

Anomaly Detection in Time Series Data: Comprehensive Survey of Machine Learning and Deep Learning Approaches

Mahesh V Korade¹, Omkar Pattnaik² and Umesh B Pawar³

¹Research Scholar, Department of CSE, Sandip University, Nashik, India

Email: korademaheshv@gmail.com

²⁻³Associate Professor, Department of CSE, Sandip University Nashik, India

Email: omkar.pattnaik@sandipuniversity.edu.in, umesh.pawar@sandipuniversity.edu.in

Abstract—Anomaly detection in time series data is a crucial task with wide-ranging applications in finance, healthcare, manufacturing, and cybersecurity. Detecting unusual patterns or behaviors in data streams is essential for ensuring system reliability, security, and efficiency. This paper presents a comprehensive survey of machine learning (ML) and deep learning (DL) techniques for anomaly detection in time series data. By examining state-of-the-art algorithms, our research aims to enhance the accuracy, robustness, and scalability of anomaly detection systems. We systematically review the strengths and limitations of existing methods, propose innovative approaches, and validate their performance through extensive experiments on various datasets. The findings from this study are anticipated to push anomaly detection forward, providing real-world solutions for tackling challenges in different fields and directing future research efforts.

Index Terms— Anomaly detection, unsupervised learning, autoencoders, deep learning, machine learning.

I. INTRODUCTION

The Earth continuously generates signals like temperature, wind speed, rainfall, and sunspot activity, which have been recorded to understand our environment. Industrial sectors such as business, finance, biomedicine, and manufacturing also collect extensive data to improve operations, and Industry 4.0 has increased sensor use for real-time monitoring to enhance efficiency, safety, and security [1]. Time-series data, organized sequentially, is crucial in medicine, meteorology, and economics for analyzing historical patterns and predicting future trends, with tasks like classification, clustering, prediction, and anomaly detection being essential for extracting insights. Anomaly detection, which identifies significant deviations from the norm, is critical in various applications, and traditional techniques like linear models [2], distance-based approaches [3], density-based strategies [4], and support vector machines [5] remain effective. Despite the challenges of detecting anomalies in time-series data due to the need to consider sequential order and causal relationships, deep learning has gained attention for capturing complex patterns without relying on preconceived notions, making it effective for modern time-series analysis [6-7].

A. Anomaly

Numerous efforts have been made to define anomalous data, often referred to as statistical outliers. In [8] anomaly is defined as “a node lies outside its surrounding contexts”. When applied to time-series data, anomalies can be described as data points at certain time steps that exhibit behaviours noticeably different from those observed in preceding time steps.

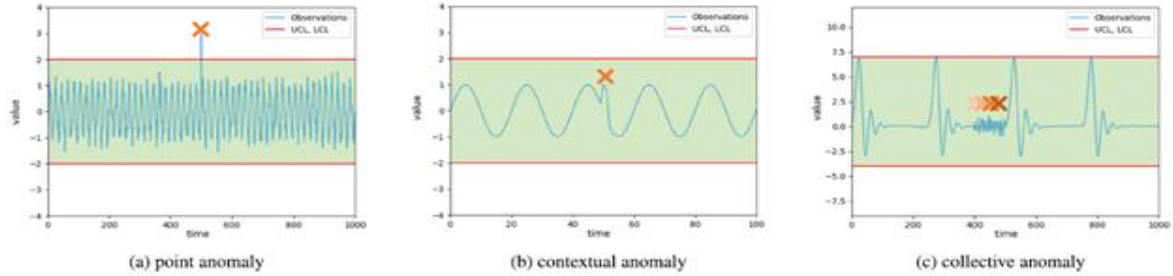


Figure I: Types of Anomalies

As per the previous literature, we classify anomalies in time-series data into distinct categories as below [1].

Point Anomaly: A single data point falls outside the control limits set by historical data (Fig I(a)).

Contextual Anomaly: Data points within control limits deviate from expected patterns in a short time frame, making them hard to detect Fig I(b)).

Collective Anomaly: Over a long period, a sequence of data points deviates from the expected pattern. Individual points might not seem anomalous, but the sequence is suspicious (Fig I(c)).

Other Anomalies: Anomalies outside the normal state include patterns like Normal, Missing, Outlier, Minor, Square, Trend, and Drift.

B. Time Series Data

The systems which are time dependent are subject to complete tasks periodically. Time is an important factor that requires a lot of consideration. To identify the anomalies, it is essential to understand the properties of time series data. The properties are Time Dependency, Dimensionality, Nonstationary and Noise.

In this paper a comprehensive survey on anomaly detection within time-series data using machine and deep learning approaches is done. We analyze the state of art systems and provide comparative analysis with future directions. The survey starts by defining anomalies and subsequently examines various sources and methodologies aligned with these definitions. The rest of the paper is organized as section II Provides background of anomaly detection. In Section III a deep literature survey is studied. Section IV discusses the limitations of existing systems and section V concludes the paper with future directions.

II. LITERATURE SURVEY

Miller et al. [9] reviewed methods to improve sustainability in non-residential buildings using unsupervised statistical learning, covering clustering, anomaly detection, motif and discord detection, rule extraction, and visual analytics, along with technologies like smart meters and control optimization. Fan et al. [10] presented a method using autoencoder architectures to identify energy consumption anomalies, showing that AEs effectively detect anomalies and reduce data preprocessing. Tasfi et al. [11] developed a deep semi-supervised CNN with confidence sampling to detect anomalies in HVAC, lighting, and heat pump electricity use, using two networks for handling labeled and unlabeled data and validating with real data.

Kravchik and Shabtai [12] investigated the use of Long Short-Term Memory (LSTM) networks and one-dimensional Convolutional Neural Networks (1D-CNNs) for anomaly detection in Industrial Control Systems (ICS). They introduced new features that capture the relationships between current and past data values. Their experiments demonstrated that 1D-CNNs not only outperformed LSTMs in terms of detection accuracy but also required less training time. Building on this, Shalyga et al. [13] developed an architecture for automatic optimization using Genetic Algorithms (GA), which evaluated Dense Neural Networks (DNNs), 1D-CNNs, and LSTMs. In a different approach, Zizzo et al. [14] designed an Intrusion Detection System (IDS) based on LSTM networks. They employed the Cumulative Sum (CUSUM) method to detect anomalies by comparing the residual error between the model's predictions and the ground truth. Li et al. [15] proposed a Generative Adversarial Network-based Anomaly Detection (GAN-AD) method for ICS, incorporating an LSTM network within the

GAN-AD to model the normal distribution of multivariate time series data from sensors and actuators. Similarly, Kim et al. [16] presented a Sequence-to-Sequence LSTM network for anomaly detection, which was trained on data representing normal conditions and utilized attention mechanisms to enhance detection accuracy.

In addition to LSTM and CNN-based solutions, various other deep learning and machine learning techniques have been employed to detect anomalies in ICS. Grammatikis et al. [17] developed an anomaly detection (AD) system tailored for the IEC 60870-5-104 protocol, commonly used in industrial environments. Their system analyzed network traffic and applied whitelist filters for legitimate MAC and IP addresses, followed by flow feature extraction evaluated by three different machine learning models: One-Class Support Vector Machine (OC-SVM), Local Outlier Factor (LOF), and Isolation Forest (IF), with the IF model achieving the highest F1-score. Khraisat et al. [18] introduced a Hybrid Intrusion Detection System (HIDS) that combines a C5 Decision Tree (C5 DT) classifier and an OC-SVM. This ensemble approach first applies the C5 DT classifier to determine if a sample matches known attack signatures, raising an alarm if it does. If no match is found, the OC-SVM further evaluates the sample for anomaly detection.

The study in [19] explores graph-based methods combined with deep learning for anomaly detection, highlighting challenges such as defining training objectives, interpreting anomalies, managing training costs, and tuning hyper parameters, particularly in unsupervised learning scenarios. The review in [20] categorizes anomaly detection techniques into seven groups, including classification, statistical distribution, graph-based, nearest neighbor, information theoretic, clustering, and spectral methods, offering a broad overview. The survey in [21] examines various deep learning methods for detecting anomalies in time series data, emphasizing the role of graph structures and the challenges faced by basic GNNs in dynamic graphs. In [22], the focus is on security and anomaly detection in Space Information Networks (SINs), proposing the use of a cybersecurity knowledge graph and GCN for data encoding. The research in [23] investigates LSTM models for anomaly detection across various domains, discussing their ability to handle multivariate time series data and adapt to changing system behaviors, and suggests integrating graph-based methods with LSTMs to improve contextual anomaly detection. The study in [24] addresses anomaly detection in IoT networks using SS-VTCN, advocating for a hybrid semi-supervised approach due to the challenge of limited labeled datasets and the prevalence of anomalous data. In [25], the focus is on enhancing trustworthiness, energy efficiency, computational efficiency and explainability in anomaly detection within the IIoT, proposing a strategy that used autoencoder and VAE for feature extraction which balances energy efficiency with accuracy and standardizes data using SKLearn. Lastly, [26] uses the K-means algorithm to evaluate anomaly detection within a simulated smart home network, examining performance metrics such as true positive rate and the impact of varying cluster sizes and initialization criteria.

In [27], an autoencoder was used for anomaly detection by learning the typical data signature from a single sensor and flagging significant deviations as anomalies. In contrast, [28] employed both LSTM and Gelerbe networks (random neural networks) to detect anomalies by identifying deviations from normal operational states. Study [41] focused on detecting SYN attacks in IoT networks using regression to predict half-open TCP ports, flagging significant deviations as anomalies. In [29], various ML techniques, including Gaussian regression and SVM, were used to generate Process Structure Integrity Graphs (PSIGs) from IoT device ELF files for anomaly detection, but without considering inter-device connections. In [30], an autoencoder was selected for its robustness against adversarial attacks and ability to exhibit reconstruction loss when encountering anomalous data. Study [31] used a Graph Deviation Network (GDN) for unsupervised anomaly detection in multivariate time series, normalizing attention coefficients and anomalousness scores to identify deviations in node relationships. In [32], MLP and logistic regression were applied to time series data, but treating it as from a single sensor led to potential information loss. Study [33] focused on feature extraction using CorrAUC for feature selection and verified using TOPSIS and Shannon entropy, with the C4.5 decision tree model performing best. In [35], ARIMA and HOT-SAX algorithms were used for classification and discrimination of anomalies in IIoT water meters, but the effectiveness of the association rule discriminator was inconclusive. Finally, [36] utilized a custom Hopfield neural network (HNN) for synchronous anomaly detection in network structures, focusing on identifying multiple faults and preprocessing a bipartite graph of faults and detections.

In [37], anomaly detection was performed at edge nodes and in the cloud using a heuristic method that compared feature vectors of input data with known anomalous and non-anomalous data lists and graphs. The process involved applying convolution to n-dimensional time series data, creating a 2D input for linear classification. However, the study did not clearly explain the use of graphs or the generation of feature vectors. In [38], an RNN was used for anomaly detection, capable of identifying various drifts such as sudden, incremental, gradual, periodic, and aperiodic by analyzing prediction errors. The network was trained incrementally and employed local window normalization, suitable for non-stationary time series data. Anomalies were detected when the RNN's predictions deviated significantly from actual data. The survey of anomaly detection methods highlights

several approaches: [38] utilized an RNN for drift detection in time series data, focusing on regression and incremental training; [39] employed an unsupervised DNN called OmniAnomaly, integrating GRU and VAE, for per-entity anomaly detection; [40] used a Conditioning GNN with GRU based on a time window for anomaly detection; [41] combined LSTM networks with naive Bayes for time series anomaly detection; [42] implemented an ensemble method with CNNs and LSTMs for vehicle-level anomaly classification; These methods illustrate a variety of techniques for detecting anomalies in different datasets.

Gómez et al. [43] introduced SUSAN, a Deep Learning-based framework for detecting cyberattacks on industrial systems, achieving a recall rate of 0.910 and a precision of 0.633 in a water treatment plant test, resulting in an F1-score of 0.747. Lee et al. [44] used a dual LSTM network for real-time anomaly detection in univariate time series data streams, achieving high accuracy without pre-extracted features or explicit labels. Lindemann et al. [45] proposed an observer-based LSTM AE model for detecting anomalies in multivariate time series data in manufacturing environments, emphasizing real-time efficiency. Ding et al. [46] combined LSTM with EWMA for contextual anomaly detection in industrial robotics, prioritizing real-time monitoring. A technique combining a Markov model with an enhanced LSTM was suggested in [47], outperforming the KNN algorithm in predicting anomalies in intelligent environments, with specific error reductions for humidity, temperature, and light intensity data. In [48] presents a digital twin-driven MTAD-GAN method for anomaly detection in oil and gas stations, using a stochastic Petri net for operational logic mapping and leveraging time series correlations through knowledge graph and temporal Hawkes attention. Experimental results show a 2.6% performance improvement over other methods, confirming its effectiveness. Swarm drone anomaly detection using deep learning was explored in [49], enhancing reliability in drone operations through a model trained on normal flight data and tested with abnormal data. An unsupervised framework integrating contrastive learning with GANs was proposed in [50], demonstrating improvements in Precision (9.28%), Recall (11.33%), and F1-score (11.73%) in anomaly detection. The qLSTM method in [51] introduced conditional quantiles and a new activation function, outperforming established methods in industrial time-series datasets from Yahoo, AWS, GE, and machine sensors. Real-time anomaly detection in the PBF-EB process using deep learning autoencoders was discussed in [52], achieving an F1 score of approximately 90% and predicting job failures up to 20 hours in advance. Finally, [53] introduced an ensemble prediction method with a signature-based selection algorithm, showing a 21.4% improvement in accuracy over neural networks by dynamically choosing the best prediction algorithm based on data drifts.

TABLE I: COMPARATIVE ANALYSIS OF ANOMALY DETECTION MODELS

Methodology	Key Findings	Limitations
Unsupervised statistical learning [9]	Effective for big data analysis in buildings; highlights challenges and improvements needed	Lack of open datasets, need for better collaboration
Autoencoders for energy data [10]	Effective for unsupervised anomaly detection	Degraded performance on big data, relies on domain-specific features
Semi-supervised CNN for electrical data [11]	Accurate anomaly detection with confidence info	Needs smaller datasets, further exploration of soft labeling impact
LSTM and 1D-CNN for ICS [18]	Effective for detecting ICS anomalies with few false positives	Tested on a single dataset, unclear generalizability
Genetic Algorithms for NN optimization [13]	Improved anomaly detection in industrial systems	Complexity in generating adversarial attacks
IDS with LSTM and CUSUM [14]	Effective time-series IDS, vulnerable to adversarial attacks	Complex attack perturbations influence optimization
GAN-based anomaly detection [15]	Effective for multivariate time-series data	GAN complexity and training time
Seq-to-Seq LSTM with attention [16]	Detects ICS anomalies using normal operational data	Difficulty detecting certain attacks
Hybrid IDS with C5 DT and OC-SVM[18]	Higher detection and lower false positives	Limited to specific attacks and dataset
Graph-based DL approaches [19]	Comprehensive review of graph anomaly detection techniques	Lack of ground-truth data, class imbalance
AD techniques survey [20]	Comprehensive overview of AD techniques	Real-life data scarcity, choosing suitable algorithms depends on multiple factors

Anomaly detection in SINs [22]	Overview of SIN security and anomaly detection	Complexity in developing a holistic security framework
LSTM-based approaches [23]	Detailed overview of LSTM-based anomaly detection	Lack of benchmark datasets, complexity in graph-based data representation
Hybrid semi-supervised approach [24]	Balances supervised and unsupervised benefits	Increased system complexity
Feature extraction with autoencoders [25]	Improved accuracy and energy efficiency for IIoT anomaly detection	Specific to IIoT, generalization needed
Markov model + enhanced LSTM for anomaly detection in time series.[47]	Lower errors (MAE, RMSE, MSE, MAPE) vs. KNN; reduced errors for humidity, temperature, light intensity.	High computational resources needed.
The digital twin-driven MTAD-GAN[48]	The performance of the MTAD-GAN anomaly detection method is improved by about 2.6% compared to other machine learning and deep learning methods.	Inconsistent or incomplete data could degrade its effectiveness. The method is tailored for the specific context of oil and gas stations and might require significant adjustments to be applied to other domains
Deep learning for anomaly detection in swarm drone flights. [49]	Enhances reliability by detecting abnormal behavior.	Scenario-specific; may need retraining.
Unsupervised anomaly detection with GANs and contrastive learning. [50]	Improves Precision (9.28%), Recall (11.33%), F1-score (11.73%).	Risk of overfitting despite contrastive loss.
qLSTM with Parametric Elliot Function for anomaly detection [51].	Outperforms iForest, DAGMM in industrial time-series datasets.	High complexity and tuning needed.
Autoencoder-based framework for real-time anomaly detection in PBF-EB process. [52]	~90% F1 score; predicts job failures up to 20 hours in advance.	Specific to PBF-EB; needs evaluation for other processes.
Ensemble method with signature-based algorithm. [53]	21.4% better accuracy vs. neural networks; adapts to data drifts.	Requires constant updates to the signature database.

III. DISCUSSION

The literature survey highlights research on anomaly detection, particularly in time series data, has made significant strides but still faces notable challenges. Current models often falter with nonstationary data, resulting in inaccurate anomaly detection in dynamic settings. Techniques like LSTM and CNN, despite their effectiveness, demand substantial computational power and long training times. The dependency on large labeled datasets is another hurdle, given the high cost and time required for data labeling. Many models also fail to address the complexity of graph-based relationships in IoT networks, treating data points in isolation, which limits their real-world applicability. Additionally, the integration of anomaly detection with energy-efficient practices in IIoT systems is still underdeveloped. Future improvements could involve hybrid models combining machine learning and deep learning to enhance detection accuracy and robustness. For instance, merging LSTM's predictive capabilities with autoencoders' feature extraction could yield more reliable results. Incorporating Graph Neural Networks (GNNs) with LSTM or CNN architectures can better capture complex graph-based relationships, enhancing detection in interconnected systems. Using Generative Adversarial Networks (GANs) for data augmentation can mitigate the issue of limited labeled data, and implementing contrastive learning within GANs can improve model generalization and reduce overfitting, thus enhancing accuracy and efficiency across various domains.

IV. CONCLUSION

In this paper, we have conducted an extensive literature survey on anomaly detection techniques applied to various domains, particularly focusing on time series data. The survey reveals significant advancements in the field, highlighting the diverse methodologies employed, including LSTM networks, autoencoders, CNNs, GANs, and graph-based models. Despite these advancements, several limitations persist, such as difficulties in handling non stationary data, high computational demands, extensive training times, and the challenge of acquiring large labeled datasets. The future scope for enhancing anomaly detection models lies in providing hybrid approaches that combine the strengths of various machine learning and deep learning techniques. Integrating LSTM networks with autoencoders can enhance feature extraction and predictive accuracy. Incorporating Graph Neural Networks (GNNs) with LSTM or CNN architectures can improve the handling of complex, interconnected data. Using Generative Adversarial Networks (GANs) for data augmentation and contrastive learning can address issues related to limited labeled data and model generalization. To improve computational efficiency, exploring

lightweight models and optimization techniques is crucial, ensuring the practicality of these models in resource-constrained environments. By adopting these advancements, future anomaly detection models can achieve higher accuracy, robustness, and efficiency across various applications.

ACKNOWLEDGMENT

I sincerely thank my Guide, Dr. Omkar Pattanaik for his valuable guidance and support throughout this research. I am also grateful to the faculty and staff of Department of Computer Science and Engineering, SOCSE, Sandip University for their assistance and technical support. Lastly, I thank my family and friends for their unwavering encouragement.

REFERENCES

- [1] Choi, Kyunghyun, et al. "Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines." *IEEE Access*, vol. 9, 2021, pp. 120043-120065.
- [2] M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn, and L. Chang, "A novel anomaly detection scheme based on principal component classifier," Dept. Elect. Comput. Eng., Univ. Miami, Coral Gables, FL, USA, Tech. Rep., Jan. 2003.
- [3] F. Angiulli and C. Pizzuti, "Fast outlier detection in high dimensional spaces," in Proc. Eur. Conf. Princ. Data Mining Knowl. Discovery (PKDD). Berlin, Germany: Springer, 2002, pp. 15_27.
- [4] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying density-based local outliers," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2000, pp. 93_104.
- [5] B. Schölkopf, J. C. Platt, J. C. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Comput.*, vol. 13, no. 7, pp. 1443_1471, 2001.
- [6] Ma, X.; Wu, J.; Xue, S.; Yang, J.; Zhou, C.; Sheng, Q.Z.; Xiong, H.; Akoglu, L. A Comprehensive Survey on Graph Anomaly Detection with Deep Learning. *IEEE Trans. Knowl. Data Eng.* **2021**.
- [7] Lindemann, B.; Maschler, B.; Sahlab, N.; Weyrich, M. A survey on anomaly detection for technical systems using LSTM networks. *Comput. Ind.* **2021**, 131, 103498.
- [8] Zheng, Y.; Jin, M.; Liu, Y.; Chi, L.; Phan, K.T.; Chen, Y.P.P. Generative and Contrastive Self-Supervised Learning for Graph Anomaly Detection. *IEEE Trans. Knowl. Data Eng.* **2021**.
- [9] Clayton Miller, Zoltán Nagy, Arno Schlueter, A review of unsupervised statistical learning and visual analytics techniques applied to performance analysis of non-residential buildings, *Renew. Sustain. Energy* 81 (2018) 1365–1377.
- [10] Cheng Fan, Fu Xiao, Yang Zhao, Jiayuan Wang, Analytical investigation of autoencoder-based methods for unsupervised anomaly detection in building energy data, *Appl. Energy* 211 (2018) 1123–1135.
- [11] N.L. Tasfi, W.A. Higashino, K. Grolinger, M.A.M. Capretz, Deep neural networks with confidence sampling for electrical anomaly detection, in: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, pp. 1038–1045.
- [12] Moshe Kravchik, Asaf Shabtai, Detecting cyber-attacks in industrial control systems using convolutional neural networks, in: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, 2018, pp. 72–83.
- [13] Dmitry Shalyga, Pavel Filonov, Andrey Lavrentyev, Anomaly detection for water treatment system based on neural network with automatic architecture optimization, 2018, arXiv preprint arXiv:1807.07282.
- [14] Giulio Zizzo, Chris Hankin, Sergio Maffei, Kevin Jones, Intrusion detection for industrial control systems: Evaluation analysis and adversarial attacks, 2019, arXiv preprint arXiv:1911.04278.
- [15] Dan Li, Dacheng Chen, Baihong Jin, Lei Shi, Jonathan Goh, See-Kiong Ng, MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks, in: Artificial Neural Networks and Machine Learning – ICANN 2019: Text and Time Series, 2019, pp. 703–716.
- [16] Jonguk Kim, Jeong-Han Yun, Hyoung Chun Kim, Anomaly detection for industrial control systems using sequence-to-sequence neural networks, 2019, arXiv preprint arXiv:1911.04831
- [17] Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis, Antonios Sarigiannidis, Dimitrios Margounakis, Apostolos Tsiakalos, Georgios Efstathiopoulos, An anomaly detection mechanism for IEC 60870-5-104, in: 2020 9th International Conference on Modern Circuits and Systems Technologies, MOCAST, IEEE, 2020, pp. 1–4.
- [18] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, Joarder Kamruzzaman, Ammar Alazab, A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks, *Electronics* 8 (11) (2019) 1210.
- [19] Ma, X.; Wu, J.; Xue, S.; Yang, J.; Zhou, C.; Sheng, Q.Z.; Xiong, H.; Akoglu, L. A Comprehensive Survey on Graph Anomaly Detection with Deep Learning. *IEEE Trans. Knowl. Data Eng.* **2021**.
- [20] Toshniwal, A.; Mahesh, K.; Jayashree, R. Overview of Anomaly Detection techniques in Machine Learning. In Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 7–9 October 2020; pp. 808–815.
- [21] Zhou, J. Research on Time Series Anomaly Detection: Based on Deep Learning Methods. *J. Phys. Conf. Ser.* **2021**, 2132, 012012.

- [22] Zhuo, M.; Liu, L.; Zhou, S.; Tian, Z. Survey on security issues of routing and anomaly detection for space information networks. *Sci. Rep.* **2021**, *11*, 1–18.
- [23] Lindemann, B.; Maschler, B.; Sahlab, N.; Weyrich, M. A survey on anomaly detection for technical systems using LSTM networks. *Comput. Ind.* **2021**, *131*, 103498.
- [24] Jia, Y.; Cheng, Y.; Shi, J. Semi-Supervised Variational Temporal Convolutional Network for IoT Communication Multi-Anomaly Detection. Proceedings of the 2022 3rd International Conference on Control, Robotics and Intelligent System (CCRIS'22), Xi'an, China, 26–28 August 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 67–73.
- [25] Huang, Z.; Wu, Y.; Tempini, N.; Lin, H.; Yin, H. An Energy-Efficient And Trustworthy Unsupervised Anomaly Detection Framework (EATU) for IIoT. *ACM Trans. Sen. Netw.* **2022**, *18*, 1–18.
- [26] Meyer-Berg, A.; Egert, R.; Böck, L.; Mühlhäuser, M. IoT Dataset Generation Framework for Evaluating Anomaly Detection Mechanisms. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES'20), Virtual, 25–28 August 2020; Association for Computing Machinery: New York, NY, USA, 2020.
- [27] Bhatia, R.; Benno, S.; Esteban, J.; Lakshman, T.V.; Grogan, J. Unsupervised Machine Learning for Network-Centric Anomaly Detection in IoT. In Proceedings of the 3rd ACM CoNEXT Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA'19), Orlando, FL, USA, 9 December 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 42–48.
- [28] Evmorfos, S.; Vlachodimitropoulos, G.; Bakalos, N.; Gelenbe, E. Neural Network Architectures for the Detection of SYN Flood Attacks in IoT Systems. In Proceedings of the 13th ACM International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'20), Corfu, Greece, 30 June–3 July 2020; Association for Computing Machinery: New York, NY, USA, 2020.
- [29] Ngo, Q.D.; Nguyen, H.T.; Tran, H.A.; Pham, N.A.; Dang, X.H. Toward an Approach Using Graph-Theoretic for IoT Botnet Detection. In Proceedings of the 2021 2nd International Conference on Computing, Networks and Internet of Things (CNIOT'21), Beijing, China, 20–22 May 2021; Association for Computing Machinery: New York, NY, USA, 2021.
- [30] Yehezkel, A.; Elyashiv, E.; Soffer, O. Network Anomaly Detection Using Transfer Learning Based on Auto-Encoders Loss Normalization. In Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security (AISec'21), Virtual, 15 November 2021 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 61–71.
- [31] Deng, A.; Hooi, B. Graph neural network-based anomaly detection in multivariate time series. In Proceedings of the AAAI Conference on Artificial Intelligence, Virtual, 2–9 February 2021; Volume 35, pp. 4027–4035.
- [32] Abbasi, F.; Naderan, M.; Alavi, S.E. Anomaly detection in Internet of Things using feature selection and classification based on Logistic Regression and Artificial Neural Network on N-BalIoT dataset. In Proceedings of the 2021 5th International Conference on Internet of Things and Applications (IoT), Online, 19–20 July 2021; pp. 1–7.
- [33] Shafiq, M.; Tian, Z.; Bashir, A.K.; Du, X.; Guizani, M. CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. *IEEE Internet Things J.* **2020**, *8*, 3242–3254.
- [34] Shafiq, M.; Tian, Z.; Bashir, A.K.; Du, X.; Guizani, M. IoT malicious traffic identification using wrapper-based feature selection mechanisms. *Comput. Secur.* **2020**, *94*, 101863.
- [35] González-Vidal, A.; Cuenca-Jara, J.; Skarmeta, A.F. IoT for Water Management: Towards Intelligent Anomaly Detection. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 858–863.
- [36] Wang, B.; Yang, H.; Yao, Q.; Yu, A.; Hong, T.; Zhang, J.; Kadoch, M.; Cheriet, M. Hopfield Neural Network-based Fault Location in Wireless and Optical Networks for Smart City IoT. In Proceedings of the 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 1696–1701.
- [37] Yu, X.; Shan, C.; Bian, J.; Yang, X.; Chen, Y.; Song, H. Adagum: An adaptive graph updating model-based anomaly detection method for edge computing environment. *Secur. Commun. Netw.* **2021**, *2021*, 9954951.
- [38] Saurav, S.; Malhotra, P.; TV, V.; Gugulothu, N.; Vig, L.; Agarwal, P.; Shroff, G. Online Anomaly Detection with Concept Drift Adaptation Using Recurrent Neural Networks. In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data (CoDS-COMAD'18), Goa, India, 11–13 January 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 78–87.
- [39] Su, Y.; Zhao, Y.; Niu, C.; Liu, R.; Sun, W.; Pei, D. Robust Anomaly Detection for Multivariate Time Series through Stochastic Recurrent Neural Network. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'19), Anchorage, AK USA, 4–8 August 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 2828–2837.
- [40] Gupta, V.; Narwariya, J.; Malhotra, P.; Vig, L.; Shroff, G. Handling Variable-Dimensional Time Series with Graph Neural Networks. *arXiv* **2020**, arXiv:2007.00411.
- [41] Wu, D.; Jiang, Z.; Xie, X.; Wei, X.; Yu, W.; Li, R. LSTM Learning With Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *16*, 5244–5253.
- [42] Javed, A.R.; Usman, M.; Rehman, S.U.; Khan, M.U.; Haghighi, M.S. Anomaly Detection in Automated Vehicles Using Multistage Attention-Based Convolutional Neural Network. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4291–4300.
- [43] Gómez, Ángel Luis Perales, et al. "SUSAN: A Deep Learning based anomaly detection framework for sustainable industry." *Sustainable Computing: Informatics and Systems* 37 (2023): 100842.

- [44] M.-C. Lee, J.-C. Lin, and E.G. Gan, "ReRe: A Lightweight Real-Time Ready-to-Go Anomaly Detection Approach for Time Series," 2020 IEEE 4th Annual Computers, Software and Applications Conference (COMPSAC), Madrid, Spain, pp. 322-327, 2020. DOI: 10.1109/COMPSAC48688.2020.0-226.
- [45] B. Lindemann, N. Jazdi and M. Weyrich, "Anomaly detection and prediction in discrete manufacturing based on cooperative LSTM networks," 2020 IEEE 16th International Conference on Automation Science and Engineering (CASE), Hong Kong, Hong Kong, 2020, pp. 1003-1010, DOI: 10.1109/CASE48305.2020.9216855.
- [46] S. Ding, A. Morozov, S. Vock, M. Weyrich, and K. Janschek, "Model-based Error Detection for Industrial Automation Systems using LSTM Networks," IMBSA: Model-Based Safety and Assessment, pp. 212-226, 2020. DOI: 10.1007/978-3-030-58920-2_14.
- [47] V. Shanmuganathan, A. Suresh, Markov enhanced I-LSTM approach for effective anomaly detection for time series sensor data, *International Journal of Intelligent Networks*, Volume 5, 2024, Pages 154-160.
- [48] Lian Y, Geng Y, Tian T. Anomaly Detection Method for Multivariate Time Series Data of Oil and Gas Stations Based on Digital Twin and MTAD-GAN. *Applied Sciences*. 2023; 13(3):1891.
- [49] Hyojung Ahn, Sonia Chung, Deep learning-based anomaly detection for individual drone vehicles performing swarm missions, *Expert Systems with Applications*, Volume 244, 2024, 122869.
- [50] Jiawei Miao, Haicheng Tao, Haoran Xie, Jianshan Sun, Jie Cao, Reconstruction-based anomaly detection for multivariate time series using contrastive generative adversarial networks, *Information Processing & Management*, Volume 61, Issue 1, 2024, 103569.
- [51] S. Saha, J. Sarkar, S. Dhavala, P. Mota and S. Sarkar, "quantile-Long Short Term Memory: A Robust, Time Series Anomaly Detection Method," in *IEEE Transactions on Artificial Intelligence*, doi: 10.1109/TAI.2024.3353163.
- [52] Cannizzaro, D., Antonioni, P., Ponzio, F. et al. Machine learning-enabled real-time anomaly detection for electron beam powder bed fusion additive manufacturing. *J Intell Manuf* (2024).
- [53] Sus, W., Nawrocki, P. Signature-based Adaptive Cloud Resource Usage Prediction Using Machine Learning and Anomaly Detection. *J Grid Computing* 22, 46 (2024).