Scientific and Social Research, 2024, Volume 6, Issue 12
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Artificial Intelligence-Enhanced Risk Management System Architecture for Customs Inspection

Mengyao Li*

College of Customs and Public Administration, Shanghai Customs University, Shanghai 200000, China

***Corresponding author:** Mengyao Li, 0210220108@m.shcc.edu.cn

Abstract: The study seeks to boost customs inspection efficiency and ensure compliance with trade data. As traditional methods struggle with the surge in international trade data, this research taps into big data technology to detect anomalies and protect national finances. This study involves a literature review to classify risks and select suitable algorithms for analysis, leading to a conceptual AI-assisted inspection framework validated by expert scoring. This represents an innovative tech approach to customs inspection.

Keywords: Customs inspection; Big data; Artificial intelligence; Risk identification

Online publication: December 31, 2024

1. Background and introduction

On February 9, 2021, China's General Administration of Customs (GACC) launched a strategic program to boost security and efficiency, in line with the "Overall Plan for Smart Customs Construction", focusing on optimizing operations and digital innovation [1–2]. The program shifts from random to targeted inspections, facing challenges like platform limitations and outdated risk knowledge bases, necessitating a sophisticated risk inspection system [3]. The AI-assisted framework integrates business needs with anomaly detection for enhanced accuracy and introduces AI-driven information management and customized intelligent inspection. It efficiently handles large data sets and complex violations, identifying irregular declarations and high-risk entities, thereby improving inspection outcomes, anti-smuggling efforts, and resource allocation, and reducing corruption potential, advancing customs law enforcement standardization and efficiency.

2. Literature review

2.1. Scopes and aims of Chinese customs

The primary aims of China's customs inspections are to oversee the creditworthiness and risk profiles of

businesses, ensure compliance with declaration regulations, scrutinize import and export licenses, verify cargo information, preserve relevant documentation, and uphold tax regulations [4]. These inspections also encompass the management of goods eligible for tax incentives and the suppression of illegal activities such as tax evasion and smuggling [5]. By filtering risk-related data and identifying suspicious pricing and illicit activities, customs inspections protect tax revenues and national interests. In the era of big data, customs authorities in developed nations and the WCO emphasize the critical role of big data technology in improving customs supervision and services [6]. China's customs administration is in step with this international trend, implementing intelligent inspection systems and leveraging big data analytics, cloud computing, and other cutting-edge technologies to pursue a digital transformation [7]. This strategic initiative aims to enhance the precision and scientific integrity of customs inspections.

2.2. Application of anomaly detection

Anomaly detection in customs is enhanced by machine learning, especially with big data analytics, covering compliance, monitoring, data sharing, and security [8]. Balancing detection accuracy and real-time performance is key [9]. Risk identification technologies, which originated in the U.S. and spread globally, gained popularity in the 1990s [10]. China started researching risk management in the late 1980s, led by the insurance industry [11]. Belgium's EasyEnsemble has improved tax fraud detection. Researchers globally are exploring anomaly detection for risk management, like XGBoost and LSTM [12]. The Isolation Forest algorithm is efficient in financial fraud detection. SVM and OCSVM are effective when abnormal data are scarce [13]. Deep neural networks are widely applicable in various fields, including image and speech recognition, and natural language processing [14].

2.3. Information management system and anomaly detection

Information systems rely on the information communication system (ICS) for information flow and the data storage system for data management [15–16]. Security measures like encryption, protocols, access controls, and legal compliance protect these systems [17]. Anomaly detection systems (ADS) use various learning methods to find unusual patterns, crucial in areas like cybersecurity and fraud detection [18–19]. Deep learning in ADS excels in feature extraction and pattern recognition but faces challenges with data annotation, model generalization, computational costs, and interpretability [20–21]. Despite these, ADS has a promising future, aiming to overcome current hurdles for more accurate and efficient anomaly detection.

3. Research design

This study addresses how to boost efficiency in customs inspections amid rising import-export data. It aims to create an AI prototype system using big data to enhance inspection efficiency. The research has three objectives: A) assessing informational challenges; B) exploring big data and risk algorithms for anomaly detection; and C) evaluating the framework's impact on efficiency. The study uses a mix-method approach, with literature reviews for objectives A and B, and a system prototype design based on these findings. For objective C, the study employs a quantitative survey for validation.

4. Development of the custom inspection system

The study synthesizes multidisciplinary knowledge to develop an AI system for customs, focusing on four core

areas: data collection, storage, analysis, and communication. It outlines a framework to facilitate AI integration in customs management.

4.1. Design of the data collection module

The data collection system module gathers inspection data, with two components: company data input and customs inspector data input (**Figure 1**). It includes a web interface for browser-based entry and an application interface requiring software installation.

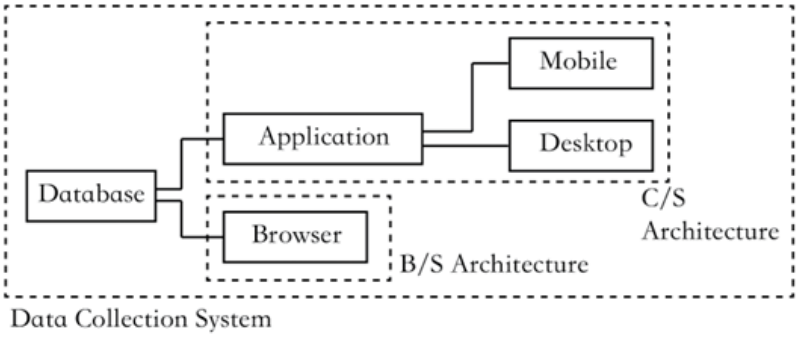

Figure 1. Architecture of data storage system

The data collection module is user-friendly, offering stability with C/S architecture and cross-platform ease with B/S. It uses SQL for data input and integrates with the data storage module, ensuring data security by allowing flow only from collection to storage.

4.2. Design of the data storage module

The data storage module is key to securing data, managing risk analysis, and daily operations (**Figure 2**). It efficiently handles data with databases and file systems and ensures consistency through a common data environment (CDE). The database engine is central for processing simultaneous data tasks, making its choice crucial for customs operations.

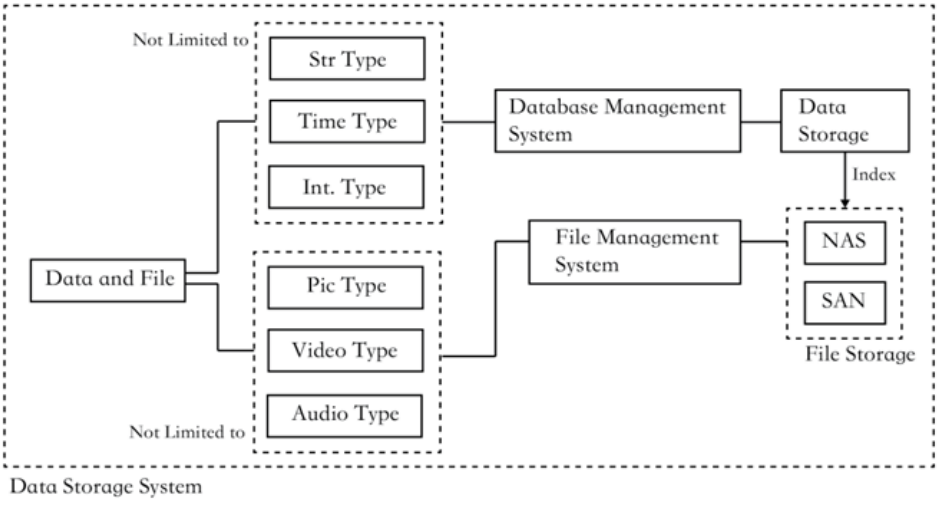

Figure 2. Architecture of data storage system

The research created two databases: one for structured data and another for files. It uses NAS/SAN with RAID for file management, ensuring data redundancy. There is a separate DBMS for data and an FMS for file transfers, with unique identifiers for database operations.

4.3. Design of the data analysis module

The data analysis system module is core to the AI inspection assistance system, analyzing large-scale customs data to spot risks, and includes a specialized algorithm library for big data anomaly detection (**Figure 3**). This library is designed for diverse data analysis and is regularly updated to maintain detection accuracy and efficiency.

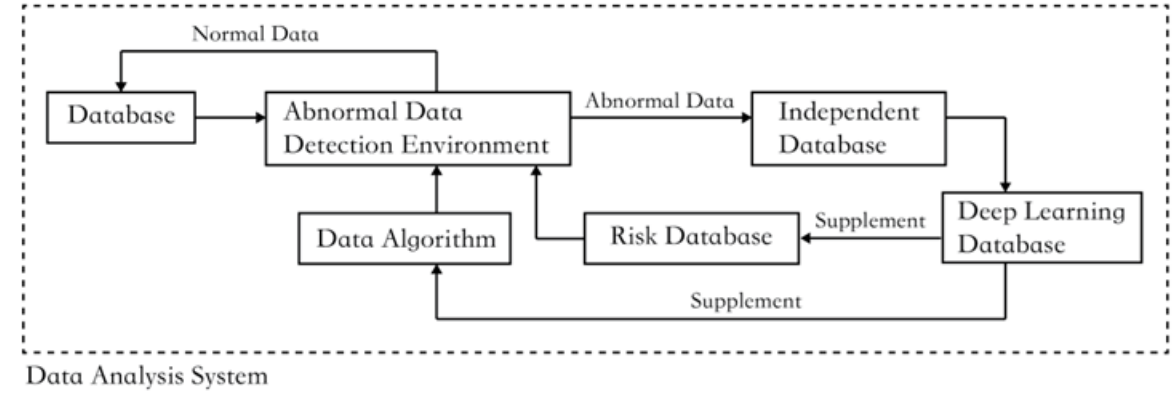

Figure 3. Architecture of data analysis system

The data analysis system module uses deep learning to enhance the detection of suspicious prices related to tax evasion and smuggling. It partners with data storage to choose optimal anomaly detection models and leverages unsupervised deep learning for price risk assessment while interfacing with customs databases for in-depth analysis and verification.

4.4. Design of the data management module

The data management system module is key for improving customs and trade communication, offering both real-time and formal messaging for swift resolutions and announcements (**Figure 4**). It facilitates text, image, and file sharing, with secure data storage and cross-platform accessibility via client interfaces.

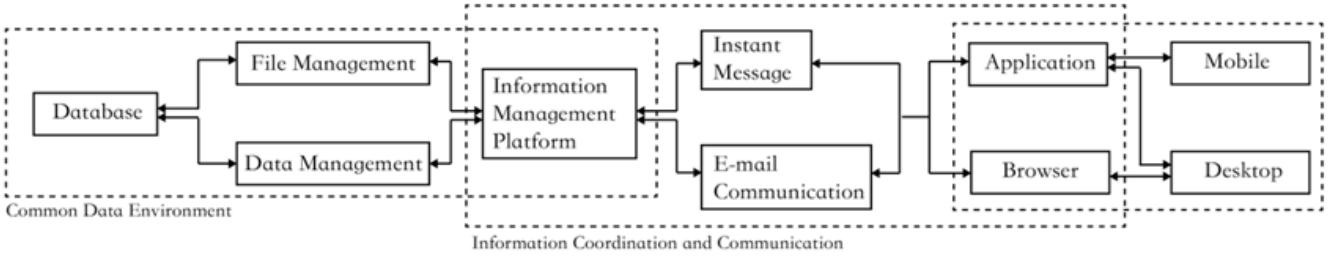

Figure 4. Architecture of data management system

The data management system needs data storage system integration for efficient file handling. It is crucial to include email and instant messaging in the information management system module for operational efficiency. The common data environment provides consistent data access across platforms. Email uses POP3 for storage and

IMAP for server sync to facilitate collaboration. Instant messaging, with its server-mediated transfers, ensures data consistency and aligns with the information management system's server-based approach.

4.5. Integration of different system modules

The article introduces an AI framework for customs risk identification, highlighting the integration of data collection, storage, analysis, and management (**Figure 5**). The study includes B/S and C/S for data gathering, file and database systems for storage, and integrates deep learning and anomaly detection in analysis. The management module handles emails and messaging, all designed to optimize customs risk assessment.

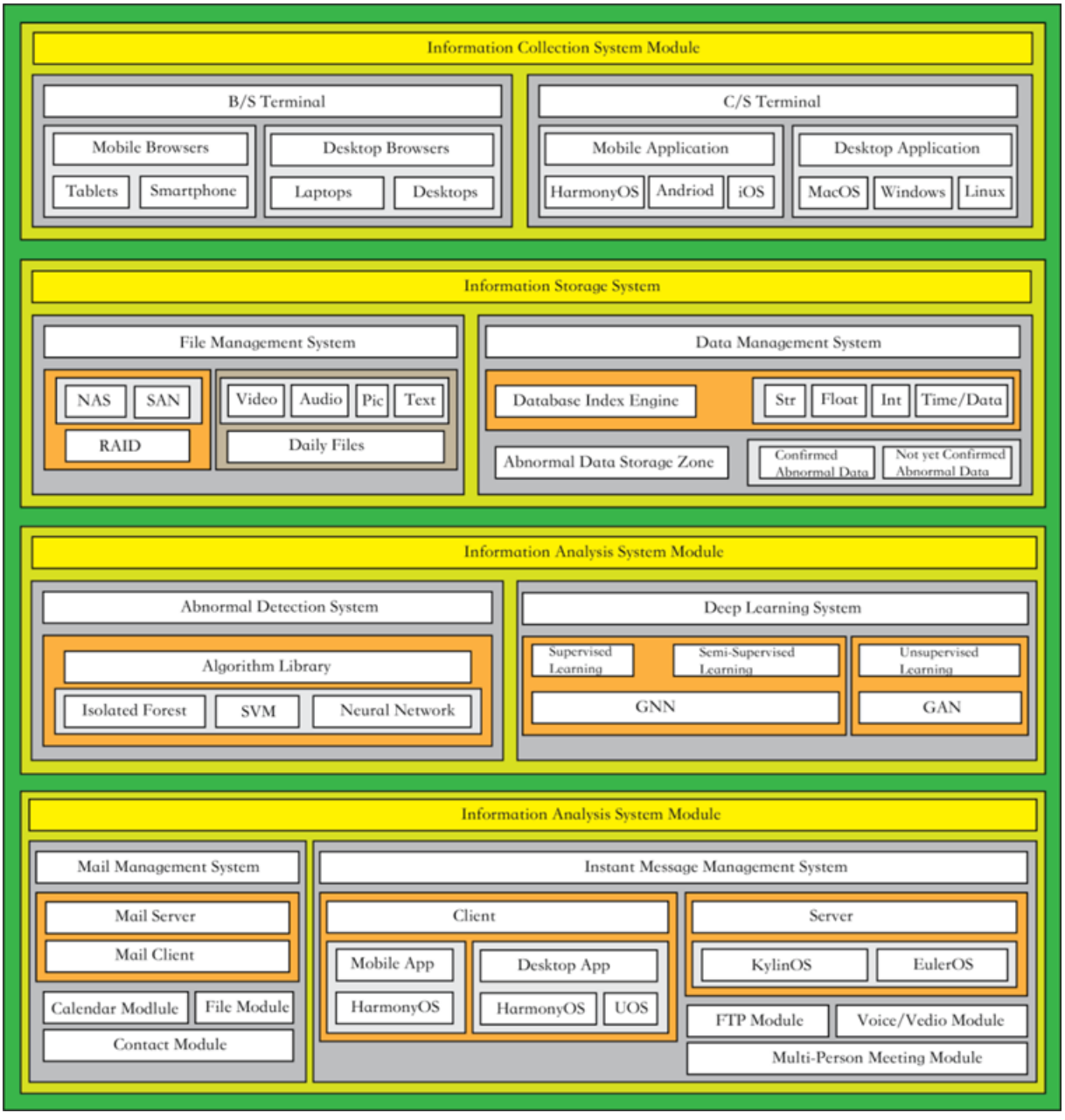

Figure 5. Architecture of the customs inspection system design

5. Validation

This study develops a system architecture for customs inspection management, focusing on enhancing data acquisition, integration, analysis, and dissemination. It outlines a framework with four dimensions—collection, storage, analysis, and management—to ensure information consistency and sharing. The study also proposes research hypotheses to guide the advancement of customs inspection informatization.

Hypothesis 1: The deployment of cross-platform applications is expected to enhance the capability of customs inspections in information collection.

Hypothesis 2: The deployment of applications within a public data environment is expected to enhance the capability of customs inspections in information coordination.

Hypothesis 3: The deployment of an anomaly detection platform leveraging multimodal deep learning is expected to enhance the capability of customs inspections in information analysis.

Hypothesis 4: The deployment of a multi-terminal internal communication platform is expected to enhance the capability of customs inspections in information dissemination.

This research has validated these four hypotheses by using the survey to investigate how strongly custom professionals are accepting the hypothesis. This research uses Python to calculate Cronbach's alpha, KMO value, and Bartlett's Test. The code is as follows.

```
import pandas as pd
import numpy as np
import pingouin as pg
from factor_analyzer import calculate_kmo
from scipy.stats import bartlett
Data = pd.read_excel("data.xlsx")
dataQuestion1 = Data.iloc[:,0]
dataQuestion2 = Data.iloc[:,1]
dataQuestion3 = Data.iloc[:,2]
dataQuestion4 = Data.iloc[:,3]
alpha, ci = pg.cronbach_alpha(data=Data, ci=0.85)
print(alpha)
print(ci)
kmo_all, kmo_model = calculate_kmo(Data)
print("KMO Value:", kmo_model)
npQ1 = np.array(dataQuestion1)
npQ2 = np.array(dataQuestion2)
npQ3 = np.array(dataQuestion3)
npQ4 = np.array(dataQuestion4)
statistic, p_value = bartlett(npQ1, npQ2, npQ3, npQ4)
print(p_value)
```

The collected sample size is 29. Through the calculation, the results are rounded for two decimals, Cronbach's alpha is 0.93, the value of KMO is 0.81, and the *P* value of Bartlett's is 0.95. These results show that the collected

data can be used for analysis. This research has calculated the mean value of each hypothesis score by using Numpy, the codes are as follows.

```
MeanValueQ1 = np.mean(npQ1)
MeanValueQ2 = np.mean(npQ2)
MeanValueQ3 = np.mean(npQ3)
MeanValueQ4 = np.mean(npQ4)
```

The results are 9.31, 9.14, 9.38, and 9.24, which are all strongly accepted. Therefore, all four hypotheses are validated.

6. Findings and discussion

This study introduces a system to enhance customs data management, prioritizing the detection of anomalies through advanced collection and storage (**Table 1**). It highlights the need for strong customs information management to pinpoint import-export risks accurately. The system is built on four capabilities: gathering, coordinating, processing, and transmitting information. It leverages cross-platform development, a shared data environment, and deep learning to broaden data sources, streamline management, and improve anomaly detection, aiming to boost communication and data consistency.

Table 1. System architecture and the enhancement of information management capability

	Cross-platform terminal	CDE	Multi-modal deep learning
Information collection capability	Expand data collection channels.	Centralize the collected import and export data.	N/A
Information coordination capability	Enhance data terminal capabilities.	Implement a unified shared data storage platform.	N/A
Information analysis capability	N/A	The robust data carrier for abnormal data detection and deep learning environments.	Strengthen the ability to identify risks associated with abnormal data.
Information delivery capability	Utilize a variety of methods to enhance the transmission of relevant data and information.	Establish a structured data storage platform for customs inspection.	N/A

This study's architecture boosts efficient and secure customs data management by integrating AI for risk analysis across the entire data lifecycle. It offers a holistic solution for customs inspections, enhancing trade risk management in a globalized world.

7. Research limitation and future research

The study recognizes the need for practical testing of its theoretical framework across China to validate its effectiveness. Its regional sample may not fully represent the national customs system, prompting future research to broaden the scope for a more comprehensive evaluation of the framework in customs inspection management.

Disclosure statement

The author declares no conflict of interest.

References

[1] Xinhua News Agency, 2024, Better Safeguard National Security through Digital Transformation and Intelligent Upgrading — The Person in Charge of the General Administration of Customs Introduces the Overall Situation of the Construction of Smart Customs. https://www.gov.cn/lianbo/bumen/202403/content_6939492.htm

[2] Fan CY, 2024, Research and Application of Key Technologies for Integrated Supervision in Smart Customs. Information Systems Engineering, 2024(5) 47–50. https://doi.org/10.3969/j.issn.1001-2362.2024.05.014

[3] Li J, 2023, Constructing a Model for Smart Customs to Promote the Development of Digital Trade in China. China Business and Market, Vol. 37, No. 5, pp. 94-104, 2023, https://doi.org/10.14089/j.cnki.cn11-3664/f.2023.05.009

[4] Xiao Yu, Le Hui, Jiang Yundan, Qu Kai, Che Xiangdong, and Wu Chen, "Exploration of Digital Twin Application in Smart Customs Logistics Supervision," (in Chinese), China Port Science and Technology, Vol. 5, No. 10, pp. 71-78, 2023, https://doi.org/10.3969/j.issn.1002-4689.2023.10.011

[5] Wang S, Liu QS, Gao Y, 2023, The Implementation Path of Science and Technology Exchange and Cooperation in the Construction of Smart Customs. Science and Technology Vision, 2023(1): 81–84. https://doi.org/10.3969/j.issn.2095-2457.2023.01.020

[6] Cui JG, 2018, Data Intelligence: The Key to Unlocking the Construction of Smart Customs. Journal of Customs and Trade, 39(2): 44–56. https://doi.org/10.3969/j.issn.1674-1765.2018.02.005

[7] Wang JW, 2019, Creating a Smart Customs to Open a New Situation in Border Control. China Inspection and Quarantine, 2019(4): 36–37. https://doi.org/10.3969/j.issn.1002-4689.2019.04.011

[8] Nassif AB, Talib MA, Nasir Q, et al., 2021, Machine Learning for Anomaly Detection: A Systematic Review. IEEE Access, 2021(9): 78658–78700. https://doi.org/10.1109/ACCESS.2021.3083060

[9] Xia X, Pan XZ, Li N, et al., 2022, GAN-based Anomaly Detection: A Review. Neurocomputing, 493(C): 497–535. https://doi.org/https://doi.org/10.1016/j.neucom.2021.12.093

[10] Thudumu S, Branch P, Jin J, et al., 2020, A Comprehensive Survey of Anomaly Detection Techniques for High Dimensional Big Data. Journal of Big Data, 7(1): 42. https://doi.org/10.1186/s40537-020-00320-x

[11] C. Huang, Z. Wu, J. Wen, Y. Xu, Q. Jiang, and Y. Wang, "Abnormal Event Detection Using Deep Contrastive Learning for Intelligent Video Surveillance System. IEEE Transactions on Industrial Informatics, 18(8): 5171–5179. https://doi.org/10.1109/TII.2021.3122801

[12] Zhang L, Li S, Cheng Y, et al., 2024, Learning Dual Updatable Memory Modules for Video Anomaly Detection. Multimedia Systems, 31(1): 3. https://doi.org/10.1007/s00530-024-01597-1

[13] Solaas JRV, Mariconti E, Tuptuk N, 2024, Systematic Literature Review: Anomaly Detection in Connected and Autonomous Vehicles. IEEE Transactions on Intelligent Transportation Systems, 1–16. https://doi.org/10.1109/TITS.2024.3495031

[14] Trilles S, Hammad SS, Iskandaryan D, 2024, Anomaly Detection Based on Artificial Intelligence of Things: A Systematic Literature Mapping. Internet of Things, 2024(25): 101063. https://doi.org/https://doi.org/10.1016/j.iot.2024.101063

[15] Erhan L, Ndubuaku M, Mauro MD, et al., 2021, Smart Anomaly Detection in Sensor Systems: A Multi-Perspective Review. Information Fusion, 2021(67): 64–79. https://doi.org/https://doi.org/10.1016/j.inffus.2020.10.001

[16] Samaila YA, Sebastian P, Sawaran SNS, et al., 2024, Video Anomaly Detection: A Systematic Review of Issues and

Prospects. Neurocomputing, 2024(591): 127726. https://doi.org/https://doi.org/10.1016/j.neucom.2024.127726

[17] Dong S, Xia Y, Peng T, 2021, Network Abnormal Traffic Detection Model Based on Semi-Supervised Deep Reinforcement Learning. IEEE Transactions on Network and Service Management, 18(4): 4197–4212. https://doi.org/10.1109/TNSM.2021.3120804

[18] Dong S, Xia Y, Wang T, 2024, Network Abnormal Traffic Detection Framework Based on Deep Reinforcement Learning. IEEE Wireless Communications, 31(3): 185–193. https://doi.org/10.1109/MWC.011.2200320

[19] Babu JJS, Tanmay T, 2024, Abnormal Event Detection using Convolutional LSTM. 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC), 7–12. https://doi.org/10.1109/AIC61668.2024.10730967

[20] Wang W, 2024, Abnormal Traffic Detection for Internet of Things based on an Improved Residual Network. Physical Communication, 2024(66): 102406. https://doi.org/https://doi.org/10.1016/j.phycom.2024.102406

[21] Sabuhi M, Zhou M, Bezemer CP, Musilek P, 2021, Applications of Generative Adversarial Networks in Anomaly Detection: A Systematic Literature Review. IEEE Access, 2021(9) 161003–161029. https://doi.org/10.1109/ACCESS.2021.3131949