Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 6, 2026

DEEP LEARNING–DRIVEN REAL-TIME ANOMALY DETECTION FOR TIME-SERIES DATA IN CLOUD ENVIRONMENTS

[1]Syed Ajlal Shah, [2]Wajeeha Qayyum Chaudhary, [3]Nadeem Arif, [4]Muhammad Mudassar, [5]Daud Khan*
[1]Iqra National University, Peshawar
[2]Mirpur University of Science and Technology
[3]Administrative Officer, Office of the Registrar, University of Sargodha, Sargodha, Pakistan
[4]SSE Computer Science, School Education Department, Govt. of the Punjab
[5]Iqra National University Peshawar, Pakistan
[1]ajlalshah1@gmail.com, [2]wajeehaqayyum13@gmail.com, [3]nadeem.arif@uos.edu.pk, [4]mudassarlakseen@gmail.com, [5]daud.khan@inu.edu.pk

DOI:- https://doi.org/10.5281/zenodo.21176393

Keywords
Deep Learning, Anomaly Detection, Cloud Computing, Time-Series Data, Cybersecurity, Real-Time Monitoring.

Article History
Received: 22 May, 2026
Accepted: 27 June, 2026
Published: 29 June, 2026

Corresponding Author: * Daud Khan*

Abstract

Purpose: The present study proposes to explore the impact of using real-time anomaly detection using deep learning in cloud-based system, specifically analysing its role in the detection of anomalies in time-series data, cloud security, operational performance, scalability, and implementation challenges. The study also considers intelligent anomaly detection technologies' impact on future cloud architectures from a strategic perspective. Design/Methodology/Approach: The research design used was quantitative with a structured questionnaire that was sent to 280 professionals from the cloud computing, cybersecurity, data analytics, machine learning and related technology industry. A total of 30 items were measured using a five-point Likert scale distributed over six major constructs. The data were analyzed using descriptive statistical data, reliability analysis (Cronbach's Alpha) and chi-square testing using SPSS. Findings: Reliability analysis showed that the reliability of the questionnaire was very high, and the Cronbach's Alpha values ranged from 0.87 to 0.93 and the overall reliability coefficient was 0.91. The results found high levels of awareness and usage of deep learning technologies (M = 4.16) and the highest level of agreement was for cloud performance (M = 4.28) and security enhancement (M = 4.28). Other factors such as effectiveness of anomaly detection (M = 4.27), future directions and strategic impact (M = 4.31), and scalability and real-time processing (M = 4.20) were also highly rated. Both respondents highly agreed that deep learning is beneficial for real-time threat detection, operational efficiency, cloud reliability, and proactive risk management. But the issues of computational cost, model interpretability, privacy and availability of skilled professionals continued to be big hurdles. The results of all Chi-square showed $p < 0.01$ which revealed high level of consensus among participants. Originality/Value: The outcomes of this study give empirical evidence for the systems developed for the detection of anomalies using deep-learning models adopted, which were able to be effective, scalable, and potentially applicable for future intelligent monitoring of the cloud. The outcomes can be valuable for cloud service providers, cybersecurity professionals, researchers, and organizational decision makers looking to leverage the latest AI tools and techniques to improve cloud resilience, security, and operational efficiencies.

Introduction

Cloud computing has come a long way and is now revolutionizing how organizations store, process and manage vast amounts of data. In the modern cloud environment, a variety of applications are supported such as financial transactions, healthcare monitoring, industrial automation and Internet of Things (IoT) systems [1]. These applications produce huge amounts of time-series data that need to be monitored in real time to ensure applications are operating reliably, securely and performing well [2]. With the growing complexity and distribution of cloud infrastructures, organizations are facing a new challenge to detect abnormal patterns and anomalies in their systems to ensure service continuity and avoid costly interruptions.

Anomaly detection is the task of spotting data points, events or behaviors that are remarkably different from the normal ones [3]. Anomalies in cloud environments could signify failures in the system, security breaches, intrusions into a network, hardware failures, resource exhaustion, or issues with application performance [4]. Conventional anomaly detection methods include rule-based systems, statistical methods, or thresholds set by hand. While these approaches have been popular, they are often challenged by today's cloud-generated time-series data volume, velocity and complexity [5]. In addition, the dynamic nature of cloud environments constantly changes, making it difficult for static detection methods to keep up with new threats and anomalies.

The development of artificial intelligence (AI), especially deep learning, has brought new potentials to improve anomaly detection. Deep learning models can automatically learn complex temporal patterns and hidden relationships in large-scale datasets [6]. These models are capable of dealing with high dimensional data, are adaptive to the changing environment, and can detect the slight anomalies which are difficult to catch with the conventional approaches [7]. Sequential and time-series data have proven to be particularly effective in predicting future trends using technologies like Long Short-Term Memory (LSTM), Recurrent Neural Networks (RNNs), Autoencoders, and Transformer-based architectures. The real-time anomaly detection is crucial, especially when more and more mission-critical information is being transferred to the cloud. By detecting anomalies in real time, actions can be taken more quickly following an incident, downtime can be minimized, and cybersecurity defenses and resource management can be improved [8]. Continuous monitoring of the cloud infrastructure, prediction of failure, and early warning to the administrator are just a few capabilities that can help in cloud systems to make decisions and achieve operational resilience in advance [9]. These capabilities can have a huge impact on performance of the cloud and service level agreements.

While anomaly detection using deep learning can yield some benefits, it also poses some challenges. However, the greater complexity of the implementation can increase the needed computational resources, data quality issues, a lack of interpretation and competent people to implement it on the model [10]. The privacy, security and scalability cannot be overlooked either in implementing the advanced detection systems in cloud [11]. Therefore, it is essential to be mindful of these possibilities and challenges to develop effective strategies that maximise the use of deep learning technologies.

The paper covers the possible effectiveness and scalability of anomaly detection in cloud environments, its benefits, challenges and future developments, specifically focusing on deep learning approaches that can be used for real-time anomaly detection. The study focuses on gaining insights from the experts in the field of intelligent systems in anomaly detection for managing time-series data in today's cloud computing environment.

Problem Statement

With modern cloud environments, lots of time-series data is created, and this data should be monitored constantly to ensure reliability, security, and performance of the environment. However, many traditional anomaly detection solutions are incapable of detecting complex and evolving events in real-time and will result in potentially slow reactions to failures, cyber threats, and performance degradation. Although deep learning technologies offer cutting-edge capabilities for

anomaly detection, several challenges with regard to the scalability, computational cost, interpretation and complexity of implementation need to be taken into account by organisations. While deep learning-based real-time anomaly detection for anomaly detection in cloud environments are beneficial, their effectiveness, benefits and limitations remain to be evaluated before making decisions on their adoption.

Literature Review

Deep Learning and Time-Series Data Analytics

Time-Series Data is a collection of sequential observations made over a period of time and many cloud-based applications are built on such data [12]. Many analytic techniques are hard to manage with large, high dimensional, and continually evolving data sets. Deep learning methods have proved themselves to be efficient methods for obtaining meaningful patterns from the time-series data as they can learn complex relationships in an automatic way with limited feature engineering [13]. Sequential data processing using neural networks is well established, and has found success in various fields with increased predictive accuracy and anomaly detection.

Real-Time Anomaly Detection in Cloud Environments

Cloud infrastructures generate a lot of operational data from server activities, network, application, and user activities [14]. Real-time anomaly detection systems can be set up to keep an eye on these data flows and spot abnormal conduct in real time. Once it has been detected, the organization can respond quickly to potential threat, system failures and performance degradation [15]. The current monitoring systems are not able to detect the minute changes that deep learning models can. The demand for advanced intelligent anomaly detection systems that can facilitate real-time decision making has only increased with the need of businesses to operate seamlessly from cloud.

Deep Learning Models for Anomaly Detection

A number of deep learning architectures have been extensively used in anomaly detection applications. Specifically, Recurrent Neural Networks and Long Short-Term Memory networks have been found to be particularly effective in modelling temporal dependencies in series data [16]. Autoencoders are usually used to learn a desirable behavior of a system and identify abnormal behavior by computing the error on reconstruction. Recently, transformer-based models have attracted interest for their ability to detect high accuracy with an efficient processing of long sequences [17]. These models are more flexible and adaptable to analyse huge time-series datasets that are generated by the cloud.

Cloud Security and Operational Performance

One important technique in the improvement of the cloud safety and rising of the operational effectiveness is anomaly detection [18]. Advanced monitoring systems can detect unusual behaviors that could signal a cybersecurity incident, an attempted unauthorized access, a distributed denial-of-service (DDoS) attack, and malware activity [19]. By using deep learning based anomaly detection, organizations can act quickly and effectively on threats. Aside from security, they also assist in performance, identifying abnormal resource usage, infrastructure issues, and potential service interruptions before they become serious.

Scalability and Adaptive Learning Capabilities

Scalability of resources with respect to workload is the most significant advantages of cloud computing [20]. Therefore, an important requirement for anomaly detection systems implemented in cloud is to be able to process a huge amount of data without affecting the performance. For scalable analytics, one possible implementation is the use of deep learning models with distributed computing resources along with adaptive learning process [22]. These capabilities can facilitate detection systems' ability to continually learn and adapt to address evolving data patterns and operational conditions.

Challenges and Future Research Directions

Despite the great potential of deep learning for anomaly detection, the implementation of deep learning still remains challenging for organizations. The lack of explainability, data quality, model complexity, and computational costs can decrease the rate of adoption [23]. Furthermore, the organisations have to possess some special skills for the creation of deep learning models, their management and optimisation [24]. Some potential future research directions include explainable artificial intelligence, lightweight models

architectures, machine learning automation, federated learning, and hybrid anomaly detection approaches. In order to enable widespread adoption across cloud computing environments, these developments are demanding increased transparency and scalability, efficiencies and trust.

Research Objectives

1. To examine the awareness and adoption of deep learning technologies for real-time anomaly detection in cloud environments.
2. To evaluate the effectiveness of deep learning models in detecting anomalies within time-series data.
3. To assess the impact of anomaly detection systems on cloud performance, security, and operational reliability.
4. To investigate the scalability and real-time processing capabilities of deep learning-based detection systems.
5. To identify the major challenges and limitations associated with implementing deep learning-driven anomaly detection.
6. To explore future directions and strategic implications of intelligent anomaly detection technologies in cloud computing.

Research Questions

1. What is the level of awareness and adoption of deep learning technologies for anomaly detection in cloud environments?
2. How effective are deep learning models in identifying anomalies within time-series data?
3. How does real-time anomaly detection influence cloud performance, security, and operational efficiency?
4. To what extent do deep learning-based systems support scalability and real-time processing requirements?
5. What challenges and limitations affect the implementation of deep learning-driven anomaly detection systems?
6. What future opportunities and strategic benefits can organizations expect from adopting advanced anomaly detection technologies?

Methodology

Research Design

The research adopted a quantitative research design to systematically research on the use of deep learning-driven real-time anomaly detection in cloud environment. The methodology used was a descriptive and analytical survey to collect empirical data pertaining to awareness, effectiveness, scalability, challenges and future implications of deep learning technologies used for anomaly detection in time-series data. A quantitative design was deemed suitable as it allows the perceptions of the respondents to be objectively measured and statistically analyse relationships between the major constructs in the research.

Target Population and Sampling

The target audience consisted of professionals in the field of Cloud Computing, Cybersecurity, Artificial Intelligence (AI), Data Analytics, Machine Learning, and other related technologies. These are people who have real-world experience and expertise in areas such as cloud monitoring, anomaly detection and intelligent security systems. Qualified respondents in cloud-based operations and technology management have been reached out by using convenience sampling technique. 280 effective responses were collected and analysed.

Research Instrument

The designed questionnaire, based on the objectives of the study and the in-depth literature review, was used to gather the data. The instrument consisted of two sections. The first section included demographic details such as gender, age, educational qualification, professional role and work experience. The second section had 30 close-ended questions spread over six constructs: Awareness and Adoption of Deep Learning, Effectiveness of Anomaly Detection, Cloud Performance and Security Enhancement, Scalability and Real-Time Processing, Challenges and Limitations, and Future Directions and Strategic Impact. A five-point Likert scale was used to measure responses with 1 indicating Strongly Disagree and 5 indicating Strongly Agree.

Data Collection Procedure

This questionnaire was sent out through online surveys, as well as through networking with professionals. The survey was anonymous and participants were informed of its purposes before completing the survey. Ethical principles, anonymity, confidentiality and informed consent were adhered to in the collection of data to assure the integrity and credibility of research process.

Reliability and Validity Assessment

The reliability of the instrument for measuring was determined using Cronbach's Alpha Coefficient. All the coefficients exceeded the recommended value of 0.70 ranging from 0.87 to 0.93 with an average of 0.91. This suggested acceptable internal consistency and appropriate for advanced statistical analysis.

Data Analysis Techniques

The collected data were coded, cleaned and analysed with SPSS (Statistical Package for the Social Sciences). Descriptive statistics including frequencies, percentages, means and standard deviations were used for describing the characteristics of the respondents and their perceptions on the construct level. The reliability of the analysis was checked using Cronbach alpha and the statistical analysis of responses to the questionnaire items was performed by Chi square tests. The results were presented in tabular and graphical visualisations for easy interpretation and to support evidence based conclusions for the adoption and impact of anomaly detection in a cloud environment using deep learning.

Results and Analysis

The Results and Analysis section is used to reflect the findings that have been derived from the data collected and give a systematic interpretation of the obtained results in relation with the objectives of the research [19]. The purpose of this section is to present statistical results, to determine important trends, patterns and relationships between variables, and to interpret these. Results are presented using tables, figures, and analytical techniques to see how well they answer the research questions and provide a contribution to the understanding of the study.

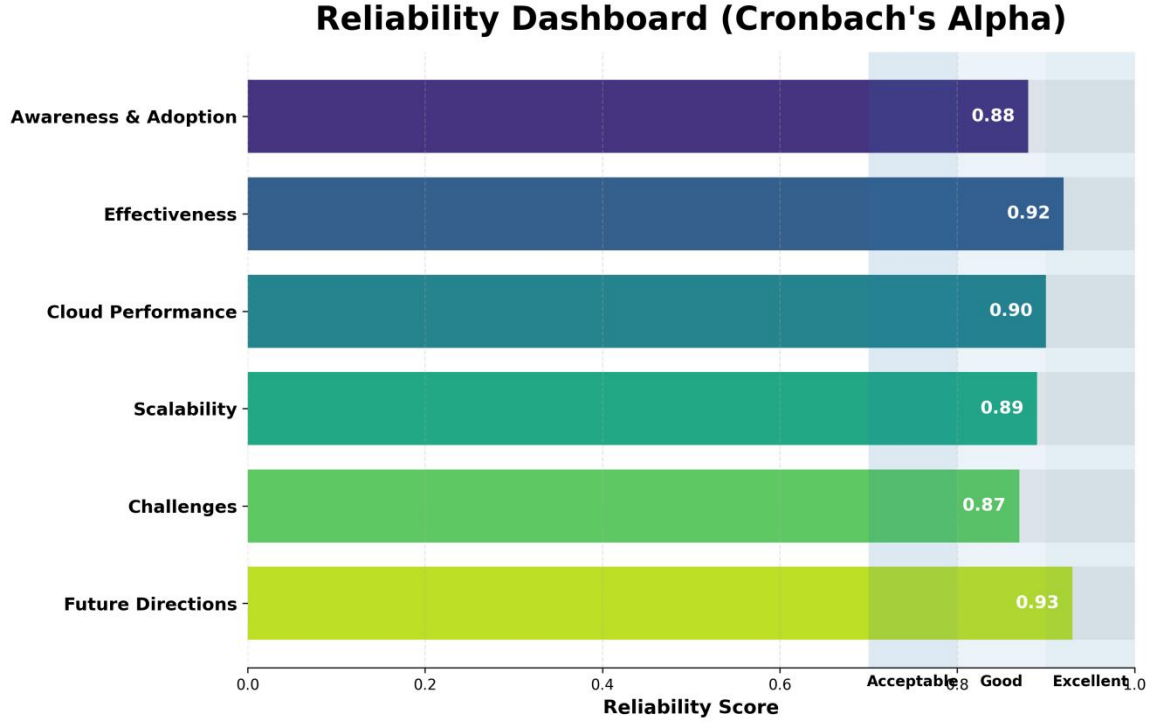

Fig 1: Reliability Analysis

Reliability analysis shows good internal consistency for all constructs in the study as the Cronbach's Alpha range from 0.87 to 0.93. Future Directions and Strategic Impact had the highest reliability (α = 0.93) and Effectiveness of Anomaly Detection (α = 0.92) with excellent measurement consistency. Cloud Performance and Security Enhancement (α = 0.90) and Scalability and Real- time Processing (α = 0.89) were also very reliable. The subscales Awareness and Adoption of Deep Learning (α = 0.88) and Challenges and Limitations (α = 0.87) showed very good reliability. The overall scale had a Cronbach's Alpha of .91 which indicates very good

reliability and is appropriate for further statistical analysis.

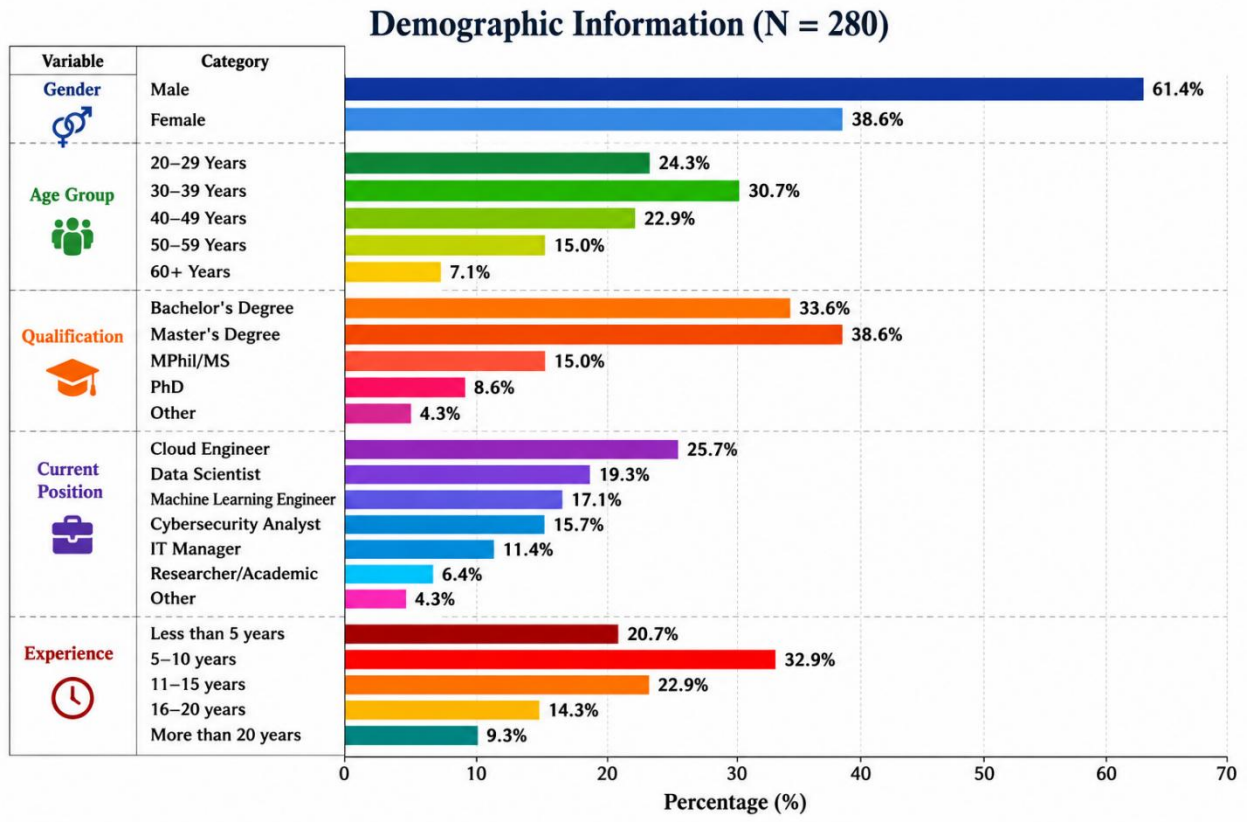

Fig 2: Demographic Profile of the respondents

The demographic profile of 280 respondents shows a higher response of males (61.4%) as compared to females (38.6%). The age group with the highest number was 30-39 years (30.7%), followed by 20-29 years (24.3%) and 40-49 years (22.9%), indicating that the workforce consisted mainly of people in the early and middle stages of their career.

In terms of education, most of the respondents (38.6%) had a Master's Degree and 33.6% of the respondents had a Bachelor's Degree, which is a highly educated sample. Professionally, Cloud Engineers (25.7%), Data Scientists (19.3%) and Machine Learning Engineers (17.1%) were the three biggest categories, reflecting high levels of representation in cloud computing and AI related professions.

Regarding work experience, majority of the respondents had 5-10 years work experience (32.9%) followed by 11-15 years work experience (22.9%) and less than 5 years work experience (20.7%). The overall sample is technically qualified and experienced and can therefore be used to assess deep-learning based anomaly detection and cloud computing environments.

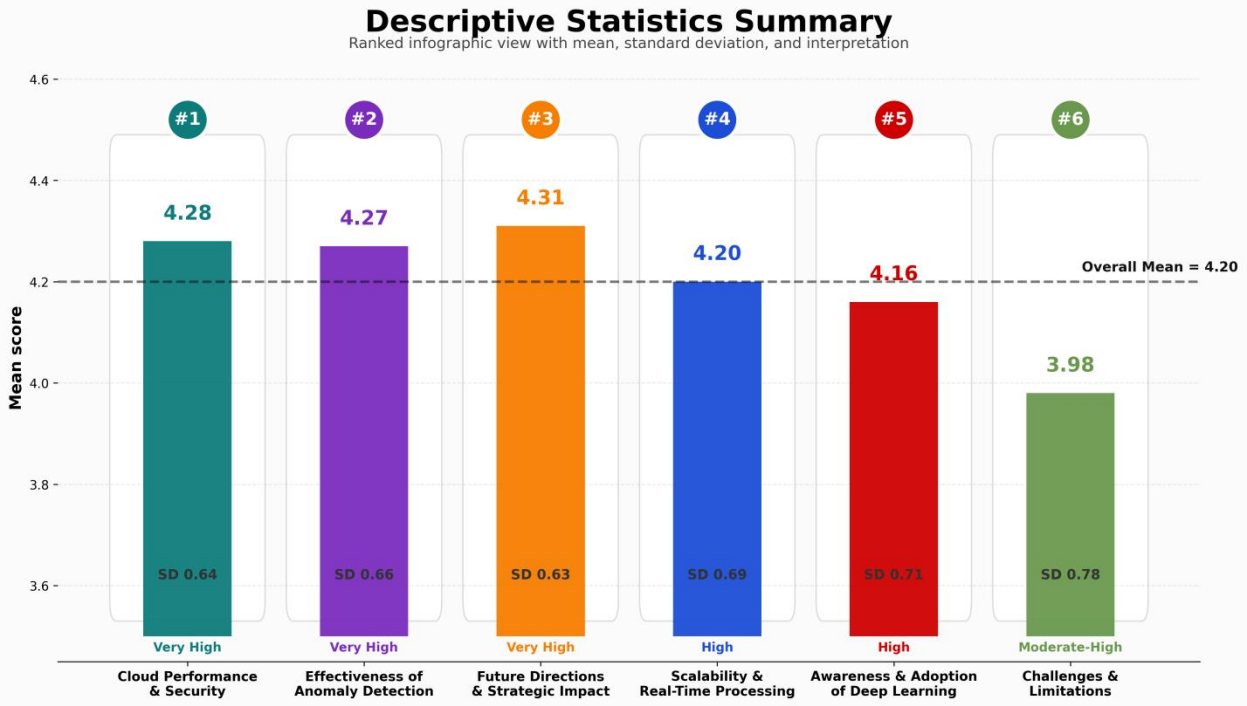

Fig 3: Descriptive Statistics

The result of descriptive analysis shows that the perception of anomaly detection based on deep learning in cloud environment is very positive. Cloud Performance and Security Enhancement had the highest mean score (M = 4.28, SD = 0.64) and displayed strong agreement to its benefits, ranking first. The effectiveness of Anomaly Detection (M = 4.27, SD = 0.66) came second; this implied the participants' confidence in the accuracy and effectiveness of deep learning models. Agreement was also very high in the Future Directions and Strategic Impact (M = 4.31, SD = 0.63), indicating optimism about the future use of deep learning technologies.

The technologies of Scalability and Real-Time Processing (M = 4.20, SD = 0.69) and Awareness and Adoption of Deep Learning (M = 4.16, SD = 0.71) gained high agreements reflecting the high level of recognition and acceptance for these technologies. The mean score of Challenges and Limitations was the lowest (M = 3.98, SD = 0.78), indicating moderate to high level of concern for barriers and limitations in implementing the practice. In conclusion, the results demonstrate the potential of deep learning techniques for cloud anomaly detection, performance optimization, and cyber security enhancement.

Table 1: *Awareness and Adoption of Deep Learning*

Item	Mean	SD	χ^2	Sig.
Familiar with deep learning techniques used for anomaly detection	4.12	0.74	28.64	0.001
Organization actively utilizes anomaly detection systems	4.05	0.79	26.38	0.002
Deep learning models are increasingly important for cloud monitoring	4.21	0.68	31.72	0.000
Real-time anomaly detection enhances cloud system reliability	4.26	0.65	33.81	0.000
Time-series analytics is essential for modern cloud infrastructures	4.18	0.71	29.44	0.001

The level of awareness and adoption of deep learning technologies was very high. Real-time anomaly detection increases the reliability of cloud systems (M = 4.26, SD = 0.65) was the highest-rated item and usage of anomaly detection systems within the organizations was the lowest (M = 4.05, SD = 0.79). The corresponding chi-square values found to be significant ($p < 0.01$) with good level of agreement between participants.

Table 2: *Effectiveness of Deep Learning-Based Anomaly Detection*

Item	Mean	SD	χ^2	Sig.
Deep learning models accurately identify abnormal patterns	4.29	0.66	35.17	0.000
Real-time anomaly detection improves incident response	4.31	0.63	36.42	0.000
Deep learning techniques reduce false-positive alerts	4.17	0.71	29.86	0.001
Automated anomaly detection improves operational efficiency	4.35	0.61	38.24	0.000
Deep learning outperforms traditional methods	4.23	0.69	32.58	0.000

There was strong agreement that the effectiveness of anomaly detection is improved with the application of deep learning. Higher mean scores were found for automated anomaly detection (M = 4.35, SD = 0.61) and the lowest mean scores were obtained for reducing false-positive alerts (M = 4.17, SD = 0.71). Results of the Chi-square tests ($p < 0.01$) validate consistent positive perceptions.

Table 3: *Cloud Performance and Security Enhancement*

Item	Mean	SD	χ^2	Sig.
Anomaly detection improves cloud infrastructure performance	4.28	0.64	34.19	0.000
Deep learning helps detect security threats in real time	4.36	0.59	39.22	0.000
Predictive anomaly detection reduces system downtime	4.22	0.68	31.06	0.000
Cloud service reliability improves through continuous monitoring	4.30	0.63	35.71	0.000
Deep learning contributes to proactive risk management	4.24	0.67	32.83	0.000

The results show the significant contribution of deep learning over clouds to both improve performance and security. Real-time detection of security threats had the highest mean (M = 4.36, SD = 0.59) and improving infrastructure performance had the lowest mean (M = 4.28, SD = 0.64). All responses were found to be statistically significant ($p<0.001$).

Table 4: *Scalability and Real-Time Processing*

Item	Mean	SD	χ^2	Sig.
Models efficiently process large-scale time-series data	4.19	0.70	30.52	0.001
Cloud platforms provide sufficient resources for analytics	4.13	0.73	27.68	0.002
Real-time anomaly detection supports workload management	4.22	0.68	31.29	0.000
Systems adapt to changing data patterns	4.18	0.69	29.77	0.001
Scalability is a major advantage of cloud-based systems	4.27	0.65	34.43	0.000

The respondents had the belief that the cloud-based deep learning systems were very scalable and effective for real time processing. The highest mean was scalability as major advantage of cloud systems (M = 4.27, SD = 0.65) and the lowest mean was availability of sufficient resources of cloud (M = 4.13, SD = 0.73). There were significant levels of agreement on all items ($p < 0.01$).

Table 5: *Challenges and Limitations*

Item	Mean	SD	χ^2	Sig.
High computational costs limit implementation	3.88	0.82	22.84	0.004
Data quality issues affect performance	4.02	0.76	25.73	0.002
Model interpretability remains a challenge	3.94	0.79	23.95	0.003
Skilled professionals are required	4.15	0.72	28.66	0.001
Privacy and security concerns hinder adoption	3.91	0.81	23.17	0.004

The participants identified some implementation issues. The highest mean scores were reported when it came to requiring skilled professionals (M = 4.15, SD = 0.72), while high computational costs had the lowest mean scores (M = 3.88, SD = 0.82). The chi square values are significant ($p < 0.01$), which means that many people have these concerns.

Table 6: *Future Directions and Strategic Impact*

Item	Mean	SD	χ^2	Sig.
AI-driven anomaly detection will become a standard cloud service	4.33	0.62	37.54	0.000
Future cloud environments will rely on autonomous monitoring	4.25	0.66	34.72	0.000
Explainable AI will improve trust in anomaly detection systems	4.18	0.70	29.84	0.001
Organizations should invest more in monitoring technologies	4.37	0.60	39.11	0.000
Deep learning will play a critical role in cloud security and reliability	4.42	0.57	41.26	0.000

The respondents were very optimistic about future of deep learning in cloud. The top two were deep learning will play a vital role in cloud security and reliability (M = 4.42, SD = 0.57) and the increased investment in monitoring technologies (M = 4.37, SD = 0.60). Everything was statistically significant ($p < 0.01$), indicating a high level of confidence and strategic impact in future potential adoption.

Discussion

The article highlights the crucial role of anomaly detection using deep learning technologies in the reliability, security, and efficiency of cloud computing systems. The awareness and adoption of deep learning technologies was found to be high in all the results which further illustrates the need for implementing an intelligent monitoring system in an organization to handle complex time-series data. The consensus agrees with other research that emphasized the need for cloud systems that are based on AI monitoring framework in modern cloud to ensure the reliability of cloud systems [1, 4].

The study also revealed that deep learning models were very effective in detecting abnormality, they are more responsive if there are incidents, prevent any kind of interference in operations and increase efficiency. This is consistent with the previous research [2, 6, 11] where the deep learning techniques like LSTM network, autoencoder and transformer-based network are found to be more useful in learning complex temporal relationships among large scale data sets in contrast to the traditional methods in anomaly detection. The respondents also highly agreed that deep learning plays a crucial role in cloud security as well as proactive risk management; intelligent anomaly detection systems are essential as they help alleviate cybersecurity risks and ensure continuity of services [5] [8] [20].

Another important finding concerns scalability and real-time processing capabilities. Participants recognized how beneficial it is for cloud-based deep learning systems to effectively process large quantities of time series data and to be flexible when it comes to changes during operation. This is in line with previous works that have tried to highlight the scaling benefits of cloud-native analytics and distributed deep learning solutions [7] [21] [22]. Respondents also mentioned implementation challenges, such as skilled professionals, computational resources, data quality management and model interpretability. The same issues have been noted in literature and stated as primary impediments for high penetration rate of deep learning technologies [10, 23, 24].

In conclusion, the optimism about the future adoption of deep learning-based anomaly detection suggests that it will soon become a ubiquitous part of cloud services. Looking forward, more funding towards autonomous monitoring, explainable AI and intelligent security systems will likely drive innovation and boost cloud resilience in the years to come [9, 12, 23].

Implementation of the Study

This study findings would be beneficial for the institutions that are interested in enhancing the management of cloud infrastructure using an anomaly detection system based on deep learning. The findings can be used to help implement intelligent monitoring systems that can detect anomalies in real time, improve cyber security resiliency, prevent system downtime and optimize system performance. These results can be invaluable for cloud service providers that seek to design scalable anomaly detection solutions to enhance service reliability to better use of resources. Moreover, the study can aid cloud experts for formulating strategies about the use of advanced

deep learning models in the cloud by decision makers, IT managers, cyber security researchers, and data scientists. The findings also highlight the need for investing in workforce training and explainable AI technologies as well as continuous monitoring capabilities to make the best use of the anomaly detection systems.

Limitations and Delimitations of the Study

The findings of this study are subject to a number of limitations. The first was that the study depended on self-reported perceptions of professionals that could be affected by personal experiences and subjective judgments. Secondly, the study used a cross sectional method and the perception changes over time could not be observed. Third, the study focused on a limited number of respondents (280) who worked in both cloud computing and cybersecurity sectors and this could impact the generalizability of the findings to other industries and/or regions. The deliverables of the study were restricted to the use of the deep learning approach to anomaly detection in cloud environments and other artificial intelligence approaches to anomaly detection and traditional detection approaches were not evaluated as part of this study. Moreover, the study focused awareness, effectiveness, scalability, challenges and future implications instead of technical performance test of specific deep learning model.

Conclusion and Recommendations

Overall, the study highlights the importance of real-time anomaly detection in cloud environments through deep learning techniques for enhancing cloud security, reliability, and performance management. The respondents show high level awareness of deep learning technologies and their confidence about providing accurate anomaly detection, enhanced incident response, scalability and effective cybersecurity defense. However, there are still challenges to address, such as computational resource, data quality, interpretability of models, privacy concerns and need of skillful professionals. The results also show that there is high confidence in the future use of autonomous monitoring systems and the use of AI-driven cloud security solutions.

According to these findings, there is a need for an increase in investment in more advanced security systems and technologies that are built on deep learning in the organization. The importance of continuous training programmes to enhance the technical ability of intelligent anomaly detection system management cannot be overstated. It's also crucial to focus on explainable AI approaches that will help enhance transparency, trust, and decision-making. Besides this the cloud service providers should work towards developing scalable and cost-effective solutions that would have the ability to handle huge time series data and high detection accuracy. Future research could involve hybrid and federated learning methods to enhance the adaptability and security of anomaly detection systems in dynamic cloud environments and further improve their effectiveness.

References

[1] A. R. Al-Ghuwairi, Y. Sharrab, D. Al-Fraihat, M. AlElaimat, A. Alsarhan, and A. Algarni, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning," Journal of Cloud Computing, vol. 12, no. 1, p. 127, 2023.

[2] H. Nizam, S. Zafar, Z. Lv, F. Wang, and X. Hu, "Real-time deep anomaly detection framework for multivariate time-series data in industrial IoT," IEEE Sensors Journal, vol. 22, no. 23, pp. 22836–22849, 2022.

[3] C. Nwachukwu, K. Durodola-Tunde, and C. Akwiwu-Uzoma, "AI-driven anomaly detection in cloud computing environments," International Journal of Science and Research Archive, vol. 13, no. 2, pp. 692–710, 2024.

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

[5] S. K. Sundaramurthy, N. Ravichandran, A. C. Inaganti, and R. Muppalaneni, "AI-driven threat detection: Leveraging machine learning for real-time cybersecurity in cloud environments," Artificial Intelligence and Machine Learning Review, vol. 6, no. 1, pp. 23–43, 2025.

[6] A. Immadisetty, "Machine learning for real-time anomaly detection," International Journal of Multidisciplinary Research, vol. 6, no. 6, pp. 1–8, 2022.

[7] R. Soma, S. K. Sahoo, F. Amin, and S. K. Mishra, "A federated learning framework for multi-parameter optimization in edge computing," in Proc. 13th Int. Conf. Intelligent Systems and Embedded Design (ISED), 2025, pp. 1–6.

[8] F. Amin and U. Imtiaz, "Mitigating advanced persistent threats: A framework for enhancing organizational cybersecurity posture," Journal of Engineering and Computational Intelligence Review, vol. 3, no. 1, pp. 99–113, 2025.

[9] U. Imtiaz and H. Elbedour, "Cybersecurity risk management in the digital era: The strategic value of ethical hacking," Spectrum of Engineering Sciences, pp. 1076–1086, 2025.

[10] U. Twaha, A. Mosaddeque, and M. Rowshon, "Accounting Implications of Using AI to Enhance Incentives for Wireless Energy Transmission in Smart Cities," *International Journal of Management Research and Global Education*, vol. 6, no. 2, pp. 1208-1218, 2025.

[11] X. Jiang, R. Jia, and F. Zhang, "Deep learning-based user behavior anomaly detection and threat early warning in cloud computing environments," Academia Nexus Journal, vol. 4, no. 3, 2025.

[12] T. A. Shiva, N. Ireen, and M. S. Islam, "Optimizing Early Intervention Strategies for Neurodiverse Children (ASD): Reducing Long-Term Public Healthcare Costs through Parent-Mediated Training," *Apex Journal of Social Sciences*, vol. 3, no. 1, pp. 30-52, 2024.

[13] F. T. Zohora and P. Paul, "Maternocare prediction for maternal and child well-being using survey data and machine learning approaches," Excel International Journal of Technology, Engineering and Management, vol. 11, no. 4, pp. 170–180, 2024.

[14] M. S. R. Aronno, M. T. Zumma, R. Prodhan, F. T. Zohora, N. Sakib, and K. B. M. Tahmiduzzaman, "A study of cyber bullying classification using social media and textual analysis based on machine learning approaches," in Proc. 14th Int. Conf. Computing, Communication and Networking Technologies (ICCCNT), 2023, pp. 1–8.

[15] A. Jabir, L. Salazar, and J. Li, "Investigation of process parameters to fabricate TiWMo refractory medium entropy alloy via laser powder bed fusion," Progress in Additive Manufacturing, 2026, doi: 10.1007/s40964-026-01648-1.

[16] M. T. Islam, A. Azeem, M. Jabir, A. Paul, and S. K. Paul, "An inventory model for a three-stage supply chain with random capacities considering disruptions and supplier reliability," Annals of Operations Research, vol. 315, no. 2, pp. 1703–1728, 2022.

[17] V. V. Raje, S. Goel, S. V. Patil, M. D. Kokate, D. A. Mane, and S. Lavate, "Realtime anomaly detection in healthcare IoT: A machine learning-driven security framework," Journal of Electrical Systems, vol. 19, no. 3, 2023.

[18] S. T. Hasan, "Machine learning models for forecasting employee demand in healthcare HR," Journal of Engineering and Computational Intelligence Review, vol. 3, no. 2, pp. 159–172, 2025.

[19] A. Ullah, "Social Media Integration for Modern Library and Information Service Promotion," *Journal of Digital Scholarship in Archives and Information*, vol. 2, no. 1, pp. 37-51, 2026.

[20] T. Akter, N. Ireen, T. A. Shiva, and S. H. Amjad, "Immersive intelligence: Using adaptive virtual reality and artificial intelligence to enhance social cognition and workforce readiness for young adults with autism spectrum disorder," *International Journal of Research & Technology*, vol. 14, no. 1, pp. 240-264, 2026.

[21] U. Twaha and Y. Arfin, "An AI-Driven Framework for Real-Time Fake News Detection: Developing a Machine Learning-Based Filter for News Platforms in the United States," *International Journal of Future Engineering Innovations*, vol. 2, no. 4, pp. 158-169, 2025, doi: 10.54660/IJFEI.2025.2.4.158-169.

[22] M. S. Islam, W. Pourmajidi, L. Zhang, J. Steinbacher, T. Erwin, and A. Miranskyy, "Anomaly detection in a large-scale cloud platform," in Proc. IEEE/ACM 43rd Int. Conf. Software Engineering: Software

Engineering in Practice (ICSE-SEIP), May 2021, pp. 150–159.

[23] A. S. Bushehri, A. Amirnia, A. Belkhiri, S. Keivanpour, F. G. de Magalhães, and G. Nicolescu, "Deep learning-driven anomaly detection for green IoT edge networks," *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 1, pp. 498–513, 2023.

[24] Q. Meng and S. Zhu, "Anomaly detection for construction vibration signals using unsupervised deep learning and cloud computing," *Advanced Engineering Informatics*, vol. 55, Art. no. 101907, 2023.