Corrosion Management ISSN: 1355-5243

(https://corrosion-management.com/)

Volume31, Issue 01–June 2021

SCOPUS

Anomaly detection with CNN autoencoders for Cloud-based AI systems

1st Rahul Vadisetty Electrical Engineering,)

Wayne State University) Detroit, MI, USA rahulvy91@gmail.com

Abstract:

Nowadays, the most important problem is anomaly detection. If anomalies are not detected in time it can cause severe damage to the organization's reputation and revenue. To detect anomalies, organizations use different techniques like Convolutional Neural Network autoencoders which can easily detect anomalies. Other techniques are seasonal ESD, and Seasonal hybrid ESD which use time series to detect anomalies. Machine learning techniques like supervised learning, unsupervised learning, and semi-supervised learning are also implemented in cloud-based AI systems to detect anomalies before any damage is done. Anomalies detection techniques face many challenges like big data, imbalance data, and noise which lead them to detect false anomalies.

Index Terms: Anomalies, Convolutional Neural Network, Challenges, learning, cloud-based AI system.

1. Introduction:

A. Background:

Convolutional Neural Networks are composed of neurons that improve through learning. Every neuron based on an artificial neuron network receives an input and performs its tasks and entire network expresses a single perceptive score function from input raw vectors to the final output of the class score. Last layer attached to the classes has loss functions and all tips and tricks apply to traditional Artificial Neural Networks. The major difference between Convolutional Neural Networks and traditional Artificial Neural Networks is that Convolutional Neural Networks are used in the market of pattern recognition images. This enables us to encode image-specific features into architecture (O'Shea & Nash, 2015).

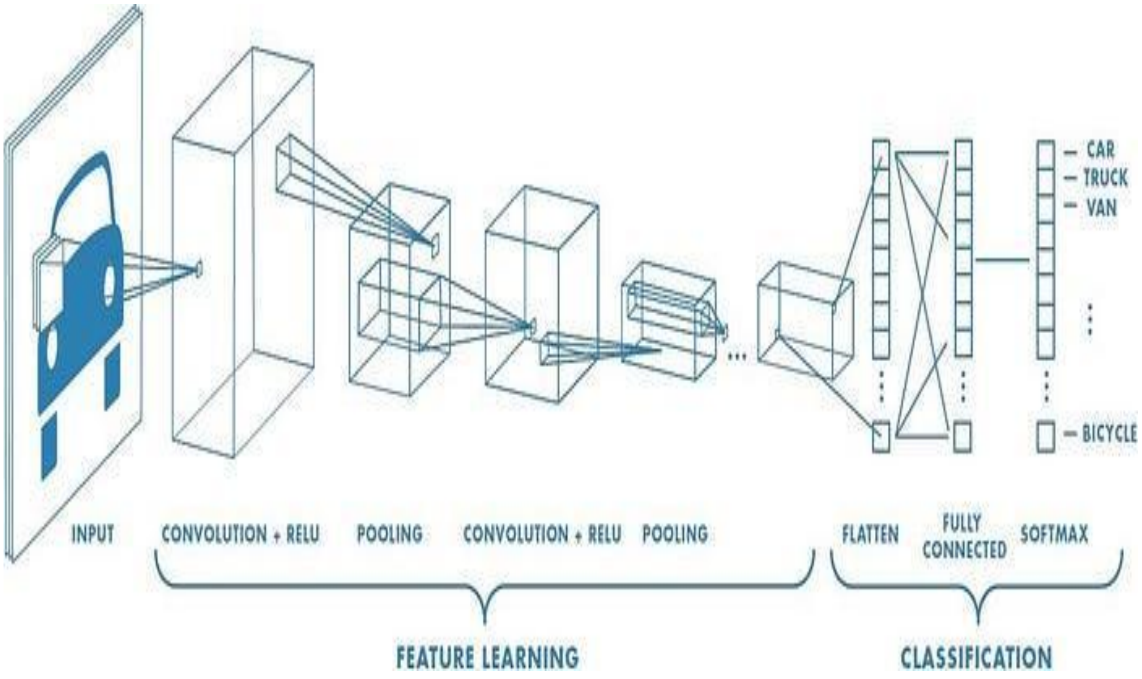

Figure 1Convolutional Neural Networks (Saha, 2018).

Convolutional Neural Networks create computer vision and image processing. Convolutional Neural Networks have a network architecture and general structure which is shown above in the diagram, its general structure involves several connected layers that follow a series of Convolutional blocks.

Cloud computing has great use in industries like IoT applications, content delivery, and disaster recovery. Cloud computing is the second important technology that follows artificial intelligence. While using cloud computing, several issues arise including data security issues. Anomaly detection allows providers to check systems for suspicious activities to increase cloud computing security. It enables providers to detect unknown attacks, and early warning systems, and reduce false positives. Cloud security makes sure that the right individuals have proper access to resources by containing various critical facets like identity and asset management. Disaster recovery strategies have their focus on data restoration objectives. Data Security is another important concern—service security management, third-party tools, and application-level security practices for the software development process (Hagemann & Katsarou, 2020).

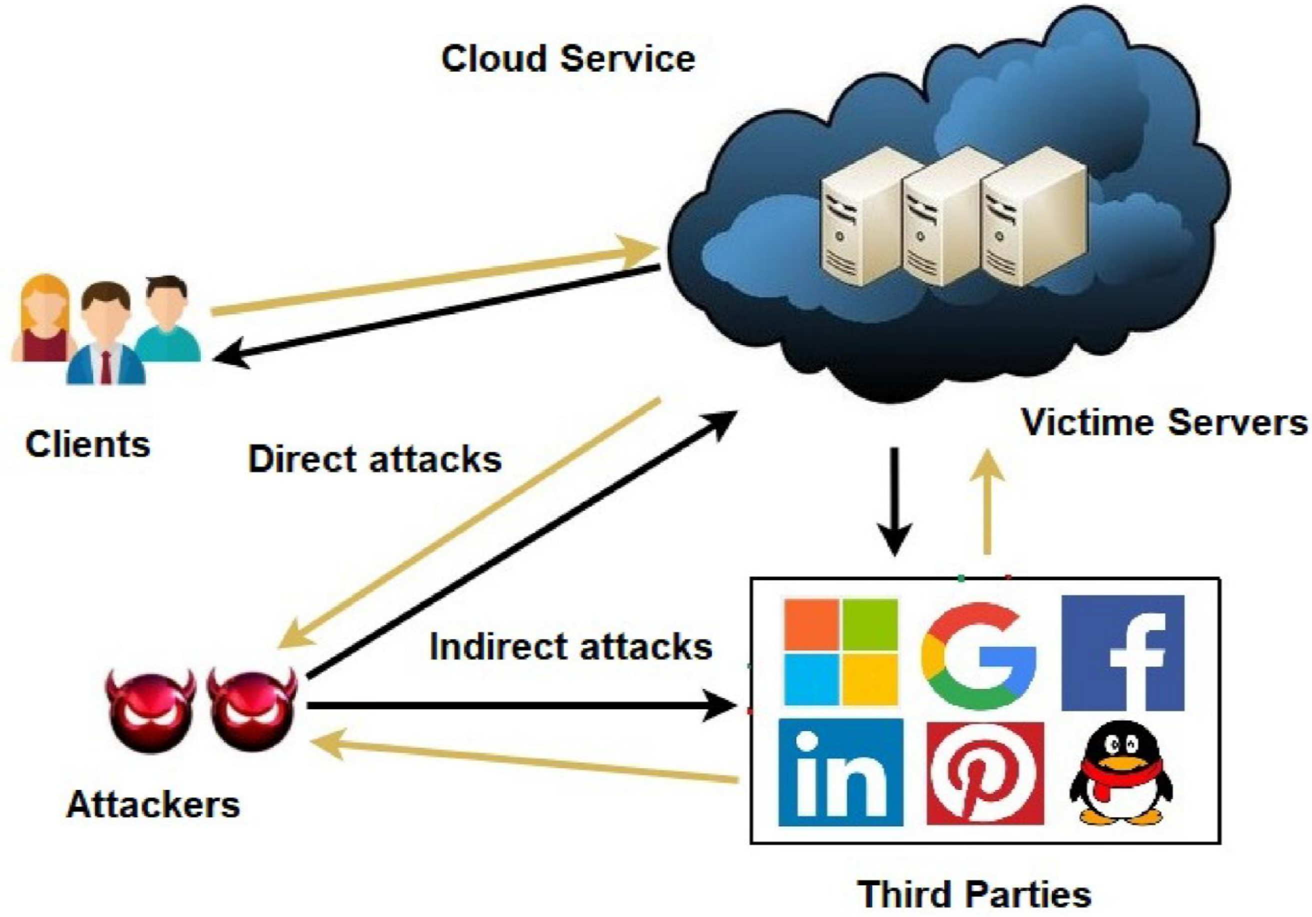

Figure 2 Artificial Intelligence Algorithm: Cloud Computing Environment (Gill, et al., 2019).

B. Problem Statement:

Cloud-based AI systems have been a center of attraction in recent years but they have many issues like data security and cyber security. Data protection is the main concern for every individual and organization. Every organization using cloud-based AI systems has a high level of threats of data leakage as organizations have personal and sensitive information stored in their systems. If their information leak, it can cause damage to organizations. For using cloud-based AI systems, we need anomaly detection techniques to make sure that our data is safe. Present methods are available in cloud-based AI systems for data protection but they are not enough to handle the complexity of data.

Strong anomaly detections are needed to identify anomalies before any damage is done. Anomaly detection is an important factor in increasing the security and performance of cloud-based AI systems. Methods that are available for cloud-based AI systems are not able enough to handle the volume and complexity of data so it is important to develop more methods required by Computational Neural Networks auto encoders to avoid efficiencies while using Cloud-based AI systems. We should enhance the methods of Computational Neural Networks autoencoders to detect the anomalies before any damage is done.

Biggest problem when using Computational Neural Networks in anomaly detection is that we have very large data volumes which are very complex and anomalies cannot be detected by different techniques, which creates many risks and often costs organizations a lot. There are anomaly detection algorithms to detect anomalies but sometimes they cannot detect anomalies due to noise. Noise affects the algorithms that cause the algorithms to detect false anomalies. We must use different innovative engineering techniques so that we can detect anomalies well before any damage occurs.

C. Objectives:

In my article on "Anomaly detection with CNN auto encoders for Cloud-Based AI Systems," the main objectives are to implement more methods for anomaly detection in cloud-based AI systems to detect risk before any damage is done. Our main objectives are to improve computational efficiency and to develop algorithms in CNN that enable them to detect anomalies and work more efficiently and fast. We should ensure that anomaly detection protects the data from any harm and maintains data integrity. If the data is not protected well, it can cause a lot of damage to the company, so it is important to adopt such techniques that can protect the data and alert the company in advance of the impending threat will keep the data protected and the company will not suffer any loss.

D. Research Questions:

This study aims to answer the following questions:

- How are Convolutional Neural Networks different from traditional Artificial Neural Networks in Cloud-based AI systems?
- What are the disadvantages of implementing Convolutional Neural Network auto encoders for anomaly detection?
- What are the advantages of using Convolutional Neural Network auto encoders for anomaly detection?
- How can we improve Convolutional Neural Network auto encoders for detection of anomalies in Cloud-Based AI Systems?

Answering these questions will help to improve Convolutional Neural Network autoencoders to detect the anomalies so that we prevent our data from any type of damage; it helps to develop strong methods which can be able to handle the complexity of data.

E. **Contribution of the study**:

The research is vital for several reasons:

Anomalies Detection with Convolutional Neural Networks:

Considering Anomalies detection with Convolutional Neural Network autoencoders as a primary discussion of the article, several innovative techniques for anomalies detection, and challenges in anomalies detection are discussed in the context of cloud-based AI systems.

Knowledge contribution:

Understandings from existing literature add Knowledge to the content of anomaly detection with CNN auto encoders for Cloud-Based AI Systems.

Security improvement:

The findings, discussions, and results of the article provide valuable insights to improve anomaly detection techniques, implementation of innovative techniques to detect anomalies in Cloud-Based AI Systems.

F. Paper's Structure:

The paper is organized as follows

Chapter 1: Introduction that focuses on discussing background information, Problem statement, and research questions.

Chapter 2: Literature review, A detailed examination of existing studies on Anomaly detection with Convolutional Neural Network autoencoders for Cloud-based AI Systems, techniques to improve anomaly detection techniques and challenges.

Chapter 3: Methodology The methods and techniques are used to evaluate the Anomaly detection techniques in detail.

Chapter 4: Results and discussion, an analysis of the findings and their implications.

Chapter 5: Conclusion and future framework, a summary of the research, its contributions and future direction.

2. Literature Review:

Introduction:

A. **Anomalies detection in cloud-based AI Systems**:

Anomaly detection refers to the techniques of finding patterns in data that cause changes in normal behavior. Anomaly detection systems are very important tools as they are used to detect unusual traffic situations and financial fraud. Anomaly detection plays an important role in ensuring the security of cloud-based AI systems. Many organizations use cloud services for their needs so it is important for them to detect anomalies to maintain their organization's integrity. Anomalies can be in different forms like data breaches, system faults, or resource misuse. Innovative techniques are required to identify the unique characteristics of cloud-based AI systems as it is impossible for monitoring approaches to handle the complexities of cloud-based infrastructures.

We can improve security and optimize resource allocation by implementing effective Anomaly detection. Organizations can reduce the effect of security breaches by identifying the anomalies. Anomalies can happen in domains like system logs, financial transactions, and network traffic. While anomaly detection techniques use statistical, and machine learning approaches to find and learn the normal behavior of the system. They are important components of many applications like cybersecurity, fraud detection, and quality control. It enables timely response to risks and ensures the security of systems

B. Techniques to detect anomalies:

Nowadays, anomaly detection is a much greater problem which is concerned with identifying data patterns to protect the data. It is important to identify the important information about the system's functioning and detection of abnormalities in the system. One such solution for anomaly detection is Convolutional Neural Network. They have become the important factor for recent innovations and allowed many advances in various applications like semantic image segmentation. If we identify the problem in advance, it becomes easier to identify and solve the problem (Staara, Lütjena, & Michael, 2019). For example, preventing system failure, and spotting stolen credit cards. Big data has the characteristics of large volume and velocity of data generation. Anomalies in big data can cause revenue and reputational loss to the company. Many organizations are now focusing on techniques for anomaly detection. We have some techniques for anomaly detection like statistical learning-based techniques which can automatically detect anomalies in time series data (Hochenbaum, Vallis, & Kejariwal, 2017). The following are the techniques to detect anomalies:

Seasonal Hybrid ESD:

In some time series, the mean and standard deviation are highly at risk of anomalies. Seasonal hybrid ESD then used the statistics median and median absolute deviation to detect anomalies.

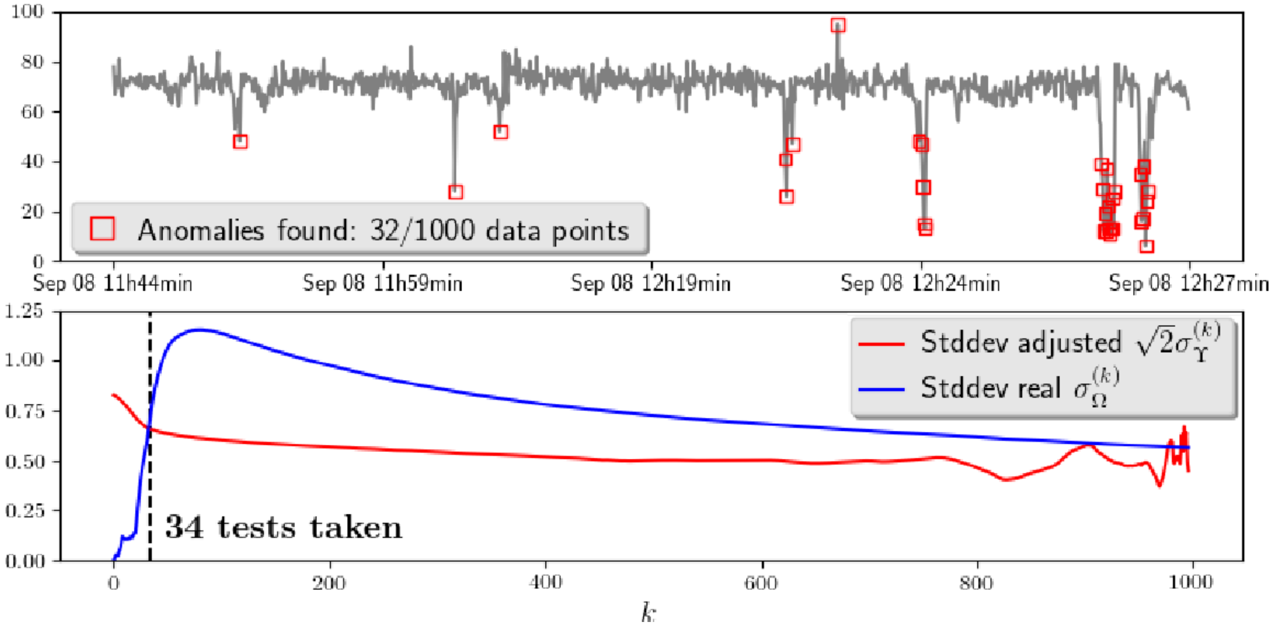

Figure 3Seasonal Hybrid ESD technique (Vieira, Filho, & Semolini, 2018)

Seasonal ESD:

Seasonal ESD uses time series decomposition to determine the resulting time then Seasonal ESD applies to detect the anomalies.

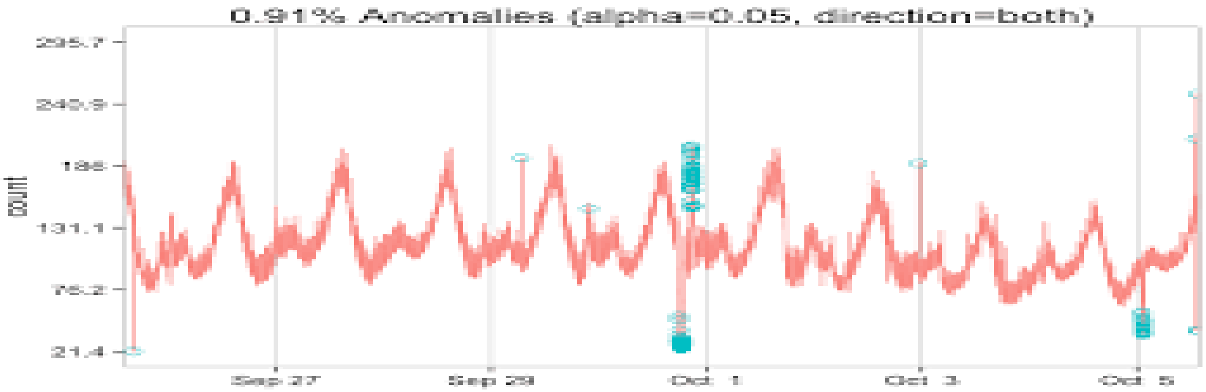

Figure 4 Seasonal Trend Decomposition (Gao, 2015)

C. Machine learning-based techniques:

Machine learning-based techniques use algorithms that are helpful to identify patterns from labeled or unlabeled data to identify anomalies. Following are the techniques based on the type of learning employed.

Supervised learning:

In this learning, anomalies are identified from labeled data that highlights the normal and anomalous instances. For labeled data, algorithms like Random forests, and Neural Networks are trained to classify new instances as normal or anomalous.

Unsupervised learning:

In this learning, they do not depend on labeled data but they are trained to detect anomalies based on the characteristics of data. In Unsupervised learning, algorithms like DBSCAN and K-means clustering detect anomalies.

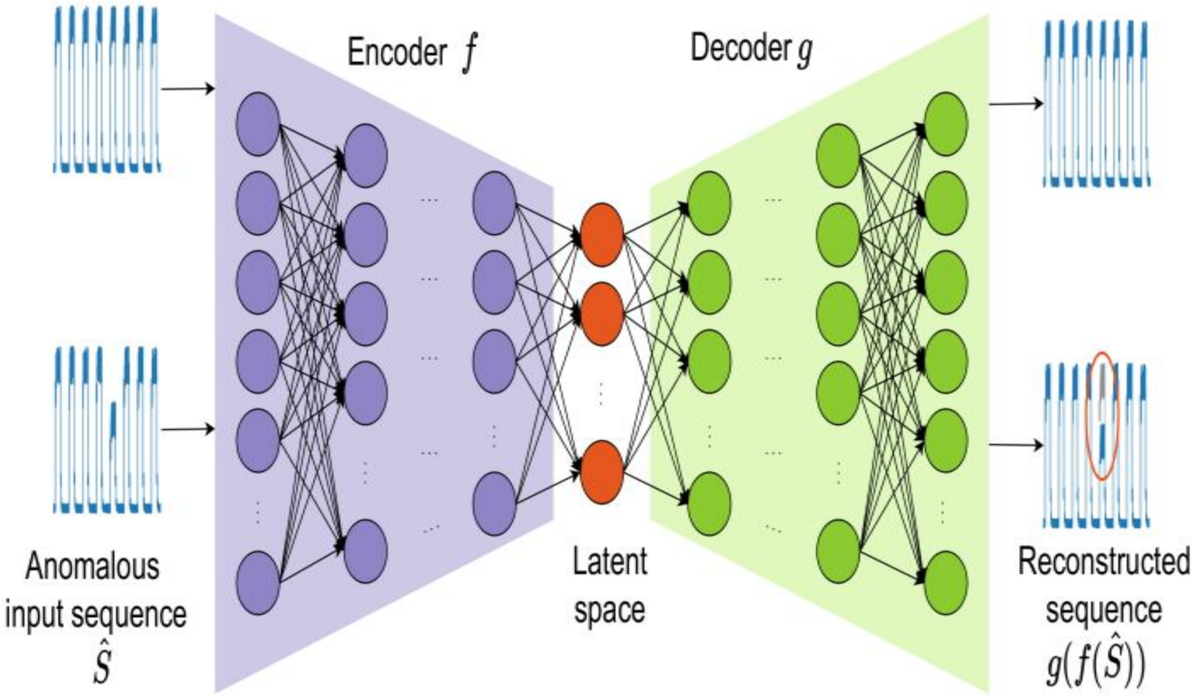
Encoder f
Decoder g
Anomalous input sequence $\hat{S}$
Latent space
Reconstructed sequence $g(f(\hat{S}))$

Figure 5 Unsupervised Anomaly detection (Ahmed, Mahmood, & Hu, 2016).

Semi-supervised learning:

In this learning, the elements of supervised and unsupervised are combined to detect anomalies. They use a small amount of labeled data with a large amount of unlabeled data to detect anomalies. This technique is useful when there is a shortage of labeled data.

D. Challenges in anomaly detection:

Following are the challenges in anomaly detection in cloud-based AI systems that need to be known to achieve accurate anomaly detection.

Big data:

Cloud-based systems produce large amounts of data from various sources like network traffic, which is difficult to detect accurate anomalies because it exhibits large volumes. Anomaly detection algorithms can cause complexity due to large amount of volume

Dynamic nature of cloud-based systems:

Cloud-based systems are highly dynamic due to their scaled resources. The behavior of the system can change due to high workloads and infrastructure changes. Anomaly detection techniques need to update their models continuously for normal behavior.

Imbalance data:

Imbalance data refers to outweighs of number of anomalous instances. Imbalance data can cause favoritism towards the majority. Which can cause loss to minorities. Techniques like under sampling are used for imbalanced data.

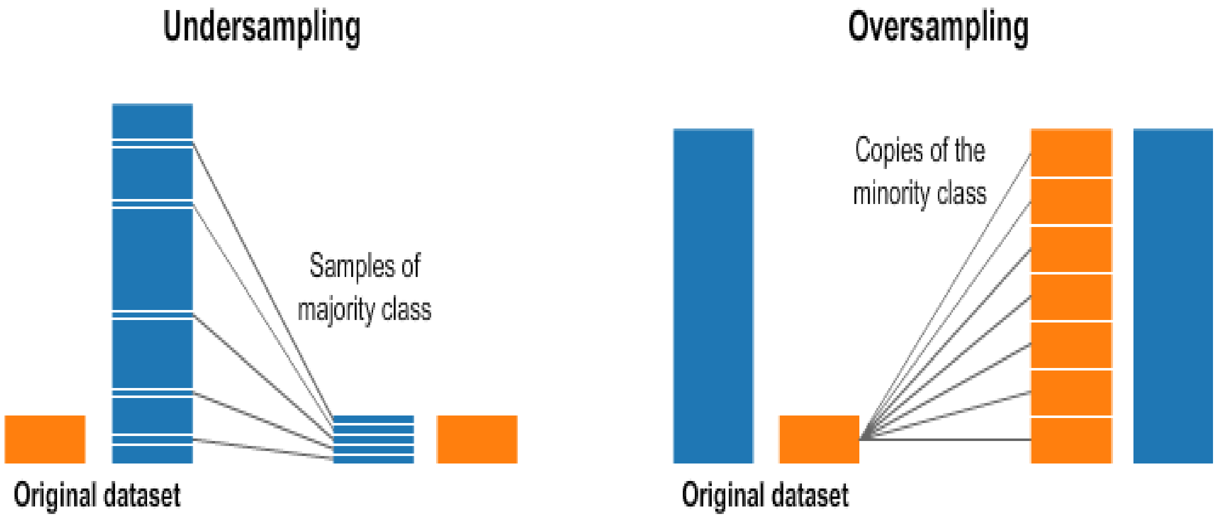

Figure 6 Random Under sampling and Oversampling (Agarwal, 2020)

Noise and outliers:

Cloud-based systems can be affected by noise and outliers like system failures. Noise can trigger false alarms and make it difficult to detect anomalies.

To deal with these challenges, robust anomaly detection algorithms and innovative engineering techniques are required. More accurate anomaly detection systems can be developed by overcoming these challenges.

E. Summary:

This chapter describes that anomaly detection techniques are important to detect anomalies. Anomalies can harm the organization's integrity so it is very important for organizations to apply different techniques to prevent anomalies. Different techniques like Convolutional Neural Network auto encoders are used to detect anomalies. Anomalies can detect by different learnings like supervised, unsupervised, and semi-supervised. Organizations can suffer the most due to anomalies. Anomalies can damage reputation and revenue of organizations. To prevent anomalies, organizations use techniques like seasonal hybrid ESD and seasonal hybrid which help them to detect accurate anomalies. This chapter also discussed the challenges in anomaly detection that it can be difficult to detect anomalies due to big data, imbalance data or noise.

III. Methodology

1. Introduction

This study has used a mixed-methods approach for anomaly detection with CNN autoencoders for cloud-based AI systems. The research used primary and secondary data to develop a comprehensive methodology. The study has employed a comprehensive approach to anomaly detection with CNN autoencoders for cloud-based AI systems. In this chapter, there is a research method that explores the study that analyzes anomaly detection with CNN autoencoders for cloud-based AI systems. In this chapter, full attention will be paid to those points that are linked to the ethical considerations. The main focus will be on methodologies to conduct the research without violating any ethical considerations.

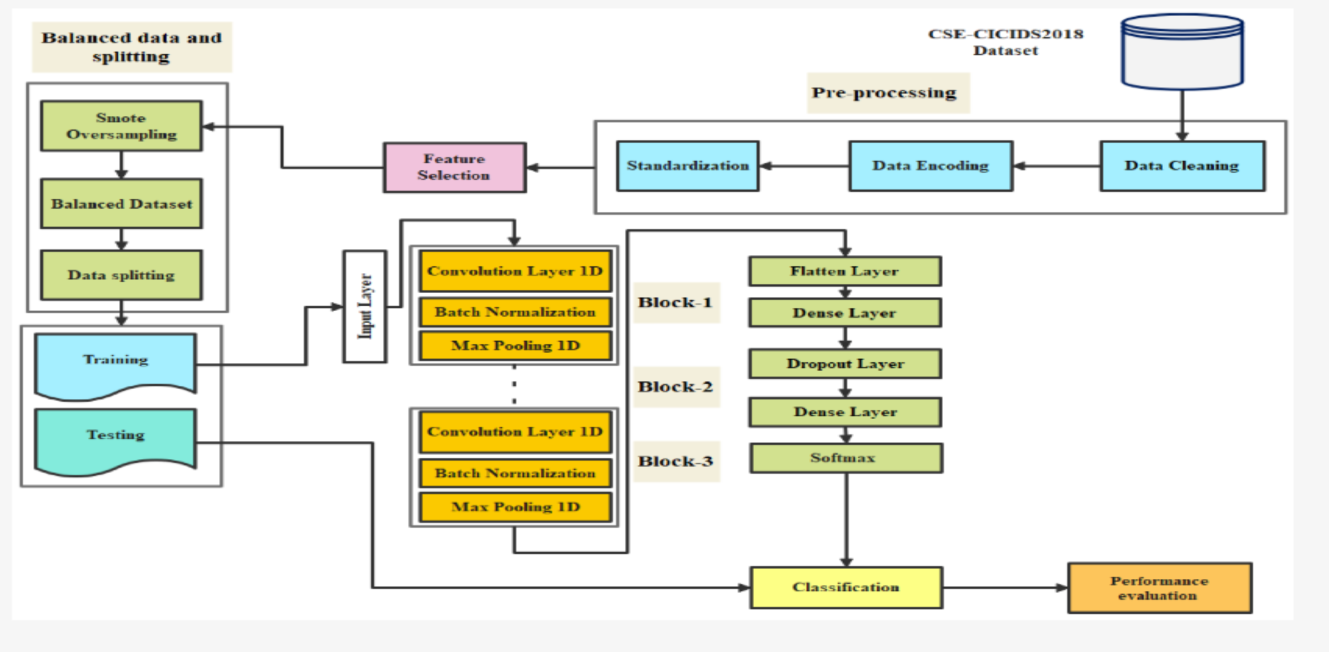

Figure 7. CNN model (Liu, Yan, & Yang, 2018).

2. Research Design

In this research, there is the research design that will use the research questions and research objectives. These research questions and research objectives are already mentioned and highlighted in Chapter number 1. This research paper will assess both methods qualitative and quantitative to give an elaborative and comprehensive look at anomaly detection with CNN autoencoders for cloud-based AI systems. In research design, it is a strategy and procedure to answer the research questions and answer the problems of research.

3. Qualitative Method

Research study for the collection of data uses both methods of anomaly detection with CNN autoencoders for cloud-based AI systems. In the qualitative method of data collection of the research question, there will be used of a lot of journals, reports, and cases. The article assists in collecting the data. In this research paper, the study will try to collaborate with other scholars to explore the research in their field of study. In the qualitative method of data collection, there is a thematic analysis. The thematic analysis is defined as the process of collecting data and information based on opinions and suggestions of scholars and specialists and information that is received from the reviews of the literature. This whole process of gathering or collecting information through qualitative methods is called the thematic analysis. The study also gathered secondary data using a detailed review of the literature. For the collection of data, we have used the secondary method or qualitative method. We collected the qualitative data. This qualitative data is collected from the cases, articles, and reports. Secondary data in this research is collected through the qualitative study. Data collection in this study focuses on findings of anomaly detection with CNN autoencoders for cloud-based AI systems.

4. Quantitative Method

Experimentalism is the process in which experiments are conducted and simulated for the collection of data through quantitative methods. This is another method of collecting data through experiments is a secondary method or quantitative method of data collection. It focuses on anomaly detection with CNN autoencoders for cloud-based AI systems. To recognize and identify the abnormal and change behaviors in the network system, data is utilized that is called Autoencoder. The main focus of the research is to learn and utilize the deep techniques of the Cloud security system where several resources and services are assured and guaranteed. This learning of the deep techniques can assist in detecting the anomaly. The main aim of quantitative analysis is to provide a rationale for the conclusions and prove the efficiency and effectiveness of the methods of anomaly detection with CNN autoencoders for cloud-based AI systems.

The research has used the primary method for the collection of data. For this purpose, the survey was used. In this survey, there were many participants and these participants were free to answer and there was no restriction or pressure on the participants to answer the survey according to their own choice. All the ethical considerations were considered in the survey. The survey was conducted through social media. The main objective of the survey was to collect as much data as possible. The process of data collection included people of all ages, groups, races, and genders.

5. Data Collection Method

Collection of data is a very important procedure for any type of research work. The research has used quantitative and qualitative methods for the collection of data. The data is collected based on the research questions that are mentioned in Chapter 1. The data has been collected by using mixed methods.

A. Literature Review

Data that has been obtained from the articles, papers, cases, and reports is from the literature reviews. The data that has been collected is about anomaly detection with CNN autoencoders for cloud-based AI systems. The data is collected from different sources and these sources could be articles, journal articles, academic journals, and professional journals, and all those articles, cases, and reports that are presented at the conferences. The articles that are used for the collection of data can be academic, professional articles, and journal articles. Reports that are included in the collection of data could be industry reports, medical reports, and official reports.

B. Expert Interviews

For anomaly detection with CNN autoencoders for cloud-based AI systems, in the field of cloud service systems, different interviews were conducted. These interviews have highlighted anomaly detection in a Cloud-based AI system and the efficiency of CNN encoders to identify abnormal and unusual behaviors within the network system. There is a point that has been highlighted in the interviews by the experts that the deep learning techniques must be enhanced and promoted to increase the study of abnormal and behavioral variation in the network system.

C. Experimental Data

For the collection of data, the experiments were performed in the form of surveys and case studies. These case studies and surveys that are conducted for the collection of quantitative data have revealed that anomaly detection is crucial in a Cloud-based AI system and CNN encoders are efficient and effective for the identification and recognition of abnormal and behavioral variations within the network system.

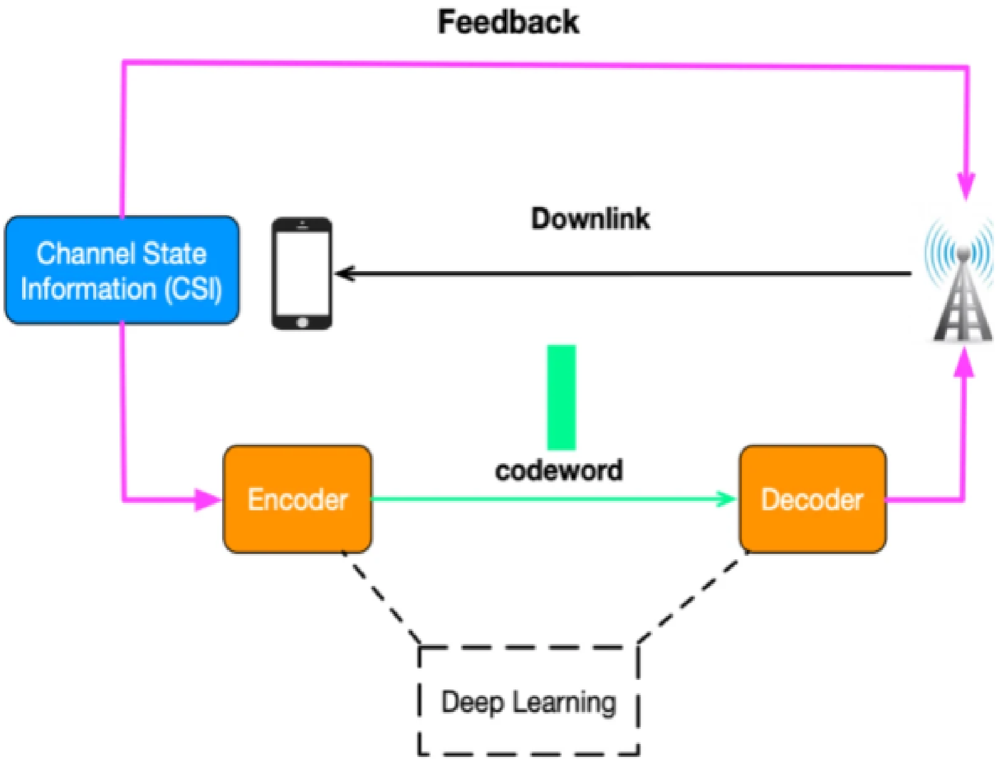

Figure 8.Deep learning in CNN encoders (Liu, Jiang, Song, Huang, & Yang, 2020).

6. Data Analysis Techniques

In data analysis techniques, the collected data through qualitative method and quantitative methods is analyzed through the techniques of thematic analysis, survey, literature reviews, experiments, and interviews. The two subtopics qualitative data analysis and quantitative data analysis are used for the analysis of both primary and secondary data and conclude.

A. Qualitative Data Analysis

Data that has been obtained from the articles, journals, white papers, cases, and reports from the literature reviews is qualitative and it is analyzed by the technique of thematic analysis. The data that has been collected is about anomaly detection with CNN autoencoders for cloud-based AI systems. The data is collected from different sources and these sources could be articles, journal articles, academic journals, and professional journals, and all those articles, cases, and reports that are presented at the conferences are analyzed. In the qualitative method of data collection, there is a thematic analysis this technique is used for the analysis of data. The thematic analysis is defined as the process of collecting data and information based on opinions and suggestions of scholars and specialists and information that is received from the reviews of the literature. This whole process of gathering or collecting information through qualitative methods is called the thematic analysis. The collected data is analyzed and their advantages and disadvantages are stated based on the analysis. It makes recommendations regarding the CNN encoders that are effective for the recognition of abnormal and behavioral changes within the network of the Cloud service system.

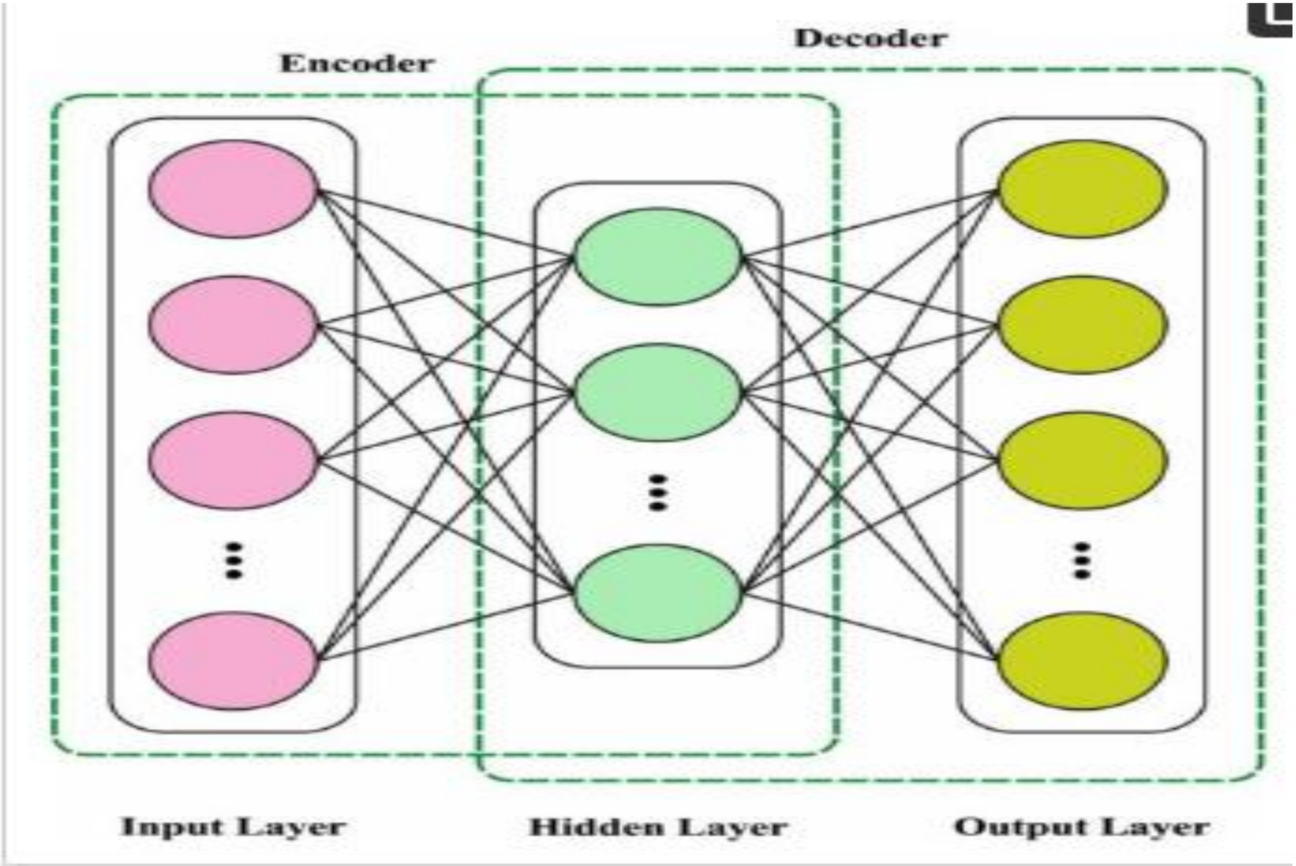

Figure 9. Structure of Encoder and Decoder (Liu, Jiang, Song, Huang, & Yang, 2020).

B. Quantitative Data Analysis

Experienced data are the amounts that are obtained through experimentation and simulations. The data is statistically analyzed. The statistical data is described through graphs and charts. Ultimately, the statistical analysis looks at the results of the profiling procedures to help make an informed choice.

6. Evaluation Matrix

In this article evaluation matrix is used for the accurate determination of data assurance quality systems. Accuracy, efficiency, scalability, reliability, and validity are considered while collecting the data for the data assurance quality in anomaly detection with CNN autoencoders for cloud-based AI systems. Training programs assist the researcher in evaluating the accuracy and consistency of the results. It helps the author determine whether the model can function optimally. In this, the model that is functioned is the Kaggle dataset and it had given the Confusion matrix graph and the ROC curve. The interpretation of the graphs is given below.

A. Confusion matrix

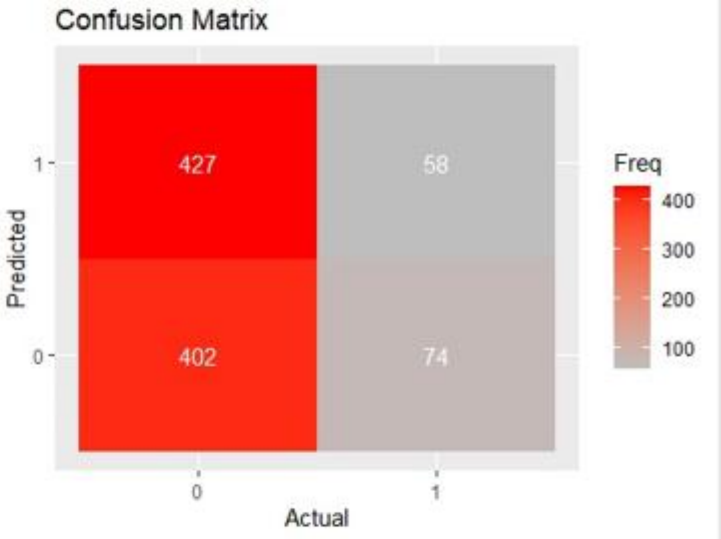

Figure 10. confusion Matrix.

The study effectively demonstrates Anomaly detection with CNN autoencoders for Cloud-Based AI Systems. The results of the confusion matrix and ROC curves show Anomaly detection with CNN autoencoders for Cloud-Based AI Systems and maintaining model performance. During the experiment, the accuracy and efficiency of the model were significantly high. Data protection can process huge amounts of data faster than data quality and analyse the behaviour variation within the network system. Additionally, they can detect vulnerabilities and predict **threats with unprecedented accuracy.**

B. ROC Curves:

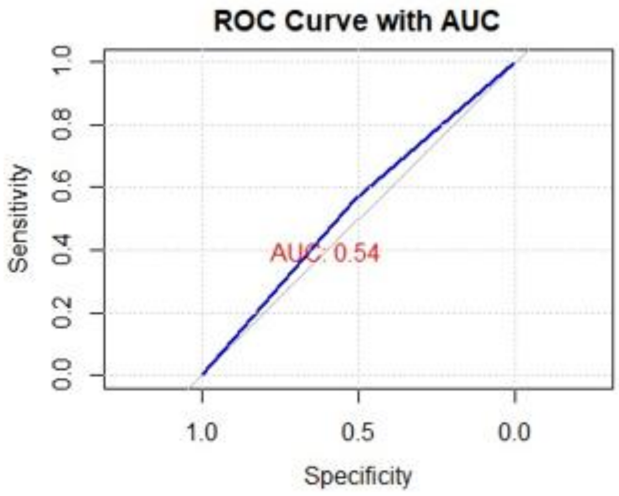

Figure 11. ROC Curve.

The ROC curve presented in Figure 11 shows the actual positive rate between categories within anomaly detection with CNN and autoencoders for Cloud-Based AI Systems. This also shows that the AI model effectively reduces network security risks and abnormal behaviour of the network system. From the above simulation model curve, it can be seen that the true positive rate increases and the false positive rate decreases. The AUC value of the ROC curve varies depending on the category. The curve slopes toward the upper left corner, indicating that the model has a higher true positive rate and a lower false positive rate, representing better performance as shown in figure 11.

7. Ethical Considerations

A. Proper Citation (Credit):

In this paper, proper citation is given to give credit to the authors. Proper citation is necessary to avoid any ethical issues in the completion of the research. Proper information regarding previous authors assists the researcher in effectively conducting the research.

B. Protection:

Data gathered from the articles is safe and protected as data protection is the main concern of the research. By assuring the ethic of protection, the data that is used will be protected. The research should consider data protection as the most important measure. If any disruption happens in the data protection, the researcher should write it in the research. Data will only be used for the information purposes. It should not be considered for any unethical purposes (Ducato, 2020).

C. Confidentiality:

Research provides information regarding the confidentiality of the data. Protective measures are adopted by the researcher to maintain the confidentiality of the research participant. The study also provides insights into who will access the data of previous studies. The credit of the authors will be written for smooth functioning. It will not be used in any other part of the research. The researcher would avoid unauthorized access to the article's data.

D. Conflict:

The researcher would avoid those factors that can create conflicts in the research. Research obtained from the articles will be done smoothly and efficiently to achieve productive outcomes. The study will be conducted effectively by considering the factors to avoid conflicts in the research. This was done for only information purposes. This understanding increases researcher information and assists the researcher in gaining more information from the participants (Heinrich, et al., 2020).

E. Free:

Another important ethical consideration was that the participants who were involved in the survey were free to respond. The people who participated in the survey were not pressured and restricted. They were free and independent to respond to the survey.

F. **Consent**:

Participants are voluntary and free to respond to the study at any time without any hurry or obstacles. Participants were informed that their privacy would not be harmed. The participants were first fully informed of the information and data that was provided.

G. Privacy:

When a survey is conducted, the participants that are involved in the data collection are assured and promised to keep their data private and their privacy will not be disturbed during the whole scenario. The privacy of the participants will not be threatened and the privacy of the data collection should not be affected.

8. Summary

The research aims to identify anomaly detection with CNN autoencoders for cloud-based AI systems. The main aim of the research was to collect data through primary and secondary methods. In this chapter, we collected data about anomaly detection with CNN autoencoders for cloud-based AI systems. by using mixed methodologies. The study provides valuable insights into anomaly detection with CNN autoencoders for cloud-based AI systems. This enables the researcher to generate productive outcomes in the completion of the research. Previous studies help the researcher gain valuable information about anomaly detection with CNN autoencoders for cloud-based AI systems.

IV. Results and discussion:

A. Introduction:

In this chapter, the author assesses the aims that the researcher tends to find. In this chapter, it was highlighted what has been done, how it is done, and how it is useful in the future. It demonstrates the efforts used in the research for validation of the data. This chapter contains the results of the findings conducted in the article. It provides valuable insights to describe what the study has achieved in this article. The results and discussion chapter of the study focuses on the experiment and simulation of the collected data. This section presents the results of the research and details related to anomaly detection with CNN autoencoders for cloud-based AI systems.

B. Data processing

The type of data used in the research is taken from the Kaggle dataset. In the Kaggle dataset, the data obtained is interpreted in the ROC curve graph and confusion matrix. The data set obtained from the data processing data will be further categorized into training and test data. This data set will help to perfectly evaluate the performance of the findings of the anomaly detection with CNN autoencoders for Cloud-Based AI Systems.

C. Data set description:

The research used data for the analysis is the Kaggle dataset which is a classic dataset in anomaly detection The Kaggle dataset contains extensive material related to artificial intelligence computing and online secured quantum processing. This dataset centers on various components to study Anomaly detection with CNN autoencoders for Cloud-Based AI Systems. The data set has been taken by Kaggle and then there is a description stated in the graphs of the ROC curve graph and confusion matrix as shown in figs 10 and 11and these graphs are interpreted.

D. Data normalization:

Data normalization is used to improve the learning and training of all the images in the research of anomaly detection with CNN autoencoders for Cloud-Based AI Systems. The normalization step is crucial because it scales and arranges all the values of the article. In the research, the normalization of data is one of the crucial steps before processing collected data from the database. It aimed to ensure the contribution of training of the model equally. The data from the dataset were normalized in the standard range which is typically from 0 to 1. Furthermore, the range is used to manage the measurement of variables on different scales within the Kaggle dataset.

9. Standardization:

All the steps used in the model of the Kaggle dataset, are for the accuracy and consistency of the research. These methods enhance the convergence of the model and make it faster than before. All the unit features are scaled for standardization.

10. Results

The research focuses on the level of accuracy of the model which is used to test the model. The test results show the anomaly for detection with CNN auto encoders for Cloud-Based AI Systems. It can be seen that preparation and testing accuracy directly affect the effectiveness of the model. This reflects how anomaly helps in the detection of the abnormal and the behavior variation within the network system. The results also show that the limitations of the model warrant expectations for the dataset used in the review.

11. Discussion:

These results help the author to evaluate Anomaly detection with CNN autoencoders for Cloud-Based AI Systems. These results also support the author to solve problems like privacy by using the results. The results achieved with accurate formation enable the author to complete the research reliably and validly.

G. Practical implications:

The findings and results of the article are accurate and consistent and organizations can also use these results to develop data quality assurance Anomaly detection with CNN auto encoders for Cloud-Based AI Systems.

V. Conclusion and Future Work:

In this paper, the data set was used to provide effective results and that data set was taken from the Kagal model dataset. The results provide valuable methods and models to consider in the data quality assurance in Anomaly detection with CNN autoencoders for Cloud-Based AI Systems.

A. Conclusion:

The article provides a valuable understanding of Anomaly detection with CNN auto encoders for Cloud-Based AI Systems. The research used the Kaggle dataset to conclude effective results.

This study demonstrates that results conduct useful information that can be used by the organization for effective implications of Anomaly detection with CNN auto encoders for Cloud-Based AI Systems. The training test and confusion model provides effective information about the classes that help in operating more accurate results. The researcher used a mixed method for better understanding that generates productive outcomes. The main findings of the results provide effective solutions to the problem statement. Overall, the research was useful and its implications can be used in organizations and workplaces shortly. The research evaluates anomaly detection with CNN auto encoders for Cloud-Based AI Systems. The research focuses on integrating protection with AI using Kaggle datasets. The research shows that artificial consciousness plays an important role in monitoring information protection. ROC curves and matrixes show that Anomaly detection with CNN and autoencoders for Cloud-Based AI Systems are effective methods of studying abnormal behavior within the network system.

B. Future work:

The article provides a valuable understanding of anomaly detection with CNN autoencoders for Cloud-Based AI Systems. The research used the Kaggle dataset model to conclude effective results. This study demonstrates that results conduct useful information that can be used by the organization for anomaly detection with CNN auto encoders for Cloud-Based AI Systems. The training test and confusion model provide effective information about the classes that help in operating more accurate results. The researcher used a mixed method for better understanding that generates productive outcomes. The main findings of the results provide effective solutions to the problem statement. Overall, the research was useful and its implications can be used in organizations and workplaces shortly. Data protection in the digital environment and detection of abnormal and changed behavior in the network system are becoming increasingly important for key development. Future research will focus on anomaly detection with CNN autoencoders for Cloud-Based AI Systems.

Bibliography

Aad, G., Abbott, B., Abbott, D., Abud, A. A., Abeling, K., Abhayasinghe, D., . . . Abulaiti, Y. (2020, april 2). ATLAS data quality operations and performance for 2015–2018 data-taking. *Journal of Instrumentation*. Retrieved from https://iopscience.iop.org/article/10.1088/1748-0221/15/04/P04003/meta

Abdulrahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2020). A Survey on Federated Learning: The Journey From Centralized to Distributed On-Site Learning and Beyond. *IEEE Internet of Things Journal, 8*(7), 5476-5497. Retrieved from https://ieeexplore.ieee.org/abstract/document/9220780

Agarwal, R. (2020). *The 5 Most Useful Techniques to Handle Imbalanced Datasets*. Retrieved from KD Nuggets: https://www.kdnuggets.com/2020/01/5-most-useful-techniques-handle-imbalanced-datasets.html

Alvarez-Rodriguez, U., M. Sanz, L. L., & Solano, E. (2018, october 4). Quantum Artificial Life in an IBM Quantum Computer. *Scientific Reports*. Retrieved from https://www.nature.com/articles/s41598-018-33125-3#Sec1

Aoki, N. (2020). An experimental study of public trust in AI chatbots in the public sector. *Science Direct, 37*(4), 101490. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0740624X1930406X

Arifin, S. R. (2018). Ethical Considerations in Qualitative Study. *International Journal of Care Scholar, 1*(2), 30-33. Retrieved from https://doi.org/10.31436/ijcs.v1i2.82

Bhandari, P. (2020, 6 12). *What Is Quantitative Research? | Definition, Uses & Methods*. Retrieved from Scribbr: https://www.scribbr.com/methodology/quantitative-research/https://www.scribbr.com/methodology/quantitative-research/https://www.scribbr.com/methodology/quantitative-research/

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., . . . Lebensold, J. (2020, april 15). Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims. *arxiv logo*. Retrieved from https://arxiv.org/abs/2004.07213

Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review, 34*(2), 257-268. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S026736491830044X

Cai, L., & Zhu, Y. (2015). The Challenges of Data Quality and Data Quality Assessment in the Big Data Era. *DATA SCIENCE JOURNAL, 14*. Retrieved from https://account.datascience.codata.org/index.php/up-j-dsj/article/view/dsj-2015-002

Chung, C. K., & Pennebaker, J. W. (2018). Textual analysis. *Measurement in social psychology*, 153-173. Retrieved from https://www2.psych.ubc.ca/~schaller/528Readings/ChungPennebaker2019.pdf

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Qubahan Academic Journal, 67*, 99-117. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S108480451600028X

Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review, 37*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364920300170

Elhoushi, M. (2011). *Quantum circuit example.* Retrieved from ResearchGate: https://www.researchgate.net/figure/Quantum-circuit-example_fig8_263928386

Enengel, B., Muhar, A., Penker, M., Freyer, B., Drlik, S., & Ritter, F. (2012). Co-production of knowledge in transdisciplinary doctoral theses on landscape development—An analysis of actor roles and knowledge types in different research phases. *Landscape and Urban Planning, 105*(1-2), 106-117. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0169204611003550

Gao, S. (2015, february). *Seasonal Trend Decomposition*. Retrieved from RPubs: https://rpubs.com/SophiaGao/58821

Geeksforgeeks. (2020, November 23). *Qubit Representation*. Retrieved from Geeksforgeeks: https://www.geeksforgeeks.org/qubit-representation/

Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Singh, K. V., . . . Misra, S. (2019, december). Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things, 8*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S2542660519302331#preview-section-introduction

González-Martínez, A., J., Bote-Lorenzo, L., M., Gómez-Sánchez, E., & Cano-Parra, R. (2015, january). Cloud computing and education: A state-of-the-art survey. *Computers & Education*, 132-151. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0360131514001985

Gudivada, V. N., Apon, A., & Ding, u. (2017). Data Quality Considerations for Big Data and Machine Learning: Going Beyond Data Cleaning andTransformations. *International Journal on Advances in Software, 10*. Retrieved from https://personales.upv.es/thinkmind/dl/journals/soft/soft_v10_n12_2017/soft_v10_n12_2017_1.pdf

Gupta, R., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Machine Learning Models for Secure Data Analytics: A taxonomy and threat model. *Computer Communications, 153*(1), 406-440. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0140366419318493

Hagemann, T., & Katsarou, K. (2020, deecember). *A Systematic Review on Anomaly Detection for Cloud Computing Environments*. Retrieved from ACM DIGITAL LIBRARY: https://dl.acm.org/doi/fullHtml/10.1145/3442536.3442550

Handelman, G. S., Kok, H. K., Chandra, R. V., Razavi, A. H., Huang, S., Brooks, M., & Lee, M. J. (2018). Peering Into the Black Box of Artificial Intelligence: Evaluation Metrics of Machine Learning Methods. *American Journal of Roentgenology, 212*(2), 38-43. Retrieved from https://ajronline.org/doi/full/10.2214/AJR.18.20224

Heinrich, M., Appendino, G., Efferth, T., Fürst, R., Izzo, A. A., Kayser, O., . . . Viljoen, A. (2020). Best practice in research – Overcoming common challenges in phytopharmacological research. *Journal of Ethnopharmacology, 246*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0378874119330338

Hochenbaum, J., Vallis, O. S., & Kejariwal, A. (2017, april). Automatic Anomaly Detection in the Cloud Via Statistical Learning. *arXiv*, 13. Retrieved from https://arxiv.org/abs/1704.07706

Janssen, M., Brous, P., Estevez, E., S.Barbosa, L., & Janowski, T. (2020, july). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly, 37*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0740624X20302719#preview-section-abstract

Janssen, M., Voort, H. v., & Wahyudi, A. (2017, january). Factors influencing big data decision-making quality. *Journal of Business Research*, *70*, 338-345. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0148296316304945#preview-section-abstract

Krstinić, D., Braović, M., Šerić, L., & Božić-Štulić, D. (2020). Multi-label classifier performance evaluation with confusion matrix. *Computer Science & Information Technology, 1*, 1-14. Retrieved from https://csitcp.com/paper/10/108csit01.pdf

Lee, J., Suh, T., Roy, D., & Baucus, M. (2019, september). Emerging Technology and Business Model Innovation: The Case of Artificial Intelligence. *Journal of Open Innovation: Technology, Market, and Complexity, 5*. Retrieved from https://www.sciencedirect.com/science/article/pii/S2199853122009817

Namasudra, S. (2018). Cloud computing: A new era. *Journal of Fundamental and Applied Sciences, 10*. Retrieved from https://www.ajol.info/index.php/jfas/article/view/172066

Ntoutsi, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M.-E., . . . Kompatsiaris, I. (2020, february 3). Bias in data-driven artificial intelligence systems—An introductory survey. *Wiley Interdisciplinary Reviews, 10*. Retrieved from https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1356

O'Shea, K., & Nash, R. (2015). An Introduction to Convolutional Neural Networks. *ArXiv*, 10. Retrieved from https://arxiv.org/pdf/1511.08458

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? *International business review, 29*(4), 101717. Retrieved from https://drjustinpaul.com/wp-content/uploads/2022/04/IBR-Art-of-Lit.pdf

Publications, M. (2020). *All about Hadamard Gates*. Retrieved from Medium: https://manningbooks.medium.com/all-about-hadamard-gates-f36110cd14a0

Saha, S. (2018, December 15). *A Comprehensive Guide to Convolutional Neural Networks — the ELI5 way*. Retrieved from MEDIUM: https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53

Séguin, L. J. (2017). The good, the bad, and the ugly: Lay attitudes and perceptions of polyamory. *Sage Journals , 22*(4). Retrieved from https://journals.sagepub.com/doi/abs/10.1177/1363460717713382

Shabbir, J., & Anwer, T. (2015, august). Artificial Intelligence and its Role in Near Future. *JOURNAL OF LATEX CLASS FILES, 14*. Retrieved from https://arxiv.org/pdf/1804.01396

Staara, B., Lütjena, M., & M. F. (2019). Anomaly detection with convolutional neural networks for industrial surface inspection. *ScienceDirect*, 484-489. Retrieved from https://pdf.sciencedirectassets.com/282173/1-s2.0-S2212827119X00025/1-s2.0-S2212827119302409/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjENn%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJIMEYCIQCiaPBcnjiuI4wZWLv2Tm9TRW57sVMCZDcoGaXJexb%2FmwIhAOpAeIa70d

Vanderplas, S., Cook, D., & Hofmann, H. (2020). Testing statistical charts: What makes a good graph? *Research Gate*, *7*(1), 61-88. Retrieved from https://www.researchgate.net/profile/Susan-Vanderplas/publication/338386060_Testing_Statistical_Charts_What_Makes_a_Good_Graph/links/600597e645851553a0522eef/Testing-Statistical-Charts-What-Makes-a-Good-Graph.pdf

Vieira, R. G., Filho, M. A., & Semolini, R. (2018, may 10). An Enhanced Seasonal-Hybrid ESD Technique for Robust Anomaly Detection on Time Series. *SEMANTIC SCHOLAR*. Retrieved from emanticscholar.org/paper/An-Enhanced-Seasonal-Hybrid-ESD-Technique-for-on-Vieira-Filho/43c6231a682bae1696ae787a655b39722cf3cc12

Vikas Hassija, V. C., Saxena, V., Chanana, V., Parashari, P., Mumtaz, S., & Guizani, M. (2020, december 2). Present landscape of quantum computing. *The Institute of Engineering and Technology, 1*(2), 42-48. Retrieved from https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-qtc.2020.0027

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access*, *8*(1), 23817-23837. Retrieved from https://ieeexplore.ieee.org/abstract/document/8963730