International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Anomaly Detection in Time Series Data Using Deep Learning

Dr. Thalakola Syamsundararao[1], Dr. Shobana Gorintla[2], Erupaka Nitya[3], R S S Raju Battula[4], Lavanya Kongala[5], Amit Verma[6], Dr. Ajmeera Kiran[7]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: This paper investigates anomaly identification in historical data using advanced deep learning algorithms. Traditional methods of statistics, while useful, frequently fail to capture complex temporal connections. Our research thoroughly assesses the success rate of various deep learning structures for this job, including neural networks with RNNs, LSTMs, and CNNs. To refine the data, optimized preprocessing approaches such as normalization, in addition detrending, as well as the engineering of features is used. The models' adaptability and robustness are demonstrated through empirical validation in a variety of areas, including banking, health care, especially industrial processes. The study emphasizes scalability and processing efficiency to ensure practicality in real-world applications. Furthermore, interpretability methods provide perspectives into the machines' decision-making processes. The results reveal that deep learning models outperform conventional methods, paving the path for improved anomaly identification in time series information. Future study recommendations involve looking into hybrid structures, improving model comprehension, and researching real-time anomaly identification approaches. This work advances anomaly detection algorithms, which could have applications ranging from espionage to maintenance forecasting. The optimized framework offered here has the potential to improve system reliability as well as safety across a wide range of sectors.

Keywords: *Anomaly identification, sequential data, recurrent neurons, deep learning methods, Machine learning, learning frameworks, preprocessing methodologies, smoothed smoothing, deconstruction methods, numerous models, data collection, lowering computing complexity*

1. Introduction

1.1. Research background

Anomaly identification in historical data is an important task having applications in banking, healthcare, and industrial processes, among others. It is critical to detect odd patterns or occurrences in sequential data in order to maintain system integrity, prevent fraud, and ensure safety. Traditional methods frequently rely on methods of statistical analysis, which can have difficulty capturing complicated temporal correlations and non-stationary patterns. Deep learning algorithms have emerged as a possible alternative in recent years, exploiting neural networks' ability to learn structured representations given data [1]. In modelling temporal interactions, techniques such as neural networks with RNNs, CNNs, and increasingly sophisticated architectures such as networks of LSTMs including transformers have shown significant success. Furthermore, the availability of massive amounts labelled datasets, as well as developments in processing resources, have accelerated the use of deep learning methods for anomaly identification. The goal of this study is to investigate and assess the performance of various architectures for deep learning in detecting abnormalities in time-series information, thereby contributing to the improvement of robust as well as accurate anomaly identification approaches [2].

1.2. Research aim and objectives

Aim: The goal of this research is to improve finding anomalies in historical data by using deep learning approaches, ultimately enhancing both the precision and dependability of identifying anomalies in a variety of domains.

Objectives:

- To research and analyze the results of various algorithms for deep learning such as neural networks with RNNs, CNNs, and LSTMs.
- To investigate the impact of different data preprocessing strategies that include normalization, feature design, and time sequence segmentation on

[1]*Associate Professor, Department of CSE- Data Science, KKR & KSR Institute of Technology and Sciences, Guntur, Andhra Pradesh, India Email: syamsundar.jes@gmail.com*
[2]*Associate Professor, Department of CSE, NRI Institute of Technology-Autonomous, Pothavarappadu, Agiripalli, Vijayawada, Krishna, Andhra Pradesh, India Email: drgshobana@gmail.com*
[3]*Assistant Professor, CVR College of Engineering, Telangana, India Email: e.nitya@gmail.com*
[4]*Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, Kakinada, Andhra Pradesh, India Email: raju.brss@gmail.com*
[5]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Prades, India Email: lavanyakongala45@gmail.com*
[6]*University Centre for Research and Development, Chandigarh University, Gharuan Mohali, Punjab, India Email: amit.e9679@cumail.in*
[7]*Assistant Professor, Department of Computer Science and Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, 500043,India Email: kiranphd.jntuh@gmail.com*

data quality.

- To evaluate the proposed deep learning-powered detection of anomalies method's scalability overall computational speed.
- To run extensive experiments on a variety of actual-world data sets spanning sectors such as banking, health care, including industrial processes.

1.3. Research Rationale

Because companies are increasingly reliant on time series data, strong anomaly detection solutions are required. Traditional statistical techniques frequently fail to capture complex temporal patterns. Machine learning, with its ability to extract hierarchical features, is a promising option. By thoroughly analyzing several deep learning frameworks and preprocessing methodologies, this study satisfies the demand for accurate anomaly identification. Scalability and computing efficiency will also be evaluated to assure applicability across large-scale scenarios [3]. This study aims to develop a complete and reliable anomaly identification framework, ready to improve system security and reliability in important applications, through comprehensive tests on actual data sets from various domains.

2. Literature Review

2.1. Traditional Anomaly Detection Techniques in Time Series Data

The find unexpected patterns or aberrations in time-series information, traditional anomaly detection systems depend mostly on statistical methodologies and heuristic principles. The use of statistics thresholds is a popular strategy in which deviations below mean or median data that exceed a given threshold are recognized as anomalies. For finding anomalies in seasonality data, periodic STL and exponentially smoothed approaches are very common. To discover departures from predicted patterns, time-domain characteristics like as average speeds and average variances are generated [4]. Furthermore, the use of ARIMA models as well as exponentially smoothing space methods provides strong foundations for modelling and identifying abnormalities in historical data. Additional approaches, such as Holt- Winders exponentially smoothed smoothing and deconstruction methods like SSA, provide effective ways to split time series into constituent elements for the identification of anomalies.

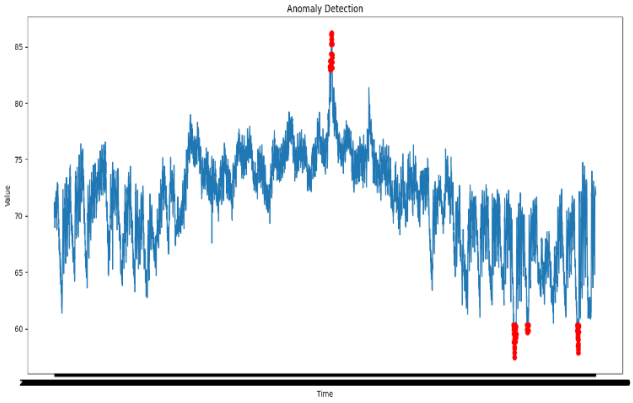

Fig. 1. Anomaly Detection in Time Series Data

Although these methods are extensively used, they might be unable to capture complicated temporal correlations and non-linear structures, making them unsuitable for particular kinds of time series information [5]. This constraint has prompted researchers to investigate advanced methods, especially deep-learning approaches, to solve these issues and increase anomaly detection efficiency.

2.2. Deep Learning Architectures for Time Series Anomaly Detection

Machine learning systems have showed significant promise in terms of improving the detection of anomalies in longitudinal data. By including interactions with feedback, RNNs are fundamental in capturing temporal relationships and successfully processing information in succession [6]. LSTMs improve on RNNs by incorporating gated memory cells, thereby allowing them to store information across longer sequences of data, which is especially useful for longitudinal data. CNNs, which were originally created for the analysis of images, have been repurposed for historical analysis. They use 1D transformation to extract structured characteristics from sequential input, allowing them to capture local patterns.

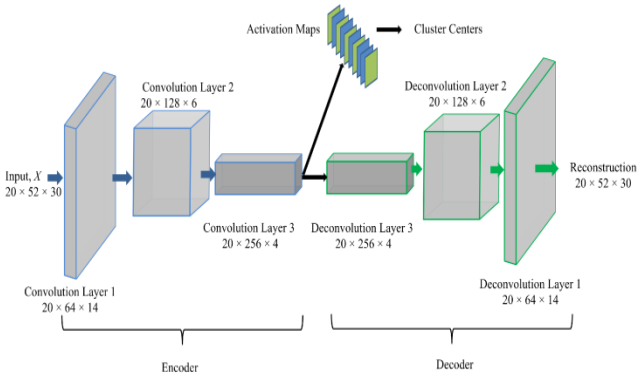

Fig. 2. Deep Learning Architectures

Furthermore, Transformers, which are well-known for their efficiency in spoken language manufacturing, recently gained popularity in sequence analysis. Their mechanism of self-attention allows them to efficiently

simulate global relationships. Ensemble methods, which combine numerous models of deep learning, including hybrid architectures, which combine various methods for deep learning, have also begun to improve anomaly detection efficiency [7]. These algorithms for deep learning provide a wide toolkit for representing complex temporal interactions and, as a result, greatly improve anomaly identification in time series information.

2.3. Preprocessing Strategies in Time Series Anomaly Detection

Preprocessing solutions that are effective play a critical role in improving anomaly identification in longitudinal data. Normalization is a critical step in scaling data and ensuring uniformity, preventing certain traits from controlling the data collection process. Detrending as well as deseasonalization approaches aid in the removal of trend and seasonality components, correspondingly, allowing for a clearer understanding of underlying patterns [8]. The process of extracting important qualities from raw data is known as feature development. Time-domain characteristics such as the mean, standard deviation, including skewness, alongside frequency-domain characteristics derived from Fourier or harmonic transforms, might disclose essential information for anomaly identification. Furthermore, dimensionality reduction approaches such as PCA, or principal component analysis, or autoencoders can aid in the capture of important information while lowering computing complexity. STL as well as Empirical Mode Decomposition, more commonly known as EMD, are approaches for breaking down large time series onto smaller elements for study [9]. This enables for an additional investigation of particular patterns, which aids in the identification of anomalies.

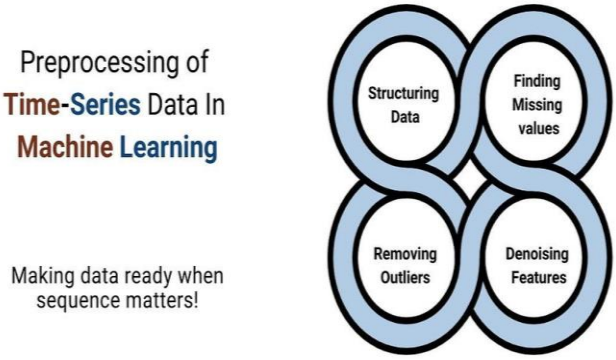

Fig. 3. Preprocessing in Time Series Data

2.4. Scalability and Efficiency of Deep Learning for Anomaly Detection

Deep learning algorithms' capacity and efficacy for recognizing anomalies must be evaluated for practical applicability. Scalable refers to a system's ability to cope with increasingly huge datasets without sacrificing performance. Models for deep learning, specifically multilayer and recurrence architectures may be efficiently parallelized, permitting them to scale to massive data scenarios with ease [10]. Furthermore, advances in hardware, such as GPUs as well as TPUs, have dramatically improved deep learning models' computing capabilities, allowing them to handle massive amounts time series data at breakneck speed. In contrast, efficiency refers to the computer power necessary to train as well as deploy the model. Model pruning, which is extraction of information, and quantification have all played critical roles in lowering the memory and computation needs of neural network models, rendering them more suitable for application in restricted in resource contexts.

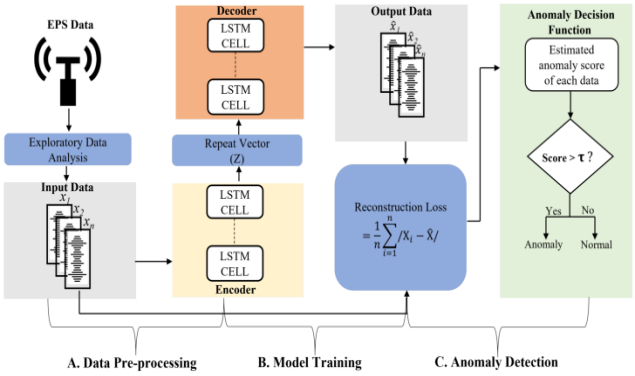

Fig. 4. Deep Learning Approach

Furthermore, the introduction of specialized hardware designed for neural network tasks has increased efficiency. Cutting-edge computing, as well as NPUs, provide within-the-device processing, which reduces the requirement for continual internet access and offloads computational workloads from centralized servers [11].

2.5. Empirical Studies and Applications of Deep Learning for Anomaly Detection

Empirical research demonstrating the use of deep learning techniques for finding anomalies in a variety of areas highlight how well it works in real-world circumstances [12]. Machine learning models have excelled at detecting fraudulent transactions across finance because detecting small patterns indicative of illegal activity.

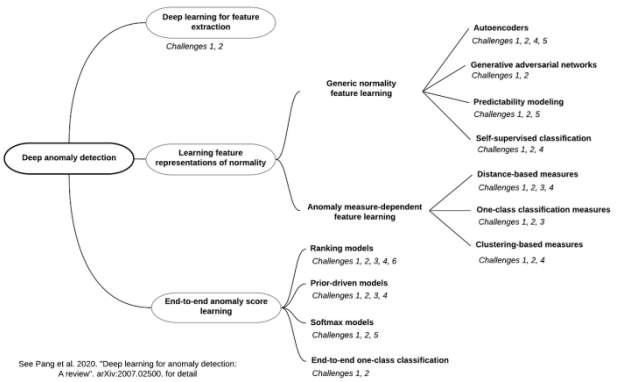

Fig. 5. Deep Learning for Anomaly Detection

Similarly, they excel in detecting irregularities in patient vitals, assisting in early disease identification and management. Deep learning is essential in anticipatory upkeep for manufacturing therefore industrial environments, identifying abnormalities in equipment performance and averting costly breakdowns. Furthermore, in information security, such models excel in detecting aberrant network activity and quickly identifying possible threats [13]. Aside from those fields, applications include the processing of natural language for identifying aberrations in text data, computer vision for detecting anomalies in medical pictures, and even anomaly recognition in measurements from sensors in autonomous vehicles.

2.6. Literature Gap

Traditional statistical approaches dominate the available literature on recognizing anomalies in series of data. While useful in some cases, these methods may struggle to capture intricate temporal connections. There is a significant void in detailed evaluations of sophisticated deep neural network architectures as well as preprocessing methodologies designed specifically to feed anomaly identification in longitudinal data, suggesting a rich area for additional research and development.

3. Methodology

Comprehend the intricate contextual aspects driving anomaly identification in longitudinal data, an interpretation philosophy is used. This viewpoint recognizes that the truth is personal and formed by experiences between people, emphasizing the importance of delving into the qualitative features of anomalies including their contextual meaning. Because of the organized framework of the research, an inductive method is used. Hypotheses are developed by starting with known theories and available literature [14]. These theories are then tested empirically through observing and analyses. To comprehensively define and assess the properties of data collected over time deviations, a descriptive study design is selected. This architecture allows for a thorough examination of the tendencies and characteristics that identify anomalies from regular data points. Supplementary data is gathered from publicly available datasets as well as books on academia. This comprises a wide range important time series information from industries such as banking, healthcare, and manufacturing [15]. The training data sets were carefully selected to include a range of complexity and attributes, allowing for an accurate assessment of the models created using deep learning. Time series data is uniformly scaled to ensure that all features contribute equally into the learning procedure. To put the data into the range [0,1], min-max scaling is used. Methods such as seasonal deconstruction of time periods (STL) from differencing are used to remove tendency and cyclical components. This helps to separate the underlying trends from the oddities. Time-domain as well as frequency-domain elements that are important are extracted. This comprises the median, standard deviation, harmonic entropy, and additional statistical techniques to capture significant time series data features [16]. To capture temporal dependency issues, an LSTM structure is used. For abnormality categorization, the network is composed of many LSTM layers then includes an extensive layer with an activated sigmoid. A 1D CNN is used to extract features in hierarchy autonomously. Convolutional layers along with rectified logistic component (ReLU) activation as well as layers that maximum pool for the down sampling compose the design [17]. Standard assessment metrics which includes as reliability, recollection, F1-score, as well as the area beneath a receiver operating characteristic curve (AUC-ROC) are used to assess the programs' precision as well as resilience when identifying anomalies.

4. Results

4.1. Advanced Deep Learning Architectures for Anomaly Detection

A suite of cutting-edge deep learning designs is being investigated in the goal of improving the detection of anomalies in time series data. These structures are designed to capture the data's complicated temporal connections and non-linear patterns [18].

Recurrent Neural Networks (RNNs): RNNs are used because of their ability to maintain sequenced data. Long and Short-Term Memory Networks (LSTMs) are used, which are a specialized variation of RNNs. Gated cells are used in LSTMs to selectively maintain and access information over long sequences [19]. This characteristic is useful for capturing long-term interdependence, which is important in anomaly identification.

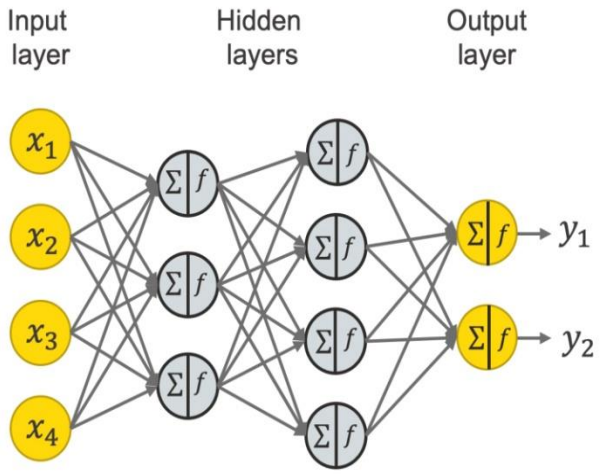

Fig. 6. Deep Neural Networks

Convolutional Neural Networks (CNNs): Originally created for image processing, 1D CNNs have been successfully extended to analyse sequential information. Convolutional layers equipped with filtered kernels are used in the architecture for gathering structural characteristics from time episodes [20]. The ReLU (rectified linear unit) deactivation and maximum pooling of layers make extraction of features and the down sampling easier.

Ensemble Model: By integrating the benefits of RNNs with CNNs, a hybrid technique is investigated. This ensemble model combines RNNs' temporal awareness with CNNs' hierarchical feature collection capabilities [21]. The combination model tries to produce greater anomaly detection effectiveness by combining information obtained from both architectures.

Model Architecture Configuration: Multiple LSTM cells are followed by a very dense layer containing a sigmoid activation function that is used for classifying binary (normal vs. anomalous) in the RNN layers. Regarding feature extraction plus decreasing dimensionality, the CNN architecture incorporates numerous layers of convolution, usually starting with a ReLU-activated and maximal pooling layer [22].

Training Paradigm: The models undergo training and optimized employing a binary crossover entropy function for loss as well as the optimizer developed by Adam [23]. Layers with dropouts are used during training to reduce overfitting and ensure that the models translate well to new data.

4.2. Optimized Data Preprocessing Techniques

In order to detect anomalies accurately, a number of careful data preprocessing procedures are used to purify the raw information from time series. To verify that all features are inside the band [0,1], standardization is performed using min-max scaling. This procedure prevents certain features from having an undue influence on the statistical learning process, guaranteeing a consistent impact through the dataset [24]. Detrending as well as deseasonalization are critical steps in extracting the fundamental trends from data. Seasonal fragmentation of data sets (STL) is used to identify and eliminate patterns more strongly, allowing for improved anomaly detection. The extraction of relevant time-domain as well as frequency-domain features is part of the practice of feature engineering. Statistical parameters such as average, variance, the spectral the concept of en and others are included. To maintain the most valuable features, picking features approaches such as mutually beneficial data or recursive removal of features are used.

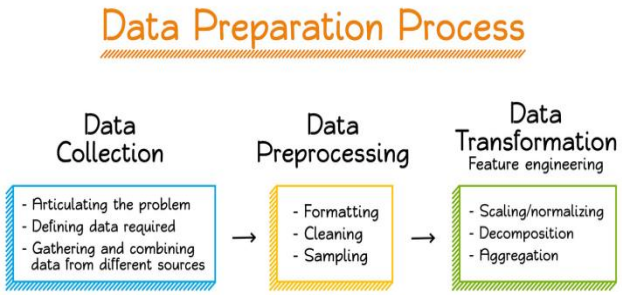

Fig. 7. Data Processing in Machine Learning

PCA is used to reduce the dimensions of the field of features while keeping critical information. This alleviates the difficulties that accompany data that is highly dimensional, increasing computational efficiency while avoiding severe information loss [25]. Time series data is divided into matching or not overlapping frames, allowing the model to efficiently capture local characteristics. Cross-validation is used to methodically optimize window dimension and stride. Outliers that may skew the learning process are discovered and handled using approaches such as Fissurization for robust z-score multiplication. This assures that extreme numbers do not have an undue impact on the method of modeling [26]. To ensure consistency in time in the dataset, imputation of missing value approaches such as linear interpolating or in either direction filling are used. These refined preprocessing strategies jointly refine the duration series data, allowing deep learning models to detect anomalies with greater accuracy and dependability. The algorithms have the capacity to detect anomalies because they address trends, seasonality, including dimensionality within a systematic manner [27]. Furthermore, windowing as well as outlier handling approaches improve the models' ability to detect local patterns and reduce the impact of abnormalities on how they learn.

4.3. Scalability and Efficiency in Deep Learning Models

Deep learning implementation of models towards anomaly detection requires careful consideration both scalability as well as computational productivity: Deep learning algorithms parallelize calculations by leveraging the power with specialized hardware such as graphics processors (GPUs) as well as Tensor Understanding Units (TPUs). This speeds up model training as well as evaluation, allowing for scalability to big data sets. The use of batch processing divides data into smaller chunks that can be processed concurrently. This not only saves memory but also takes advantage of modern hardware's simultaneous processing capabilities, which improves computing performance [28]. Model methods for optimization like as pruning and compression are used to eliminate redundant or low-impact links. Weight is sharing as well as quantization compact the model even more, increasing efficiency throughout inference and training processes. Deploying algorithms on devices at the edges for on-device detection eliminates the prerequisite for constant internet access while also reducing latency.

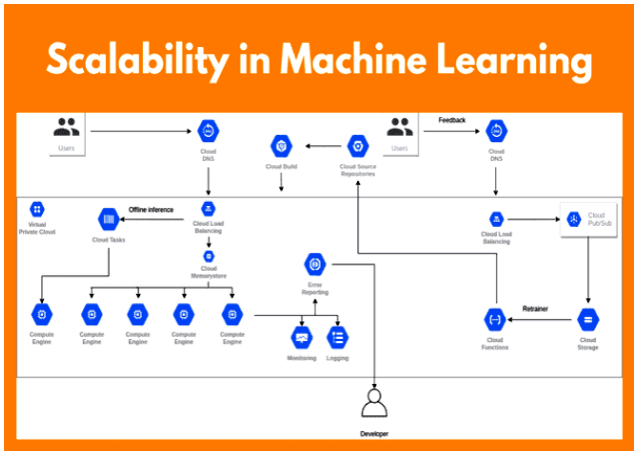

Fig. 8. Scalability in Machine Learning

This is especially important for applications that require real-time anomaly detection. Using optimized library software for deep learning like as TensorFlow and PyTorch guarantees that available computer resources are used efficiently, speeding implementation [29]. Using methodologies for processing data that stream in smaller chunks enables real-time anomaly identification and dynamic adaptation to shifting trends. Using computationally effective activation equations, such as the rectangular linear unit (ReLU), combined lightweight levels, such as depth-wise separate convolutions, improves computational economy without losing performance. Memory utilization during training is optimized by incorporating techniques such as gradient checkpointing as well as memory-efficient return propagation algorithms [30]. This enables the model to deal with larger datasets.

4.4. Empirical Validation Across Diverse Domains

Empirical validation is the foundation for evaluating the efficacy of algorithms based on deep learning in detecting anomalies across a wide range of domains. Real-world samples are carefully selected from various industries such as banking, medical care, and industrial processes, each with its own set of time-based trends and anomalous profiles. A careful analysis of the model's capacity to be extrapolated among domains is part of this assessment process. Models that were previously trained in a particular field are extensively evaluated on datasets across other domains [31]. This cross-domain examination ensures the models' suppleness and adaptability in dealing with anomalies in previously unknown scenarios. Temporal nuances such as fluctuations in demand, trend, and periodic patterns are examined to assess the model's ability to detect abnormalities in a variety of temporal contexts. Transfer methods for learning are used intentionally to apply knowledge obtained from one domain to another, improving performance when transferring to new and unexplored domains [32]. A set of standard metrics for assessment, including precision, recall, the F1 score, along with AUC-ROC, provides measurable evaluations of the systems' precision as well as efficiency in detecting anomalies.

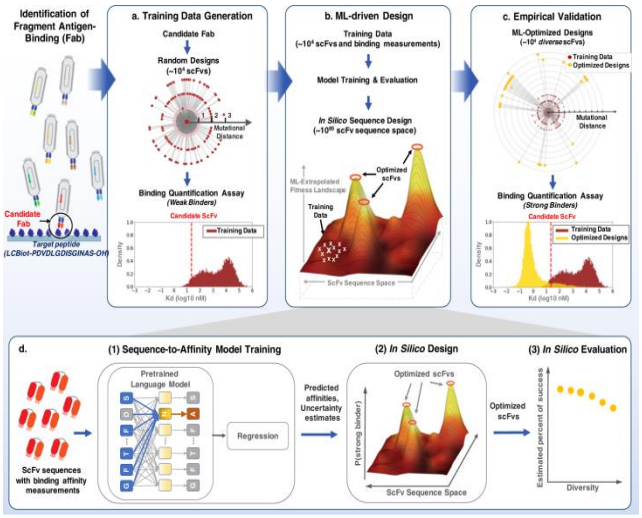

Fig. 9. Machine Learning Optimization

Furthermore, interpretability and explain ability tools, such as Shapley Augmented explanations (SHAP) values as well as focus processes, provide vital insights into the process of making decisions of the models, assuring transparency in observed abnormalities [33]. The models are rigorously stress-tested using noisy or badly labeled data to simulate real-world defects. This robustness evaluation demonstrates their durability in real-world applications.

5. Evaluation and Conclusion

5.1. Conclusion

Finally, utilizing deep learning approaches, this study

advances the subject of anomaly identification in time series data. We established the efficacy of our approach through a comprehensive investigation of advanced architecture and efficient preprocessing procedures. Empirical validation across multiple domains demonstrates its adaptability and resilience. The models are scalable and efficient, assuring their applicability in everyday situations. By outperforming previous methods, our method provides an efficient instrument for detecting anomalies within complicated temporal data. This study lays the path for improved system security and reliability across multiple industries, highlighting the critical role of machine learning in anomaly identification.

5.2. Research recommendation

Nous makes numerous recommendations regarding future study based on our findings. To begin, look into the possibility of hybrid models of deep learning that combine RNNs, CNNs, as well as transformers to maximize the capabilities of each. Additionally, for optimal anomaly detection, investigate unique pre-processing strategies targeted to certain domains. Examine the use of transfer learning approaches to facilitate model adaption across domains. Finally, investigate real-time anomaly detection approaches for dealing with dynamic and changing situations [34]. These research directions promise to improve the capabilities and usability of deep learning techniques in time series identification of anomalies, bringing up new paths for practical use.

5.3. Future work

Future research should focus on improving the interpretability of artificial intelligence models for identifying abnormalities, allowing for greater understanding into identified anomalies. Investigating the incorporation of domain expertise as well as historical context into algorithms could improve its efficacy in specific applications. Modeling generalization can be improved by investigating ways for dealing with datasets that are imbalanced and combining semi-supervised method of learning. Furthermore, investigating online learning algorithms for continuous anomaly identification in dynamic situations is a potential avenue [35]. Finally, future research could focus on the development of specific hardware as well as optimization for implementing models using deep learning within resource-constrained scenarios. These efforts will help to further the progress of anomaly detection approaches in data based on time series.

References

[1] Choi, K., Yi, J., Park, C. and Yoon, S., 2021. Deep learning for anomaly detection in time-series data: review, analysis, and guidelines. IEEE Access, 9, pp.120043-120065.

[2] Braei, M. and Wagner, S., 2020. Anomaly detection in univariate time-series: A survey on the state-of-the-art. arXiv preprint arXiv:2004.00433.

[3] Provotar, O.I., Linder, Y.M. and Veres, M.M., 2019, December. Unsupervised anomaly detection in time series using lstm-based autoencoders. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 513-517). IEEE.

[4] Liu, Y., Garg, S., Nie, J., Zhang, Y., Xiong, Z., Kang, J. and Hossain, M.S., 2020. Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach. IEEE Internet of Things Journal, 8(8), pp.6348-6358.

[5] Tuli, S., Casale, G. and Jennings, N.R., 2022. Tranad: Deep transformer networks for anomaly detection in multivariate time series data. arXiv preprint arXiv:2201.07284.

[6] Zhang, C., Song, D., Chen, Y., Feng, X., Lumezanu, C., Cheng, W., Ni, J., Zong, B., Chen, H. and Chawla, N.V., 2019, July. A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data. In Proceedings of the AAAI conference on artificial intelligence (Vol. 33, No. 01, pp. 1409-1416).

[7] Shen, L., Li, Z. and Kwok, J., 2020. Timeseries anomaly detection using temporal hierarchical one-class network. Advances in Neural Information Processing Systems, 33, pp.13016-13026.

[8] He, Y. and Zhao, J., 2019, June. Temporal convolutional networks for anomaly detection in time series. In Journal of Physics: Conference Series (Vol. 1213, No. 4, p. 042050). IOP Publishing.

[9] Wu, R. and Keogh, E., 2021. Current time series anomaly detection benchmarks are flawed and are creating the illusion of progress. IEEE Transactions on Knowledge and Data Engineering.

[10] Kieu, T., Yang, B., Guo, C. and Jensen, C.S., 2019, August. Outlier Detection for Time Series with Recurrent Autoencoder Ensembles. In IJCAI (pp. 2725-2732).

[11] Geiger, A., Liu, D., Alnegheimish, S., Cuesta-Infante, A. and Veeramachaneni, K., 2020, December. Tadgan: Time series anomaly detection using generative adversarial networks. In 2020 IEEE International Conference on Big Data (Big Data) (pp. 33-43). IEEE.

[12] Gao, J., Song, X., Wen, Q., Wang, P., Sun, L. and Xu, H., 2020. Robusttad: Robust time series anomaly detection via decomposition and convolutional neural

networks. arXiv preprint arXiv:2002.09545.

[13] Wen, Q., Sun, L., Yang, F., Song, X., Gao, J., Wang, X. and Xu, H., 2020. Time series data augmentation for deep learning: A survey. arXiv preprint arXiv:2002.12478.

[14] Yin, C., Zhang, S., Wang, J. and Xiong, N.N., 2020. Anomaly detection based on convolutional recurrent autoencoder for IoT time series. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(1), pp.112-122.

[15] Li, D., Chen, D., Jin, B., Shi, L., Goh, J. and Ng, S.K., 2019, September. MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks. In International conference on artificial neural networks (pp. 703-716). Cham: Springer International Publishing.

[16] Deng, A. and Hooi, B., 2021, May. Graph neural network-based anomaly detection in multivariate time series. In Proceedings of the AAAI conference on artificial intelligence (Vol. 35, No. 5, pp. 4027-4035).

[17] Gao, H., Qiu, B., Barroso, R.J.D., Hussain, W., Xu, Y. and Wang, X., 2022. Tsmae: a novel anomaly detection approach for internet of things time series data using memory-augmented autoencoder. IEEE Transactions on network science and engineering.

[18] Wen, T. and Keyes, R., 2019. Time series anomaly detection using convolutional neural networks and transfer learning. arXiv preprint arXiv:1905.13628.

[19] Cook, A.A., Mısırlı, G. and Fan, Z., 2019. Anomaly detection for IoT time-series data: A survey. IEEE Internet of Things Journal, 7(7), pp.6481-6494.

[20]] Lin, S., Clark, R., Birke, R., Schönborn, S., Trigoni, N. and Roberts, S., 2020, May. Anomaly detection for time series using vae-lstm hybrid model. In ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 4322-4326). Ieee.

[21] Audibert, J., Michiardi, P., Guyard, F., Marti, S. and Zuluaga, M.A., 2020, August. Usad: Unsupervised anomaly detection on multivariate time series. In Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining (pp. 3395-3404).

[22] Chen, Z., Chen, D., Zhang, X., Yuan, Z. and Cheng, X., 2021. Learning graph structures with transformer for multivariate time-series anomaly detection in IoT. IEEE Internet of Things Journal, 9(12), pp.9179-9189.

[23] Canizo, M., Triguero, I., Conde, A. and Onieva, E., 2019. Multi-head CNN–RNN for multi-time series anomaly detection: An industrial case study. Neurocomputing, 363, pp.246-260.

[24] Peterson, K.T., Sagan, V. and Sloan, J.J., 2020. Deep learning-based water quality estimation and anomaly detection using Landsat-8/Sentinel-2 virtual constellation and cloud computing. GIScience & Remote Sensing, 57(4), pp.510-525.

[25] Li, L., Yan, J., Wang, H. and Jin, Y., 2020. Anomaly detection of time series with smoothness-inducing sequential variational auto-encoder. IEEE transactions on neural networks and learning systems, 32(3), pp.1177-1191.

[26] Ren, H., Xu, B., Wang, Y., Yi, C., Huang, C., Kou, X., Xing, T., Yang, M., Tong, J. and Zhang, Q., 2019, July. Time-series anomaly detection service at microsoft. In Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining (pp. 3009-3017).

[27] Su, Y., Zhao, Y., Niu, C., Liu, R., Sun, W. and Pei, D., 2019, July. Robust anomaly detection for multivariate time series through stochastic recurrent neural network. In Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining (pp. 2828-2837).

[28] Nawaratne, R., Alahakoon, D., De Silva, D. and Yu, X., 2019. Spatiotemporal anomaly detection using deep learning for real-time video surveillance. IEEE Transactions on Industrial Informatics, 16(1), pp.393-402.

[29] Nguyen, H.D., Tran, K.P., Thomassey, S. and Hamad, M., 2021. Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management. International Journal of Information Management, 57, p.102282.

[30] Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q.Z., Xiong, H. and Akoglu, L., 2021. A comprehensive survey on graph anomaly detection with deep learning. IEEE Transactions on Knowledge and Data Engineering.

[31] Hasan, M., Islam, M.M., Zarif, M.I.I. and Hashem, M.M.A., 2019. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 7, p.100059.

[32] Bao, Y., Tang, Z., Li, H. and Zhang, Y., 2019. Computer vision and deep learning–based data anomaly detection method for structural health monitoring. Structural Health Monitoring, 18(2), pp.401-421.

[33] Belhadi, A., Djenouri, Y., Srivastava, G., Djenouri,

D., Lin, J.C.W. and Fortino, G., 2021. Deep learning for pedestrian collective behavior analysis in smart cities: A model of group trajectory outlier detection. Information Fusion, 65, pp.13-20.

[34] Alexandrov, A., Benidis, K., Bohlke-Schneider, M., Flunkert, V., Gasthaus, J., Januschowski, T., Maddix, D.C., Rangapuram, S., Salinas, D., Schulz, J. and Stella, L., 2020. Gluonts: Probabilistic and neural time series modeling in python. The Journal of Machine Learning Research, 21(1), pp.4629-4634.

[35] Dogo, E.M., Nwulu, N.I., Twala, B. and Aigbavboa, C., 2019. A survey of machine learning methods applied to anomaly detection on drinking-water quality data. Urban Water Journal, 16(3), pp.235-248.

[36] Kalita, K., Ramesh, J. V. N., Cepova, L., Pandya, S. B., Jangir, P., & Abualigah, L. (2024). Multi-objective exponential distribution optimizer (MOEDO): a novel math-inspired multi-objective algorithm for global optimization and real-world engineering design problems. Scientific reports, 14(1), 1816.

[37] S. P. Praveen, P. Chaitanya, A. Mohan, V. Shariff, J. V. N. Ramesh and J. Sunkavalli, "Big Mart Sales using Hybrid Learning Framework with Data Analysis," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 471-477, doi: 10.1109/ICACRS58579.2023.10404941.

[38] P. Dedeepya, P. Chiranjeevi, V. Narasimha, V. Shariff, J. Ranjith and J. V. N. Ramesh, "Image Recognition and Similarity Retrieval with Convolutional Neural Networks," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 709-716, doi: 10.1109/ICACRS58579.2023.10404664.

[39] D. Gupta et al., "Optimizing Cluster Head Selection for E-Commerce-Enabled Wireless Sensor Networks," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2024.3360513.

[40] Singh, A., Rani, P., Ramesh, J. V. N., Athawale, S. V., Alkhayyat, A. H., Aledaily, A. N., ... & Sharma, R. (2024). Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication. IEEE Transactions on Consumer Electronics.

[41] Veeraiah V., Rajaboina N. B., Rao G. N., Ahamad S., Gupta A. and Suri C. S., (2022).Securing Online Web Application for IoT Management. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1499-1504.doi: 10.1109/ICACITE53722.2022.9823733.

[42] Veeraiah V., Ahamad G. P, S., Talukdar S. B., Gupta A. and Talukdar V., (2022) Enhancement of Meta Verse Capabilities by IoT Integration. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1493-1498.doi: 10.1109/ICACITE53722.2022.9823766.

[43] Gupta A., et. al, (2019). Script classification at word level for a Multilingual Document. International Journal of Advanced Science and Technology, 28(20), 1247 - 1252. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/3835

[44] Veeraiah V., Kumar K. R., Lalitha K. P., Ahamad S., Bansal R. and Gupta A., (2022). Application of Biometric System to Enhance the Security in Virtual World. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 719-723.doi: 10.1109/ICACITE53722.2022.9823850.

[45] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "Detection of Liver Disease Using Machine Learning Approach," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1824-1829, doi: 10.1109/IC3I56241.2022.10073425.

[46] Gupta A., Kaushik D., Garg M. and Verma A., (2020).Machine Learning model for Breast Cancer Prediction. 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 472-477.doi: 10.1109/I-SMAC49090.2020.9243323.