INTELLIGENT SOFTWARE SYSTEMS FOR MULTI-TENANT CLOUD ENVIRONMENTS: CHALLENGES AND SOLUTIONS

Veljko Paković*,
[0009-0003-9932-4303]

Angelina Njeguš
[0000-0001-8682-7014]

Singidunum University,
Belgrade, Serbia

Abstract:

The rapid adoption of cloud computing has transformed software development and deployment, particularly through multi-tenant architectures that facilitate resource sharing while ensuring data isolation. This paper examines the role of intelligent software systems in multi-tenant cloud environments, addressing key challenges such as scalability, security, and adaptability to diverse user needs. A comprehensive analysis of existing research on multi-tenant cloud applications, security challenges, and IoT integration is presented. Additionally, the results of an experimental study on the use of autonomous drones for precision spraying in hazelnut plantations were observed and analysed. These drones operate within a cloud-based infrastructure hosted on Microsoft Azure, employing intelligent algorithms for route optimization, weather analysis, and real-time pesticide distribution adjustments. The multi-tenancy aspect is addressed by designing a system that enables multiple plantation owners to use a shared platform while maintaining individualized data and operational configurations. Our findings underscore critical concerns related to data privacy, performance optimization, and fault tolerance in shared cloud environments. Furthermore, we analyse security risks such as cross-tenant data leakage and access control vulnerabilities, offering recommendations for risk mitigation. This study contributes to the advancement of intelligent, cloud-based software architectures, showcasing how AI-driven systems can enhance efficiency and automation in multi-tenant applications. Future research will explore machine learning-based predictive analytics to further optimize resource utilization and strengthen security mechanisms in cloud-based IoT ecosystems.

Keywords:

Multi-Tenant Cloud, Intelligent Software Systems, IoT, Autonomous Drones, Cloud Security, AI in Agriculture.

INTRODUCTION

In the modern era, cloud computing serves as the foundation for the development and implementation of advanced software solutions. Multi-tenant cloud applications enable multiple users to simultaneously utilize a software system, where each user (tenant) has logically isolated data and personalized experience. This approach offers numerous advantages, including resource optimization, scalability, and reduced infrastructure maintenance costs. However, the implementation of intelligent software systems in a multitenant cloud environment presents several challenges, such as data security, system performance, adaptability to different users,

Correspondence:
Veljko Paković

e-mail:
veljko.pakevic.24@singimail.rs

DOI: 10.15308/Sinteza-2025-48-54

and efficient resource allocation. Additionally, the development and integration of intelligent algorithms in such environments require specialized strategies and architectural solutions to ensure optimal system performance.

The objective of this paper is to analyse the key aspects of applying intelligent software systems in multitenant cloud applications, highlighting challenges and proposed solutions. Understanding and enhancing intelligent software systems in multitenant cloud applications is a crucial step toward optimizing business processes, increasing security, and improving operational efficiency in environments that support multiple users. This paper aims to provide a comprehensive insight into the current state and potential future developments in this field, analysing concrete examples and trends shaping the future of intelligent software systems.

2. LITERATURE REVIEW

Cloud computing (CC) is a model enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources [1]. It is characterized by scalability, flexibility, and cost efficiency. Cloud environments are typically categorized into three main service models, such as: Infrastructure as a Service - IaaS (provides virtualized computing resources, such as virtual machines, storage, and networking), Platform as a Service - PaaS (development platform with tools and infrastructure for application deployment) and Software as a Service - SaaS (delivers software applications over the internet, eliminating the need for local installation and maintenance).

Multitenancy is a software architecture in which a single instance of software runs on a server and serves multiple tenants, ensuring data isolation and customization for each client within a shared infrastructure [2]. Each tenant operates within a logically isolated environment while sharing a common infrastructure, leading to cost savings and improved scalability. There are three primary multitenancy models:

1. Single Tenant: Each customer has a dedicated instance of the application and database.
2. Shared Database, Isolated Schema: A single database instance is used, but each tenant has a separate schema.
3. Shared Database, Shared Schema: All tenants share the same database schema, with mechanisms in place to differentiate their data.

Intelligent software systems integrate artificial intelligence (AI), specifically machine learning (ML) algorithms to enhance decision-making, automation, and predictive capabilities. These systems use algorithms to process data, recognize patterns, and adapt their behaviour. The key components of intelligent systems in cloud environments include:

1. Machine Learning Models: Algorithms that learn from data to make predictions and automate processes.
2. Natural Language Processing (NLP): Enables systems to understand and generate human language.
3. Predictive Analytics: Uses historical data to forecast future trends and behaviours.
4. Autonomous Decision-Making: AI-driven mechanisms that optimize system performance and resource allocation.

Intelligent software systems in multitenant cloud applications can be categorized based on their functionality and implementation into:

1. AI-Assisted Resource Management: uses ML models to predict and allocate cloud resources dynamically based on workload demands.
2. Security and Anomaly Detection: AI-driven systems analyse patterns in network traffic, user behaviour, and system logs to detect anomalies, help prevent security breaches, detect fraud, and respond to cyber threats in real time.
3. Personalized User Experience: AI models analyse user behaviour, preferences, and interactions to customize application UI, recommendations, and workflows, and enhance user engagement and retention through tailored experiences.
4. Automated Customer Support: AI-powered chatbots and virtual assistants handle common customer queries, reducing response times and improving efficiency.
5. AI-Powered Edge Computing & IoT Analytics: AI processes real-time IoT data at the edge to reduce cloud latency.
6. AI-Powered Workflow Automation: Automates repetitive tasks in cloud applications, improving productivity. Uses AI-driven decision-making for business process automation (BPA).

AI in multitenant cloud applications is expanding rapidly, enhancing efficiency, security, and user experience. From AI-driven resource management to intelligent automation, these systems provide robust solutions across multiple industries. However, several challenges and issues still need to be addressed. Some key issues are:

1. Data Security and privacy concerns - Multitenant cloud environments require strong data isolation to prevent leaks between tenants. AI-driven automation introduces additional security risks. Challenges are: data breaches due to misconfigured access controls, AI models unintentionally exposing sensitive tenant data, and compliance with GDPR, CCPA, HIPAA, and other data regulations.
2. AI Bias & Ethical Concerns - AI models may unintentionally favour certain groups due to biased training data. Challenges are AI-driven hiring, lending, and insurance decisions showing discrimination; lack of explainability in AI decision-making, and ethical concerns over AI surveillance and misuse of customer data.
3. Scalability & Performance Bottlenecks - AI-driven cloud applications require massive computing resources. Autoscaling isn't always efficient, therefore challenges are high latency in real-time applications, Cloud resource overutilization, leading to increased costs, and AI workload balancing across multiple tenants.
4. Cost Management & Optimization - AI-powered cloud solutions consume extensive resources, leading to high operational costs. Challenges are over-provisioning cloud resources in multitenant models, and unexpected cloud service cost spikes (e.g., AI training costs).
5. Real-Time Data Processing Challenges - Multi-tenant cloud applications generate massive real-time data streams from IoT, user activity, and AI workflows, therefore challenges are high-latency AI predictions for real-time applications and AI models struggling to process live sensor data efficiently.

Studies, described in Table 1, contribute valuable insights into the development and optimization of intelligent software systems within multitenant cloud environments, offering frameworks and methodologies to enhance security, performance, and resource management.

The study addresses the challenges inherent in multi-tenant cloud systems, such as data isolation risks, resource contention, and susceptibility to cyber threats. It explores the integration of adaptive resource management techniques and artificial intelligence (AI)--driven threat mitigation to enhance system robustness. The proposed framework utilizes machine learning models for dynamic resource allocation and real-time detection and prevention of cyber threats. The study found that integrating adaptive resource management with AI-driven threat mitigation significantly improved security and performance in multi-tenant cloud environments. The framework optimized workload distribution, reducing resource contention and enhancing overall system efficiency. AI-driven security mechanisms successfully identified and mitigated cyber threats in real-time, strengthening data protection. Performance metrics showed notable improvements, including reduced latency and increased throughput, while the risk of attacks was significantly minimized. Overall, the approach demonstrated a secure, scalable, and efficient solution for managing multi-tenant cloud computing systems. [3]

The paper provides a comprehensive analysis of the security challenges associated with deploying multi-tenant Field Programmable Gate Arrays (FPGAs) in cloud computing environments. It examines various deployment models, including spatial and temporal multi-tenancy, and evaluates their respective adversary models and security guarantees. The study highlights the vulnerabilities inherent in these models, particularly focusing on potential attacks such as Row hammer, cache side-channel attacks, and remote physical attacks that exploit the FPGA fabric. Additionally, the paper discusses the implications of untrusted cloud providers and the risks of intellectual property piracy, emphasising the need for robust security measures in multi-tenant FPGA deployments. The study found that integrating adaptive resource management with AI-driven threat mitigation significantly improved security and performance in multi-tenant cloud environments. The framework optimized workload distribution, reducing resource contention and enhancing overall system efficiency. AI-driven security mechanisms successfully identified and mitigated cyber threats in real-time, strengthening data protection. Performance metrics showed notable improvements, including reduced latency and increased throughput, while the risk of attacks was significantly minimized. Overall, the approach demonstrated a secure, scalable, and efficient solution for managing multi-tenant cloud computing systems. [4]

The research explores the integration of adaptive resource management and AI-driven threat mitigation to enhance security and performance in multi-tenant cloud computing environments. It addresses key challenges such as data isolation risks, resource contention, and cyber threats, proposing a framework that utilises machine learning algorithms for dynamic workload distribution and real-time threat detection. The study demonstrated that AI-powered security mechanisms significantly improved threat detection and prevention, reducing cyber risks. The adaptive resource management framework optimised workload distribution, leading to lower latency, increased system efficiency, and better scalability. The approach proved effective in securing multi-tenant cloud infrastructures while ensuring high performance and reliability. [5]

The study examines multi-tenant architectures in cloud computing, focusing on SaaS solutions, resource sharing, and data isolation. It explores AI-driven observability frameworks and advanced security mechanisms to enhance scalability and efficiency. Integrating AI and security measures improved scalability by 70% and reduced operational costs by 60%, optimising resource utilisation and system performance. [6]

Investigates the integration of AI into cloud security frameworks to enhance protection in multi-tenant environments. The study focusses on employing advanced threat detection and real-time monitoring mechanisms to identify and mitigate security threats proactively. The proposed model leverages ML algorithms to detect anomalous behaviours, predict potential security breaches and automate threat mitigation strategies. The study demonstrates that AI-driven security solutions significantly enhance threat detection accuracy and response times in multi-tenant cloud environments. The research highlights improvements in identifying unauthorised access and potential data breaches by implementing ML algorithms capable of real-time anomaly detection. Additionally, the paper addresses challenges related to integrating AI into existing cloud infrastructures, such as ensuring data privacy and managing computational overhead. [7]

The paper examines resilient multi-tenant cloud architectures, focusing on fault tolerance, security, and performance optimisation for reliable service. Implementing redundancy, data replication, and security protocols improved scalability, reliability, and data protection, ensuring uninterrupted cloud services. [8]

Provides a comprehensive analysis of security concerns associated with cloud computing (CC), focusing on various infrastructure levels: application, network, host, and data. It delves into significant challenges that could impact the CC business model and discusses documented solutions for each security issue. A particular emphasis is placed on multi-tenancy—a core feature of CC—which, while offering benefits like elasticity and flexibility, also introduces vulnerabilities such as abuse, unavailability, data loss, and privacy violations. The study aims to identify open problems and offers practical recommendations for future research to enhance overall CC security. The study underscores the substantial impact of multi-tenancy on cloud security, highlighting its contribution to various issues across all infrastructure levels. It emphasises the necessity for focused efforts to mitigate security vulnerabilities arising from multi-tenancy. By identifying specific challenges and suggesting targeted research directions, the paper contributes valuable insights to the broader discourse on cloud security, advocating for initiatives aimed at strengthening the resilience of cloud infrastructures. [9]

Additionally, since this paper examines this topic through an experimental study on the use of autonomous drones for precision spraying in plantations, where these drones operate within a cloud-based infrastructure employing intelligent algorithms for route optimisation, weather analysis, and real-time pesticide distribution adjustments, the analysis of relevant research papers is also analysed.

In a study [10], authors explored the use of reinforcement learning to optimise agricultural drone navigation for pesticide spraying. The research implements a Deep Q-learning algorithm that enables drones to autonomously adjust flight paths, avoid obstacles, and enhance spraying efficiency. The results demonstrate that this AI-driven approach significantly reduces pesticide wastage, minimises battery consumption, and improves overall spraying accuracy compared to traditional path-planning algorithms.

The research [11] focusses on optimising drone flight paths using a Bi-directional Long Short-Term Memory (Bi-LSTM) model integrated with a Deep Q-Network (DQN). This hybrid AI approach enhances UAV adaptability to changing environmental conditions while ensuring precise pesticide distribution. Experimental results demonstrate a reduction in redundant spraying, improved coverage accuracy, and lower operational costs for farmers.

The study [12] presents a data-driven optimization model for agricultural drone flight planning. By utilising a spray distribution model, the framework determines ideal flight speeds and pass widths to achieve uniform pesticide coverage. The study confirms improved spraying efficiency, minimised overlapping coverage, and better adaptability across different crop types and UAV models, enhancing precision agriculture practices.

The study [13] presents a modular, low-cost autonomous spraying control system integrated into traditional agricultural drones. The system utilises a machine learning-based spray uniformity algorithm, which optimises pesticide application by analysing real-time environmental data. By implementing a coefficient of variation-based approach, the study aims to ensure uniform pesticide distribution across plantations, reducing excessive chemical use and improving precision spraying efficiency. Experimental testing demonstrated a high level of spraying accuracy, with the system achieving a targeted distribution efficiency between 87.1% and 98.8%. The intelligent control mechanism significantly reduced over-spraying and under-spraying issues, leading to more effective pest control and lower chemical waste. The study confirms that AI-driven spray control can enhance agricultural productivity while minimising environmental impact.

3. METHODOLOGY AND EXPERIMENT

Traditional methods of crop spraying involve significant labour and machinery costs and inconsistent pesticide and fertiliser application. Optimising drone flight paths, ensuring precise pesticide application, and managing different plantation requirements are major challenges. Additionally, a scalable and intelligent system is needed to support multiple plantations while maintaining efficiency and security.

To address these challenges, we propose an intelligent, cloud-based drone management system that enables multiple plantation owners to utilise the same infrastructure while ensuring individual operational independence. The system leverages AI for flight path optimisation, real-time environmental monitoring, and automated pesticide application

System architecture and its components are:

- Multitenant Cloud Infrastructure (Azure-Based)
  - Each tenant operates within a logically isolated environment, allowing for personalized configurations and settings. This ensures that the operations and data of one tenant remain unaffected by others.
  - Azure Kubernetes Service (AKS) manages the deployment and scaling of containerized applications, such as drone control systems, ensuring high availability and efficient resource utilization.
  - Azure IoT Hub facilitates secure and reliable communication between drones and the cloud, enabling real-time data collection and monitoring of drone operations.
  - Azure SQL Database service stores plantation-specific data securely, implementing row-level security to ensure that each tenant can access only their respective data, maintaining data privacy and integrity.
- AI-Powered Flight Path Optimisation
  - Machine learning algorithms process terrain and weather data to plan optimal flight routes, considering factors like elevation changes and forecasted weather patterns.
  - Drones adjust their flight paths in real-time by analysing current wind speeds and humidity levels, ensuring stable flight and effective data collection.
- Intelligent Spraying System
  - Drones equipped with cameras and AI algorithms detect plant density and signs of disease, enabling targeted spraying only where needed.
  - Sensors monitor variables like wind direction and speed, ensuring chemicals are applied accurately, reducing drift, and enhancing effectiveness.
- Tenant Management and Access Control
  - Secure Login via Azure Active Directory B2C provides authentication and user management, allowing plantation owners to securely access their dedicated environments.
  - Implements strict access controls so that each tenant can only view and manage their data and analytics, preventing unauthorised access.
- Automated Reporting and Compliance
  - Azure Machine Learning generates predictive analytics on crop health and pest threats.
  - Reports are automatically generated for regulatory compliance and plantation management.

By integrating these components, the system aims to enhance the efficiency, precision, and sustainability of plantation management through advanced cloud-based solutions and artificial intelligence.

3.1. SCALABILITY

Challenge: During peak spraying seasons, the system must efficiently handle increased workloads without compromising performance.

Solution: Azure's auto-scaling capabilities dynamically adjust resources to meet demand. By utilising services like Azure App Service's automatic scaling, the system can automatically scale the number of application instances based on real-time metrics such as HTTP request volume or CPU usage. This ensures optimal performance during high-demand periods and cost savings during low-demand periods.

Implementation Steps

- Set rules that specify when to scale out (add resources) or scale in (remove resources) based on predefined thresholds.
- Use Azure Monitor to track application performance and trigger scaling actions as needed.
- Conduct load testing to ensure the system scales appropriately under various conditions.

3.2. DATA SECURITY

Challenge: Ensuring that each tenant's data remains secure and inaccessible to unauthorized users.

Solution: Implement Azure Role-Based Access Control (RBAC) and robust encryption mechanisms. RBAC allows you to assign specific permissions to users based on their roles, ensuring they access only the resources necessary for their tasks. Encryption safeguards data both at rest and in transit, protecting it from unauthorized access.

Implementation Steps

- Assign built-in or custom roles to users, groups, or service principals, limiting access to resources based on the principle of least privilege.
- Use Azure Disk Encryption for virtual machines and ensure that data stored in Azure Storage and Azure SQL Database is encrypted by default.
- Utilize Azure Key Vault to securely store and manage encryption keys, secrets, and certificates.

3.3. REAL-TIME DATA PROCESSING

Challenge: The system must process telemetry data from drones in real-time to dynamically adjust spraying parameters for optimal efficiency.

Solution: Leverage Azure Stream Analytics, a real-time analytics service designed to process large streams of data with low latency. By integrating Azure Stream Analytics with Azure IoT Hub, the system can ingest, process, and analyze telemetry data from drones, enabling immediate adjustments to spray parameters.

Implementation Steps:

- Configure Azure IoT Hub to collect telemetry data from drones.
- Develop queries that analyse incoming data streams and output results to appropriate services or storage.
- Use the analysed data to trigger functions or alerts that adjust drone operations in real-time.

3.4. COST MANAGEMENT

Challenge: Providing a cost-effective solution that scales with the needs of both small and large plantation owners.

Solution: Adopt Azure's pay-as-you-go pricing model, which charges users based on actual resource consumption. This model ensures that plantation owners pay only for the computing resources they use, making the system financially accessible regardless of farm size.

Implementation Steps:

- Utilise Azure Cost Management and Billing to track and analyse resource consumption.
- Establish spending limits and configure alerts to notify users when approaching budget thresholds.
- Regularly review and adjust resource allocations to prevent over-provisioning and minimise unnecessary costs.

The implementation of intelligent software systems in a multitenant cloud environment significantly enhances the efficiency of drone-based plantation spraying. By leveraging AI, IoT, and cloud computing, the proposed solution enables multiple plantation owners to share a robust, scalable, and intelligent infrastructure. This approach not only optimises spraying operations but also reduces costs, minimises environmental impact, and improves overall agricultural productivity.

4. CONCLUSION

Integrating intelligent software systems into multi-tenant cloud applications offers significant advantages and challenges. This study focused on multi-tenancy aspects such as resource optimisation, security, and system adaptability, particularly in agriculture, by examining autonomous drones for plantation spraying. Experiments demonstrated that a cloud-based, AI-driven drone management system on Microsoft Azure can effectively serve multiple plantation owners while ensuring data isolation and operational customisation. Results indicate that intelligent automation in agriculture enhances efficiency, reduces costs, and provides scalable solutions for precision farming. A review of existing literature on multi-tenant cloud computing, security, and IoT offered insights into technical and architectural challenges, including cross-tenant security risks, resource allocation, and performance optimisation. The study emphasises the need for robust isolation mechanisms, dynamic scaling, and AI-enhanced security solutions.

REFERENCES

[1] S. K. a. S. Tim. Mather, “Cloud security and privacy: An Enterprise Perspective on Risks and Compliance, First. Sebastopol,” in *O’Reilly*, 2009.

[2] N. Ruparelia, “Cloud Computing, Revised and Updated Edition,” 2023. [Online]. Available: https://mitpress.mit.edu/9780262546478/cloud-computing. [Accessed 1 April 2025].

[3] M. Sathik, “Enhancing Security and Performance in Multi-Tenant Cloud Computing Environments Through Adaptive Resource Management and AI-Driven Threat Mitigation - QIT Press,” 3 2025. [Online]. Available: https://qitpress.com/articles/QITP-IJCC_05_01_002. [Accessed 27 Mart 2025].

[4] G. Dessouky, A. R. Sadeghi and S. Zeitouni, “SoK: Secure FPGA multi-tenancy in the cloud: Challenges and opportunities,” in *2021 IEEE European Symposium on Security and Privacy, Euro S and P 2021,* 2021.

[5] M. R. Mekala, “AI-driven optimization for multi-tenant cloud platforms: balancing cost, performance, and security,” *International journal of computer engineering and technology*, vol. 16, no. 1, pp. 1381-1400, 1 2025, doi: https://doi.org/10.34218/IJCET_16_01_104

[6] R. K. Sharma, “Multi-Tenant Architectures in Modern Cloud Computing: A Technical Deep Dive,” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 11, no. 1, pp. 307-317, 1 2025, doi: https://doi.org/10.32628/CSEIT25111236.

[7] S. Chippagiri, “A Study of Cloud Security Frameworks for Safeguarding Multi-Tenant Cloud Architectures,” *International Journal of Computer Applications,* vol. 186, no. 60, pp. 50-57, 2025.

[8] S. A. Dave, N. K. Gannamneni, B. Gajbhiye, R. Agarwa, S. Jain and P. K. Gopalakrishna, “Designing Resilient Multi-Tenant Architectures in Cloud Environments,” *International Journal for Research Publication and Seminar,* vol. 11, no. 4, pp. 356-373, 12 2020, doi: https://doi.org/10.36676/JRPS.V11.I4.1586.

[9] M. A. Hayat, S. Islam and M. F. Hossain, “Securing the Cloud Infrastructure: Investigating Multi-tenancy Challenges, Modern Solutions and Future Research Opportunities,” *International Journal of Information Technology and Computer Science*, vol. 16, no. 4, pp. 1-28, 2024.

[10] Y.-Y. Huang, Z.-W. Li, C.-H. Yang and Y.-M. Huang, “Automatic Path Planning for Spraying Drones Based on Deep Q-Learning,” *Journal of Internet Technology*, vol. 24, no. 3, pp. 565-575, 2023.

[11] H. Fu, Z. Li, W. Zhang, Y. Feng, L. Zhu, X. Fang and J. Li, “Research on Path Planning of Agricultural UAV Based on Improved Deep Reinforcement Learning,” *Agronomy*, vol. 14, no. 11, p. 2669, 2024.

[12] R. V. Nanavati, Y. Meng, M. Coombes and C. Liu, “Generalized data-driven optimal path planning framework for uniform coverage missions using crop spraying UAVs,” *Precision Agriculture*, vol. 24, no. 4, pp. 1497-1525, 2023.

[13] P. Wang, A. S. Hanif, S.-H. Yu, C.-G. Lee, Y. H. Kang, D.-H. Lee and X. Han, “Development of an autonomous drone spraying control system based on the coefficient of variation of spray distribution,” *Computers and Electronics in Agriculture*, vol. 227, no. 1, 2024.