNN	DS2OS	A=99.20%, P=99.11%, R=99.13%.	High detection accuracy and small system size.	The feasibility of the system has not been validated.

Adi, L. W. P., Mandala, S., Nugraha, Y.: DDoS attack detection system using neural network on Internet of Things. In: 2022 International Conference on Data Science and Its Applications (ICoDSA), pp. 41–46, IEEE, Bandung, Indonesia (2022)

Varma, P., RR, S., Vanitha, M.: Enhanced Elman spike neural network based intrusion attack detection in software defined Internet of Things network. Concurrency and Computation: Practice and Experience, Art. no. e7503 (2023)

Firas Mohammed Aswad, F. M. A., Ali Mohammed Saleh Ahmed, A. M. S. A., Nafea Ali Majeed Alhammadi, N. A. M. A., Bashar Ahmad Khalaf, B. A. K., Mostafa, S. A., & Mostafa, S. A.: Deep learning in distributed denial-of-service attacks detection meth-od for Internet of Things networks. Journal of Intelligent Systems 32, 1–13 (2023)

Yousuf, O., Mir, R. N.: DDoS attack detection in Internet of Things using recurrent neural network. Computers and Electrical Engineering 101, Art. no. 108034 (2022)

Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., Singh, P. K.: Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Transactions on Emerging Telecommunica-tions Technologies

Network Traffic-based Intrusion Detection

Scheme	Tech.	Dataset	Result	Advantage	Disadvantage
HUMA *(Z. Huam et al., 2021)*	DRNN	DS2OS, UNSW-NB15	A=98.56%, P=98.25%, R=98.36%.	High accuracy in classifying the 16 types of attacks.	High time complexity, and it has not been deployed on a real platform.
LE *(K. Le et al., 2022)*	CNN	UNSW-NB15	A=96.69%.	It could detect 9 types of network attacks with high f-score.	The detection accuracy of IMIDS for the Backdoor attack was low.
PARRA *(G. Parra et al., 2020)*	DCNN, LSTM	N_BaIoT	A=94.3%, F1=93.58%.	High detection rates for DDoS and Botnet.	The detection of attack types was limited. High time complexity.
ZHAO *(R. Zhao et al., 2021)*	LNN	UNSW-NB15, Bot-IoT	A=98.94%, 99.99%.	High detection accuracy and low time complexity.	The system has not been deployed and tested in a real platform.
ASG *(H. Asgharzadeh et al., 2023)*	CNN	TON-IoT	A=99.99%, P=99.99%, R=99.99%.	Low computational costs and training expenses.	Challenges still existed in practical deployment.
ELAZIZ *(M. Elaziz et al., 2023)*	DNN	NSL-KDD, BoT-IoT, KDD99	F1=92.7%, 99.9%, 76.8%.	Low computational costs and training expenses.	Performing poorly in terms of accuracy and generalization.

Huma, Z. E., Latif, S., Ahmad, J., et al.: A hybrid deep random neural network for cyberattack detection in the industrial internet of things. IEEE Access 9, 55595–55605 (2021)

Le, K. H., Nguyen, M. H., Tran, T. D., Tran, N. D.: IMIDS: An intelligent intrusion detection system against cyber threats in IoT. Electronics 11(4), Art. no. 524 (2022)

Parra, G. D. L. T., Rad, P., Choo, K. K. R., Beebe, N.: Detecting Internet of Things attacks using distributed deep learning. Journal of Network and Computer Applications 163, Art. no. 102662 (2020)

Zhao, R., Gui, G., Xue, Z., Yin, J., Ohtsuki, T., Adebisi, B., Gacanin, H.: A novel intrusion detection method based on lightweight neural network for internet of things. IEEE Internet of Things Journal 9(12), 9960–9972 (2021)

Asgharzadeh, H., Ghaffari, A., Masdari, M., Gharehchopogh, F. S.: Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm. Journal of Parallel and Distributed Computing 175, 1–21 (2023)

Abd Elaziz, M., Al-qaness, M. A., Dahou, A., Ibrahim, R. A., Abd El-Latif, A. A.: Intrusion detection approach for cloud and IoT

Device Behavior-based Intrusion Detection

Scheme	Tech.	Intrusion handled	Dataset	Results	Advantage	Disadvantage
LATIF *(S. Latif et al., 2021)*	DRNN	DDoS, Scanning	TON_IOT	A=99.14%.	It exhibited good accuracy performance in binary classification.	The model exhibited high time complexity and energy consumption.
BHOR *(H. Bohr et al., 2022)*	DBN	CMRI, MPCI, RECO	KDD CUP'99	A=90%, P=90%, R=92%.	It was superior in terms of accuracy and has a low false alarm rate.	When the number of hidden neurons was low, the false alarm rate was high (> 10%).
ZHANG *(Y. Zhang et al., 2022)*	GNN	FDIA, MATM, PF	Gas pipeline dataset	A=97.2%, P=98%, R=99%.	High performance in small training sets and unbalanced class data.	The types of attacks that could be detected effectively are limited.
BASATI *(A. Basati et al., 2022)*	CNN	DoS, Probe	UNSW-NB15, KDD CUP'99, CICIDS2017	A=100%, 99.92%, and 99.43%.	High detection accuracy performance.	The system had a high time complexity, and it has not been deployed on a real IoT platform.
KASONGO *(S. Kasongo et al., 2023)*	RNN	–	NSLKDD, UNSW-NB15	F1=99.47% and 80.84%.	It was suitable for resource-constrained situations.	The detection accuracy was low for a minority of certain types.

Latif, S., Huma, Z. E., Jamal, S. S., et al.: Intrusion detection framework for the internet of things using a dense random neural network. IEEE Transactions on Industrial Infor-matics 18(9), 6435–6444 (2021)

Bhor, H. N., Kalla, M.: TRUST- based features for detecting the intruders in the Internet of Things network using deep learning. Computational Intelligence 38(2), 438–462 (2022)

Zhang, Y., Yang, C., Huang, K., Li, Y.: Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks. IEEE Transactions on Network Science and Engineering 10(5), 2894–2905 (2022)

Basati, A., Faghih, M. M.: Efficient network intrusion detection in IoT using parallel deep auto-encoders. Information Sciences 598, 57–74 (2022)

Kasongo, S. M.: A deep learning technique for intrusion detection system using a Re-current Neural Networks based framework. Computer Communications 199, 113–125 (2023)

Device Behavior-based Intrusion Detection

Scheme	Tech.	Intrusion handled	Dataset	Results	Advantage	Disadvantage
SANJU *(P. Sanju er al., 2023)*	LSTM	Botnet	IoT-23, CICIDS2017	A=98.12% and 99.98%.	It could capture both local and global patterns in the data.	Poor model generalization performance.
SAHRMA *(B. Sharma et al., 2023)*	DNN, GAN	DoS	UNSW-NB15	A=84%.	It could reduce the number of features before classification, thus lowering the cost.	It had slightly lower accuracy and cannot predict trust values in real-time.
ROUZ *(H. Rouzbahani et al., 2021)*	Snapshot Ensemble DNN	–	DS2OS	A=90.58%, P=87.42%.	The detection accuracy was acceptable.	The lack of testing on a real platform prevented accurate classification of attacks.
PACH *(J. Pacheco et al., 2020)*	ANN	Flood attack for fog nodes	Self-created dataset	A=97.5%, P=98.4%, R=98.9%.	High detection rates, low false-positive alerts, and small time overhead.	The types of attacks that could be detected effectively are limited.

Sanju, P.: Enhancing Intrusion Detection in IoT Systems: A Hybrid Metaheuristics-Deep Learning Approach with Ensemble of Recurrent Neural Networks. Journal of En-gineering Research, Art. no. 100122 (2023)

Sharma, B., Sharma, L., Lal, C., Roy, S.: Anomaly based network intrusion detection for IoT attacks using deep learning technique. Computers and Electrical Engineering 107, Art. no. 108626 (2023)

Rouzbahani, H. M., Bahrami, A. H., Karimipour, H.: A snapshot ensemble deep neural network model for attack detection in industrial internet of things. In: Karimipour, H., Derakhshan, F. (eds.) AI-Enabled Threat Detection and Security Analysis for Industrial IoT, pp. 181–194, Springer (2021)

Pacheco, J., Benitez, V. H., Felix-Herran, L. C., Satam, P.: Artificial neural networks-based intrusion detection system for internet of things fog nodes. IEEE Access 8, 73907–73918 (2020)

Part 03

Challenges & Open Problems

Challenges & Open Problems

Challenges

1. DNNs are frequently associated with high computation-al complexity and storage demands, potentially hindering real-time performance.

2. DNNs are susceptible to adversarial attacks. Attackers could deceive IDSs by adding subtle perturbations, making them unable to correctly identify intrusions.

Mitigation methods

1. Lightweighting the model, implementing hardware acceleration, and optimizing algorithms.

2. The adversarial training and defense mechanisms.

Challenges & Open Problems

Challenges	Mitigation methods
3. Intrusion detection data is typically highly imbalanced, with normal data far out-numbering the anomalous data. It could lead to models being biased towards overfitting to normal data and neglecting anomalous samples during DNN training.	3. Appropriate sampling strategies or the use of specific loss functions.

Part 04

Research Directions

Research Directions

An IDS based on Federated Learning and Transfer Learning

In intrusion detection, FL can be utilized to improve detection performance by leveraging different network traffic datasets and knowledge of various intrusion types.

Besides, through the utilization of transfer learning, researchers can leverage knowledge acquired from one or multiple related tasks and transfer it to the target task, effectively addressing issues related to data imbalance and few-shot learning.

Research Directions

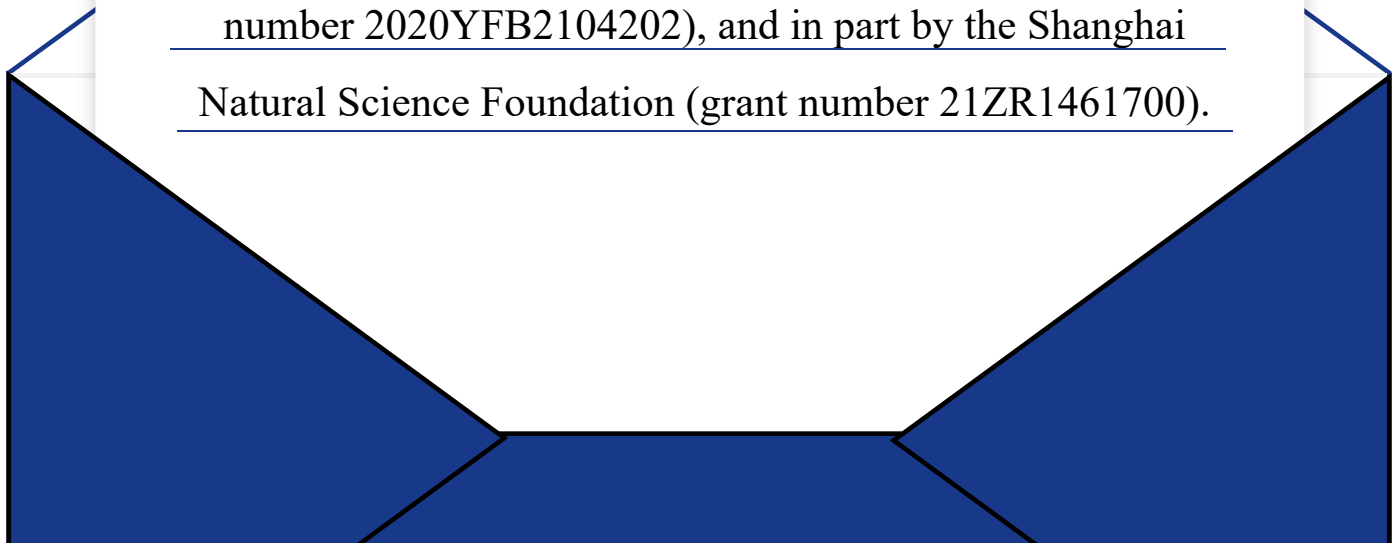
An IDS Using Explainable DNNs

Explainable artificial intelligence (XAI) is a methodology and set of techniques designed for artificial intelligence systems with the aim of making their decision-making and operational processes understandable and explainable.

By combining explainability with adversarial training, the model's ability to withstand adversarial attacks can be enhanced and explanations provided.

Acknowledgment

This study was funded in part by the Key Research and Development Task Special Project of the Xinjiang Uygur Autonomous Region (grant number 2022B01009), in part by the Shanghai Science and Technology Innovation Action Plan (grant number 21DZ1200600), in part by the National Key Research and Development Program (grant number 2020YFB2104202), and in part by the Shanghai Natural Science Foundation (grant number 21ZR1461700).



Thanks!

Q & A