Journal of Sustainable Solutions
ISSN : 3048-6947 | Vol. 1 | Issue 4 | Oct - Dec 2024 | Peer Reviewed & Refereed

Using AI for Real-Time Cloud-Based System Monitoring

Laxmana Kumar Bhavandla*
Independent Researcher, USA.

Accepted: 01/10/2024 Published: 02/11/2024 * Corresponding author

How to Cite this Article:
Bhavandla, L. (2024). Using AI for Real-Time Cloud-Based System Monitoring, *Journal of Sustainable Solutions*, 1(4), 187-196.
DOI: https://doi.org/10.36676/j.sust.sol.v1.i4.51

Abstract
This paper aims to discuss the application of the real-time cloud-based system-monitoring system with the help of artificial intelligence while describing its advantages, limitations, and possible developments. Due to the increase in cloud solution sophistication, AI solutions provide approaches for a massive co-scale scalability and the capacity to discover and dodge severe issues efficiently while improving overall efficiency. The critical capabilities of AI are, for example, anomaly detection, predictive analytics and automatic response. However, there are some issues that include; data availability issues, model bias issues, and the problems associated with model integration in order to support deployment of the AI ML. The paper explores prospects of AI in the monitoring of clouds with focus on; enhanced prediction mechanisms, edge computing and explainable AI.

Keywords
AI, cloud monitoring, anomalous behaviour detection, predictive analysis

Introduction

Cloud computing is gaining widespread acceptance and has become integrated to IT infrastructure over the last couple of years as it provides mainly scale and flexibility. However, as cloud systems continue to become more and more complex, the need for real time monitoring cannot be overemphasised for the sustenance of the effectiveness and security of the system. It is also important to note that traditional monitoring tools typically fail to process large amounts of information and detect incidents promptly. This is where Artificial Intelligence (AI) comes into play facilitating intelligent monitoring processes than traditional methods. AI solutions use machine learning as well as predictive analytics so as to identify risks, potential problems, as well as provide responses automatically. The adoption of AI within cloud computing is therefore not limited to cutting the costs of cloud monitoring but also provides scalability and security of any cloud system.

Real-Time Monitoring

Real-time monitoring in cloud environment facilitated by AI as a powerful solution for cloud system's optimization, effective performance, and security. It not only enhances the conventional monitoring features where AI is implemented but also represents the new generation of cloud monitoring – Temporal, Automated and Self-vigilant monitoring systems.

The basic cloud monitoring methods that have been developed are proactive and predominantly focused on the use of rules/checklists and performance thresholds. These existing systems, although efficient in some contexts, are not adequate because they are unable to process huge amounts of data or respond to dynamic environments.

On the other hand, AI-based monitoring, AI/ML/DL, and related approaches are applied to the analysing, recognising, and predicting of data and monitoring the system to be more effective. One of the important aspects of AI application in real-time monitoring is its capability of analysing large amount of data that cannot be feasibly done by the traditional systems.

Cloud computing platforms produce vast amounts of data from servers, virtual machines, network equipment, and applications. Such big data and unstructured information can be handled and analysed in real time by AI algorithms to gain comprehensible insights.

At the same time, relying on Machine learning models, they can learn from the data accumulated in the course of their work and adjust the prognosis made by them according to evolving tendencies (Stutz et al., 2024). This makes it possible for the AI enabled system to proactively identify incidences such as; traffic surges, downtimes, or degradations within much shorter time frames than with rule-based systems.

As a tool in monitoring clouds, Anomaly detection is one of AI's keys uses due to helping minimize the occurrence of major problems as well as increase the durability of systems by providing early indication of possible problems on the horizon. Also, the foresight of probable failures or limitations within performance can be done using AI in real-time monitor an added advantage of using AI.

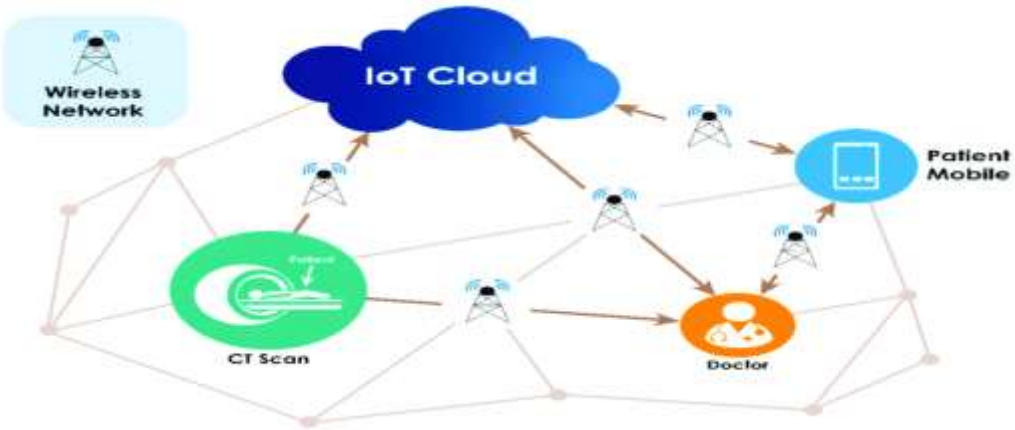

Figure 1 Prototype model for remote patient monitoring with cloud-based AI Model (ResearchGate, 2023)

It is, for example, possible to use predictive analytics and machine learning algorithms to point at future problems, such as lack of resources or hardware failure. For instance, based on the data of usage, AI can predict when a certain server may run out of space or when an application's performance may deteriorate (Olabanji et al., 2024).

Before such events happen, the forecast can help the cloud administrators take precautionary measures that will help to avoid such problems, and thus, prevent their occurrence telling them that more resources are needed, workload is poorly optimized or that maintenance is required to avoid a system crash.

It is in this regard that predictive maintenance not only enhance the operational effectiveness, but also decrease costs related to system breakdowns and requiring an urgent fix. Real-time monitoring also contains another option – the function of AI in increasing the protection level of the system. As cloud systems evolve to be more refined and integrated, more threats have wider access, defeating the intent of extensive security surveillance.

AI informed real time monitoring systems can identify and addressing security threats faster than conventional systems. Indeed, AI algorithms are capable of recognizing tendencies connected with

negative actions, including attempts to enter the system from unfamiliar accounts, high levels of traffic, or attempting to read restricted information.

These can be set up to provide log and generated alerts or take corrective measures such as blocking the IP address and / or moving the suspect computer off the network to avoid its exposure to a certain kind of security threat (Olabanji et al., 2024). Compared to rule-based IDS, Machine learning-based IDS can learn and update with time making it almost impossible for it to produce false alarms and take much less time to detect real threats.

Next to anomaly detection and prediction for maintenance, AI can improve real-time monitoring with help of decision making by itself. AI systems can take decision related to systems performance and resource availability based on different log, metrics, and network traffics.

For instance, AI can dynamically optimize the portion of CPU for workloads thus avoiding bottlenecks on performance. By using AI, the cloud infrastructure, its resources can be arranged and relocated for the benefit of resource utilization in other areas of the organizational system to save on ceilings.

AI gains the capacity to reason unto itself and make independent decisions on the acquired data for controlling cloud systems with minimal intervening human interaction and constantly optimal performance (Rahaman et al., 2024). Also, if real-time performance of the system is monitored using AI, it is possible to obtain more detailed data.

Figure 2 Is AI the Future of Cloud Management? (Zesty, 2023)

Traditional forms of monitoring are not very useful as they provide only a narrow view into the system and resources such as CPU or memory usage. That said, the problem with these metrics is that they do not tell the whole story of how specific parts of the cloud system are working.

Computation models of AI can further explain how a system behaves at a different stratum where other complex interrelationships between parts of a system can also be revealed (Srinivas et al., 2024). For instance, AI can be used to relate the characteristics of traffic over the network to performance of an application and always identify the problem.

While virtualization provides visibility into the physical machine layer and allows cloud administrators to take more precise actions to address issues, this higher level of abstraction offers much better insight into complicated application topologies and helps administrators make much more precise decisions regarding trouble shooting at the physical level.

It is expected that AI-based real-time monitoring can be challenging when integrated with current cloud architecture. Most cloud service providers like AWS, Microsoft Azure or Google Cloud services have native monitoring solutions, however these tools are not always integrated with AI-based tools.

The integration of the AI models to an existing monitoring system is a complex process that needs planning and engineering knowledge. Also, monitoring systems with the involvement of AI should be trained on big data for the model to succeed in what it does, and this takes a lot of computing power.

Therefore, organisations must have infrastructures and adequately implement the right data management processes that can support AI models (Chanthati, 2024). There are obstacles which needs to be considered; yet, one must start with mentioning that the advantages of AI-level monitoring overcome the costs of initial preparations relatively quickly, especially considering the constant improvement of AI technologies and extensive integration of them into cloud services' offerings.

The future of real time cloud monitoring using AI is bright since there are ongoing developments of machine learning, natural language processing and other technologies that improve the performance of monitoring systems.

Thus, whilst AI continues to advance in capability, it can be expected that the monitoring of the cloud will also become referred to as even more intelligent and self-governing and increasingly entwined into the rest of cloud environment (Sanodia, 2024). For instance, AI will find applications in multi-cloud and hybrid cloud environments, where businesses may need to implement systems in multiple clouds and monitor them as well.

AI could also assist in getting the most out of new technologies like edge computing, which refers to the use of enhanced computations instead of general-purpose cloud computing data centres. AI introduces flexibility to these environments, whereby organizations utilizing cloud-based systems can guarantee the effectiveness and securitization of their systems, besides easing the workload for human administrators.

Real-time monitoring by the power of AI is one of the many advances in the approach to managing and maintaining cloud systems. Using AI systems' ability to analyse big data, identify risks, and provide recommendations for various operations, decision-making can result in higher cloud performance, security, and reliability.

With the increasing sophistication and size of cloud environments, AI monitoring shall remain primal in affordance as it prevents disruptions in the system. The further advancement of AI technologies means promising prospects for cloud-based system monitoring in the future; the prospects bring even more benefits in terms of increasing efficiency and reducing expenses as well as increasing protection degrees.

Technologies and Tools

AI & ML solutions in modern cloud environments can significantly support their monitoring in real time, as the usage of the mentioned technologies unfolds rapidly in this sphere. The relationship that can be realized in the cloud stratagem is the ability of the businesses to comfortably deploy, govern, and accommodate the lancinating applications and or services but the hard narrowly of analysing, proactively, the well-being of these systems.

Most of these systems are based on physical and logical rules and require a great amount of attention from an administrator, missing the mark when it comes to the actual mass of cloud environments today (Rehan, 2024). While leveraging other tools, organizations must study large volumes of complex data and make appropriate decisions in real time, and this is where AI tools act as powerful tools that help achieve the right goals by measuring and controlling organizational performance and security.

The array of technologies and tools that underpin this transition include traditional monitoring tools, Cloud-native monitoring tools, third-party developed AI tools, all of which enhances the monitoring capabilities to be smarter, more integrated and automated. Today, the leading cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud have invested a great deal in supplying native tools for monitoring cloud systems.

Figure 3 The Evolution of AI in Cloud Computing: From Basics to Advanced Applications (MEGA, 2023)

For example, the AWS has a CloudWatch which is an integrated solution that metrics, logs and events from multiple AWS resources. CloudWatch, although suitable for routine monitoring, is not equipped with machine learning algorithms as are needed for actual time monitoring of complex systems.

This is where we get to the AI part of the equation, or the Artificial Intelligence as is commonly referred to (Chavan et al., 2024). There is also the CloudWatch feature which can come in handy in providing predictions on system failures and anomalous behaviour from the previous data feed to enable the Machine Learning application to develop models for use in decision making. This makes it possible for cloud administrators to get ahead of potential problems they could result in worst situations, like resource or workload reallocation.

The similar tool that can be used in Microsoft Azure environment is Azure Monitor which gives an insight into usage and state of the resources. Almost all kinds of data are gathered: from virtual machines through databases to applications (Jones, 2024). Azure Monitor has also included elements of AI processing algorithms in its functionality, for example, based on machine learning, which allows for sorting metrics and logs, finding outliers and features that can be considered unusual.

AI tools in Azure allow an organization to identify quickly any performance problems, security threats, or any other issues in the system rather than using conventional monitoring techniques. Google Cloud Operations Suite is also another cloud-native monitoring software that was formerly called Stack driver and is equipped with AI overtones to provide performance data.

Google Cloud's monitoring tools can have lessons from the data coming in and adjust its future predictions toward resource utilization appropriately. In addition to the native monitoring tools available from all cloud providers, there is a plethora of other tools designed to enrich cloud real-time monitoring. Most of these are AI-driven and built to work well with the preferred cloud setting/stack; some of the benefits of these include; predictive analysis, enhanced anomaly detection, incorporation of an auto-response mechanism.

An example is Datadog that offers an end-to-end monitoring tool that focuses on cloud-native infrastructure and applications, logs. By employing its own machine learning, the company is able to detect any abnormality in the various components of the system in order to easily establish whether there are any performance or security problems (Villegas et al., 2024). It also provides compatibility

with other monitoring solutions and helps the program gather information from numerous cloud services, generating a single perspective of system status.

Another third-party solution of interest is New Relic, which offers full-stake observability for cloud-based applications. With the help of AI and ML, New Relic's platform identifies and prevents issues in application performance, predicts failure in a system, and optimizes resource utilization.

New Relic can then use this intelligence to adapt alert thresholds to a much more effective level where it provides real-life dynamic alerts because alerts do not come from pre-set, rigid limits. This way, the much-despised alert fatigue phenomenon is avoided, and administrators are notified in case of emergent events only. Like any other device, Splunk is another intelligent AI-based tool that can also analyse different machine data for IT operations.

This acquires a host of data from different sources such as cloud platforms and automatically learns and scales to capture patterns and anomalies that might point out to problems. Splunk also allows monitoring tool and other intelligent artificial solutions to be connected to build an intelligent monitoring environment.

However, there are other artificial intelligence technologies which support monitoring in real-time mode: Some examples of representative technologies include machine learning, deep learning, and natural language processing (NLP), all of which are already being included in cloud monitoring tools (Barua et al., 2024).

Data gathered can be used to train a machine learning program for pattern recognition, and utilize this information to influence future performance, with cloud administrators able to act in advance to mitigate potential problems of resource unavailability or poor usage. Machine learning sub-discipline known as deep learning involves a larger number of layers within the neural networks and can be applied in application areas such as: anomaly identification and predictive analysis. Gradual learning with big data and small features provides deep learning models better accuracy to understand overall system performance.

Natural language processing, another important AI technology, is also being employed to proactively improve the way that cloud monitoring tools analyse unstructured information. This includes logs, error messages, and alerts because these are usually written in natural language and are hard for script-based tool to parse. The use of NLP makes it easier for monitoring tools to analyse text-based information and respond to such data, making incidents to be detected and solved with a glance.

In order to show the variety of the tools and their possibilities, below is the table which describes several AI-based monitoring solutions for cloud platforms:

Tool	Platform	AI Capabilities	Key Features
AWS CloudWatch	AWS	Anomaly detection, prediction	Metrics, logs, event tracking
Azure Monitor	Microsoft Azure	ML-based anomaly detection	Supervision, notification, discovery
Google Cloud Operations Suite	Google Cloud	AI performance monitoring	Integrated supervision of individuals or quantity and app services
Datadog	Multi-cloud	ML anomaly detection, logs	Full-stack, infrastructure monitoring
New Relic	Multi-cloud	Forecasting, improvement	App controlling, resource utilization

Splunk	Multi-cloud	Pattern recognition and outliers detecting	Machine data Real-time business insights

They are the building blocks for AI-real time monitoring in cloud systems. As a result, the monitoring processes of an organization can become more precise and efficient when becoming based on machine learning and AI. However, the ability of these technologies to assimilate into other existing cloud structures is not as easy.

Incorporating them requires more tact and best practice in training of the models to realize that they can run on the available cloud resources perfectly. However, the implementation of these monitoring tools powered by artificial intelligence compensates the drawbacks tremendously providing enhanced results, security, and scalability.

In this vein, with the growing AI development, cloud monitoring tools can and will deliver the self-healing tools and the complete automation of resources management.

This view is especially true for organizations that require continuing growth within the competitive cloud market environment; thus, resorting to using AI-driven real-time monitoring tools is gradually becoming indispensable. These tools not only give higher visibility and manageability for the cloud resources but also helps to ensure secure and optimised and more adaptive to the dynamic business and customer requirement systems (Panduman et al., 2024). As AI advances, the future of cloud monitoring will be smarter, more effective to suit the escalating and sophisticated issues organisations experience in cloud computing.

Benefits

- Proactive Issue Detection: Through AI it is possible to detect system abnormalities and failures then take precaution so that it does not worsen.
- Improved Efficiency: The automation of monitoring tasks enables the teams to give their attention to critical issues that require regular attention than having them spend most of their time on manual monitoring.
- Cost Savings: By predicting the resources demand and avoiding inconvenient time, AI minimizes the use of resources, hence reducing the operating expenses.
- Faster Incident Response: AI models also can synthesise large volumes of information in real-time, which makes response time to an issue or an event much faster.
- Scalability: AI systems may grow with enhancing cloud environments, continuing to monitor even when scales of infrastructure increases.
- Enhanced Security: Thanks to the ability of noticing the trends not typical for the system, AI can identify possible security violations, including data leakage or unauthorized access attempts.
- Accuracy: AI-generated tools lower the number of false alarms since the system is able to learn from past occurrences and provide new thresholds degrees.
- Better Decision-Making: Real time analysis of huge amount of data is possible through AI to make more effective and meaningful reports in a faster manner.
- Predictive Maintenance: Using such shrewd tracking, problems relating to hardware and software can be prevented since the AI will anticipate them and prompt maintenance to be done.
- Integration with Other Tools: AI complements existing cloud structures and APIs for the third-party monitoring tools to have an improved performance overall.

Challenges

- Data Overload: AI systems are dependent on data to perform, and in cloud infrastructure, there is massive data that generates a challenge to the tools that monitor the services. The real-time processing and analysis of this data are often highly resource demanding and may require sophisticated algorithms.
- Integration Complexity: Implementing professional AI surveillance systems means that it has to integrate with existing use of cloud services and other external systems (Munagandla et al., 2024). While using BIM, many organizations are confronted with compatibility challenges of transferring information across different platforms, which might create disruptions or have low productivity.

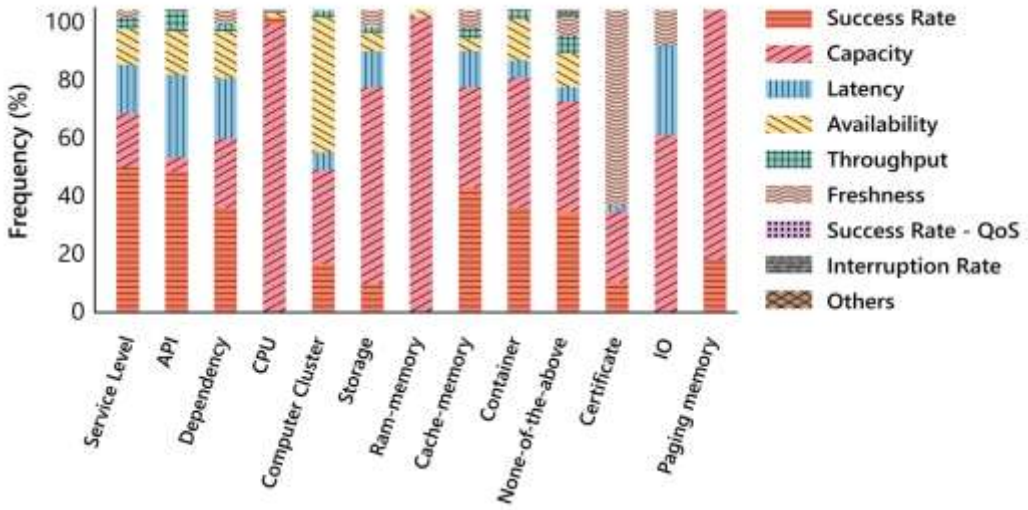

Figure 4 Intelligent monitoring: Towards AI-assisted monitoring for cloud services (Microsoft, 2023)

- Training AI Models: AI and machine learning models need to be trained on high quality data the most of the time. Training of these models, involves process of collection, cleaning and labelling of data which may take a lot of time and money. Inexperienced models can cause the prediction as well as monitoring outcomes to go wrong resulting to poor outcome.
- False Positives/Negatives: Even sophisticated calculations may lead to AI systems giving false positives, that is, indicating that there is an issue, when there is none, or false negatives, that is, not seeing an issue when it is present. They can end up with alert fatigue for IT teams or in completely missing important problems, and compromise the whole reliability of the monitoring system.
- Real-Time Processing Demands: Real time cloud monitoring enhanced by use of artificial intelligence demands for adequate computing resources to process data and make competent decisions in real-time. Preservation of low latency and high availability of these AI models may present a concern especially in environments with many users.
- Resource and Cost Constraints: AI-based monitoring tools may involve a fair amount of infrastructure, processing power, and storage and may therefore be expensive to implement. As for the third implementation cost, for small-scale organizations, these costs may be too expensive to purchase and thus AI integration becomes challenging.
- Model Bias: There is a nature of exposing AI models to some kind of biases depending on the data fed into them. The problem lies with the bias, when the training dataset is either limited or contains data that are not reflective of the real-world situation, the system's decisions may be skewed leading to poor ability to monitor or gain good insights.

- Security Concerns: AI systems are vulnerable to adversarial attacks, which are a potentially serious threat – an attacker introduces changes into the data that the AI system is supposed to analyse. The main concern is AI-Monitoring systems being targeted or used erroneously or intentionally, that can be a problem.
- Lack of Transparency: Most of the AI algorithms work in 'closed' systems, or as the phrased it 'black box systems' thus explanation of decision making is often difficult. This lack of transparency also makes it impossible for the IT teams to understand why some decisions were made, or why some predictions used in the models were made, and this hamper troubleshooting and system optimization processes.
- Skill Gaps: The implementation and administration of artificial intelligence-based cloud monitoring also call for the expertise in AI, Machine Learning as well as cloud computing. A challenge that organisations might encounter is where to source or how to train capable professionals to optimize these complex systems.

Future Directions

AI real-time cloud monitoring will continue to mature in future through increased level of automation, improvements in prediction quality and connectedness to other systems. Over time, AI models become smarter in identifying rich patterns during data analysis and come up with even better predictions and early intervention of emerging problems.

By incorporating AI with the help of edge computing it will consequently result in faster data processing to eliminate latency issues. Also, Innovative XAI solutions will help to achieve higher levels of transparency and trust in automated decisions (Kanth, 2024). As cloud environments become more sophisticated, artificial intelligence shall step in even further into helping enhance performance, security and utilization of resources.

Conclusion

The application of Cognitive Technology in the monitoring of cloud computing real-time cloud infrastructure has many benefits including better operational efficiency through real-time detection of emergent problems. Despite these issues like data inundation, model bias, and integration issues, there is enormous progress in the AMAI and edge computing that uses AI and machine learning for achieving the highest level of monitoring capabilities. With more organisations adopting cloud services as a way of delivering their IT services, the use of AI is expected to be even more paramount as it will act as an enabler for smooth, secure and efficient service delivery in the cloud environment. Subsequent advancements of AI in future will still improve the probability, discovery and mitigation of such problems making cloud systems a more reliable and intelligent system.

References

Kanth, T. C. (2024). AI-POWERED THREAT INTELLIGENCE FOR PROACTIVE SECURITY MONITORING IN CLOUD INFRASTRUCTURES. https://philpapers.org/rec/CHAATI-6

Munagandla, V. B., Dandyala, S. S. V., & Vadde, B. C. (2024). AI-powered cloud-based epidemic surveillance system: A framework for early detection. Revista de Inteligencia Artificial en Medicina, 15(1), 673-690. http://redcrevistas.com/index.php/Revista/article/view/176

Panduman, Y. Y. F., Funabiki, N., Fajrianti, E. D., Fang, S., & Sukaridhoto, S. (2024). A Survey of AI Techniques in IoT Applications with Use Case Investigations in the Smart Environmental Monitoring and Analytics in Real-Time IoT Platform. Information, 15(3), 153. https://doi.org/10.3390/info15030153

Villegas-Ch, W., García-Ortiz, J., & Sánchez-Viteri, S. (2024). Towards Intelligent Monitoring in IoT: AI Applications for Real-Time Analysis and Prediction. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3376707

Chavan, P., & Chavan, P. (2024, June). Automation of AD-OHC Dashbord and Monitoring of Cloud Resources using Genrative AI to Reduce Costing and Enhance Performance. In 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET) (pp. 1-9). IEEE. https://doi.org/10.1109/ICICET59348.2024.10616299

Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 1(1), 132-151. https://ojs.boulibrary.com/index.php/JAIGS/article/view/89

Sanodia, G. (2024). Leverage AI to Improve Cloud Transformation. Journal of Scientific and Engineering Research, 11(8), 95-105. https://www.researchgate.net/profile/Geetesh-Sanodia-2/publication/383978285_Leverage_AI_to_Improve_Cloud_Transformation/links/66e2e967b1606e24c224dec6/Leverage-AI-to-Improve-Cloud-Transformation.pdf

Srinivas, P., Husain, F., Parayil, A., Choure, A., Bansal, C., & Rajmohan, S. (2024, April). Intelligent Monitoring Framework for Cloud Services: A Data-Driven Approach. In Proceedings of the 46th International Conference on Software Engineering: Software Engineering in Practice (pp. 381-391). https://doi.org/10.1109/TCSET64720.2024.10755518

Olabanji, S. O., Marquis, Y., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-driven cloud security: Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science*, *17*(3), 57-74. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4709384

Stutz, D., de Assis, J. T., Laghari, A. A., Khan, A. A., Andreopoulos, N., Terziev, A., ... & Grata, E. G. (2024). Enhancing Security in Cloud Computing Using Artificial Intelligence (AI). Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection, 179-220. https://doi.org/10.1002/9781394196470.ch11

Rahaman, M., Lin, C. Y., Pappachan, P., Gupta, B. B., & Hsu, C. H. (2024). Privacy-centric AI and IoT solutions for smart rural farm monitoring and control. Sensors, 24(13), 4157. https://doi.org/10.3390/s24134157

Chanthati, S. R. (2024). Artificial Intelligence-Based Cloud Planning and Migration to Cut the Cost of Cloud Sasibhushan Rao Chanthati. American Journal of Smart Technology and Solutions, 3(2), 13-24. https://www.researchgate.net/profile/Sasibhushan-Rao-Chanthati/publication/382952222_Artificial_Intelligence-Based_Cloud_Planning_and_Migration_to_Cut_the_Cost_of_Cloud_Sasibhushan_Rao_Chanthati/links/66bcfc2e2ff54d6c9ed0b287/Artificial-Intelligence-Based-Cloud-Planning-and-Migration-to-Cut-the-Cost-of-Cloud-Sasibhushan-Rao-Chanthati.pdf

Jones, R. (2024). The Impact of AI on Secure Cloud Computing: Opportunities and Challenges. The Indonesian Journal of Computer Science, 13(4). https://doi.org/10.33022/ijcs.v13i4.4383

Barua, B., & Kaiser, M. S. (2024). AI-Driven Resource Allocation Framework for Microservices in Hybrid Cloud Platforms. arXiv preprint arXiv:2412.02610. https://doi.org/10.48550/arXiv.2412.02610