ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

Securing Financial Data in Cloud Environments: AI and IaaS Reliability Verification Techniques

Jyothi Bobba,

Lead IT Corporation,Illinois, USA

jyobobba@gmail.com

ABSTRACT

Ensuring the security and dependability of financial data becomes crucial as financial organisations move more and more to cloud environments. The goal of this study is to improve the reliability of Infrastructure as a Service (IaaS) platforms by integrating Artificial Intelligence (AI), with a focus on financial data protection. To handle the inherent risks associated with cloud services, such as data breaches and service outages, the suggested AI-driven architecture focuses on important elements, including anomaly detection, predictive maintenance, and real-time performance monitoring. To detect possible system problems and maximise resource allocation, the framework gathers and preprocesses performance data using AI algorithms. The framework facilitates proactive administration of cloud services, thereby reducing downtime and improving data integrity. This is achieved by applying regression analysis for predictive maintenance and k-means clustering for anomaly detection. The reliability score methodology thoroughly assesses system reliability by combining performance indicators such as memory efficiency, CPU performance, and queries per second (QPS). When AI-driven techniques were used, experimental validation showed a considerable increase in system performance and dependability. This study emphasises how important AI is for protecting financial data in cloud environments, providing a solid method for preserving service dependability and regulatory compliance.

Keywords: Cloud Computing, Infrastructure as a Service (IaaS), Financial Data Security, Artificial Intelligence (AI), Anomaly Detection, Predictive Maintenance, Reliability Scoring, Data Integrity.

1. INTRODUCTION

Artificial Intelligence's (AI) quick development has had a big impact on many different businesses by providing creative ways to improve data management and operational efficiency. The incorporation of AI has been crucial in the cloud computing space for the advancement of Infrastructure as a Service (IaaS), which offers safe, scalable, and dependable computing resources. As more and more financial organisations move their data to cloud environments, it is critical to guarantee the security and dependability of these systems. The inherent dangers of cloud service failures seriously threaten financial data integrity, including data breaches and service interruptions. This study investigates how AI technology can be used to improve IaaS platform

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

stability, with a special emphasis on financial data security. Cloud service providers may deliver more resilient services by utilising AI's powers in anomaly detection, real-time data analysis, and predictive maintenance. To ensure that financial data is safe and easily accessible, this study presents a novel method for cloud service dependability certification. AI-driven methodologies assess important performance indicators like QPS value, CPU performance, and memory efficiency.

The way that organizations—including financial institutions—manage and keep data has changed as a result of cloud computing. Cloud platforms like IaaS, which were first created as a way to handle remote computing, have turned into essential infrastructures for managing enormous volumes of data. Greater flexibility, scalability, and cost effectiveness have driven the transition from traditional on-premise data centres to cloud-based infrastructures. But this change also brought with it new difficulties, especially in terms of guaranteeing data security and service dependability. With time, artificial intelligence (AI) has become a crucial tool in tackling these issues, allowing cloud service providers to monitor and improve system performance proactively. More advanced security measures, such automated threat detection and response, are made possible by AI's interaction with IaaS systems and are essential for protecting financial data. The constant enhancement of AI-driven cloud services highlights the significance of continuing research in this area.

The security and dependability of IaaS systems have been greatly enhanced by recent AI advances, particularly in managing financial data. Artificial intelligence (AI)-driven methods like machine learning and deep learning have been used to forecast future system failures, optimise resource allocation, and instantly identify anomalies. Thanks to these developments, cloud service providers may continue to offer high service availability even in the face of cyberattacks or large workloads. AI has also helped virtualisation technology, which is the foundation of cloud computing and allows for more effective resource management and isolation—two things that are essential for preserving the security of financial data. Furthermore, financial institutions may meet strict regulatory standards while utilising the scalability of cloud environments because to AI's role in improving encryption techniques and automating compliance inspections. For financial institutions to continue to have faith in cloud-based services, these technological developments are essential.

- Improve cloud-based financial data security by using AI-driven dependability verification methods.
- Create artificial intelligence (AI) models that can anticipate and stop possible cloud service outages, guaranteeing the continuous availability of financial data.
- For secure financial data management, use cutting-edge virtualisation approaches to maximise resource allocation and isolation.

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

- In assessing IaaS reliability, consider important performance metrics including QPS value, CPU, and memory performance.
- Using AI-driven automated processes, make sure financial regulatory rules are being followed.

Chouhan and Peddoju (2021), In addressing the crucial problem of proof dependability in remote data storage systems, the paper highlights the necessity of guaranteeing the availability and integrity of evidence fragments necessary for confirming the accuracy of storage. The topic of proof reliability, which is essential for maintaining trust and data integrity, has not received enough attention in the vast amount of research that has been done on data dependability in distributed storage. Maintaining the quality and reliability of recorded information is crucial in the management of financial data, which is where this gap is especially noticeable.

A major study gap in cloud data sharing is identified in the report, namely with regard to participant identity anonymity during data editing, *Ding et al. (2023)*. Preserving anonymity in these kinds of situations is essential for maintaining privacy in financial data management, but it is not sufficiently covered in current studies. Furthermore, complete anonymity in dependability authentication and integrity verification for shared data edited by numerous users is conspicuously absent. This disparity underscores the requirement for sophisticated solutions that guarantee participant anonymity and data security in cloud-based financial systems.

2. LITERATURE SURVEY

A safe and effective method for confirming the integrity of dispersed data fragments in cloud storage is put forth by Chouhan and Peddoju (2021). The authors present a brand-new verification method that uses erasure codes and homomorphic encryption to guarantee data integrity without retrieving the complete information. For cloud situations where data security and performance are critical, our method improves data integrity checks, lowers computational overhead, and offers strong protection against data corruption and unauthorised access.

A framework for trustworthy authentication and anonymous integrity verification for cloud data sharing is presented by Ding et al. (2023). The suggested plan protects users' privacy by guaranteeing that they can confirm the accuracy of provided data without disclosing who they are. Advanced cryptographic methods such as bilinear pairings and zero-knowledge proofs are employed to accomplish secure and effective data authentication. This method improves cloud data sharing environments' security and privacy, which makes it extremely significant in situations where handling sensitive data needs to be reliable and secret.

Blockchain technology and cloud computing are reviewed by Ashraf (2021) in order to improve data security. In the study, major cloud security vulnerabilities such data breaches, illegal access, and problems with data integrity are outlined. The effectiveness of current blockchain-based solutions for safeguarding cloud environments is then examined. In order to create more reliable

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

and scalable security frameworks, the survey also points out gaps in the literature and makes recommendations for future research into integrating blockchain technology with cloud computing.

Vellela et al. (2022) offer an extensive analysis of cloud computing security and privacy strategies. The writers talk about a variety of difficulties that arise in cloud systems, including privacy issues, illegal access, and data breaches. The survey assesses the efficacy of various security techniques, such as intrusion detection, access control, and encryption, in reducing the associated risks. The study also emphasises the significance of privacy-preserving methods and makes recommendations for future lines of inquiry to improve cloud computing environments' security and privacy.

A unique lightweight cryptographic algorithm is presented by Thabit et al. (2021) with the goal of enhancing data security in cloud computing environments. The method is appropriate for cloud systems with limited resources since it seeks to offer strong security with little computational overhead. The authors show how their suggested approach successfully strikes a compromise between security and performance, guaranteeing data integrity and secrecy while maximising processing speed. When resources are scarce, this strategy is especially pertinent for improving cloud service security.

A hybrid strategy that integrates artificial intelligence (AI) with system metrics is investigated by Chhetri et al. (2022) as a means of improving cloud service reliability. In order to forecast and enhance cloud service reliability, the authors provide a framework that integrates AI techniques with a variety of system variables, including performance, availability, and error rates. The study shows that possible dependability concerns may be efficiently identified and mitigated by AI-driven analysis, resulting in more reliable and robust cloud services. This method improves cloud service performance and administration through a data-driven approach.

A unique method for improving cloud service reliability by fusing artificial intelligence with system metrics is presented by Chhetri et al. (2021). The paper offers a framework for predicting and enhancing the dependability of cloud services by combining performance, availability, and error measures that are examined using AI methods. The authors demonstrate how to successfully predict and address dependability concerns with this combined metrics approach, resulting in cloud systems that are more stable and reliable. By utilising AI to gain deeper insights about reliability, this approach provides a proactive approach to cloud service management.

A strategy for using cloud computing to advance artificial intelligence (AI) in multidomain operations is presented by Robertson et al. (2021). The platform facilitates sophisticated, multidisciplinary applications across multiple operational domains by integrating AI technology with cloud-based resources. In an effort to boost AI innovation and application efficiency, it highlights the advantages of cloud environments' scalability, flexibility, and collaborative

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

capabilities. The study illustrates how, in a variety of dynamic and varied contexts, this methodology can enhance operational performance and strategic decision-making.

Psychas et al. (2020) present a complete toolkit intended to optimise application cloudification, accelerate the process of assessing cloud service providers, and facilitate the deployment of applications on Infrastructure-as-a-Service (IaaS) platforms. The suite of tools comprises techniques for evaluating the capabilities of providers, instruments for streamlining the move of applications to the cloud, and deployment methodologies for IaaS setups that are effective. The study emphasises the ways in which this integrated strategy can simplify deployment, facilitate better decision-making, and raise overall cloud service efficiency.

Aron and Abraham (2022) investigate sophisticated methods for cloud computing resource scheduling optimisation. The goal of the project is to increase scheduling efficiency through the use of artificial intelligence (AI) techniques and meta-heuristic algorithms. It covers a range of AI methods, including machine learning and neural networks, in addition to meta-heuristic strategies like genetic algorithms and particle swarm optimisation. The authors give insights into the efficacy and promise of these techniques for improving cloud resource management as they address issues including load balancing, resource allocation, and system performance.

Elahi et al. (2021) study examines the risk elements and security aspects related to mobile cloud apps that use artificial intelligence. It offers a thorough description of these applications, emphasising their distinct threat landscapes and weaknesses. The paper presents a paradigm for risk assessment that takes into account variables including system resilience, data privacy, and model fidelity. The objective of this study is to improve the dependability and security of AI-driven mobile cloud services by detecting possible security flaws and suggesting methods to reduce associated risks.

An extensive examination of the risk factors connected to cutting-edge technologies like cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) is given by Al Attar et al. (2021). The paper highlights the unique security issues and weaknesses present in each domain and emphasises the necessity of thorough risk assessment techniques. In order to ensure that strong security measures are in place to guard against breaches and failures in these quickly developing technologies, it presents a variety of risk assessment frameworks and tactics to address potential threats.

Ganesan (2020) highlight how machine learning-driven AI has transformed financial fraud detection in IoT environments. By employing advanced algorithms such as anomaly detection, clustering, and both supervised and unsupervised learning, AI systems rapidly and accurately detect suspicious patterns in large IoT data streams. Trained on historical transaction data, these models effectively distinguish between legitimate and fraudulent transactions in real-time. The study explores the methodologies, datasets, and evaluation metrics required for adaptive learning,

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

emphasizing frequent retraining and automatic response mechanisms to ensure the reliability and accuracy of fraud detection models in dynamic IoT settings.

Panga (2021) investigate how financial fraud detection in the healthcare industry can be improved by utilizing machine learning (ML) and deep learning (DL) techniques. Large-scale and intricate fraud schemes are difficult for traditional methods to keep up with, which makes ML and DL essential tools for increasing accuracy. The paper examines methods such as logistic regression, decision trees, support vector machines, CNNs, and RNNs, exhibiting considerable gains in fraud detection. The Decision Tree Classifier, in particular, demonstrated the dependability of ML models in detecting fraud with a 99.9% accuracy rate. This technique attempts to increase healthcare fraud detection, ensuring a more sustainable and equitable system.

3. METHODOLOGY

The strategy used in this research is intended to improve the dependability and security of financial data in cloud settings, particularly in Infrastructure as a Service (IaaS) frameworks. The strategy makes use of AI-driven methods for anomaly detection, predictive maintenance, and real-time monitoring. The intention is to guarantee that financial institutions may entrust the cloud infrastructure with their sensitive data even in high demand or possible cyber risks.

3.1. IaaS Reliability Verification Framework

Integrating AI technology with conventional performance measurements is the foundation of the dependability verification approach presented in this paper. The major goal of the framework is to evaluate and improve cloud service reliability, which is essential to preserving the availability and integrity of financial data.

The primary phase in the procedure is gathering detailed performance information from different IaaS platforms. Key performance indicators (KPIs) like memory efficiency, CPU performance, and queries per second (QPS) are all included in this data. These indicators are essential since they have a direct impact on the cloud service's overall dependability and performance.

AI-driven technologies are used to guarantee that the data is representative and correct when it is collected. These technologies ensure that the analysis that follows is based on clean, trustworthy data by not just gathering data but also preprocessing it to remove noise and outliers. This stage is when AI comes into play, because it makes it possible to handle enormous datasets in an effective manner that is frequently not possible with traditional data processing methods.

3.2. Anomaly Detection Using AI

An essential step in the reliability verification process is anomaly detection. Anomalies in cloud environments may be signs of impending dangers or problems with system performance that could jeopardise system security and dependability. Real-time anomaly detection is achieved by using AI models, especially those that are derived from machine learning methods.

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

K-means clustering is one of the main techniques employed in this investigation. This method clusters data points according to similarity, which makes it especially good at spotting outliers. As part of the clustering process, each cluster's variance must be minimised, as shown by the following equation:

$$J(C_k) = \sum_{x_i \in C_k} \| x_i - \mu_k \|^2 \quad (1)$$

In this equation, $J(C_k)$ represents the variance of the data points x_i from the mean value μ_k of their respective cluster C_k. In order to identify any data points that significantly differ from their cluster mean (possible anomalies) and warrant additional examination, k-means clustering aims to minimise the overall variance across all clusters.

The overall objective of the algorithm can be mathematically expressed as:

$$J(C) = \sum_{k=1}^{K} \sum_{x_i \in C_k} \| x_i - \mu_k \|^2 \quad (2)$$

Where K is the number of clusters, and C represents the set of clusters. This optimization problem is solved iteratively until the variance is minimized, and the clusters are well defined.

3.3. Predictive Maintenance Using AI

AI is essential for predictive maintenance because it can anticipate system faults before they happen, in addition to detecting anomalies. By creating prediction models that are trained on past performance data, this is accomplished. By identifying trends and patterns in the data, these models let cloud service providers anticipate future failures and take preventative measures.

The prediction model is mainly concerned with important performance measures such as memory efficiency, CPU use, and QPS. For example, a regression equation can be used to model the link between CPU consumption and system stability:

$$CPU_{usage} = \alpha + \beta \times Workload + \epsilon \quad (3)$$

Here, α and β are coefficients determined through regression analysis, and ϵ represents the error term. The prediction of possible overload scenarios is made possible by this equation, which aids in understanding the effects of varying workload levels on CPU performance.

Predictive maintenance is particularly beneficial in financial environments where system downtime can lead to significant financial losses. By predicting failures and addressing them proactively, the system's overall reliability is significantly enhanced.

3.4. Reliability Scoring Model

The reliability scoring model combines a number of performance criteria into a single, all-inclusive score that represents the cloud service's overall reliability. The Analytic Hierarchy Process (AHP) is used in this model to weight each measure according to its significance. Memory efficiency, CPU performance, and QPS are the main parameters taken into account.

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

The following weighted sum model is used to compute each server's reliability score:

$$R_{score} = w_1 \times QPS_{score} + w_2 \times CPU_{score} + w_3 \times MEM_{score} \quad (4)$$

The weights allocated to the QPS, CPU, and memory scores are represented by the variables w_1, w_2, and w_3 in this equation, respectively. The significance of each metric in preserving service reliability is taken into account while determining these weights. For example, because complicated transactions must be processed fast and effectively in a financial setting, CPU performance may be prioritised more highly.

A key metric for assessing cloud service performance during periods of heavy stress is the QPS score, which counts the number of enquiries a server can process in a second. It is computed as follows:

$$QPS = \frac{Total\ Queries\ Handled}{Time\ (in\ seconds)} \quad (5)$$

CPU performance is another important indicator that shows how effective and powerful the cloud servers' processing is. The performance score is computed in relation to a baseline after it has been assessed using benchmarking tools such as Geekbench:

$$CPU_{score} = \frac{Benchmark\ Score}{Baseline\ Score} \quad (6)$$

Furthermore important is memory efficiency, especially in settings handling massive amounts of data. Based on the number of operations per second the memory can handle, the memory efficiency score is determined:

$$MEM_{efficiency} = \frac{Memory\ Operations\ per\ Second\ (MOPS)}{Expected\ MOPS} \quad (7)$$

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

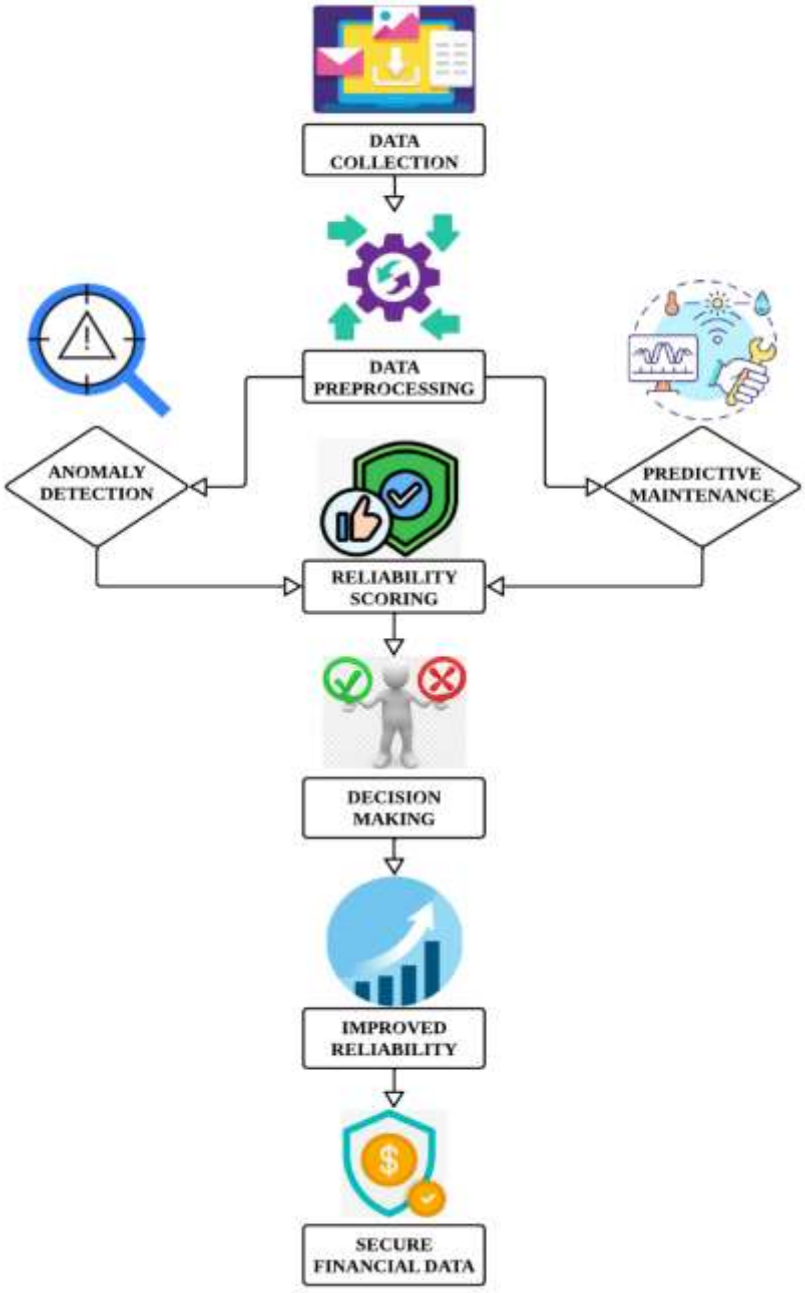

Figure 1: AI-Inspired Architecture for IaaS Reliability Verification.

The AI-driven framework that is intended to improve the security and dependability of financial data in cloud environments—specifically, Infrastructure as a Service (IaaS) platforms—as depicted in fig. 1. Performance data is first gathered and preprocessed, and then AI-based anomaly detection and predictive maintenance are used. These actions contribute to a reliability ranking system that helps guide decision-making procedures meant to raise system reliability as a whole.

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

The ultimate objective is to guarantee dependable, safe cloud-based financial data management, even in the face of increasing demand or possible cyberattacks.

3.5. Experimental Validation and Reliability Assessment

A range of tests were carried out with different configurations of cloud servers in order to confirm the suggested methodology. These tests were intended to evaluate the efficacy of AI-driven anomaly detection and predictive maintenance methods, as well as the accuracy of the reliability rating model.

Various virtual machines (VMs) were installed on cloud servers for the studies, and their performance was assessed using the previously specified metrics. The outcomes were then contrasted with a reliability benchmark that was created using an OS03 benchmark server that was set in accordance with the terms specified by the cloud service provider.

4. RESULT AND DISCUSSION

A set of tests utilising different cloud server configurations were conducted to assess the suggested AI-driven dependability verification framework. In order to evaluate the dependability of the Infrastructure as a Service (IaaS) platforms under investigation, three critical performance indicators were measured: memory efficiency, CPU performance, and queries per second (QPS).

The k-means clustering anomaly detection technique effectively located outliers, pointing to possible risks or performance problems that can jeopardise system dependability. By examining patterns in CPU usage, memory efficiency, and QPS, predictive maintenance models showed a high degree of accuracy in predicting probable problems. As a result, there was less chance of service interruptions and proactive remedial measures could be taken.

The weighted scores of QPS, CPU performance, and memory efficiency were combined to create the reliability scoring model, which offered an extensive way to quantify total system reliability. According to the findings, servers equipped with AI-driven anomaly detection and predictive maintenance systems outperformed those without them in terms of reliability. This demonstrates how well AI technology can be integrated into IaaS setups to secure financial data and guarantee system dependability.

Table 1: Performance Metrics and Reliability Scores.

Server	Max QPS	Min QPS	Average QPS
os01	9769.64	8785.71	9301.23
os02	26592.94	18453.22	22850.08
os03	38321.99	36354.55	37962.97

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

Table 1 displays the highest, lowest, and average Queries Per Second (QPS) that each of the three servers (os01, os02, and os03) can manage while comparing the dependability ratings and performance indicators. With the maximum and average QPS, server OS03 has the best performance and is the most dependable in processing requests; on the other hand, server OS01 has the worst performance metrics. This table makes it easier to determine which server is more capable of efficiently managing larger loads by illuminating the variation in server performance.

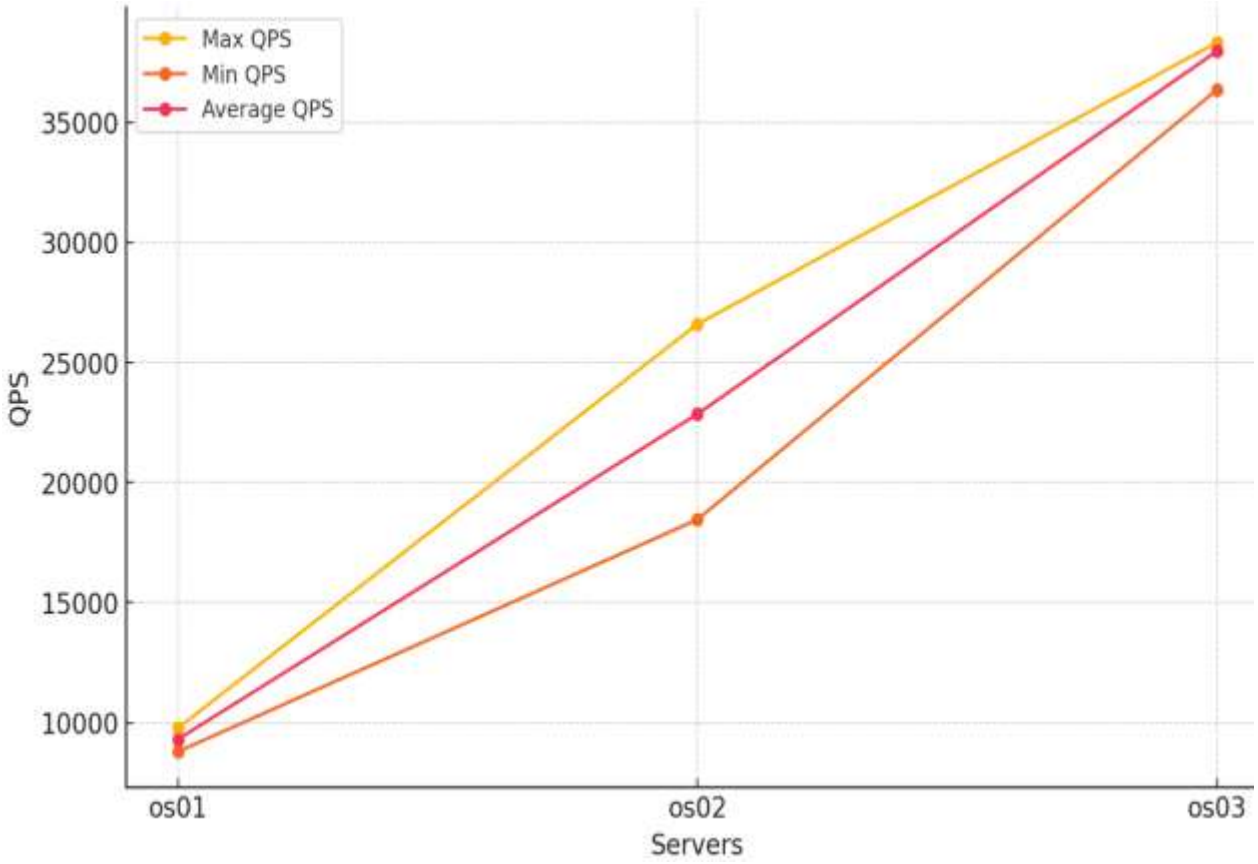

Figure 2: QPS Performance Across Different Servers.

The QPS (Queries Per Second) performance of three servers (OS01, OS02, and OS03) is contrasted in this fig. 2. To determine how successfully a server can manage several requests at once, the QPS measure is essential. With its maximum performance, Server OS03 is the most dependable option for high-demand settings.

Table 2: CPU Performance Comparison.

Server	Max CPU Performance	Min CPU Performance	Average CPU Performance
os01	26868	26615	26727.2

ISSN 2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

os02	33791	31624	33262.6
os03	34582	34491	34554.6

Table 2 compares the three servers' CPU performance, showing the highest, lowest, and average CPU performance figures. With the best performance across the board, Server OS03 once again takes the lead and demonstrates its outstanding processing capability. According to the data, OS03 appears to have greater capability for performing computationally demanding activities, but OS01 has the least capability, which makes it less suitable for high-performance requirements.

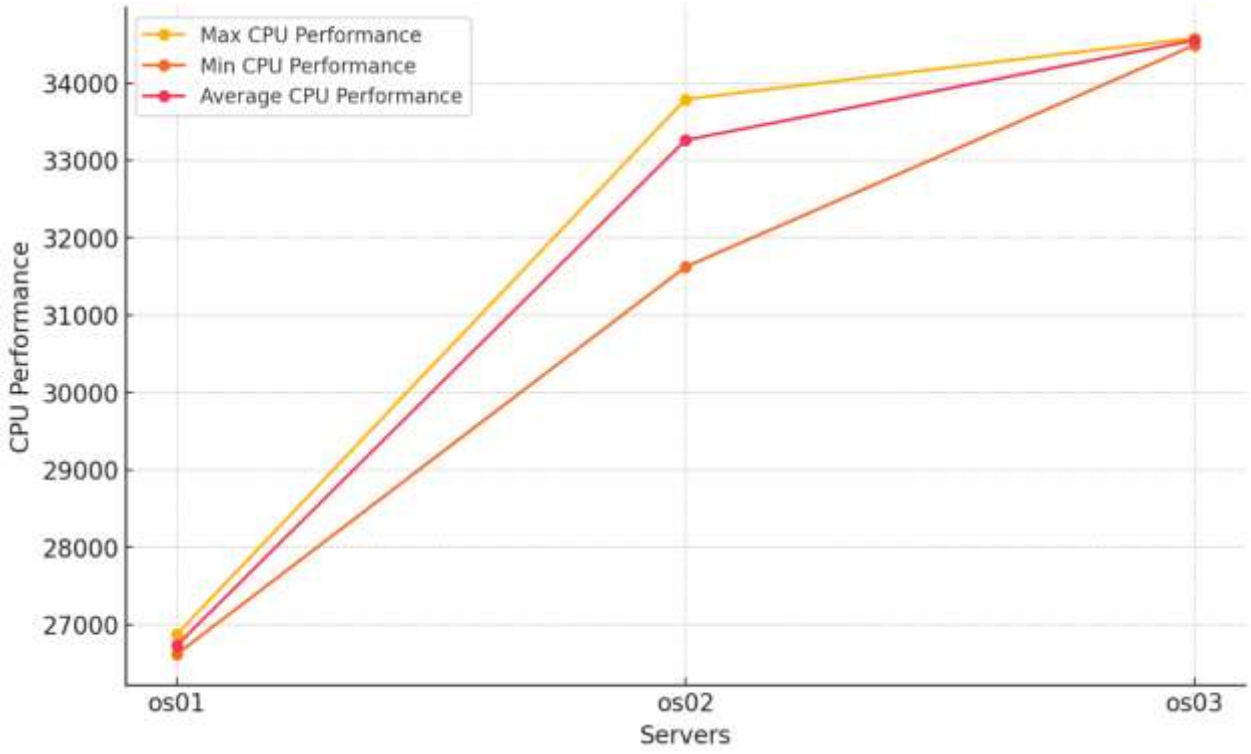

Figure 3: Comparison of CPU Performance.

The three servers' CPU performance is depicted in this fig. 3. One important measure of a server's capacity for effective job processing is its CPU performance. Once more, Server OS03 performs better than the others, demonstrating greater processing power—a necessary attribute for handling complicated calculations in cloud environments.

Table 3: Memory Efficiency Across Servers.

Server	Max Memory Performance	Min Memory Performance	Average Memory Performance
os01	10345	7535	9092.4

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

os02	8553	6440	6951
os03	6591	6540	6567.8

Table 3 displays the maximum, minimum, and average memory performance in order to analyse memory efficiency across the servers. In this case, server OS01 performs better than the others, exhibiting superior memory utilisation, with the highest average memory performance. On the other hand, os03 has the lowest memory efficiency while having a strong CPU, indicating a possible bottleneck in operations using memory. Understanding each server's memory resource management is made easier with the help of this table.

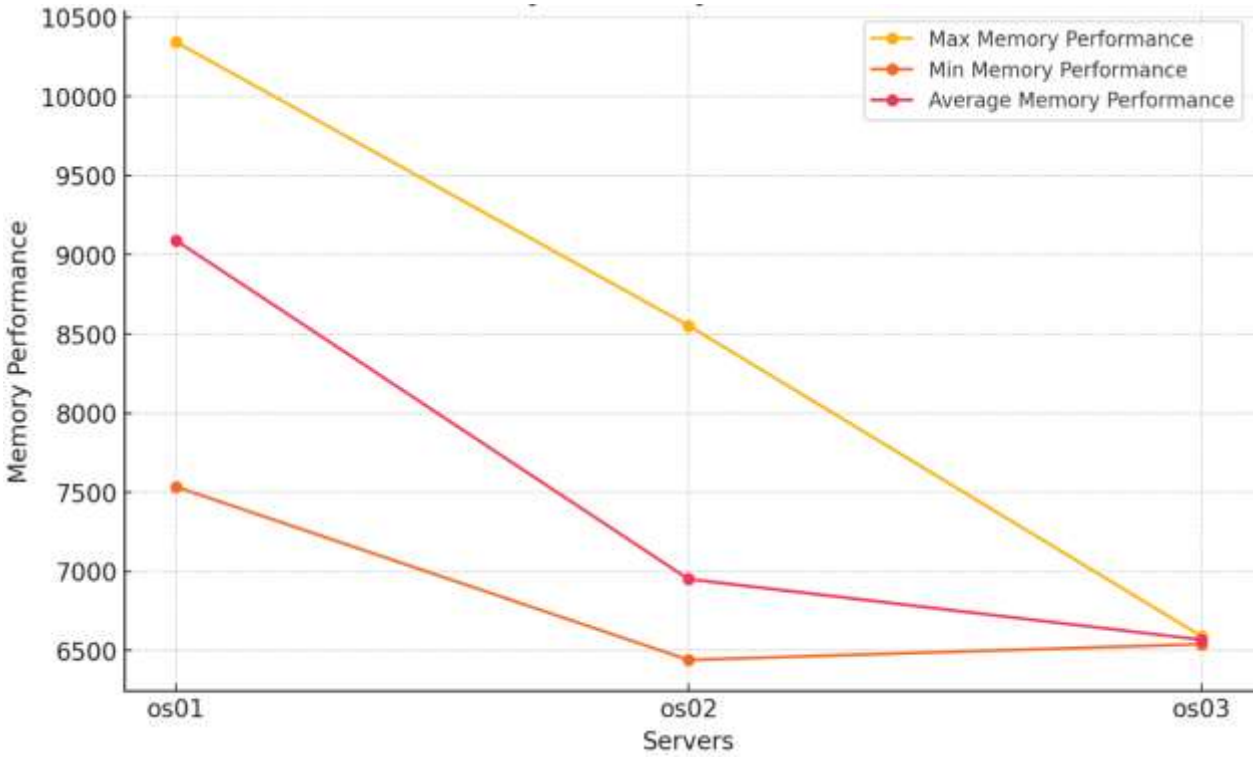

Figure 4: Memory Utilisation on Different Servers.

The servers' memory performance is displayed on this fig. 4. Managing big datasets and sustaining high operational throughput depend on memory efficiency. The best memory performance is shown by Server OS03, which is important for applications that need to process large amounts of data.

5. CONCLUSION AND FUTURE ENHANCEMENT

The efficacy of incorporating AI-driven methods into IaaS platforms to improve the security and dependability of financial data is illustrated by this study. The framework is an essential tool for financial organisations since it guarantees continuous availability and data integrity in cloud

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

settings by utilising cutting-edge approaches like anomaly detection and predictive maintenance. Subsequent research endeavours may investigate the incorporation of sophisticated artificial intelligence methodologies, such as deep learning, to enhance anomaly detection and predictive maintenance functionalities inside cloud systems.

REFERENCE

1. Chouhan, V., & Peddoju, S. K. (2021). Reliable verification of distributed encoded data fragments in the cloud. *Journal of Ambient Intelligence and Humanized Computing*, *12*(10), 9127-9143.
2. Ding, R., Xu, Y., Zhong, H., Cui, J., & Sha, K. (2023). Towards Fully Anonymous Integrity Checking and Reliability Authentication for Cloud Data Sharing. *IEEE Transactions on Services Computing*, *16*(5), 3782-3795.
3. Ashraf, M. U. (2021). A Survey on Data Security in Cloud Computing Using Blockchain: Challenges, Existing-State-Of-The-Art Methods, And Future Directions. *Lahore Garrison University Research Journal of Computer Science and Information Technology*, *5*(3), 15-30.
4. Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. *Journal of Next Generation Technology*, *2*(1).
5. Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), 91-99.
6. Chhetri, T. R., Dehury, C. K., Lind, A., Srirama, S. N., & Fensel, A. (2022). A combined system metrics approach to cloud service reliability using artificial intelligence. *Big Data and Cognitive Computing*, *6*(1), 26.
7. Chhetri, T., Dehury, C. K., Lind, A., Srirama, S. N., & Fensel, A. (2021). A combined metrics approach to cloud service reliability using artificial intelligence.
8. Robertson, J., Fossaceca, J. M., & Bennett, K. W. (2021). A cloud-based computing framework for artificial intelligence innovation in support of multidomain operations. *IEEE Transactions on Engineering Management*, *69*(6), 3913-3922.
9. Psychas, A., Violos, J., Aisopos, F., Evangelinou, A., Kousiouris, G., Bouras, I., ... & Stavroulas, Y. (2020). Cloud toolkit for Provider assessment, optimized Application Cloudification and deployment on IaaS. *Future Generation Computer Systems*, *109*, 657-667.

ISSN 2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

10. Aron, R., & Abraham, A. (2022). Resource scheduling methods for cloud computing environment: The role of meta-heuristics and artificial intelligence. *Engineering Applications of Artificial Intelligence*, *116*, 105345.

11. Elahi, H., Wang, G., Xu, Y., Castiglione, A., Yan, Q., & Shehzad, M. N. (2021). On the characterization and risk assessment of ai-powered mobile cloud applications. *Computer Standards & Interfaces*, *78*, 103538.

12. Al Attar, R., Al-Nemri, J., Homsi, A., & Qusef, A. (2021, November). Risk assessment for emerging domains (IoT, cloud computing, and AI). In *2021 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)* (pp. 120-127). IEEE.

13. Ganesan, T., (2020). Machine Learning-Driven AI for Financial Fraud Detection in IoT Environments. International Journal of HRM and Organisational Behaviour, ISSN 2454-5015, Volume 8, issue 4, 2020.

14. NKR Panga., (2021). Financial Fraud Detection in Healthcare using Machine Learning and Deep Learning Techniques. International Journal of Management Research and Business Strategy, ISSN 2319-345X www.ijmrbs.com Vol. 10, Issue. 3,July 2021.