Comprehensive Survey on Detection of Anomalies in Edge Computing Network and Deep Learning Solutions

Sonali Jadhav[1][a] and Dr. Arun Kulkarni[2][b]
[1]Department of Computer Engineering, Thadomal Shahani Engineering College, University of Mumbai, Mumbai, India
[2]Department of Information Technology, Thadomal Shahani Engineering College, University of Mumbai, Mumbai, India

Keywords: Edge Computing, Deep Learning, Edge Network Anomalies, DNN, GAN.

Abstract: Edge computing is an innovative computing model that plays an essential role in offering faster computation, increased security, and lower transfer costs to the production applications that run on collection of IoT devices, sensors, and the network. Today, IoT has become extensively utilized technology in a variety of applications, including medical, industrial, agriculture, transport, manufacturing, surveillance and so on. Edge computing involves processing a variety of data closer to its source, allowing for faster processing rates over the large volumes and more effective outcomes in real time. However, with the increasing number and complexity of IoT devices in Edge networks, as well as the never-ending accumulation of network data, monitoring in Edge networks and identifying abnormal network behavior is getting increasingly challenging. Anomaly detection is a significant issue that has received extensive attention across all range of disciplines and application do-mains. Deep Learning is a branch of machine learning that deals with approaches inspired by the structure and function of artificial neural networks which can be used to solve many real-world problems. The objective of this research paper is to survey and illuminate the role of deep learning techniques in tackling the edge computing anomalies and provides an extensive overview on deep Learning techniques used for detecting them. The research work also covers the case study on anomaly detection over edge computing using deep neural network (DNN) and generative adversarial network (GAN) models.

1 INTRODUCTION

The Internet of Things (IoT) consists of large number of small devices or networks of sensors that continuously generate large volumes of data. Due to the limited computing and memory capabilities, raw data is typically sent to centralized systems or the cloud for analysis. Later, machine learning (ML) and deep learning (DL) algorithms could be deployed on edge devices, making it possible to bring intelligence to the Internet of Things [28].

In Edge computing platform, various anomalies are existing and represent a significant threat to the security, performance, and reliability of communication networks. The process of monitoring business networks for unusual behavior is known as network behavior anomaly detection [1]. As is widely recognized, flows make up the data that is sent through a network. There is always a temporal link between flows, and anomalous traffic in the network is no different [2]. Anomalies can arise from various sources including malicious attacks, software bugs, misconfigurations, and hardware failures.

Traditional anomaly detection methods such as rule-based systems, statistical analysis, and machine learning algorithms have limitations in effectively identifying and mitigating these anomalies due to their static nature and inability to adapt to evolving threats, with the advent of deep learning techniques, there has been a paradigm shift in anomaly detection approaches. The ability of deep learning algorithms to automatically derive hierarchical representations from raw data, have shown promising results in detecting complex and previously unseen network anomalies. Deep learning uses a

complicated architecture or combination of non-linear transformations to achieve high level

[a] https://orcid.org/0009-0001-3731-3823
[b] https://orcid.org/0009-0008-7699-8272

Jadhav, S. and Kulkarni, A.
Comprehensive Survey on Detection of Anomalies in Edge Computing Network and Deep Learning Solutions.
DOI: 10.5220/0013344100004646

In *Proceedings of the 1st International Conference on Cognitive & Cloud Computing (IC3Com 2024)*, pages 37-45
ISBN: 978-989-758-739-9

abstractions in data [3]. Therefore, this survey aims to provide a comprehensive overview of network anomalies and the application of deep learning for their detection and mitigation. The objective of this research paper is to recognize the behavioral patterns of various network anomalies in regards to the environments in which they exist, determine the different types of network anomalies exists in the edge computing network, contrasting over the different edge computing network anomalies and suitable deep learning techniques, proposing the common architecture for data modelling using deep learning and detection of edge anomalies using deep learning techniques and finally proposing a case study on anomaly detection in medical applications over the edge network.

2 RELATED WORK

There is limited literature on implementations of edge computing anomaly detection using deep learning is available. Some of the important aspects in the literature are explained as follows.

Shagufta Mehnaz Elisa Bertino [30], has explained six categories of malicious attacks: Brute Force, Denial-of-service (DoS), Web Attacks, Infiltration, Botnet, and Distributed denial-of-service (DDoS). To detect anomalies authors have explained deep neural network (DNN), convolutional neural network (CNN), recurrent neural network (RNN) techniques. Ahmed Dawoud, Seyed Shahristani, Chun Raun [31] has proposed a model that uses an autoencoder (AE) to identify samples exhibiting anomalous behavior; an attack classifier is then employed to categories anomalies according to the sort of attack they represent. Daniel Alejandro, Oscar Augusto et al [32] has proposed the rule-based neural network model with supervised machine learning technique to perform optimal detection of any type of network anomalies over Network Intrusion Detection (NIDS). Zeyuan Fu [33] has proposed the rule-based neural network model with supervised machine learning technique to perform optimal detection of any type of network anomalies over Network Intrusion Detection (NIDS). Yuhuai Peng, Aiping Tan, Jingjing Wu, Yuanguo Bi [34] has proposed Conceptual frameworks of three main deep anomaly detection approaches like Feature Extraction, Learning Feature Representations of Normality, and End-to-end Anomaly Score Learning. Mohab Sameh, Abdel-Wahab et al. [35] has explained the different machine learning and deep learning approaches that can be used to detect network anomalies in Intrusion Detection Systems. Haolong Xiang & Xuyun Zhang[36] has proposed IDForest, and IoT- based edge computing-powered anomaly detection framework that uses insertion and deletion strategies to update the tree structure of data.

3 METHODOLOGY

The methodology for proposed survey covers the following aspects of solutions.

3.1 Edge Computing Network Anomalies

Due to the distinctive features and difficulties of distributed computing at the network edge, edge computing is susceptible to network anomalies. The primary contribution is the recommendation of an edge computing architecture that can do anomaly detection in multiple sources at numerous ends [4].

3.1.1 Communication Failures:

Due to unstable network connections or interference, edge devices and nodes may occasionally have connectivity problems or communication failures. These errors might obstruct the flow of data and cause service interruptions. Network Instability is also one of the reasons for Communication Failure. It is essential to build the edge network with redundancy, prioritize key data, maximize network capacity, implement strong error handling and recovery mechanisms, and often monitor and maintain the network architecture to reduce these communication failures. when one node fails, there could be

cascading failures that have a negative influence on the service's delivery and make it impossible to achieve certain goals [5].

3.1.2 Latency Spikes:

Latency spikes in edge computing refer to sudden and significant increases in the time it takes for data to travel between edge devices and the processing or storage resources. These spikes can have several causes and can negatively impact the performance and responsiveness of edge applications. Edge computing includes processing data nearer to the data source, at the network edge. However, latency spikes can cause delays in data processing and response times due to a lack of computing resources or congestion in the edge network.

3.1.3 Scalability Issues:

Scalability issues can occur in edge computing due to

various factors like Growing Number of Edge Devices, Increased Data Volume, Resource Limitations, Data Synchronization and Consistency, Dynamic Edge Environment, Network Capacity. Edge computing systems must scale dynamically in response to shifting workload needs. When the system struggles to handle abrupt increases in workload or fails to allocate resources effectively, anomalies might occur if the network architecture or edge nodes are not appropriately setup for scalability.

3.1.4 Edge Network Congestion:

Edge computing edge network congestion difficulties can emerge for a variety of reasons. Here are some major causes of edge network congestion- Increased Data Traffic, Bandwidth Limitations, Network Infrastructure Bottlenecks, Inefficient Routing, Bursty Traffic congestion, which can result in performance deterioration, increased latency, and packet loss. There are several strategies that can be used to deal with edge network congestion concerns.

3.1.5 Resource Constraints:

Resource constraint issues can arise in edge computing due to several factors inherent to the edge environment like Power Limitations, Limited Computational Power, Storage Capacity, Memory Constraints, Storage Capacity, Network Bandwidth, Heterogeneous Hardware, Scalability Challenges. The compute, memory, and energy resources of edge devices are frequently constrained. When these resources are used up or improperly maintained, anomalies can develop that affect the edge network's overall performance.

3.1.6 Edge infrastructure Failures:

Edge infrastructure failures can occur in edge computing due to various factors such as Power Outages, Network Connectivity Issues, Hardware Failures, Software and Firmware Issues, Environmental Factors, Insufficient Capacity, Edge computing depends on the edge servers, routers, switches, and other networking hardware that make up the network edge. Anomalies can happen because of hardware malfunctions, power outages, or environmental variables, which can cause service interruptions or total system failure.

3.1.7 Edge infrastructure Failures:

Edge node overload issues can occur in edge computing due to several factors such as resource constraints, high workload demand, sudden spikes in data or user activity, Inefficient task scheduling, Insufficient load balancing, Device mobility, Inadequate scalability planning. Compared to centralized servers, edge nodes' processing power is constrained. An edge node may get overloaded if the workload is greater than its capacity, which could lead to performance patterns, Resource Contentions. Edge networks degradation and service disruptions.

3.3 Deep Learning Techniques

Anomaly detection methods using deep learning fall into three categories: super-vised, hybrid, and unsupervised [29]. The labels in the dataset mostly determine the appropriate anomaly detection technique. Applying deep learning techniques to anomaly detection has several benefits. First and foremost, these strategies are in-tended to handle multivariate and highly dimensional data. This eliminates the need to model anomalies independently for each variable and average the results, making it easier to integrate data from several sources. The classification of various deep learning methods is shown in Fig. 1.

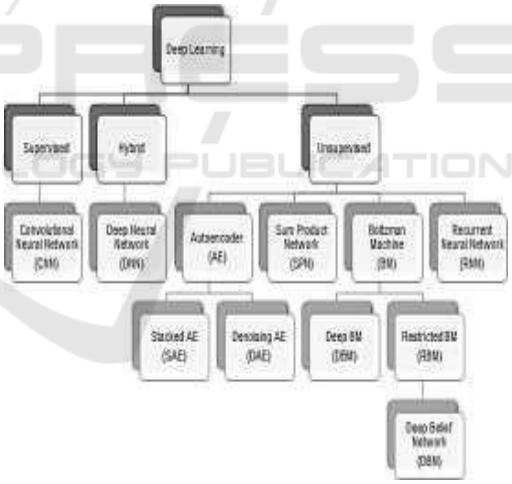


Figure 1: Classification of Deep learning method.

Performance is yet another benefit. Deep learning techniques provide the chance to model intricate, nonlinear relationships inside data and use these interactions for the task of anomaly identification. Deep learning models are excellent for situations involving large amounts of data because their performance may scale as relevant training data become available. Deep learning uses a complicated architecture or combination of non-linear transformations to achieve high level abstractions in data [3]. Table 1 represents different deep anomaly detection (dad) techniques.

Metho	Superv
	ised
	Unsup
	ervised
Applicati	Hybrid
	Model
	Fraud Detection
	Medical Anomaly
	Detection Internet of
	Things (IoT)
	Industrial Damage
	Detection Big-data

Beyond specifying generic hyper parameters (number of layers, units per layer, etc.), deep learning approaches are also well- suited to jointly modeling the interactions between multiple variables with respect to a given task. Deep learning models only need minor tuning to produce effective results. The different Deep Anomaly Detection techniques are listed in Table 1.

In edge computing contexts, network anomalies can be detected using deep learning techniques. Here are several methods that are frequently used:

3.3.1 Recurrent Neural Networks (RNNs)

RNNs, LSTM networks with long short-term memory, are excellent at analyzing sequential data. RNNs can examine time- series data from edge devices and nodes in the context of edge computing to find anomalies in network traffic, resource usage, or other performance parameters. An extension of a traditional feed-forward neural network is the recurrent neural network (RNN). RNNs are effective for simulating sequences because they have cyclic connections; unlike feed forward neural networks [3],[8]. The RNN-IDS model enhances intrusion detection accuracy and offers a fresh approach to intrusion detection research [9].

3.3.2 Generative Adversarial Networks (GANs):

GANs can be used to discover the distribution of typical network edge behavior. While the discriminator network distinguishes between real and created data, the generator network is trained to produce artificial normal data. By evaluating the discriminator's capacity to categorize fresh data samples, anomalies can be found. Researchers are dedicated to correctly and effectively identifying aberrant photos in real-world applications and use them in the field of anomaly detection [10].

3.3.3 Autoencoders

Autoencoders can be used to figure out how network traffic typically behaves or how resources are used at the edge. The autoencoder can reconstruct and compare new data instances by being trained on regular data. Recently, a deep learning technique utilizing Autoencoder (AE) models has gained acceptance for locating inappropriate characteristics present in the huge network traffic samples [11]-[14].

3.3.4 Attention Mechanisms

Deep learning models can incorporate attention mechanisms to concentrate on facets or time intervals of network input. Attention mechanisms can increase the accuracy of anomaly detection in edge computing environments by drawing attention to important features or trends [15]. Neural networks can digest input data while dynamically focusing on pertinent portions of it through attention processes.

3.3.5 Variational Autoencoders (Vaes)

The VAEs are used in edge computing to capture the distribution of network activity and resource usage. Variational autoencoders (VAEs) are generative deep learning models that can process a wide range of data types, including images and text. VAEs represent neural networks' posteriors and frequently beat autoencoders and one-class support vector machines in recognizing unknown threats [16- 18].

3.3.6 Reinforcement learning (RL)

Reinforcement learning has Deep Q- Networks (DQNs) method that enhances the network administration and detects the edge anomalies. For improving the efficiency and security of edge infrastructure, the RL agents are trained to allocate resources, route traffic, and respond to the anomalies. The Reinforcement learning supports variety of patterns and data formats, including text and images and used to address the issues related to resource allocation [19].

3.3.7 Graph Neural Networks (GNNs)

GNNs can identify abnormalities based on graph patterns or irregularities in the edge network topology by modelling the relationships and interactions between edge devices, nodes, and their properties. The suitable deep learning technique must be chosen based on the unique properties of the edge network

data, the kinds of anomalies to be found, and the resources and computational power available at the edge devices or nodes. Anomaly detection in edge computing environments can also be improved by combining various approaches or hybrid methods with conventional machine learning algorithms.

3.3.8 Convolutional Neural Networks (CNNs)

CNNs can be used to examine data gathered from edge nodes about network traffic. CNNs can learn to recognize patterns and anomalies in network traffic by considering it as a sequential data stream or a time-series, assisting in the identification of anomalous behavior or assaults. The Convolutional Neural Network (CNN) uses these fixed-size feature matrices to detect insider threat after converting the retrieved characteristics into them [7]. For applications like image identification, object detection, and image segmentation, CNNs are quite effective.

4 ARCHITECTURE FOR DATA MODELLING USING DEEP LEARNING

The architecture for data modeling using deep learning poses various stages. The block diagram for anomaly detection and forecasting using deep learning using various stages is shown in Fig. 2. The diagram illustrates the various components and steps involved in the process.

Figure 2: Model for anomaly detection using deep learning algorithms.

The different stages used in the above model are explained as follows:

Data Collection: The process starts with the collection of datasets from various sources, including real-time transactions, credit card uses patterns, and merchant transactions.

Preprocessing: To prepare for model training, the obtained data is pre- processed, which includes cleaning, normalization, and feature extraction.

Feature Selection: This stage entails picking the most relevant characteristics from the pre-processed data to serve as input for the deep learning models.

Model Training: Deep learning models, such as LSTM, Autoencoder, LSTM- Autoencoder, Transformer, and GAN, are trained on the selected features to learn the patterns and relationships in the data.

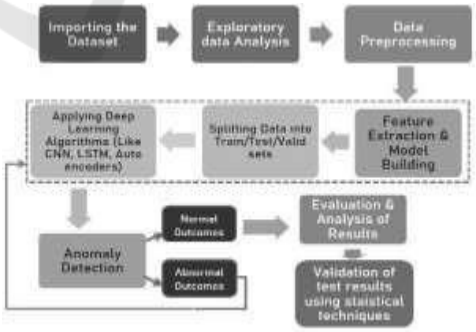
Anomaly Detection: The trained models are then used for anomaly detection, where they analyze incoming data in real- time to identify any deviations from normal patterns.

Feedback Loop: Anomaly detection results are fed back into the system for evaluation and further refinement of the models to improve their accuracy over time. Evaluation & Analysis of results:

The performance of the deep learning models in detecting anomalies and forecasting time series data is evaluated using benchmark datasets and metrics and perform the comparative analysis of results from proposed solution with results from existing machine learning and deep learning solutions. Validation of test results using statistical techniques: Further the results of proposed model are validated against statistical method like hypothesis testing using Chi-Square & ANOVA Methods.

4.3 Detection of Edge Anomalies Using Deep Learning Techniques

There are many datasets are available for anomaly detection in edge computing network, in each of the dataset, data preprocessing and modeling is required for getting efficient and optimal results. Based on type of anomaly in the edge platform, different datasets have been used by many authors in their respective research. The various datasets and examples of deep anomaly detection are explained as follows. Table 2 demonstrate a list of possible network anomalies in edge computing environments,



as well as the deep learning methods that can be applied to spot those anomalies over the suitable dataset [22]- [29].

Table 2: Detection of Edge Anomalies using Deep learning techniques on a Suitable dataset

Sr. No.	Edge Anomalies	Deep Learning Technique	Data set	Example
1	Communication Failures	Convolutional Neural Networks (CNN), LSTM	NSL-KDD	It contains various features derived from network traffic data such as TCP/UDP connections, packet payloads, etc.
2	Latency Spikes	Recurrent Neural Networks (RNNs) or LSTM	MAWI (Measurement and Analysis on the WIDE Internet) & NSL-KDD	It contains time-stamped network traffic measurements, including metrics such as round-trip time (RTT), packet loss, and throughput.
3	Scalability Issues	Reinforcement Learning (RL), CNN	UNSW-NB15	CNNs are well-suited for processing spatial data like images, and sequential data like network traffic.
4	Edge Network Congestion	CNN or RNN, LSTM	MAWI	It is used to detect and predict instances of edge network congestion using deep learning techniques.
5	Resource Constraints	Variational Autoencoders (VAEs)	IoT (Internet of Things) network traffic	It is used to detect anomalies related to resource constraints, such as instances where edge devices experience high CPU usage or memory exhaustion.
6	Edge Infrastructure Failures	RNN, LSTM, Autoencoders	Logs or telemetry data collected from edge devices, routers, switches	Logs collected over Edge server from a real-world edge computing network detects anomalies related to edge infrastructure failures.
7	Edge Node Overload	LSTM, Autoencoders	Logs collected from edge nodes, such as CPU usage, network traffic	The dataset consists of time-series data collected from multiple edge nodes deployed in a network.
8	Anomalous Traffic Patterns	CNN or RNN	Contains features such as packet rates, packet sizes, protocols, source & dest IP	The deployed CNN model successfully identifies instances of abnormal traffic patterns in a live edge computing network.
9	Security Breaches	RNN, LSTM	NSL-KDD, MAWI & Logs or telemetry data collected from edge devices, routers, switches	LSTM-based RNN model successfully identifies instances of security breaches in a live edge computing network, enabling rapid response and mitigation of security threats.
10	Data Inconsistencies	Auto encoder, Graph Neural Networks (GNNs)	Missing data, conflicting data, outliers, irregularities in data patterns.	The deployed auto encoder model successfully identifies instances of data inconsistencies in a live edge computing network, enabling proactive measures to ensure data integrity and reliability.

Furthermore, for this purpose, alternative deep learning methods like Convolutional Neural Networks (CNNs) or hybrid models that combine CNNs and LSTMs could be investigated [20]- [21].

5 CASE STUDY

There are many real-world applications where edge computing plays an important role for making the computational speed of application faster along with providing high privacy and security. Some of the colossal benefits of edge computing platform are enhanced scalability, lowers network latency, cost savings, improved reliability, and real- time analytics. But due to the different types of anomalous attacks these benefits would get compromised resulting in slow performance, high latency, compromised security and connectivity. Because of which anomaly detection plays an important role in making the edge devices secured. Some of the real-world applications of edge computing are Autonomous vehicles, Smart cities for connected cars, cameras, and traffic signals, healthcare, and telemedicine etc. In Healthcare and Telemedicine, the edge computing is used for processing of medical data in real time that help doctors to monitor patient health remotely.

5.1 Anamoly Detection in Medical Applications over Edge Network

In medical applications, edge computing plays an important role in collecting processing and storing the medical data at nearby edge locations where doctors can easily monitor the patient health and provide effective treatment. The doctors take the various readings of the patient's health records by using the various sensory devices placed on the human body. The readings taken from sensors further used for getting the results related to diagnosis of disease based on that they provide the accurate treatment. The benefits of the edge computing for medical applications are higher computational speed for processing, speedy results of diagnosis, higher storage for maintaining report records in various formats, scalability, and easy accessibility. Therefore, any compromise in the sensors data would result in inaccurate disease diagnosis may result in wrong treatment.

That is why the consistency must be maintained in the data of the medical applications.

For example, suppose the sensory devices of IoT edge have been used for collecting the pulse and temperature data from the patient body. Any inaccuracy or data inconsistency in the pulse or temperature data may results in imposing the wrong treatment for the patient or sometimes putting the patience life in danger. The latency in edge may result in slower generation of results of reports may delay the treatment and the communication failure may result in unavailability of reports may delay the treatment of critical patient.

Therefore, it is necessary to get the accurate sensory data over the edge and maintain integrity of

it. The various stages of edge computing enabled medical applications involves selecting the nearby edge network devices and sensors, data acquisition and processing, applying the deep learning algorithms and get the automated results where accuracy is important. The problem of anomaly detections comes into Classification model of deep learning which classifies the anomalous and normal data separately from dataset.

To evaluate and validate the edge computing enabled anomaly detection using deep learning for medical applications, the experimentation has been conducted on UNSW-NB15 dataset for detecting the attacks that causes latency spike, communication failure and the data inconsistency in the data [37]. For experimentation, UNSW-NB15 dataset have been used which has 2,57,673 Samples. About 1,64,673 samples having anomalous data. The different deep learning models like Deep Neural Network (DNN) and Generative Adversarial Networks (GAN) have been used for classification of data incurring anomalies over the labeled dataset that has sensor data recorded at regular intervals. It verifies in each dataset whether the anomalies exist or not. It is used for validating the accuracy and F1-Score of the different anomalies like latency spike, communication failure or data inconsistency exist over the given data set [38][39]. In this experiment we have trained a model on number of samples 85699 for 25 epochs and verified the accuracy with 29000 testing dataset and same samples have been used with 25 epochs for GAN model [39]. The result of classification models like DNN and GAN generates the confusion matrix in the classification that has four quadrant values like True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). Based on the confusion matrix, evaluation metrics like Accuracy (A), Recall (R), Precision (P) and F1-Score have been calculated to test the anomalous behavior of the Edge data. The formulas for various evaluation metrics for classification are shown in Table 3.

Table 3. Formulas of evaluation metrics for classification.

Parameter	Formula
Precision (P)	P= TP/(TP+FP) & TN/(TN+FN)
Recall (R)	R=TP/(TP+FN) & TN/(TN+FP)
F-Score(F)	F=(2*P*R)/(P+R)
Accuracy (A)	A=(TP+TN)/(TP+TN+FP+FN)

The results obtained from both DNN and GAN models over the given dataset is given in Table 4.

Table 4: Results obtained from DNN and GAN models.

Models →	Deep Neural Network			Generative Adversarial Networks		
Attacks ↓	Precision	Recall	F1-score	Precision	Recall	F1-score
DOS	0.53	0.73	0.65	0.98	0.98	0.99
EXPLOIT	0.75	0.63	0.69	0.83	0.94	0.90
GENERIC	0.99	0.97	0.99	0.99	0.96	0.97
NORMAL	0.98	0.98	0.99	0.99	0.9	0.88
ACCURACY			**0.8325**			**0.9375**

From above results, it has been observed that DNN model gives the precision, recall, and F1-Score average value of 0.8325, whereas the GAN model gives the average value of 0.9375. That means GAN models gives accuracy of 93.75% which is more than DNN and has reduced loss than DNN.

The conclusion of above experiment is more the loss in the attack samples lesser the accuracy. The lesser accuracy results in more percent of attacks that result in increase in increase of latency spike, communication loss or sometimes data inconsistency.

The future scope for above experiment would be use of fuzzy neural network which may give more accuracy than the above two models.

6 CONCLUSION

The expanding number of IoT devices and the continual collection of network data have highlighted the relevance of anomaly detection in edge computing networks. This research study discusses the difficulty in monitoring edge networks and detecting unexpected network behavior, emphasizing the importance of having effective anomaly detection tools and a relevant dataset. This research study has quickly reviewed the various features of edge computing anomalies that exist in different settings. It also discusses the classification of various deep learning methods and the relationships between different types of data. The various datasets utilized for edge computing anomaly detection have also been examined. Finally, a model for using deep learning techniques on edge computing data sets to detect anomalies has been developed. Finally, the case study on anomaly detection in medical applications over the

edge network has been discussed. It has covered the importance of edge computing for medical application along with detection of anomalies using the two deep learning models like DNN and GAN. In the results, the accuracy of GAN appears better than DNN with lesser loss and seems better in detecting anomalies than DNN. In the future scope, same could be implemented using fuzzy neural classifier to get better results than the DNN and GAN.

ACKNOWLEDGEMENTS

We gratefully acknowledge to Dr. Bhushan Jadhav at Thadomal Shahani Engineering College who helped and support during the research process. Their contributions were instrumental in shaping the direction and scope of this work. Additionally, we acknowledge the reviewers whose thoughtful comments and suggestions greatly enhanced the clarity and depth of the manuscript. Lastly, we express our appreciation to Springer and the editorial team for their professionalism and assistance in the publication process.

REFERENCES

1. Chalapathy, R., Chawla, S., 2019. Deep Learning for Anomaly Detection: A Survey. *arXiv:1901.03407.*
2. Zhu, M., Ye, K., Wang, Y., Xu, C.Z., 2018. A Deep Learning Approach for Network Anomaly Detection Based on AMF- LSTM. In: *15th IFIP International Conference on Network and Parallel Computing (NPC)*, Muroran, Japan, pp. 137-141. Springer.
3. Kim, J., Kim, J., Thu, H.L.T., Kim, H., 2016. Long short-term memory recurrent neural network classifier for intrusion detection. In: *Platform Technology and Service (PlatCon), International Conference on*, pp. 1-5. Springer.
4. Anantha, A.P., Daely, P.T., Lee, J.M., Kim, D.S., 2020. Edge Computing-Based Anomaly Detection for Multi-Source Monitoring in Industrial Wireless Sensor Networks. In: *ICTC 2020*, pp. 1890- 1892.Springer.
5. Majeed, A.A., Kilpatrick, P., Spence, I., Varghese, B., 2022. CONTINUER:Maintaining Distributed DNN Services During Edge Failures. In: IEEE International Conference on Edge Computing and Communications (EDGE), 24 August 2022. Springer.
6. Hu, P., Chen, W., 2019. Software- Defined Edge Computing (SDEC): Principles, Open System Architecture and Challenges. In: IEEE SmartWorld, Ubiquitous Intelligence &Computing (SmartWorld/ SCALCOM/UIC/ATC/CB D Com/IOP/SCI). Springer.
7. Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., Fang, B., 2018. Insider threatdetection with deep neural network. In: International Conference on Computational Science, pp. 43-54. Springer.
8. Kwon, D., Kim, H., Kim, J. et al., 2019. A survey of deep learning-based network anomaly detection. Cluster Computing, pp. 949–961.
9. Yin, C., Zhu, Y., Fei, J., He, X., 2017. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, vol. 5, pp. 21954-21961.
10. Zhang, L., Fan, F., Dai, Y., He, C., 2022.Analysis and research of generative adversarial network in anomaly detection. In: 7th International Conference on Intelligent Computing and Signal Processing (ICSP), IEEE.
11. Zhang, B., Yu, Y., Li, J., 2018. Network intrusion detection based on stacked sparse autoencoder and binary tree ensemble method. In: Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), pp. 1–6.
12. Yan, B., Han, G., 2018. Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system. IEEE Access, vol. 6, pp. 41238–41248.
13. Al-Qatf, M., Lasheng, Y., Al-Habib, M., Al- Sabahi, K., 2018. Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. IEEE Access, vol. 6, pp. 52843–52856.
14. Xu, W., Jang-Jaccard, J., Singh, A., Wei, Y., Sabrina, F., 2021. Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL- KDD Dataset. IEEE Access, vol. 9, pp. 140136-140146.
15. Liang, Y., Chen, Z., Lin, D., Tan, J.,Yang, Z., Li, J., Li, X., 2023. Three-Dimension Attention Mechanism and Self-Supervised Pretext Task for Augmenting Few-Shot Learning. IEEE Access, vol. 11, pp. 59428- 59437.
16. Kingma, D.P., Welling, M., 2013. Auto- encoding variational Bayes. arXiv:1312.6114.
17. An, J., Cho, S., 2015. Variationalautoencoder-based anomaly detection using reconstruction probability. SNU Data Mining Center, Seoul, South Korea, Tech. Rep.
18. Zavrak, S., Skefiyeli, M., 2020. Anomaly- Based Intrusion Detection from Network Flow Features Using Variational Autoencoder. IEEE Access, vol. 8, pp. 108346-108358.
19. Li, Q., Zhu, Y., Ding, J., Li, W., Sun, W., Ding, L., 2021. Deep Reinforcement Learning based Resource Allocation for Cloud Edge Collaboration Fault Detection in Smart Grid. CSEE Journal of Power and Energy Systems, pp. 1-10.
20. Jozefowicz, R., et al., 2016. Exploring the limits of language modeling. arXiv:1602.02410.
21. Graves, A., Mohamed, A.R., Hinton, G., 2013. Speech recognition with deep recurrent neural networks. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE.

22. Jayasinghe, M., Seneviratne, S., Seneviratne, A., 2017. Deep learning for anomaly detection in network traffic data. In: IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE.
23. Banga, G., Dubey, K.K., Mishra, K.K., 2018. LSTM-RNN based network anomaly detection. In: International Conference on Computing, Power and Communication Technologies (GUCON). IEEE.
24. Chalapathy, R., Chawla, S., 2018. Deep Learning for Anomaly Detection: A Survey. ACM Computing Surveys (CSUR), vol. 51, no. 3.
25. Yao, H., Zheng, S., Wen, H., Li, X., 2020.Deep Learning for Anomaly Detection: A Review. ACM Computing Surveys, vol. 53, no. 2.
26. Pham, K.H., Bui, T.D., Venkatesh, S., 2019. Anomaly Detection in Edge Computing Systems Using Deep Learning. IEEE Transactions on Services Computing, vol. 12, no. 1, pp. 114-127.
27. Kiran, A., Basavaraju, T.G., 2021.Anomaly Detection in IoT-Based Edge Computing Using LSTM Autoencoder. In: International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).
28. Huc, A., Šalej, J., Trebar, M., 2023. Analysis of Machine Learning Algorithms for Anomaly Detection on Edge Devices. MDPI.
29. Elsayed, M.S., Le-Khac, N.-A., 2020.Network Anomaly Detection Using LSTM- Based Autoencoder. In: Q2SWinet '20, ACM, Alicante, Spain.
30. Mehnaz, S., Bertino, E., 2020. Privacy- preserving Real-time Anomaly Detection Using Edge Computing. In: IEEE 36th International Conference on Data Engineering (ICDE), May 2020, pp. 469-480. IEEE.30.
31. Dawoud, A., Shahristani, S., Raun, C., 2019. Deep Learning for Network Anomalies Detection. In: International Conference on Machine Learning and Data Engineering (iCMLDE), IEEE, pp. 149-153.
32. Li, R., Zhou, Z., Liu, X., et al., 2021.GTF:An Adaptive Network Anomaly Detection Method at the Network Edge. Security and Communication Networks, vol. 2021, Article ID 3017797, pp. 1-12.
33. Ferrari, P., Rinaldi, S., Sisinni, E., et al., 2019. Performance evaluation of full- cloud and edge-cloud architectures for Industrial IoT anomaly detection based on deep learning. IEEE, pp. 420-425.
34. Peng, Y., Tan, A., Wu, J., Bi, Y., 2019.Hierarchical Edge Computing: A Novel Multi-Source Multi-Dimensional Data Anomaly Detection Scheme for Industrial Internet of Things. IEEE Access, vol. 7, pp. 111257-111270.
35. Abdel-Wahab, M.S., et al., 2021. A Comparative Study of Machine Learning and Deep Learning in Network Anomaly- Based Intrusion Detection Systems. IEEE, February 2021.
36. Xiang, H., Zhang, X., 2022. Edge computing empowered anomaly detection framework with dynamic insertion and deletion schemes on data streams. IEEE.
37. Samariya, D., Ma, J., Aryal, S., Zhao, X., 2023. Detection and explanation of anomalies in healthcare data. Journal of Health Information Science and Systems, Springer.
38. Schneible, J., 2017. Anomaly Detection on the Edge. In: MilCom 2017, IEEE Cyber Security and Trusted Computing.
39. Sharma, B., Sharma, L., Lal, C., Roy, S., 2023. Anomaly based network intrusion detection for IoT attacks using deep learning technique. Journal of Computers and Electrical Engineering, Elsevier