An Overview of Emerging Anomaly Detection Methods and a Research Agenda for Internet of Everything and Industry 5.0 Contexts

Francesco Cauteruccio
Department of Information Engineering (DII)
Polytechnic University of Marche
f.cauteruccio@univpm.it

Enrico Corradini
Department of Information Engineering (DII)
Polytechnic University of Marche
e.corradini@univpm.it

Abstract

In the rapidly evolving contexts of the Internet of Everything (IoE) and Industry 5.0 (I5.0), anomaly detection plays a crucial role. This study focuses on the unique data characteristics of these domains and proposes a taxonomy-oriented overview, together with a comprehensive discussion, of the literature regarding emerging anomaly detection methods in these contexts. Based on the collected contributions, this study also proposes a research agenda centered on the evolution of this research strand. It focuses on different key aspects, such as novel techniques, scalability, robustness, and interpretability, and advocates for further research in this field.

1 Introduction

The advent of the digital age has resulted in transformative advancements such as the Internet of Everything (IoE) and Industry 5.0 (I5.0). IoE extends the IoT by linking people, processes, data, and things for enhanced efficiency. In parallel, Industry 5.0 emphasizes human-machine cooperation, merging human creativity with machine precision. These developments have catalyzed an explosion in data generation, from sensor networks, bioinformatics, smart infrastructure, to e-commerce and social media streams [16, 22]. However, the rapid growth of these technologies has also increased their vulnerability to cyber-attacks and anomalies, necessitating effective anomaly detection mechanisms. Anomaly detection in the IoE and I5.0 is a critical area of research, with significant implications for the security and efficiency of these systems. Anomaly detection in these contexts leverages machine learning approaches, including deep learning frameworks [7], and specific supervised learning models [23, 12]. These approaches have shown promising results in detecting and predicting known and unknown patterns of anomalies. Nevertheless, the problem of anomaly detection results significantly understudied within these two contexts.

This study aims to provide an overview of the current state of anomaly detection in the context of the IoE and I5.0. We will review and analyze various emerging approaches to detect anomalies in these environments. Our goal is to provide a clear understanding of the current methodologies, their strengths and weaknesses, and the challenges that lie ahead in this field. Also, thanks to this overview and the inherent novelty of the contexts, we propose a research agenda that we believe will be useful to all researchers and practitioners interested in contributing in these fields.

The outline of this paper is as follows. In Section 2 we present the literature review protocol we followed in this overview. Then, in Section 3, we present and discuss the collected documents. Afterwards, in Section 4 we propose the research agenda. Finally, in Section 5 we draw our conclusion.

2 Literature Review Protocol

To conduct the investigation of the literature, we resort to the classical Systematic Literature Review (SLR) methodology [15]. The primary aim of SLR is to provide a comprehensive and unbiased assessment of the existing literature by defining and applying a rigorous and reproducible protocol. We follow a (designedly simple) SLR protocol consisting of two stages, namely, *(i)* research questions, digital libraries and research queries, and *(ii)* documents selection and taxonomy definition. The output of this protocol is a set of documents representing the academic literature we conduct our study on. Figure 1 depicts a graphical representation of the protocol.

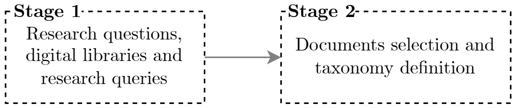
Stage 1
Research questions, digital libraries and research queries
Stage 2
Documents selection and taxonomy definition

Figure 1. The SRL protocol employed in our literature review

We start by defining the motivating research questions. Our study revolves around anomaly detection methods exploited in two contexts, namely, IoE and I5.0; therefore, we focus on two research questions, namely, **(RQ1)** *What are the most studied aspects regarding anomaly detection in the* *contexts of Internet of Everything and Industry 5.0?*, and **(RQ2)** *How a research agenda should be defined to drive future studies on anomaly detection in these contexts?*. We believe our RQs are self-explanatory. In particular, the first one helps defining a bird's-eye view of the usage of anomaly detection in these context, while the second one lays the foundations for how this research strand should evolve.

Then, we proceed with the selection of the digital libraries to use. Here, we decide to search for scholarly literature published since 2010 and written in English. The digital library of choice is Scopus[1]. We choose Scopus because it indexes several other repositories, such as ACM Digital Library and others, and it tends to consider only reliable sources and avoid not peer-reviewed documents.

Finally, the last objective of this stage is to define the research query to apply on the digital library of choice. The research query we use is reported below in the syntax of the Scopus digital library:

```
TITLE-ABS-KEY ( ("anomaly detection" OR "anomaly")
AND ( "industry 5.0" OR "internet of everything"
OR "I5.0" OR "ioe" ) ) AND PUBYEAR > 2009
```

The application of the research query on Scopus reported a list containing a total number of 27 documents. Given the compact number of documents, we manually checked whether each of them correctly addressed the topics of our concerns, e.g., anomaly detection, I5.0 and IoE. Among these, 21 documents were selected. To organize the documents, and the consequently analysis of them, we defined a taxonomy, i.e., a categorization of the collected contributions in several aspects, which is reported in Table 1. In our opinion, the selected aspects are useful to effectively drive an overview on anomaly detection methods in the two contexts.

3 Anomaly Detection for IoE and I5.0

The advent of the IoE and I5.0 has brought about a paradigm shift in how we perceive and interact with the world around us. These advanced systems, characterized by the integration of physical and digital components, have the potential to revolutionize various sectors, from manufacturing to healthcare, transportation, and beyond. In this section, we present an overview of the documents collected in our investigation.

3.1 Anomaly Detection Techniques

Anomaly detection techniques form the backbone of many systems designed to ensure the security and efficiency of IoE and I5.0. These techniques often leverage advanced machine learning and artificial intelligence algorithms to identify patterns and behaviors that deviate from the norm. Different approaches in anomaly detection have been proposed in the past, which include:

- In [18], the authors develop a *feedback- and voting-based anomaly imputation technique* that improves IoE data availability by imputing anomalous sensor data. They propose a feedback- and voting-based feature selection method that extracts crucial features from raw datasets using mini-batch data, achieving an accuracy up to 94.88% and 97.96%.
- The authors of [1] propose a *method for detecting network traffic anomalies* based on the use of a number of statistical, correlation, and informational parameters of network traffic as additional features.
- The research described in [19] proposes a new *anomaly detection algorithm that combines time-frequency domain analysis and artificial intelligence technology*, showing high accuracy of 98.12
- In [14], the authors propose *APAD, an autoencoder-based payload anomaly detection method for industrial IoE*, showing a higher detection rate compared with other methods.
- [7] introduces a *new generic deep learning (DL) framework for anomaly detection in the IoE*, combining decomposition methods, deep neural networks, and evolutionary computation to detect outliers effectively.
- [9] presents *PredictDeep, a novel security analytics framework for anomaly detection and prediction*, leveraging log data with graph analytics and deep learning techniques. In the context of intrusion detection systems (IDS), the authors of
- [28] propose an *intrusion detection system for IoT based on an improved Back Propagation (BP) neural network*, designed to improve the security of IoT networks.
- Another example can be found in [17] where an *effective intrusion detection method based on pruning deep neural networks* is proposed, achieving a detection rate of 0.9904 for known attacks and 0.1050 for unknown attacks.

These varied approaches to anomaly detection underscore the complexity and multifaceted nature of the challenge, each addressing different aspects of the problem and offering unique solutions.

3.2 Applications of Anomaly Detection

The applications of anomaly detection in IoE and I5.0 are different. From smart homes to fire prediction in indoor parking lots, anomaly detection techniques are being used to improve safety, efficiency, and overall performance.

For example, in [13], the authors propose a technology for predicting the degree of fire anomaly by machine learning using the air quality sensor of the indoor parking lot. The paper uses an autoencoder-based anomaly detection method for fire prediction, predicting a high risk of fire when the collected data exceeds the threshold. This approach demonstrates the potential of anomaly detection in ensuring safety in indoor environments. The authors of [25] provides a comprehensive review of how bridge information modeling, finite element modeling, and bridge health monitoring are integrated to create digital twins of bridges. These digital models can generate damage scenarios that can be used by anomaly detection algorithms for damage detection on bridges, particularly those with cultural heritage value. In [8], the authors explain the use of vibration data to monitor and detect anomalies in machinery and equipment in the context of I5.0. The paper uses a correlation coefficient model

[1] https://www.scopus.com

Table 1. Summary of the presented taxonomies

Property	*Description*	*Papers*
Anomaly Detection Techniques	Strategies using advanced algorithms to spot deviations in data patterns within systems like the Internet of Everything and Industry 5.0, improving their security and reliability.	[18, 1, 19, 14, 7, 9, 28, 17]
Applications of Anomaly Detection	Anomaly detection techniques are applied across sectors like energy, safety, logistics, healthcare, and manufacturing, enhancing efficiency and performance by identifying unusual data patterns.	[13, 27, 21, 8, 5, 25]
Efficiency and Prediction in Industry 5.0	Supervised machine learning and anomaly detection play key roles in enhancing efficiency, predicting climate patterns, and improving machine performance.	[23, 26, 2]
Data Analysis and Anomaly Detection	Advanced machine learning algorithms to analyze data, identify patterns, and predict trends, thus enhancing the capabilities of intrusion detection systems and improving system security.	[12, 20]
Network Structures and Anomalies	Anomalies in network structures and the security in edge computing are crucial in the IoE and Industry 5.0 landscape, shedding light on the challenges and solutions to ensure system stability and security.	[24, 29]

and an LSTM-autoencoder (long short-term memory) model to enhance the accuracy of the anomaly detection process in a vertical carousel storage and retrieval system (VCSRS). The combination of these models resulted in an accuracy rate of 97.70% for detecting anomalies. The authors of [5] proposes a novel Internet of Things (IoT)-based and cloud-assisted monitoring architecture for smart manufacturing systems to evaluate their overall status and detect eventual anomalies occurring into the production. The proposed solution is a five-layer scalable and modular platform in I5.0 perspective that embeds a novel anomaly detection solution, designed by leveraging control charts, autoencoders (AE) long short-term memory (LSTM) and Fuzzy Inference System (FIS). The proposed architecture provides to human operators information about anomalous events, where they occur, and crucial information about their risk levels. The research presented in [27] proposes a cyber-physical platform framework applying the IoE and Digital Twin (DT) technologies to promote information integration and provide smart services for different stakeholders in the cold chain logistics (CCL). The platform uses deep learning techniques for accident identification and indoor localization based on Bluetooth Low Energy (BLE) to actualize real-time staff safety supervision. The platform also enables paperless operation for shipment, remote temperature and humidity (T&H) monitoring, anomaly detection and warning, and customer interaction. Finally, the authors of [21] discuss the importance of robust systems that act as a bridge between different sensors and systems to facilitate knowledge sharing and empower their detection and prediction capabilities in healthcare monitoring and ambient assisted living technology. The paper highlights the potential of cloud-based platforms in providing services for input sensors, IoE devices and processes, and context providers all at the same time. These platforms aim to bridge the gap between symptoms and diagnosis trend data in order to predict health anomalies accurately and quickly.

3.3 Efficiency and Prediction in I5.0

Efficiency and prediction in I5.0 are closely tied to anomaly detection. Research in this area has focused on using supervised machine learning and anomaly detection for efficiency prediction. For instance, in [23], the authors study the use of Multivariate Linear regression of supervised machine learning to predict the efficiency of I5.0. The efficiency of the model is dependent on various factors such as security protocols, Industrial IoT performance, connectivity, reachability, and availability. The authors propose to improve the efficiency of the model by updating these components and the use of Quorum blockchain to implement ultimate security in I5.0. The authors of [26] explores the use of device-free sensing (DFS) and neural networks in climate change detection. The authors construct a deep classification system for the convolutional neural network and demonstrate the benefits of deep learning in addressing the problems of climate patterns. The neural network algorithm accurately forecasts an increase and drop in temperature throughout the next ten years by generating explicit depictions using the month-to-month temperature records of 30 years. In [2], the authors depict a digital triplet which discloses the potency of retrofitting a conventional drilling machine. The digital triplet D3 encompasses intelligent activities based on human awareness and the convergence among cyberspace, physical space, and humans. The performance parameters of the digital triplet D3 paradigm for retrofitting were eventually confirmed through appraising, anomaly analysis, and real-time monitoring.

3.4 Data Analysis and Anomaly Detection

Data analysis is a critical aspect of anomaly detection in IoE and I5.0. It involves the use of advanced machine learning algorithms and models to analyze and interpret data, identify patterns, and predict future trends. The research described in [12] provides a comprehensive and structured study of various research works based on the Australian Defence Force Academy Linux Dataset (ADFA-LD) for host-based anomaly detection. The ADFA-LD comprises thousands of normal and attack processes system call traces for the Linux platform and is the benchmark dataset used for dynamic approach-based anomaly detection. The paper presents a comparative analysis of different machine learning methods for anomaly detection in Linux host systems, highlighting the potential of machine learning in enhancing the capabilities of intrusion detection systems. In [20], the authors propose a novel approach to atmospheric environmental health monitoring. They leverage the power of spatial Bayesian networks to design a multi-functional, low measurement error, low power consumption, and low-cost atmospheric environment monitoring system. The system is designed to address key atmospheric environment indicators such as temperature, humidity, carbon monoxide concentration, and suspended particle concentration. The authors also propose an improved spatial Bayesian network model and a system model that combines anomaly detection with other detection mechanisms to significantly improve the accuracy of detection and reduce the false alarm rate.

3.5 Network Structures and Anomalies

Anomalies in network structures can have significant impacts on the performance and security of IoE and I5.0 systems. Research in this area has proposed classifications of anomalies in relation to the states of particular nodes in the network structure and the impact of these anomalies on phase transitions in the network structures. For instance, in [24], the authors discuss the occurrence of anomalies affecting the process of phase transitions in network structures, particularly in IT networks, IoT, and IoE. They propose a classification of anomalies in relation to the states of particular nodes in the network structure, including homogeneous, heterogeneous, individual, and cyclic disorders. The results of their tests and simulations show the impact of these anomalies on phase transitions in network structures. The authors of [29] review the current research status of edge computing security with a focus on IoE and industrial contexts. They analyze the security challenges of edge computing in new models, new application scenarios, and new technology environments, pointing out the security problems in five aspects: access control, key management, privacy protection, attack mitigation, and anomaly detection. The authors discuss the research achievements of the academic community in these areas and analyze their advantages and disadvantages, along with future development direction.

3.6 Final remarks

In conclusion, the field of anomaly detection in the context of the Internet of Everything (IoE) and I5.0 is rapidly evolving, with advancements in machine learning and artificial intelligence playing a pivotal role. These technologies are being leveraged to develop sophisticated models and algorithms capable of identifying deviations from expected behavior, which could signify potential threats or inefficiencies.

In the face of these challenges, the importance of continued research and development in this field cannot be overstated. As we move further into the era of IoE and I5.0, the role of anomaly detection in ensuring the security, efficiency, and overall success of these systems will only become more critical.

4 Research Agenda

In this section, we outline a research agenda, based on the conducted overview, to address the challenges and advance the state-of-the-art in anomaly detection within the IoE and I5.0 domains. We selected four key aspects to focus our research agenda on, namely, *(i)* novel algorithms and techniques, *(ii)* scalability and efficiency, *(iii)* robustness and adaptability, and *(iv)* intepretability and explainability. We describe these aspects in the following.

4.1 Novel Algorithms and Techniques

Data in IoE and I5.0 contexts have unique characteristics, such as heterogeneity of data sources, high volume, velocity, and variety of data, and real-time processing requirements. Therefore, innovative algorithms and techniques specifically tailored for anomaly detection should consider these unique characteristics. Several examples, based on recent research, can be identified as novel approaches paving the way towards IoE and I5.0 contexts.

A first example is the usage of vector databases [6]. Vector databases, also known as vectorized databases or vector storage, are a type of database technology specifically designed to store and manage vector data efficiently. In contrast to traditional relational databases that primarily handle structured data, vector databases excel in handling unstructured, high-dimensional, and spatial data. Vector databases are optimized to store vectors, which represent objects or entities in a multi-dimensional space. Each vector consists of a set of numerical values or attributes that define its position or characteristics in the space. Examples of vector data include geographic coordinates, image features, text embeddings, or sensor readings. In turn, they offer valuable capabilities for anomaly detection in both I5.0 and IoE. These databases excel at efficiently storing and querying high-dimensional data, making them well-suited for managing complex systems and large-scale sensor networks. In particular, vector databases can store sensor readings as vectors and enable similarity-based searches to identify anomalies in real time or through retrospective analysis. They support the continuous monitoring of sensor data, enabling prompt detection of abnormal behaviors and proactive intervention to prevent issues. Diverse and voluminous data generated by interconnected devices and sensors can be easily handled, making these contexts the perfect use case for such technology.

Another interesting example is the usage of Large Language Models (LLMs) as a tool for decision support in the context of I5.0 and IoE [30]. In fact, LLMs can contribute to decision support by analyzing large volumes of structured and unstructured data within I5.0 and IoE systems. They can assist in predictive maintenance by identifying patterns in historical data that precede equipment failures or anomalies, enabling optimized maintenance schedules and improved operational efficiency. Furthermore, LLMs can enhance natural language understanding and generation, facilitating effective human-computer interaction. They can interpret user queries or commands, generate contextual responses, and provide real-time assistance, improving the user experience. Imagine a human operator in a smart factory dealing with the process of creating daily-basis report of anomalous data. By exploiting a LLM continuously trained on the smart factory data, such process could be conducted easily and in a semi-automatic way.

4.2 Scalability and Efficiency

Anomaly detection systems are generally deployed either in a centralized or distributed way. In the former case, several constraints are normally present such as latency reduction and bandwidth requirements associated with transmitting data. In the latter case, instead, parallel computing approaches are investigated to enable efficient processing and analysis of data across distributed edge, fog and cloud computing infrastructures.

Although the research on these contexts is growing substantially, there are different ways forward that, in our opinion, could be considered. An example is represented by the strand of research on succinct data structures (SDS) [10]. SDS are data structures that offer efficient and compact representations of large-scale data, enabling faster query processing and reduced storage requirements. Let us consider a typical IoE context. Here, vast amounts of data are generated by interconnected devices and sensors. These data often represent sensor readings, event logs, network traffic data, etc. By compressing the data into concise representations, these structures allow for different tasks, such as nearest neighbor queries, that are commonly used in processes of infrastructure monitoring. SDS could also facilitate the processing of historical data for retrospective anomaly detection, as they enable efficient compression and indexing of large datasets, supporting timely analysis and pattern recognition.

4.3 Robustness and Adaptability

Dynamic environments such as the one within IoE and I5.0 contexts are definitely dynamics. Therefore, anomaly detection methods should be able to tackle different challenges, such as concept drift, where the statistical properties of normal and anomalous data change. To this end, novel anomaly detection methods should be designed by taking into account aspects like robustness and adaptability. Robustness refers to the ability of an anomaly detection system to function in the face of various adversarial conditions accurately and reliably. In our studied contexts, robustness implies that the system can handle and detect anomalies effectively, even in the presence of noise, uncertainties, or unexpected changes in data patterns. A robust system should be resilient to outliers, data irregularities, and fluctuations, ensuring that genuine anomalies are detected while minimizing false positives. Adaptability refers to the capacity of an anomaly detection system to learn and evolve in response to dynamic conditions and new challenges. In the IoE and I5.0, adaptability implies that the system can adjust its detection models, algorithms, or thresholds to accommodate changes in the data patterns, system configurations, or operational requirements. An adaptable system should be able to automatically update and refine its anomaly detection capabilities based on incoming data, continuously improving its accuracy and reliability.

Online learning and incremental learning techniques are currently paving the way to design anomaly detection methods able to tackle these challenges [11]. Incremental learning algorithms are well-suited for real-world applications where data arrives incrementally, making it impractical to construct new models for each data point. Limited memory and processing power in most systems necessitate the use of algorithms that operate with constant resources. Instead of building new models from scratch, incremental learning updates the existing model as new data arrives, ensuring accuracy and adaptability while minimizing resource requirements. Although online and incremental learning represent consolidated techniques, there are still to little no studies exploiting them in I5.0 and IoE contexts. This is somewhat unsurprising, considering that IoE and I5.0 represent emerging domains that have only recently gained attention within the academic sphere, with limited prior research or scholarly investigation. Also, both these contexts generally encompass dynamic and heterogeneous environments, whose data exhibit high degree of complexity, thus calling out for more peculiar approaches such as multimodal learning [4].

4.4 Interpretability and Explainability

Interpretability and explainability are essential in artificial intelligence (AI) as they foster trust, accountability, and regulatory compliance [3]. Interpretability enables understanding of AI models' decision-making processes, helping to validate, interpret, and identify biases or ethical concerns. Explainability goes further, providing human-understandable explanations that build user trust and acceptance. Indeed, these are also crucial in the context of anomaly detection as they enhance trust, understanding, and decision-making in systems. Interpreting and explaining how these systems identify anomalies helps validate their outputs and provides insights into the factors influencing the detection process. By understanding the underlying reasoning, users can uncover potential biases and assess system performance. Additionally, interpretability and explainability, especially from a user experience point of view, enable the generation of human-understandable explanations for detected anomalies, including the identification of key contributing factors and casual relationships.

There are numerous examples in industrial scenarios that can benefit from these aspects. For instance, suppose an anomaly detection algorithm identifies a sudden increase in energy consumption of a specific machine. Interpretability allows the users, such as engineers or operators, to understand why the anomaly was flagged by revealing the contributing factors or features that led to the detection. This could be due to a malfunctioning component, improper calibration, or changes in the production process. By enabling users to comprehend the reasons behind anomaly detection and providing actionable explanations, interpretability and explainability empower them to make informed decisions, take corrective actions promptly, and maintain the efficiency and reliability of I5.0 systems.

5 Conclusion

In this study, we delved into an overview of emerging anomaly detection methods in two peculiar and novel contexts, namely Internet of Everything and Industry 5.0. In particular, we conducted an investigation of the literature about anomaly detection in these contexts and we posed two research questions to drive our study. Our contribution is twofold: firstly, we proposed and discussed a survey of recent research organized according to a defined taxonomy; secondly, we designed and introduced a research agenda whose scope is to drive future steps in this research strand. Given the novelty of the two studied contexts, and the paramount importance of the general task of anomaly detection, we believe this study could be helpful for all researchers and practitioners working in these fields.

6 References

[1] D. Ageyev, T. Radivilova, O. Mulesa, O. Bondarenko, and O. Mohammed. Traffic monitoring and abnormality detection methods for decentralized distributed networks. In *Information Security Technologies in the Decentralized Distributed Networks*, pages 287–305. Springer, 2022.

[2] H. Alimam, G. Mazzuto, M. Ortenzi, F. E. Ciarapica, and M. Bevilacqua. Intelligent retrofitting paradigm for conventional machines towards the digital triplet hierarchy. *Sustainability*, 15(2):1441, 2023.

[3] A. B. Arrieta, N. Díaz-Rodríguez, J. D. Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins, R. Chatila, and F. Herrera. Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai. *Information fusion*, 58:82–115, 2020.

[4] P. Blikstein. Multimodal learning analytics. In *Proceedings of the third international conference on learning analytics and knowledge*, pages 102–106, 2013.

[5] B. Caiazzo, T. Murino, A. Petrillo, G. Piccirillo, and S. Santini. An iot-based and cloud-assisted ai-driven monitoring platform for smart manufacturing: design architecture and experimental validation. *Journal of Manufacturing Technology Management*, 34(4):507–534, 2023.

[6] Q. Chen, B. Zhao, H. Wang, M. Li, C. Liu, Z. Li, M. Yang, and J. Wang. Spann: Highly-efficient billion-scale approximate nearest neighborhood search. *Advances in Neural Information Processing Systems*, 34:5199–5212, 2021.

[7] Y. Djenouri, D. Djenouri, A. Belhadi, G. Srivastava, and J. C. Lin. Emergent deep learning for anomaly detection in internet of everything. *IEEE Internet of Things Journal*, 2021.

[8] J. S. Do, A. B. Kareem, and J. W. Hur. Lstm-autoencoder for vibration anomaly detection in vertical carousel storage and retrieval system (vcsrs). *Sensors*, 23(2):1009, 2023.

[9] M. A. Elsayed and M. Zulkernine. Predictdeep: security analytics as a service for anomaly detection and prediction. *IEEE Access*, 8:45184–45197, 2020.

[10] S. Gog and M. Petri. Optimized succinct data structures for massive data. *Software: Practice and Experience*, 44(11):1287–1314, 2014.

[11] S. C. Hoi, D. Sahoo, J. Lu, and P. Zhao. Online learning: A comprehensive survey. *Neurocomputing*, 459:249–289, 2021.

[12] P. Khandelwal, P. Likhar, and R. S. Yadav. Machine learning methods leveraging adfa-ld dataset for anomaly detection in linux host systems. In *2022 2nd International Conference on Intelligent Technologies (CONIT)*, pages 1–8. IEEE, 2022.

[13] E. J. Kim, W. You, and C. S. Pyo. A study on fire prediction method using air quality measurement sensors of smart indoor parking lot. In *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1134–1136. IEEE, 2021.

[14] S. Kim, W. Jo, and T. Shon. Apad: Autoencoder-based payload anomaly detection for industrial ioe. *Applied Soft Computing*, 88:106017, 2020.

[15] B. Kitchenham. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.

[16] P. Kohli, S. Sharma, and P. Matta. Secured privacy preserving techniques analysis of 6g driven vehicular communication network in industry 5.0 internet-of-everything (ioe) applications. In *2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, pages 1–8. IEEE, 2022.

[17] M. Lei, X. Li, B. Cai, Y. Li, L. Liu, and W. Kong. P-dnn: an effective intrusion detection method based on pruning deep neural network. In *2020 International Joint Conference on Neural Networks (IJCNN)*, pages 1–9. IEEE, 2020.

[18] L. Li, H. Wang, Y. Wang, M. Chen, and T. Wei. Improving iot data availability via feedback-and voting-based anomaly imputation. *Future Generation Computer Systems*, 135:194–204, 2022.

[19] T. Liu, Y. Zhu, H. Wang, B. Balamurugan, P. Vijayakumar, and J. Peng. Transformer anomaly detection based on time-frequency domain software-hardware cooperative analysis. *Transactions on Emerging Telecommunications Technologies*, 33(3):e3865, 2022.

[20] X. Lu, J. Chu, and W. Zhu. Design of atmospheric environmental health monitoring system based on spatial bayesian network. In *Journal of Physics: Conference Series*, volume 2066(1), page 012028. IOP Publishing, 2021.

[21] A. Manashty and J. L. Thompson. Cloud platforms for ioe healthcare context awareness and knowledge sharing. In *Beyond the Internet of Things: Everything Interconnected*, pages 303–322. Springer, 2017.

[22] V. Özdemir and N. Hekim. Birth of industry 5.0: Making sense of big data with artificial intelligence,"the internet of things" and next-generation technology policy. *Omics: a journal of integrative biology*, 22(1):65–76, 2018.

[23] P. Pant, A. S. Rajawat, S. B. Goyal, D. Singh, N. B. Constantin, M. S. Raboaca, and C. Verma. Using machine learning for industry 5.0 efficiency prediction based on security and proposing models to enhance efficiency. In *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pages 909–914. IEEE, 2022.

[24] A. Paszkiewicz. Modeling and analysis of anomalies in the network infrastructure based on the potts model. *Entropy*, 23(8):949, 2021.

[25] A. J. Rios, V. Plevris, and M. Nogal. Bridge management through digital twin-based anomaly detection systems: A systematic review. *Frontiers in Built Environment*, 9:61, 2023.

[26] P. Singh, D. Sammanit, R. N. Shaw, and A. Ghosh. Comprehension of climate change with iot-enabled cnn. In *Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022*, pages 385–394. Springer, 2022.

[27] W. Wu, L. Shen, Z. Zhao, A. R. Harish, R. Y. Zhong, and G. Q. Huang. Internet of everything and digital twin enabled service platform for cold chain logistics. *Journal of Industrial Information Integration*, 33:100443, 2023.

[28] A. Yang, Y. Zhuansun, C. Liu, J. Li, and C. Zhang. Design of intrusion detection system for internet of things based on improved bp neural network. *Ieee Access*, 7:106043–106052, 2019.

[29] H. Zeyu, X. Geming, W. Zhaohang, and Y. Sen. Survey on edge computing security. In *2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, pages 96–105. IEEE, 2020.

[30] W. X. Zhao, K. Zhou, J. Li, T. Tang, X. Wang, Y. Hou, Y. Min, B. Zhang, J. Zhang, Z. Dong, Y. Du, C. Yang, Y. Chen, Z. Chen, J. Jiang, R. Ren, Y. Li, X. Tang, Z. Liu, P. L. J.-Y. Nie, and J.-R. Wen. A survey of large language models. *arXiv preprint arXiv:2303.18223*, 2023.