COMPUTOLOGY: Journal of Applied Computer Science and Intelligent Technologies
Volume 2, Issue 2, Jul-Dec 2022, pp. 54-57
DOI: 10.17492/computology.v2i2.2206
https://www.journalpressindia.com/cjacsit

CNN-Based Anomaly Detection in Complex Systems

Sneha Mishra and Manoj Kumar***

ABSTRACT

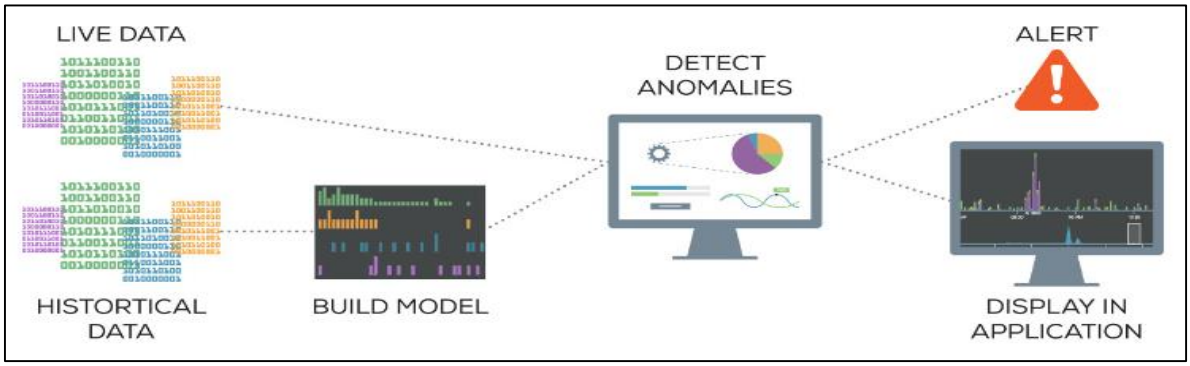
Anomaly detection is an approach used in the field of Machine learning which aims to identify the abnormal patterns. This is the vast developing area with respect to various domains such as cyber security, healthcare, fraud detection, etc. This research paper provides a comprehensive study of CNN based architecture for anomaly detection used in the complex systems. This examines and explores the machine learning approaches of CNN in reference to anomaly detection. The paper also highlights the real time applications and the challenging issues of anomaly detection. The paper further focuses on the understanding of CNN architecture and the future advancements of the vital field.

Keywords: CNN-architecture; Anomaly detection; Machine learning; Computer vision; Complex system.

1.0 Introduction

Anomaly detection [1] is the vital area of computer vision and machine learning that identifies the unusual patterns in the data. Convolutional Neural Networks (CNN) [2] is a highly effective approach which was earlier designed for the image analysis, such as medical images, industrial quality control, fraud detection and many more. The organization of the paper includes the understanding of anomaly detection, applications of CNN based anomaly detection, real-time applications areas of anomaly detection, the challenging issues of anomaly detection. Further the paper depicts the methodology, how CNN detects anomaly in complex system followed by the conclusion and the future scope.

Figure 1: Anomaly Detection Alert in Complex System



**Corresponding author; School of Engineering and Technology, Noida International University, Greater Noida, Uttar Pradesh, India (E-mail: snehariet@gmail.com)*
***Manav Rachna University, Faridabad, Haryana, India (E-mail: manojattri003@gmail.com)*

1.1 Anomaly detection

Anomaly detection [7], also known as outlier detection, is the process of identifying data points that deviate significantly from the expected or normal behavior of a system or dataset. It is a critical task in various industries to detect anomalies that may indicate faults, fraud, defects, or rare events [5]. Anomalies are often rare, making them challenging to identify using traditional methods. Figure 1 depicts the complex data which is live data and the historic data, detecting the anomalies.

2.0 Applications of CNN-Based Anomaly Detection

Anomaly detection is considered to be a very important task for the various application areas such as healthcare, defence, agriculture and many more. It is routinely applied in various real-time application areas such as public safety, military target detection, infected trees detection, rare mineral detection, etc.

Anomaly detection using CNNs has found applications in a wide range of fields

- Cybersecurity: Detecting unusual network traffic patterns that may indicate cyber attacks.
- Finance: Detecting fraudulent transactions or unusual trading behavior.
- Environmental Monitoring: Identifying anomalies in satellite images for disaster detection.

Table 1: Real-time Applications of the Anomaly Detection with their Respective Descriptions

Real-time applications	Description
Cybersecurity	Detecting unauthorized access to computer networks or abnormal user behavior that may indicate a cyberattack.
Fraud Detection	Recognizing fraudulent transactions in finance, such as credit card fraud, identity theft, or insurance fraud.
Healthcare	Identifying abnormal medical conditions or diseases in patient data, such as detecting anomalies in X-rays, MRIs, or ECGs. Monitoring patient health in real-time to detect sudden changes or deteriorations.
Manufacturing and Quality Control	Ensuring product quality by identifying defects in manufacturing processes. Detecting anomalies in sensor data from industrial machinery to predict equipment failures and prevent downtime.
Network Monitoring	Identifying anomalies in IoT (Internet of Things) sensor data for predictive maintenance.
Energy Management	Detecting energy theft or meter tampering.
Environmental Monitoring	Identifying unusual behavior in wildlife tracking data for ecological research
Log and Event Analysis	Analyzing logs and event data in IT systems to detect anomalies that may indicate security breaches or system failures. Monitoring server and application logs for performance anomalies.
Anomaly Detection in Images and Videos	Identifying unusual objects or behaviors in surveillance videos for security and safety applications. Detecting defects in manufacturing products using visual inspection systems.
Agriculture	Detecting anomalies in crop health and growth patterns using satellite imagery or drones. Monitoring soil conditions and irrigation systems for abnormalities.
Finance and Stock Market	Detecting anomalies in financial statements or accounting data for auditing purposes
Human Resources	Detecting employee behavior anomalies, such as suspicious login activities or timecard fraud. Identifying unusual patterns in employee performance or productivity metrics.
Customer Support and Feedback	Analyzing customer feedback and support ticket data to detect unusual or highly negative customer experiences.

The various real time applications described in Table 1 leads to the challenges for various researchers to figure out the best possible methods of anomaly detection in near future. The research paper also identifies the CNN architecture for the anomaly detection.

3.0 Challenging Issues for Anomaly Detection

Anomaly detection is the most efficient domain to many complex systems. Prior to studying the application areas of anomaly detection, the author came across various challenging issues of anomaly detection which are described as follows:

1. Many advanced models, such as deep learning models, lack interpretability, making it difficult to explain why an anomaly was flagged.
2. Anomaly Definition: Defining what constitutes an anomaly can be subjective and context-dependent. Anomalies may change based on different perspectives or problem domains, making it challenging to establish a universal definition.
3. Labeling Anomalies: Obtaining labeled anomaly data for model training can be expensive and time-consuming. In some cases, it may be challenging to precisely label anomalies, especially when dealing with subtle or novel types of anomalies.
4. False Positives: Avoiding false positives is crucial, especially in applications like cybersecurity and fraud detection. A high false positive rate can lead to unnecessary alerts and decreased trust in the system.

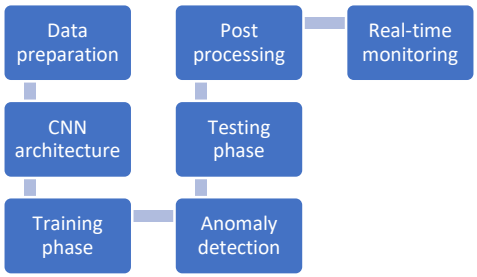
To overcome the challenges author explores the CNN architecture to get the better and efficient method to detect anomaly in various complex systems.

4.0 Methodology

By combining supervised and unsupervised learning approaches the false positive can be improved in case of anomaly detection but, CNN architecture can enhance the study of abnormal patterns with much effective rate. The paper focuses on the steps shown in figure 2, described as follows:

a. Data preparation: data preparation includes data collection and data processing.
b. CNN architecture: this consists of the steps feature extraction and the reconstruction, for anomaly detection autoencoders and variational autoencoders are applied for efficient functioning. Prior to this pretrained CNN models are applied to transfer learning.
c. Training: first train the CNN on the normal data to learn the patterns and then loss function should encourage the model to reconstruct the normal data while panelizing the anomalies.
d. Anomaly detection: use the trained CNN on the new scenes to detect the anomalies and for each test image, generate the prediction score by reconstruction error or the distance metrics.
e. Testing: after setting the threshold on the predicted score, evaluate the performance on the anomaly detection model to check the precision, recall metrics and evaluate the f-measure score.
f. Post processing: depending on the results we need to set the hyperparameters to improve the accuracy of the model.
g. Real-time monitoring: implement the model on any real time application to detect the anomalies after processing the images and raise alarms or take respective actions when anomalies are detected.

Figure 2: Flow Diagram for CNN-Based Anomaly Detection



5.0 Conclusion and Future Scope

The CNN-based anomaly detection is the most efficient way for the various complex systems of the real-time application areas and it overcomes the challenges such as fault positives and labeling anomalies. The author focused on all the relevant applications areas and the respective challenging issues of anomaly detection. The methodology covers the CNN based anomaly detection architecture for the better real-time monitoring system. The more efficient methods can be developed in near future by using R-CNN architecture for detection of unusual patterns in various complex real-time systems.

References

1. Ning S, Sun J, Liu C, Yi Y. Applications of deep learning in big data analytics for aircraft complex system anomaly detection. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. 2021; 235(5):923-940.
2. Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the Support of a High-Dimensional Distribution. Neural Computation, 13(7), 1443-1471.
3. Breunig, M. M., Kriegel, H. P., Ng, R. T., & Sander, J. (2000). LOF: Identifying Density-Based Local Outliers. ACM Sigmod Record, 29(2), 93-104.
4. Schubert, E., Wojdanowski, R., Zimek, A., & Kriegel, H. P. (2014). On evaluation of outlier rankings and outlier scores. Data Mining and Knowledge Discovery, 28(3), 527-582.
5. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation Forest. Proceedings of the 2008 Eighth IEEE International Conference on Data Mining, 413-422.
6. Markou, M., & Singh, S. (2003). Novelty detection: a review - part 1: statistical approaches. Signal Processing, 83(12), 2481-2497.
7. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1-58.
8. Ahmed, M., Mahmood, A. N., Hu, J., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.
9. Schlegl, T., Seeböck, P., Waldstein, S. M., Schmidt-Erfurth, U., & Langs, G. (2017). Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. International conference on information processing in medical imaging, 146-157.
10. Vincent, P., Larochelle, H., Lajoie, I., Bengio, Y., & Manzagol, P. A. (2010). Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. Journal of Machine Learning Research, 11(Dec), 3371-3408.