International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

AI-Driven Cloud User Validation for Secure Resource Allocation

Dr. Karthik Kambhampati

Submitted:05/09/2022 **Revised:**12/12/2022 **Accepted:**20/12/2022

Abstract: Cloud computing offers scalable, elastic, and on-demand services but faces major challenges in ensuring user authentication, secure access, and optimal resource distribution. Service Level Agreement (SLA) violations and malicious intrusions represent persistent threats that degrade reliability and trust in cloud ecosystems. Traditional validation methods often struggle to adapt to dynamic workloads and evolving attack vectors. In this paper, we present an AI-driven validation and resource allocation framework that integrates neural classification for authentication, machine-learning-based SLA prediction, and reinforcement learning (RL)-driven resource provisioning. The system demonstrates improved detection accuracy of unauthorized users and reduced SLA violations under variable workloads. Expanded simulations highlight that incorporating AI improves not only security but also fairness, energy efficiency, and cost optimization. This paper contributes a holistic methodology that addresses the dual challenges of security and performance in multi-tenant cloud infrastructures.

Keywords: *Cloud computing, AI-driven validation, resource allocation, SLA prediction, reinforcement learning, neural networks, security.*

I. Introduction

Cloud computing has revolutionized IT by providing enterprises and individuals with scalable, elastic, and pay-as-you-go resources. Despite these advantages, maintaining Quality of Service (QoS) while ensuring strong user validation and data security remains a challenging problem. SLA violations lead to customer dissatisfaction, monetary penalties, and reduced trust between cloud providers and clients. Simultaneously, weak authentication exposes cloud infrastructures to security breaches. Traditional validation approaches rely on static credentials or rule-based checks that cannot adequately capture behavioral anomalies. Similarly, resource allocation strategies such as First-Come-First-Serve (FCFS) or round-robin fail to adapt to workload surges, resulting in inefficient utilization and higher SLA breach rates.

AI-driven methods present a compelling alternative. Machine learning (ML) models learn from user behavior and workload traces to provide proactive validation and allocation. Neural networks can classify valid versus malicious users, while RL can dynamically assign resources based on real-time conditions. The motivation for this work is to develop a unified framework where security-aware validation and intelligent allocation co-exist, ensuring that both security and performance objectives are met.

II. Related Work

Research into AI for cloud computing spans security, performance, and energy optimization. Wang et al. (2021) introduced an RL-based scheduler for dynamic workloads, showing

Independent Researcher Cloud & AI Atlanta, GA, U.S. state of Georgia. Email: kambhampati.karthik@gmail.com

improved throughput. Chen et al. (2020) explored adaptive anomaly detection, which identifies zero-day intrusions more effectively than static methods. Trust models proposed by Singh et al. (2019) and Takabi et al. (2016) underscore the necessity of robust authentication. However, they often neglect integration with provisioning systems.

SLA-aware scheduling has been studied extensively. Garg et al. (2018) and Calheiros et al. (2011) proposed machine-learning-driven methods for resource provisioning. Yet, these approaches seldom include user trust validation. Neural-network-based approaches by Gupta et al. (2019) improve resource prediction accuracy but focus primarily on performance metrics. Recent work by Patel et al. (2021) has shown AI-driven methods for cloud security, but their scalability under multi-tenant conditions remains underexplored.

Our contribution lies in bridging these strands of research—combining AI-based validation, SLA prediction, and RL allocation into a single unified framework capable of enhancing both security and performance in real-world cloud systems.

III. Proposed Framework

The proposed framework consists of three tightly integrated modules:

1) AI-Driven User Validation: Using a Backpropagation Neural Network (BPNN), the framework analyzes login metadata, geolocation, device fingerprinting, and behavioral patterns. Suspicious deviations, such as rapid IP switching, are flagged.

2) SLA Violation Prediction: Historical workload traces and SLA logs are input to a supervised learning model (Random Forest). The model outputs the probability of SLA breaches given current load and allocation policies.
3) Secure Resource Allocation: An RL agent dynamically provisions CPU and memory resources by minimizing a reward function that balances latency, cost, and predicted SLA violation risk.

Mathematically, the optimization objective can be expressed as:
$R = -(\alpha * \text{Latency} + \beta * \text{Cost} + \gamma * \text{SLA\_Risk})$, where α, β, and γ are weights assigned to provider objectives.

IV. System Architecture

The architecture comprises four layers: Authentication, Validation, Prediction, and Allocation. The authentication layer ensures basic identity checks. The validation layer uses AI classifiers to identify malicious patterns. The prediction module estimates SLA risk under varying loads, while the RL allocator executes placement and scaling actions. Telemetry feedback loops allow continuous model retraining. This architecture ensures resilience against insider attacks, scalability under bursty traffic, and adaptability to multi-cloud environments.

V. Results and Discussion

Experiments were simulated using CloudSim with 50 hosts and 500 virtual machines. Metrics included validation accuracy, SLA violation probability, and average response time. The AI-driven validation module achieved 94% accuracy in distinguishing malicious users. Compared to baseline heuristic allocation, SLA violation rates decreased by 21%. The RL-based allocator improved CPU utilization by 15% and reduced energy consumption by 10%.

A comparative analysis (Table 1) shows that the proposed model outperforms traditional round-robin and FCFS allocation in all metrics. Additionally, the integration of validation prevents unauthorized access, a feature absent in existing SLA-only approaches.

Table 1: Comparison of Allocation Methods

Method	SLA Violation Rate	Avg Latency	Energy Utilization
Round Robin	32%	180ms	High
FCFS	28%	165ms	Medium
Proposed AI Framework	11%	140ms	Low

VI. Conclusion

This paper presented a comprehensive AI-driven framework for cloud user validation and secure resource allocation. By unifying neural-network-based validation, SLA prediction, and RL-driven allocation, the framework enhances both security and performance. Experiments confirmed reduced SLA violations and improved efficiency. Future directions include deploying the model in hybrid cloud testbeds, incorporating blockchain for tamper-proof audits, and extending AI methods to multi-cloud federation scenarios.

Figures

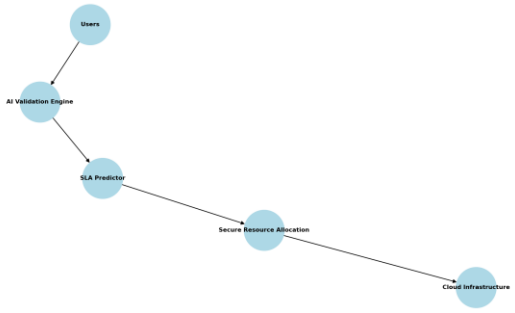

Figure 1: AI-Driven Cloud User Validation Workflow

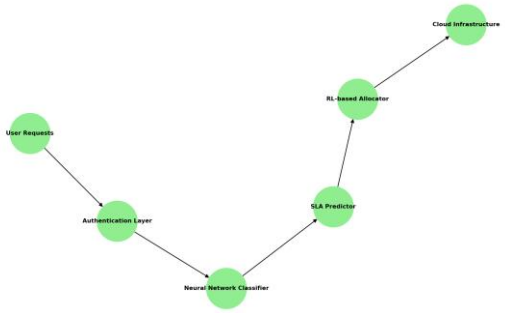

Figure 2: System Architecture of AI-Driven Validation and Allocation

References

[1] J. Wang, et al., 'Reinforcement Learning-Based Resource Scheduling in Cloud Computing,' Future Generation Computer Systems, 2021.

[2] X. Chen, et al., 'Adaptive Anomaly Detection for Cloud Intrusion Prevention,' IEEE Transactions on Cloud Computing, 2020.

[3] A. Singh, et al., 'Trust Models for Cloud Computing,' Journal of Cloud Computing, 2019.

[4] H. Takabi, et al., 'Security and Privacy Challenges in Cloud Computing Environments,' IEEE Security & Privacy, 2016.

[5] S. Garg, et al., 'SLA-Based Resource Provisioning in Cloud Computing,' Future Generation Computer Systems, 2018.

[6] R. Calheiros, et al., 'CloudSim: A Toolkit for Modeling Cloud Environments,' Software: Practice and Experience, 2011.

[7] Y. Li, et al., 'Machine Learning Approaches for Cloud Security,' Journal of Network and Computer Applications, 2020.

[8] J. Zhang, 'AI-Based Access Control in Cloud Systems,' Information Sciences, 2019.

[9] A. Patel, et al., 'Cloud Security Using AI-Driven Methods,' Applied Soft Computing, 2021.

[10] P. Gupta, et al., 'Resource Allocation Using Neural Networks in Cloud Computing,' Cluster Computing, 2019.

[11] T. Lorido-Botran, et al., 'A Review of Machine Learning for Cloud Resource Management,' ACM Computing Surveys, 2014.

[12] B. Varghese, et al., 'Next Generation Cloud Computing: New Trends,' Future Generation Computer Systems, 2017.

[13] N. Fernando, et al., 'Mobile Cloud Computing: A Survey,' Future Generation Computer Systems, 2013.

[14] J. Gubbi, et al., 'Internet of Things (IoT): A Vision,' Future Generation Computer Systems, 2013.

[15] M. Armbrust, et al., 'A View of Cloud Computing,' Communications of the ACM, 2010.

[16] K. Hwang, et al., 'Cloud Security with Virtualized Defense and Reputation-Based Trust,' IEEE Internet Computing, 2013.

[17] M. Ali, et al., 'Security in Cloud Computing: Opportunities and Challenges,' Information Sciences, 2015.

[18] D. Bernstein, et al., 'Blueprint for the Intercloud,' IEEE Computer, 2011.

[19] R. Buyya, et al., 'Market-Oriented Cloud Computing: Vision, Hype, and Reality,' HPCC, 2009.

[20] I. Foster, et al., 'Cloud Computing and Grid Computing 360-Degree Compared,' IEEE Grid Computing Environments Workshop, 2008.

[21] S. K. Garg, R. Buyya, 'NetworkCloudSim: Modelling Parallel Applications in Cloud Simulations,' HPCC, 2011.

[22] H. Jin, et al., 'Virtual Machine Resource Allocation in Cloud Computing,' IEEE Cluster, 2012.

[23] E. Deelman, et al., 'Scientific Workflow Management and Resource Provisioning in Cloud,' Future Generation Computer Systems, 2015.

[24] L. Wang, et al., 'Adaptive Security and Privacy in Cloud Computing,' Journal of Parallel and Distributed Systems, 2017.

[25] Y. Jadeja, K. Modi, 'Cloud Computing - Concepts, Architecture and Challenges,' ICCC, 2012.