Anomaly Detection in Critical-Infrastructures using Autoencoders: A Survey

Conference Paper · August 2022

DOI: 10.1109/IECON49645.2022.9968505

5 authors, including:

Harindra Sandun Mavikumbure
Virginia Commonwealth University
15 PUBLICATIONS **102** CITATIONS
SEE PROFILE

Chathurika S Wickramasinghe
Virginia Commonwealth University
40 PUBLICATIONS **845** CITATIONS
SEE PROFILE

Victor Cobilean
Virginia Commonwealth University
25 PUBLICATIONS **117** CITATIONS
SEE PROFILE

Milos Manic
Virginia Commonwealth University
276 PUBLICATIONS **6,333** CITATIONS
SEE PROFILE

Anomaly Detection in Critical-Infrastructures using Autoencoders: A Survey

Harindra S. Mavikumbure, Chathurika S. Wickramasinghe, Daniel L. Marino,
Victor Cobilean and Milos Manic, *Fellow, IEEE*
Department of Computer Science, Virginia Commonwealth University, Richmond, USA
(mavikumbureh, brahmanacsw, marinodl, cobileanv)@vcu.edu, misko@ieee.org

***Abstract*—In critical infrastructures, timely detection of anomalies is essential to detect failures, avoid catastrophic damages, and improve resilience. Neural Network models are one of the state-of-the-art approaches used for anomaly detection. Among Neural Network architectures used these days, Autoencoders (AEs) have gained significant attention due to their advantages such as unsupervised learning, dimensionality reduction, non-linear feature extraction, the ease of integration with other neural network algorithms, and ease of use. Therefore, in this paper, we present: 1) anomaly detection and types of anomaly detection, 2) recent advancements in AEs typically used in anomaly detection, 3) AE-based Anomaly Detection (AE-AD) in selected critical infrastructures such as smart grids, intelligent transportation systems, and smart buildings, and 4) future research opportunities. We hope that this systematic survey of AE-based anomaly detection approaches will help the community prioritize research efforts to address pressing issues in critical infrastructures.**

***Index Terms*—Anomaly Detection, Autoencoder, Critical Infrastructure, Intelligent Transportation Systems, Smart Grids, Smart Buildings**

I. Introduction

Critical infrastructures (CIs) represent systems that are vital to modern society. Any disruption of CI can have lasting effects on the economy, security, safety, and public health. Critical infrastructure includes crucial components in modern society such as Smart Grids, Smart Buildings, Transportation Systems, Financial Institutes, Healthcare, and Critical Manufacturing. Since CIs are an essential component for the proper functioning of the economy and normalcy in daily life, it is necessary to integrate Anomaly Detection Systems (ADSs) for timely identification of possible failures, degradation, or cyber-attacks to improve the resiliency of these systems.

Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behavior [1]. Anomalies are a strong indicator of a decrease in system performance which can lead to instabilities and failure. Often, the causes of anomalies are unknown effects within complex systems [2]. Hence, the capability of understanding and detecting these underlying effects with the aid of data is the key to ensuring the desired outcome and resilience of complex CI. ADSs are widely used in CI events such as fraud detection, mechanical fault detection, and secure remote health care [3], and efficient smart energy management [4].

Majority of the existing ADS systems were trained based on classification methods such as Naive Bayes, Random Forest, Support Vector Machines [5], thus depends on labeled data. However, data labeling is time-consuming, and one cannot label all the anomalous behavior of the system due to practical difficulties. Therefore, unsupervised techniques such as One-Class SVM, Local Outlier Factor, and Neural Networks have gained popularity over recent years.

Deep learning has shown tremendous capabilities in learning feature representations of complex data in recent years. Out of widely used DNNs for Anomaly Detection in Critical-Infrastructures (AD-CI), Autoencoder has specifically gained much attention in recent years. Figure 1 shows that the popularity of the AE algorithm being applied for anomaly detection by researchers in recent years has increased. The main reason for this is the architecture of AE allows calculating an anomalous score (using reconstruction error) for data records which can directly use for the identification of anomalies [6]. This architecture does not require labeled data for training. Thus, can be trained with data that represent the normal behavior of a given system. The second main reason for this is its unsupervised feature learning and dimensionality reduction capability [7]. This capability allows users to use AEs in hybrid architectures for building efficient ADSs [8]. Other advantages of AEs include easy implementation, easy modifications, and non-linear feature learning capability. Further, AEs have many architectures such as Stacked AE, LSTM AE, Convolution AE, and Variational AE, where each model has its advantages when it comes to anomaly detection.

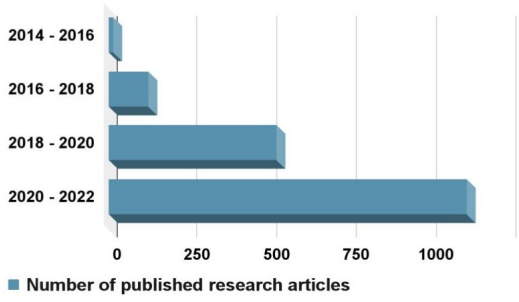

Fig. 1. Statistics of published research articles on Autoencoder based anomaly detection

Current studies have widely explored different AE architectures for building ADSs. Thus, there is an essential need for a comprehensive survey to review AE-based anomaly detection

The accepted version of the paper appearing in the 48th Annual Conference of the IEEE Industrial Electronics Society (IES) 2022

systems for CIs, discussing how AEs been successfully used, and what are the strengths of different AE architectures. Therefore, this paper presents a comprehensive study on AEs in anomaly detection in CIs, reviewing existing strategies and providing direction for building effective ADSs. The paper provides the following contributions:

1) Summary on anomaly detection and types of anomalies
2) Recent advancements in AE architectures typically used in anomaly detection
3) Survey on AE-AD use cases in selected critical infrastructures
4) Future research opportunities

The rest of the paper is organized as follows. Section II presents a general overview of anomaly detection. Section III summarizes the recent advancements in AEs. Section IV discusses the CI application areas of the existing AE-AD methods. Section V discusses future research opportunities. Finally, Section VI concludes the paper.

II. Anomalies and Anomaly Detection Algorithms

Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behavior. These nonconforming patterns are often referred to as anomalies in diverse application domains. The importance of anomaly detection is because anomalies in data translate to significant, and often critical information in CI. Thus, anomaly detection is the key to ensuring the desired outcome and resilience of complex CI.

This section first discusses what anomalies are, how they can be categorized, and specific examples for each category. Then, it presents the motivations for focusing on AE-based anomaly detection.

A. Types of Anomalies

As discussed in the Introduction, Anomalies are considered as patterns in data that do not conform to expected behavior [1]. When building data-driven ADSs, it is crucial to understand how the nature of the data and types of anomalies that can exist within the data to build efficient ADSs. These anomalies are broadly classified into point anomalies, conditional anomalies, and collective anomalies. However, it has to be noticed that there are various ways of categorizing anomalies [9].

Point Anomaly: Point anomaly can be defined as irregularity or deviation that happens randomly which can be observed separately from the other objects [10]. The majority of work in literature focuses on point anomalies. A few examples of this anomaly type are explained below.

- Counting the number of occurrences of a ”gateway on” event from a smart meter might be considered anomalous if its frequency is too low or high on a specific day In this example, each day is considered an object.
- Hourly air conditioning consumption in a building at a specific hour can be anomalous compared to previous recorded hourly values.

Conditional Anomaly: A data instance that can be identified as an anomaly considering both contextual and behavioral features is defined as a conditional anomaly [10]. The context of a given data instance is determined using the contextual attributes. For example, in spatial data sets, the longitude and latitude of a location are the contextual attributes. The non-contextual characteristics of a given data instance are identified by behavioral attributes. For example, in a spatial data set describing the average rainfall of the entire world, the amount of rainfall at any location is a behavioral attribute. Conditional anomaly-based ADSs are implemented in a wide range of areas. Some are explained below.

- Drastic temperature drop during the summer is an anomalous behavior as the temperature is normally high during the summer season.
- Hourly Heating, Ventilation, and Air Conditioning (HVAC) consumption record higher usage might be anomalous in winter, but not in summer.

Collective Anomaly: Collective anomaly is the term to guide a collection of related anomalous data instances concerning the whole data set. The single data points in a collective anomaly may not be considered anomalies by themselves, but the occurrences of these single points jointly denote an anomaly [10]. Collective anomaly-based ADSs are implemented in a wide range of areas. Some are explained below.

- Network packet data transmission identified as attacks on time series data (Denial of Service attack) by analyzing over a specific time interval.
- Measurements from the collection of sensors can be used to identify anomalous building energy consumption where individual sensor measurements can provide normal behavior.

B. Motivation towards Autoencoders

This section discusses the motivation of the paper, focusing on the main advantages and properties of AEs.

Figure 2 presents advantages of AE, focusing on anomaly detection.

Fig. 2. Motivations/Advantages of Autoencoders

Most widely used AE architectures for anomaly detection include stacked AE, LSTM AE, and VAE. Therefore, it is important to understand the advantages and limitations of AEs compared to these models. Many machine learning algorithms such as Gaussian Mixture Model and Principal Component

Analysis fail to retain sufficient accuracy due to the so-called curse of dimensionality of data. However, AE can transform high-dimensional data into a more compact and meaningful expression in low-dimensional feature space. The majority of the neural network architectures with state-of-the-art performance require labeled data to train the models which are challenging to acquire in a real-world setting whereas AE is an unsupervised algorithm that doesn't require labeled data for training. Moreover, AEs can perform automatic feature learning that eliminates the need to develop manual features by domain experts. Non-parametric machine learning algorithms do not scale well with the size of the data. For example, KNN uses the distance metric to perform data clustering. But in high dimensionsional feature space, data becomes very sparse and distance measures become increasingly meaningless. However, AEs scale well with the increase of the data due to their data compression capability. More importantly, AE is capable of performing accurate anomaly detection.

Due to their advantages, AEs are widely used for anomaly detection in CI applications. Thus, it is important to understand the applicability of AEs, challenges, and future research opportunities when using AE models.

III. Recent Advancements in AEs

Recently, various AE architectures have been proposed based on the goal of learning a mapping from high-dimensional observations to a lower-dimensional representation space.

In [11], researchers have proposed a Skip connected and Memory Guided Network (SMGNet) for video anomaly detection. The memory-guided network with skip connection helps in avoiding the loss of meaningful information such as foreground patterns, in addition to memorizing significant normality patterns. Quantile AE (QAE) is described in [12] as a novel AD method to consider data-oriented uncertainty. QAE is a variant of the AE that predicts the quantiles of the reconstruction distribution by minimizing the sum of pinball losses on multiple quantiles. Moreover, a novel neural density estimation technique based on the Group-Masked AE is presented in [13], which estimates the density of an audio time series by taking into account the intra-frame statistics of the signal. In [14], a Graph Convolutional AE is presented to detect anomalies in wind turbines based on SCADA data. This structure improves the unsupervised learning capabilities of AE by considering individual sensor measurements together with the nonlinear correlations existing among signals. In [15], researchers presented Bayesian Skip-Autoencoders for Unsupervised Anomaly Detection (UAD) in brain MRI. They proposed skip-connections, a concept that has already proven beneficial for biomedical image segmentation and image-to-image translation, and a dropout-based mechanism to prevent the model from learning an identity mapping. Moreover, there are several other recent AE architectures such as beta-VAE, structured VAE [16], and clockwork AE [17], etc. which can be modified for anomaly detection. Other novel AE-based architectures such as U-NET and variations of VAEs applied for anomaly detection are described in the next section.

IV. AE-AD use cases in critical infrastructures

This section discusses the applicability of the recent AE architectures in different critical infrastructure applications including smart grids, and intelligent transportation systems. Moreover, we summarize different data sources and types of anomalies detected in the above-mentioned applications.

Data: Data plays an important role in data-driven machine learning as it contains useful information about the real-world problems that the algorithms intended to solve. Solving real-world problems requires data from different sources to cover complex feature space. Major sources of data include sensors including PMU, and complex devices such as smart meters. etc [18]. Figure 3 presents examples of data sources for selected use-case scenarios.

Types of anomalies: Current studies have widely explored detecting different anomaly types that exist in smart grid systems, ITS, and smart buildings. Figure 3 presents a summary of work carried out to identify different anomaly types in the above-mentioned application areas.

Next, we will review the applicability of Autoencoders in three main application areas.

A. Secure Smart Grid

Smart Grid is a cyber-physical system that integrates physical components (e.g., humans, weather, power plants) and logical components (e.g., control algorithms, communication infrastructure, protocols). It integrates a network of sensors that enable communication between physical devices and users. In order to communicate between physical components with users, network communication is required [19]. Thus, making these systems vulnerable to measurement tampering and cyber-attacks. Due to the importance and the usage that it has provided to society, smart grids are successfully implemented in several systems such as energy management systems and renewable energy systems [20]. CESER (Cybersecurity, Energy Security, and Emergency Response) highlights that, anomaly detection in energy systems is important to reduce risks to the critical energy infrastructure posed by cyber and other emerging threats. Continuing to increase the security, reliability, and resiliency of energy infrastructure will help to ensure the success of grid modernization and transformation of the energy systems [21].

Data Injection: Recent research on unobservable false data injection attacks (FDIAs) reveals the high risk of secure system operations. As an example, In 2007, the Department of Homeland Security of USA staged a cyber-attack codenamed "Aurora" resulting in the explosion of the $1 million generators which is widely utilized across the USA [27].

An adversarial AE algorithm is proposed in [28], which detects false data injection attacks by capturing the unconformity between abnormal and normal measurements. The proposed method is evaluated on different measurements such as power

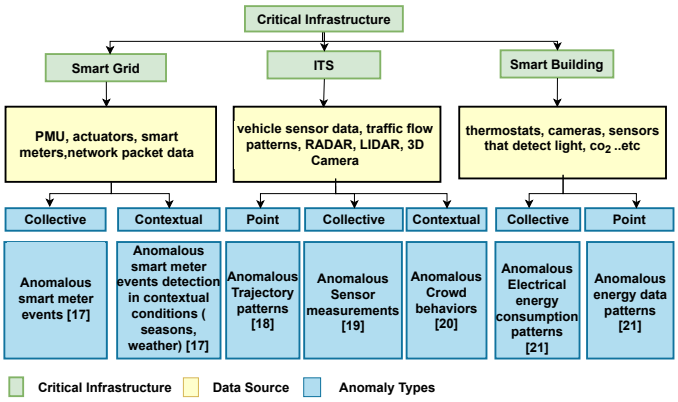

Fig. 3. Anomaly type detection in smart grid, ITS and smart buildings [22], [23], [24], [25], [26]

flow, power injection, and voltage from PMUs. In [29], an AE-based approach is proposed that learns the internal dependency of 'normal' operation data. Thus, it effectively overcomes the challenge of unbalanced training data that is inherent in power system attack detection. The detection performance of the proposed mechanism is evaluated on the IEEE 118-bus power system.

Denial of Service (DoS): DoS attacks have a critical threat to the security of smart grid systems. As an example, an electrical power station in Ukraine's Ivano-Frankivsk city was targeted for a DoS attack that affected eighty thousand (80,000) people at risk by putting them in the dark [30].

By analyzing network packet data an AE model can learn Non-linear features that are crucial for detecting DoS attacks in smart grids. However, non-linear feature learning is not enough to accurately identify attacks from time-series samples. Therefore, AE is integrated with other ML algorithms, in order to improve the accuracy of the attack detection. Some of the examples are Deep AE with Recurrent Neural Network, Deep AE with Extreme Learning Machine [31], [32].

B. Intelligent Transportation Systems

The Intelligent Transportation System (ITS) is based on the ever-increasing demands of transportation development. ITS uses advanced communication, information, and electronics technology to develop systems such as advanced traffic management systems and advanced public transportation systems, which fulfill the transportation needs. With the rapid growth of the number of vehicles and complexity of the transportation systems, the ITSs have become vulnerable due to various factors, including fault driving behaviors, subtle behaviors of pedestrians and cyberattacks on communication networks of the vehicles. Thus, building anomaly detection systems critical for ITSs to avoid failures and take precautions in a timely manner to ensure safe, reliable, and resilient operations in these systems.

Obstacle and incident detection: Obstacle detection such as a fallen tree or pedestrian in the middle of the road is an essential element for the development of efficient ITS so that accidents can be avoided, which otherwise can cost human lives.

In [33], they proposed U19-Net which is an encoder-decoder deep model that explores the deep layers of a VGG19 model as an encoder following an asymmetrical approach with a U-Net decoder designed for pixel-wise classifications. This work detects possible collisions that may arise between drivers and obstacles on roads. A Spatio-temporal AE is used in [34], which captures the spatial and temporal features of the video data. The algorithm is evaluated on a video data set that is collected from real-world traffic surveillance videos.

Trajectory-based anomaly detection: Trajectory-based anomaly detection is essential as automatic detection of abnormal activities/behaviors of pedestrians in crowded scenes or abnormal movements of vehicles in road infrastructures is critical for public safety which otherwise can cost human lives.

In [35], researchers propose Context augmented Graph Autoencoder (ConGAE), which leverages graph embedding and context embedding techniques to capture the spatial traffic network patterns. The proposed model is evaluated on real-world large-scale datasets such as the Uber Movement dataset. In [36], a spatio-temporal graph auto-encoder is presented for learning normal driving behaviours. Their approach is able to perform anomaly detection on multiple trajectories of a dynamic number of agents.

C. Other

Apart from the above application areas, recent AE architectures are applied for anomaly detection in other domains such as Smart Buildings, and Video Surveillance. In this section, we will summarize some of the use case scenarios in which the latest AE architectures are being applied.

Smart Buildings: In [37], researchers proposed a GRU-based Gaussian Mixture VAE (GGM-VAE) system for anomaly detection on multidimensional time-series data from Smart Building Sensors. They evaluated the model on Intel Berkeley Research Lab Dataset which contains humidity, temperature, light, and voltage values measured using 54 sensors.

Video Anomaly Detection: A Skip connected and Memory Guided Network (SMGNet) is proposed in [11] for video anomaly detection. The memory-guided network with skip connection helps in avoiding the loss of meaningful information such as foreground patterns, in addition to memorizing significant normality patterns. In [38], Gaussian Mixture Variational Autoencoder, which can learn feature representations of the normal samples as a Gaussian Mixture Model trained using deep learning for video anomaly detection and localization using only normal samples.

V. Future Research Opportunities

The rapid research advances of AE-based anomaly detection open up various research opportunities. In this section, we summarize the future research opportunities for effective improvement, development, and use of AE-AD methods.

Online adaptive anomaly detection: Adaptive learning is an active area of research. Online adaptive anomaly detection

is very important as it can improve the performance and accuracy of the AD system when there is a drift in normal conditions. However, current research studies on anomaly detection usually work offline and cannot timely adapt to changes in the environment. Thus, there is a research gap in adapting AE-AD systems to possible data drifts.

Interpretability of the models: Interpretable AI refers to explaining the internal decision-making process of AI models in human understandable format [39]. Interpretability of ADS systems is essential in critical infrastructure due to numerous reasons, including model debugging, model diagnosing, interpreting outcomes of ADS to operators, anomaly identification, anomaly localization, and improving user trust in the decision-making process of ADS [40, 41].

Creation of benchmark data sets that represent real-world anomalous data: Benchmark datasets are important to build accurate anomaly detection systems. Benchmark datasets are essential to evaluate new algorithms or modifications of current AE algorithms, helping to keep track of progress in the field. Because of privacy issues, real-world datasets are hard to obtain and share. There is a need for new benchmark datasets that cover complex real-world scenarios in critical application areas to build resilient anomaly detection systems.

Making AE robust to handling noisy labels: Real-world data sets suffer from noisy labels which makes a differentiation between normal vs abnormal behavior difficult. This differentiation is crucial for training AE-AD algorithms as well as for the evaluation of their performance. Thus, making AE capable of training in the presence of noisy labels for accurate anomaly detection is a vital research direction.

Federated learning-based anomaly detection: Federated learning has gained significant attention in recent years [42]. Federated learning can be used for the reduction of computational resources, reduce training time, and improve the privacy of AE-AD systems.

Distinguish between noise, outlier, and anomaly: Distinguishing between noise, outlier, and anomaly is an important problem. With the unsupervised AE-AD methods, it is difficult to resolve the problem mentioned above. One viable solution is to use semi-supervised learning in the presence of few labeled samples, which is an open research problem to tackle in the future.

VI. Conclusion

In this paper, we systematically reviewed AE-based anomaly detection in critical infrastructures. First, we discuss various anomaly types that are highly discussed in the literature. We found that there are three main types of anomalies identified in the literature: Point, Conditional, and Collective. However, we found that most ADS studies aim to detect point-based and collective-based anomalies.

Then, we discuss the applicability of recent AE architectures in selected critical infrastructure applications such as smart grids, intelligent transportation systems, and smart buildings. We found that variants of LSTM-based AE and VAE are the most used AE architectures within these fields. Further, we identified the main strengths of AE for anomaly detection, including scalability, unlabelled data, and dimensionality reduction.

Finally, we summarize possible future research opportunities for effective development, improvement, and use of AE-AD methods. We suggested future research opportunities such as improving the interpretability of the AE models and making AE robust to handle noisy labels. We hope that this systematic survey of AE-based anomaly detection approaches will help the community prioritize research efforts to address pressing issues in Critical Infrastructures.

Acknowledgements

This work was supported by the Commonwealth Cyber Initiative, an Investment in the Advancement of Cyber Research and Development, Innovation and Workforce Development (cyberinitiative.org).

References

[1] A. Jones, Z. Kong, and C. Belta, "Anomaly detection in cyber-physical systems: A formal methods approach," in *53rd IEEE Conference on Decision and Control*, 2014, pp. 848–853.

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, Jul. 2009.

[3] L. Ruff *et al.*, "A unifying review of deep and shallow anomaly detection," *Proceedings of the IEEE*, vol. 109, no. 5, pp. 756–795, 2021.

[4] G. Fenza, M. Gallo, and V. Loia, "Drift-aware methodology for anomaly detection in smart grid," *IEEE Access*, vol. 7, pp. 9645–9657, 2019.

[5] M. C. Belavagi and B. Muniyal, "Performance evaluation of supervised machine learning algorithms for intrusion detection," *Procedia Computer Science*, vol. 89, pp. 117–123, 2016.

[6] D. L. Marino, C. S. Wickramasinghe, B. Tsouvalas, C. Rieger, and M. Manic, "Data-driven correlation of cyber and physical anomalies for holistic system health monitoring," *IEEE Access*, vol. 9, pp. 163 138–163 150, 2021.

[7] C. S. Wickramasinghe, D. L. Marino, and M. Manic, "Resnet autoencoders for unsupervised feature learning from high-dimensional data: Deep models resistant to performance degradation," *IEEE Access*, vol. 9, pp. 40 511–40 520, 2021.

[8] M. Sakurada and T. Yairi, "Anomaly detection using autoencoders with nonlinear dimensionality reduction," in *Proceedings of the MLSDA 2014 2nd workshop on machine learning for sensory data analysis*, 2014, pp. 4–11.

[9] F. Lopez *et al.*, "Categorization of anomalies in smart manufacturing systems to support the selection of detection mechanisms," *IEEE Robotics and Automation Letters*, vol. 2, no. 4, pp. 1885–1892, 2017.

[10] V. Chandola, A. Banerjee, and V. Kumar, "Outlier detection: A survey," *ACM Computing Surveys*, vol. 14, p. 15, 2007.

[11] S Chandrakala, V Srinivas, and K Deepak, "Residual spatiotemporal autoencoder with skip connected and memory guided network for detecting video anomalies," *Neural Processing Letters*, vol. 53, no. 6, pp. 4677–4692, 2021.

[12] H. Seo, S. Ryu, J. Yim, J. Seo, and Y. Yu, "Quantile autoencoder for anomaly detection," in *AAAI 2022 Workshop on AI for Design and Manufacturing (ADAM)*, 2021.

[13] R. Giri, F. Cheng, K. Helwani, S. V. Tenneti, U. Isik, and A. Krishnaswamy, "Group masked autoencoder based density estimator for audio anomaly detection," *Proc. DCASE*, pp. 51–55, 2020.

[14] E. S. Miele, F. Bonacina, and A. Corsini, "Deep anomaly detection in horizontal axis wind turbines using graph convolutional autoencoders for multivariate time series," *Energy and AI*, vol. 8, p. 100 145, 2022.

[15] C. Baur, B. Wiestler, S. Albarqouni, and N. Navab, "Bayesian skip-autoencoders for unsupervised hyperintense anomaly detection in high resolution brain mri," in *2020 IEEE 17th International Symposium on Biomedical Imaging (ISBI)*, 2020, pp. 1905–1909.

[16] M. Tschannen, O. Bachem, and M. Lucic, "Recent advances in autoencoder-based representation learning," *arXiv preprint arXiv:1812.05069*, 2018.

[17] V. Saxena, J. Ba, and D. Hafner, "Clockwork variational autoencoders," *Advances in Neural Information Processing Systems*, vol. 34, pp. 29 246–29 257, 2021.

[18] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Comput. Surv.*, vol. 54, no. 5, 2021.

[19] F. Palensky PeterandKupzog, "Smart grids," *Annual Review of Environment and Resources*, vol. 38, no. 1, pp. 201–226, 2013.

[20] S. E. Widergren, M. L. Paget, T. J. Secrest, P. J. Balducci, A. C. Orrell, and C. N. Bloyd, "Using smart grids to enhance use of energy-efficiency and renewable-energy technologies," May 2011.

[21] *Cybersecurity*, [Online]. Available: https://www.energy.gov/ceser/cybersecurity, [Accessed: 23-Jun-2022].

[22] R. Moghaddass and J. Wang, "A hierarchical framework for smart grid anomaly detection using large-scale smart meter data," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5820–5830, 2018.

[23] A. Chevrot, A. Vernotte, and B. Legeard, "Cae: Contextual auto-encoder for multivariate time-series anomaly detection in air transportation," *Computers & Security*, vol. 116, p. 102 652, 2022.

[24] M. H. Hassan, A. Tizghadam, and A. Leon-Garcia, "Spatio-temporal anomaly detection in intelligent transportation systems," *Procedia Computer Science*, vol. 151, pp. 852–857, 2019.

[25] M. Ribeiro, A. E. Lazzaretti, and H. S. Lopes, "A study of deep convolutional auto-encoders for anomaly detection in videos," *Pattern Recognition Letters*, vol. 105, pp. 13–22, 2018, Machine Learning and Applications in Artificial Intelligence.

[26] Y. Zhang, W. Chen, and J. Black, "Anomaly detection in premise energy consumption data," in *2011 IEEE Power and Energy Society General Meeting*, 2011, pp. 1–8.

[27] M. Swearingen, S. Brunasso, J. Weiss, and D. Huber, "What you need to know (and don't) about the aurora vulnerability," *Power*, vol. 157, no. 9, pp. 52–52, 2013.

[28] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2021.

[29] C. Wang, S. Tindemans, K. Pan, and P. Palensky, "Detection of false data injection attacks using the autoencoder approach," in *2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, 2020, pp. 1–6.

[30] D. Faquir, N. Chouliaras, V. Sofia, K. Olga, and L. Maglaras, "Cybersecurity in smart grids, challenges and solutions," *AIMS Electronics and Electrical Engineering*, vol. 5, no. 1, pp. 24–37, 2021.

[31] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Ddosnet: A deep-learning model for detecting network attacks," in *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 2020, pp. 391–396.

[32] S. Ali and Y. Li, "Learning multilevel auto-encoders for ddos attack detection in smart grid network," *IEEE Access*, vol. 7, pp. 108 647–108 659, 2019.

[33] A. A. Cervera-Uribe and P. E. Méndez-Monroy, "U19-net: A deep learning approach for obstacle detection in self-driving cars," *Soft Computing*, vol. 26, no. 11, pp. 5195–5207, 2022.

[34] Y. Zhao, B. Deng, C. Shen, Y. Liu, H. Lu, and X.-S. Hua, "Spatio-temporal autoencoder for video anomaly detection," in *Proceedings of the 25th ACM International Conference on Multimedia*, ser. MM '17, Mountain View, California, USA: Association for Computing Machinery, 2017, 1933–1941.

[35] Y. Hu, A. Qu, and D. Work, "Detecting extreme traffic events via a context augmented graph autoencoder," *ACM Trans. Intell. Syst. Technol.*, 2022.

[36] J. Wiederer, A. Bouazizi, M. Troina, U. Kressel, and V. Belagiannis, "Anomaly detection in multi-agent trajectories for automated driving," in *Proceedings of the 5th Conference on Robot Learning*, A. Faust, D. Hsu, and G. Neumann, Eds., ser. Proceedings of Machine Learning Research, vol. 164, PMLR, 2022, pp. 1223–1233.

[37] Y. Guo, W. Liao, Q. Wang, L. Yu, T. Ji, and P. Li, "Multidimensional time series anomaly detection: A gru-based gaussian mixture variational autoencoder approach," in *Proceedings of The 10th Asian Conference*

on Machine Learning, J. Zhu and I. Takeuchi, Eds., ser. Proceedings of Machine Learning Research, vol. 95, PMLR, 2018, pp. 97–112.

[38] Y. Fan, G. Wen, D. Li, S. Qiu, M. D. Levine, and F. Xiao, "Video anomaly detection and localization via gaussian mixture fully convolutional variational autoencoder," *Computer Vision and Image Understanding*, vol. 195, p. 102 920, 2020.

[39] C. S. Wickramasinghe, K. Amarasinghe, D. L. Marino, C. Rieger, and M. Manic, "Explainable unsupervised machine learning for cyber-physical systems," *IEEE Access*, vol. 9, pp. 131 824–131 843, 2021.

[40] D. L. Marino, C. S. Wickramasinghe, and M. Manic, "An adversarial approach for explainable ai in intrusion detection systems," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 3237–3243.

[41] D. L. Marino, C. S. Wickramasinghe, C. G. Rieger, and M. Manic, "Self-supervised and interpretable anomaly detection using network transformers," *ArXiv*, vol. abs/2202.12997, 2022.

[42] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Generation Computer Systems*, vol. 115, pp. 619–640, 2021.