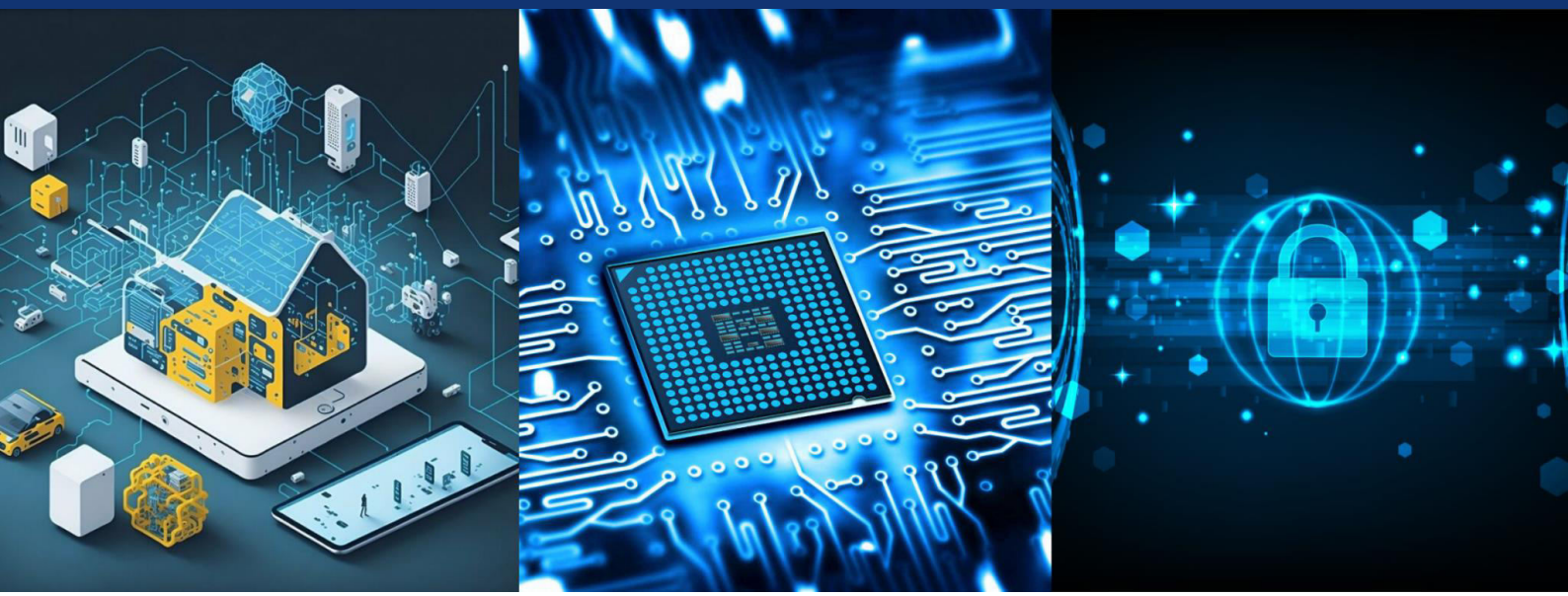
IJIRCCE

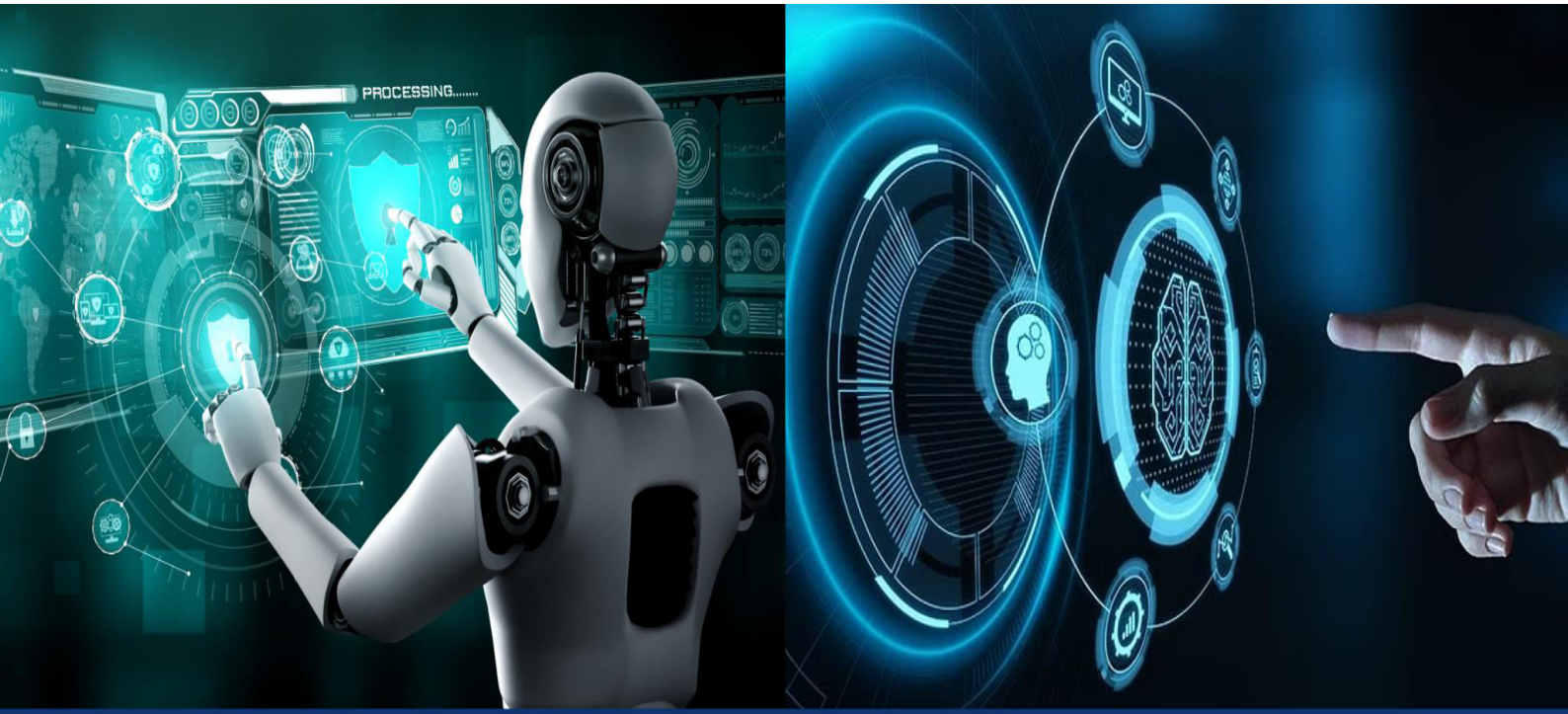
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 8, August 2026

© 2026 IJIRCCE | Volume 14, Issue 8, August 2026 DOI: 10.15680/IJIRCCE.2026.1408012

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Review of Automated Runtime Intelligence Systems for Cloud Computing

Chandan Hegde[1], Dania S[2], Kousalya C [3]

Assistant Professor, Department of Master of Computer Applications, Surana College (Autonomous), Bengaluru, India[1]

Student, Department of Master of Computer Applications, Surana College (Autonomous), Bengaluru, India[2]

Student, Department of Master of Computer Applications, Surana College (Autonomous), Bengaluru, India[3]

ABSTRACT: To guarantee the stable operation and sufficient performance of large computing systems, which may consist of many servers and are operated in centralized data centers or in cloud environments, all components have to be monitored automatically on a continuous basis. The large amount of monitoring data, which is generated by such large systems on a continuous basis, cannot be processed by manual monitoring. Therefore, many methods for the anomaly detection in such large amounts of data have been developed in the last years. However, Traditional machine learning techniques such as Isolation Forest, One-Class Support Vector Machine (OCSVM) and Local Outlier Factor may struggle to detect complex temporal relationships in system metrics. This paper provides an overview of recent approaches to automated anomaly detection, intelligent runtime monitoring, and error correction within cloud computing systems. These corresponding approaches try to combine deep learning with graph-based methods as well as with log-analysis. In addition to the survey, seven monitoring frameworks, namely AutoLog, CloudShield, The Dynamic Graph Transformer Parallel Framework (DGT-PF), ISOLATE, Maat, MoniLog and SEAD, are presented and compared to each other in terms of the used methods, the achieved goals as well as to the results, which were identified by the authors of the corresponding frameworks. This paper concludes the review by presenting the unsolved problems and research gaps, which were detected during the review.

KEYWORDS: Runtime Intelligence; Anomaly Detection; Cloud Computing; Log Analysis; Graph Neural Networks; Deep Learning; Root-Cause Localization; Automated Monitoring.

I. INTRODUCTION

The technology of automation is becoming more important in today's information world. Automation is now widely applied across multiple sectors, including healthcare, banking, education, transportation, IT security, and cloud computing. Modern large-scale software systems produce massive volumes of data, making real-time oversight and control by human operators impractical. As cloud service and online applications expand, computing systems increasingly rely on automation for effective management. This is especially critical in cloud and distributed environments, where system complexity makes manual monitoring challenging.

Cloud infrastructure generates extensive monitoring data—from CPU usage and memory consumption to network traffic, application logs, and disk activity—much of which is too voluminous and complex for efficient human analysis. To address this, automated monitoring solutions have been developed to track system behavior continuously and enhance overall performance. These systems can identify irregularities and react promptly without human intervention. Automated error detection and resolution are also gaining importance, as the sheer volume of monitoring data exceeds the capacity of traditional, manual approaches.

Overall, process automation is essential for handling the vast data streams produced by large software systems, particularly within cloud and distributed computing environments. The task of monitoring, for example, in healthcare services or in other services offered on the Internet, continuously monitoring of all servers, applications and services in the cloud, for detecting anomalies in the large amount of monitoring data automatically by analyzing them manually is a complex, time-consuming and not efficient task and thus leads to a long delay before being able to react to failures and incidents. In order to automatically monitor, log and analyze huge amounts of monitoring data of different services and applications running on clouds, many automation concepts for the runtime monitoring of cloud systems have been introduced in resent years

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Research in recent years has focused on several systems namely; MoniLog, AutoLog, CloudShield and Maat for the improvement of runtime monitoring and reliability of cloud computing systems. These automated systems enable continuous monitoring of system behaviors, detecting deviating events, and supporting the optimization of the systems under surveillance. Through these automations, human operators are freed from intensive monitoring of systems under surveillance while detection and response to errors occur at a faster rate.

Currently, there are limitations in automating error detection and correction in cloud systems. Due to the large-scale nature of cloud systems, amounts of data being monitored in the current implementations of systems in the cloud are too large to be manually-monitored especially since they run continuously throughout the year. This makes it very hard to manually identify anomalies, server crashes, network congestion, memory leaks, or any other irregularity in other components of the system which may cause system downtime and poor user experience. The current automated approaches for anomaly detection in the components of computer systems and their temporal relationships using machine learning are not always reliable due to variance in workload which causes a decrease in the accuracy of anomaly detection. There is therefore a need to develop and adopt automation approaches for error detection and correction and improve reliability of cloud systems.

To address the problem of automating error detection and correction in cloud computing systems, research has focused on developing automation approaches for anomaly detection in general. In this regard, log data is monitored and analyzed together with a large volume of other forms of monitored data using Machine Learning approaches and graph learning algorithms. Some of the approaches recently introduced in this field include ISOLATE, AnoFusion as well as new log monitoring approaches such as MoniLog introduced by recent research. Additionally, monitoring systems based on Vision Transformers have also been introduced recently.

Amongst the different techniques used in anomaly detection approaches, different Neural Networks have also been adopted in various methods. These include the Long Short-Term Memory Networks, Graph Neural Networks, Graph Attention Networks, Variational Autoencoders, and Convolution Neural Networks for processing different forms of log data, sequential data and graphs respectively. There has also been introduction of Positive-Unlabeled learning, active learning, and adversarial learning for anomaly detection in noisy environments. Automation of anomaly detection systems has improved reliability of cloud systems while reducing the downtime during failures.

II. OBJECTIVE OF THE WORK

In this paper, the authors present a survey of the state-of-the-art methods, including systems and frameworks, for automatically detecting anomalies, monitoring systems and fixing errors in the Cloud data centers.

- Classification of traditional machine learning approaches and deep learning approaches, as well as graph neural networks and log-based monitoring for the purpose of runtime anomaly detection in clouds.
- The ways in which different types of an anomaly detection can benefit from temporal information, interrelated metrics and behavior causing anomalies for fault detection and for root-cause analysis of anomalies are discussed.
- The current practice in the field is reviewed, leading to the presentation of a number of frameworks and systems (ISOLATE, CloudShield, MoniLog, AutoLog, Maat, DGT-PF, SEAD) for intelligent cloud monitoring.
- The strengths and weaknesses of the approaches used in these frameworks and systems are discussed. In addition, the author of this article tries to describe potential areas of application for each of these approaches for intelligent cloud monitoring and describe existing practical implementations in detail.
- Furthermore, the author analyzes the research gaps in terms of the level of automation and reliability of methods for building highly efficient cloud monitoring systems of a large scale.

III. LITERATURE REVIEW

AutoLog: A Log Sequence Synthesis Framework for Anomaly Detection

Huo et al. proposed AutoLog, a log sequence synthesis framework for generating runtime log sequences automatically for anomaly detection in cloud systems [1]. The main work of this paper focuses on overcoming the limitations of traditional passive log collection methods. The authors used program analysis, execution graph construction, and logging statement probing techniques to generate scalable and flexible datasets. Experimental results showed that AutoLog generated more comprehensive log events and improved anomaly detection performance compared to existing datasets.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The paper suggested that future work can focus on improving dataset realism and supporting more programming environments; however, the major research gap identified was the lack of highly diverse real-world industrial log datasets.

CloudShield: Real-Time Anomaly Detection in Cloud Environments

He and Lee proposed CloudShield, A Deep Learning Framework for Anomaly Detection in Cloud Environments [2]. The research conducted was mainly aimed at developing techniques and frameworks for detecting temporal anomalies and attacks in real-time in cloud computing environments. The created framework was using pretrained deep learning models, reconstruction error distribution, hardware performance counters, and PCA-based feature selection to monitor the clouds' behavioural patterns. The obtained results demonstrated that CloudShield could successfully detect attacks, including Spectre and Meltdown, in real-time with significantly reduced false-positive rates. The paper recommended further improvement of adaptive learning capabilities and scalability to address highly dynamic cloud workloads, which remains an open issue for the framework.

An Efficient Anomaly Localization in Cloud Infrastructures Using a Dynamic Graph Transformer Framework

He et al. introduced a Dynamic Graph Transformer Parallel Framework (DGT-PF) for detecting anomalies in cloud systems infrastructures [3]. The central message of this article is that the accuracy of anomaly localization in cloud environments can be improved. The new framework was built on the basis of Transformer-based networks, Graph Neural Networks, attention mechanisms, and dynamic graph embedding. In this study, the authors analysed the performance of the developed model and proved its effectiveness in terms of F1-scores compared to existing solutions for anomaly detection. Notably, the researchers identified a number of recommendations for future work, including optimizing the framework's computational power. At the same time, the efficient and effective processing of large amounts of unstructured data that make up cloud monitoring remains a critical area for improvement.

Identifying Performance Issues in Cloud Service Systems Based on Relational-Temporal Features

Gu et al. proposed ISOLATE, a framework for identifying performance issues in cloud service systems using relational-temporal features [4]. The research explored the identification of performance anomalies via key performance indicator (KPI) dependency and temporal patterns. The work proposed a novel approach, which utilized graph-based neural network models, GRU, convolution, attention-based techniques, along with positive-unlabeled techniques to address the problem of noisy cloud monitoring data and achieve better results in anomaly detection and root cause identification. The experiments demonstrated the effectiveness of the new method, which outperformed the state-of-the-art solutions. The authors suggest that future research should focus on scaling and optimization since their approach is still computationally expensive for large cloud platforms and remains challenging in the context of noisy and complex runtime environments.

Maat: Predicting Performance Anomalies in Cloud Services Using Conditional Diffusion

Lee et al. introduced Maat, a cloud service framework that can anticipate anomalies faster than real time [5]. The main work of this paper focused on predicting anomalies before their actual occurrence to improve cloud reliability. The framework used conditional denoising diffusion models, metric forecasting, and Isolation Forest algorithms to detect anomalies anticipation and detection. Experimental results demonstrated better anomaly anticipation performance and higher F1-scores compared with traditional real-time detectors. The authors suggested that future research on integrating domain-specific intelligence and advanced forecasting techniques; however, forecasting highly unpredictable anomalies still remains a major challenge in runtime intelligence systems.

MoniLog: An Automated System for Detecting Anomalies in Cloud Logs

Vervaet in 2016 proposed an automated log-based anomaly detection approach for large-scale systems cloud computing infrastructures, namely MoniLog [6]. In this paper, the author undertook to discover, in real time, the sequential and quantitative anomalies auto escalating from several streams of a cloud infrastructure's logs. MoniLog uses log parsing, anomaly detection and classification, and distributed monitoring to achieve a scalable cloud monitoring framework. The experiments performed to test this framework had positive outcomes, with the performance of logging monitoring being improved and supporting scalable anomalous event handling. The author also discussed future improvements to MoniLog, such as improving classification accuracy and handling unstable log streams. Thus, the analysis of noisy and evolving logs in cloud systems is a challenging research problem that has practical implications.

An Online Self - Learning for Anomaly Detection in Cloud Computing

Wang et al. in [7] proposed SEAD, Online Self-Learning for Anomaly Detection in Cloud Computing. SEAD allows for online self-evolving learning. SEAD is capable of learning newly emerged anomalies without extensive training data

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

labelling. It is because SEAD uses the runtime performance metrics, adaptive online learning algorithm, and self-evolving anomaly detection framework. The authors provided the results of the experiments that show the accuracy of the detected anomalies. They also showed how SEAD reduces the managerial overhead of the cloud managers. The autonomic cloud management is indeed one of the aspects that require improvement. Keeping the accuracy of anomaly detection high in the highly volatile cloud is also an open problem that needs to be addressed.

IV. RESEARCH GAPS IDENTIFIED

Each of surveyed approaches has some drawbacks and identifies several research challenges for automated anomaly detection in runtime intelligence for clouds.

- A range of diverse, realistic, industrial log data sets does not exist: Although AutoLog automatically generated log sequences for Anomaly Detection Models, they cannot fully test the validity of anomaly detection models using a range of diverse, realistic, industrial log data sets [1].
- There is still a big open issue when it comes to workloads that are changing heavily and are highly dynamic. Also the authors of CloudShield are dealing with this problem. For mostly static scenarios already good results are achieved by the frameworks under review, however, for highly dynamic and heavily changing workloads it is still very difficult to maintain stable and accurate detection [2][7].

• Supporting large-scale, mostly unlabelled, noisy data processing efficiently: As it was mentioned in the introduction of the text on cloud monitoring, the input data is of very large sizes and has a lot of noise. Therefore, it is a non-trivial task to process this data in an efficient and accurate way using the existing systems. To address this issue, DGT-PF and ISOLATE utilize the graph-based and attention-based techniques, respectively, which enable improving the localization and detection accuracy. At the same time, a more important task is to find ways to process such data in a much more efficient and scalable way. In other words, instead of detecting the already appeared anomalies, future work should concentrate on predicting the yet unoccurred and even unforeseen ones. Conditional diffusion models for log data in future time steps could be a first approach to tackle this problem as it is already done in Maat [5].

- Log-stream analysis is unstable: As the fully-automated log parsing and classification is already challenging for log analysis of multi-source, noisy and very dynamic cloud environments in real time, for accurate anomaly classification, it is very challenging [6].
- Lack of fully autonomous cloud management: While SEAD reduces the amount of required labeled training data for learning to detect anomalies by means of online self-evolving learning, the current state of research does not yet allow for fully autonomous cloud management without any performance degradation, even for relatively static workloads [7].

None of the approaches mentioned above can be applied singularly. The future runtime intelligence system for managing such a complex system as the cloud requires multi-faceted, multi-pronged solutions, which would bring together the best of breed capabilities of different technologies, such as diffusion-based forecasting, graph-based relational models, and self-evolving online learning, to allow for truly autonomous cloud management at enterprise scales with minimal human intervention and operational risk.

V. CONCLUSION

The following is a review that compares various automation approaches of anomaly detection, intelligent monitoring and error handling in a cloud environment. There are seven frameworks considered by the authors and reviewed in the paper. AutoLog, CloudShield, DGT-PF, ISOLATE, Maat, MoniLog and SEAD. Each uses different techniques for runtime intelligence, ranging from deep learning to graph-based approaches. Some examples include synthetic log-sequence data, diffusion-based prediction and many more. All of them are able to provide faster detection time, lower false alarms, root-cause analysis, and monitoring. In most cases they demonstrate better performance than Isolation Forest, OCSVM, and Local Outlier Factor.

However, the review also identifies certain limitations of the current state-of-the-art research in the area of runtime intelligence, which can serve as a starting point for future works . Chief among these challenges and areas of needed research are: 1) an insufficiency of sufficient numbers of diverse, realistic, and industrial-scale datasets; 2) problems related to stable performance under fluctuating workloads and large volumes of data; 3) issues efficiently dealing with large amounts of monitoring data that have not been labeled for detection purposes; and 4) robust and accurate forecasting

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

of very unpredictable anomalies. In addition to these challenges, dealing with noisy log streams that are continuously changing is very challenging. The biggest challenge, however, is the huge gap between currently available frameworks and the development of fully autonomous and self-adaptive monitoring systems. In other words, even though individual frameworks can be very strong in given evaluation settings, a unifying adaptive architecture is required to develop a production-ready runtime intelligence system for cloud monitoring.

Automated anomaly detection for intelligent monitoring and error management of cloud systems is a field of research that has recently started to mature. However, there are many open research challenges that still need to be addressed in more detail, such as not having a diverse set of industrially relevant datasets, stable performance under dynamic workloads, efficient processing of very large amounts of unlabeled monitoring data, the forecast of anomalies, stable analysis of log data that contains noise and is changing over time, and fully autonomous self-adaptive monitoring systems for runtime intelligence.

REFERENCES

[1] Huo, Y., et al. "AutoLog: A Log Sequence Synthesis Framework for Anomaly Detection."
[2] He, Z. and Lee, K. "CloudShield: Real-time Anomaly Detection in the Cloud."
[3] He, Z., et al. "Efficiently Localizing System Anomalies for Cloud Infrastructures: A Novel Dynamic Graph Transformer based Parallel Framework."
[4] Gu, J., et al. "Identifying Performance Issues in Cloud Service Systems Based on Relational-Temporal Features."
[5] Lee, C., et al. "Maat: Performance Metric Anomaly Anticipation for Cloud Services with Conditional Diffusion."
[6] Vervaet, A. "MoniLog: An Automated Log-Based Anomaly Detection System for Cloud Computing Infrastructures."
[7] Wang, T., et al. "Online Self-Evolving Anomaly Detection in Cloud Computing Environments."

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details