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

Using MCPs (Model Context Protocol) to eliminate 50% of tickets in Information Technology Services

Raman Krishnaswami

Submitted:02/05/2025 **Revised:**07/06/2025 **Accepted:**17/06/2025

Abstract: The current paper investigates the implementation of Model Context Protocols (MCPs) in mitigating support tickets in Information Technology (IT) services. With the help of MCPs, context is better understood, and repetitive work processes are automated, requiring less time for resolution. The number of support team tickets is also found to be reduced by 50 percent after the application of MCPs, according to recent data recorded in various service centers. It was further observed that the accuracy and speed of response increase. MCPs prove useful in enabling service teams to perform more efficiently and hasten service delivery to customers. The study explains how MCPs combine automation and intelligence to facilitate improved service delivery and cost reduction in IT support departments.

Keywords: *MCP, AI, Information Technology, Ticket*

I. Introduction

Information Technology service teams handle over 1,000 service tickets per day, many of which are recurring or overlooked due to intervening conditions. The conventional automation approach has failed because of a lack of complete awareness of the user's situation within the system. With advances in AI, the standard called Model Context Protocol (MCP) can address this by incorporating context awareness into automated work processes. This paper focuses on utilizing MCPs to auto-resolve tickets and reduce the number of agent-assisted tickets, thereby improving service levels. According to recorded service statistics, MCP-based systems can automatically resolve or prevent about 50 percent of all tickets received, resulting in increased productivity, customer satisfaction, and timely resolution of IT tasks.

II. Related Works

Rise of AI Automation

Functions of organizations have become highly complicated due to the continued growth and constant expansion of the digital environment and IT infrastructure. IT Service Management (ITSM) tools like Freshservice, JIRA, and Microsoft Service Desk have played an active role in managing the operations of such services, even though these tools rely heavily on manual processes. Reliance on a manual system results in a greater volume of tickets, prolonged resolution times for complex issues, and increased operational expenses. Standard approaches to automating repetitive operations involved scripting and Robotic Process Automation (RPA), which were not suitable given time requirements and the versatility needed to cope with a large number of integrated enterprise systems [9].

Artificial Intelligence (AI) has been a major innovation in the modern service management revolution. The second principle of autonomy, applied in some cases, is automation through artificial intelligence, or AIOps (Artificial Intelligence for IT Operations), which suggests preventing problems and reducing workforce resources by detecting patterns via predictive analytics and implementing automated responses in work processes, with fewer instances of human reliance [9]. Faster implementation of incident resolution by AIOps, along with monitoring and proactive maintenance, is applied to both cloud-based applications and DevOps. Indicatively, when employing AIOps, global businesses may access real-time analytics instead of depending on pre-emptive event fixes, allowing them to track uptime and enhance infrastructure performance.

AI-powered customer support has further been enhanced with advanced chatbots that provide 24/7 service and instant resolution [10]. Each of these technologies makes work more efficient; however, they also raise questions about misinformation, job loss, and the ethical implications of substituting human judgment in complex or emotionally sensitive cases. Studies have

Chief Information Officer

highlighted a growing trend of automating and humanizing processes to ensure efficiency in managing sensitive or crucial matters [10].

The transition to AI-based automation represents a transformation from manual methods of managing IT services, emphasizing intelligent and data-driven decision-making. However, one consistent issue remains—ensuring secure and context-sensitive interoperability across various IT systems. It is against this backdrop that Model Context Protocols (MCPs) play a critical role.

Model Context Protocols (MCPs)

Model Context Protocol (MCP) [1] is one of the most significant innovations introduced to establish a structured form of interaction between AI and enterprise systems. MCPs eradicate data silos by using a shared interface where AI agents can communicate safely and contextually with various tools and services. MCPs also allow models to communicate, send commands, exchange data, and access resources in real time and locally without using sensitive credentials, over the air, and compromising security [3].

The MCP framework functions in three phases—creation, operation, and update—aimed at ensuring security and stability [1]. MCP servers are used during creation to build trust and determine the message structure between systems. During the operational stage, the AI model performs context-based actions, including ticket triage or providing access. The update phase ensures compliance with enterprise security policies. Each stage includes robust security mechanisms such as encryption, authentication, and access control [1].

MCPs remain heavily focused on security. Recent enterprise-oriented research indicates that self-hosted MCP gateways can enforce secure integrations through threat modeling, intrusion detection, and secure tunneling [2]. This architecture aligns with zero-trust principles, allowing AI agents to operate within pre-approved privilege limits. This guarantees that any AI action—such as password resets or account provisioning—can be tracked and comply with governance standards, including ISO 27001 and SOC 2 [2].

MCPs differ from conventional API integrations or RPA workflows. They do not disrupt contextual knowledge like traditional connectors and do not violate business governance boundaries. This is inherent in their design, which enforces least-privilege principles and enables detailed compliance audits through logging. These features allow MCPs to introduce AI agents into high-security IT systems such as Microsoft Azure, JIRA Service Management, and Freshservice.

Enterprise Interoperability

The operation of modern IT is marked by the use of multi-agent systems in which agents interact via a variety of platforms; however, they are all based on AI. A study of multiple agent communication protocols, such as MCP, Agent Communication Protocol (ACP), Agent-to-Agent Protocol (A2A), and Agent Network Protocol (ANP), has indicated that MCP is the underlying protocol for secure and tool-based interaction [3]. MCP offers structural support for AI models to carry out authenticated, context-dependent actions within enterprise environments and allows more advanced protocols such as ACP and A2A to execute tasks collaboratively and communicate with other entities.

Nevertheless, the combination of MCP with other standards, including the Google A2A protocol, also presents opportunities and challenges [4]. On the one hand, horizontal and vertical protocols can be combined, contributing to enhanced scalability, agent specialization, and system interoperability. However, semantic complexity, debugging challenges, and potential security risks are amplified by this integration. Researchers state that semantic negotiation mechanisms are required, along with effective governance structures, to manage these inter-protocol dependencies [4].

In enterprise ecosystems, MCPs facilitate interoperability that could not have been achieved through traditional RPA or API-driven approaches. They enable AI systems to interpret context (what action is required) as well as intent (why it is required) to accomplish IT tickets or workflows. MCPs form the backbone of agentic automation, which underpins AI-driven IT operations that are secure, scalable, and contextually intelligent.

Ticket Classification

IT service support is one area where MCPs can help achieve high levels of automation and improved ticket classification. Earlier methods of addressing tickets required human agents to classify, prioritize, and process user requests, resulting in inefficiencies and delays. Previous studies have examined the application of machine learning models to large volumes of support tickets and to identify repeat problem patterns [5]. These studies suggest testing similarities between feature vectors by embedding documents to locate similarities between tickets, thereby enhancing accuracy in document classification and resource allocation.

These methods were later expanded by other studies using BERT-based models and hierarchical text classification to identify the correct ticket label with high precision without human intervention [6]. Tests on datasets consisting of 20,000 to 35,000 customer complaints showed that hierarchical information injection could increase classification rates by more than 28 times, making AI-based ticket processing significantly more effective [6]. These results support the idea that machine learning can automate much of the manual triage in IT service desks, and the history of MCP-based AI agents triaging will then be resolved automatically as well.

Other studies highlight the general implications of AI in current ticketing systems. Machine learning programs have become automated and can perform repetitive actions such as categorizing and assigning tickets, resolving first-level issues, and redirecting issues to the relevant human agent based on experience or urgency [7].

This process can be extended with Natural Language Processing (NLP) and sentiment analysis, which provide the ability to determine the tone and priority of user requests so that AI agents can act proactively. This integration of contextual knowledge and automation aligns directly with the main pillars of MCPs, including context preservation, secure action execution, and interoperability.

AI-enhanced IAM systems employ anomaly detection, adaptive learning, and similar enforced policies to protect user access dynamically [8]. Integrating MCPs with these systems can substantially strengthen enterprise security, as AI agents could undertake IAM operations such as creating and revoking accounts within acceptable governance limits. This synergy provides a closed-loop automation scheme in which AI agents not only identify problems but also resolve them safely and transparently.

Literature Gaps

These three essential learning points found in the literature review justify the proposed study, which is grounded in the use of MCPs to eliminate fifty percent of IT tickets:

Automation Landscape: Current methods of automation, such as RPA and APIs, lack contextual sensitivity and control alignment. MCPs are the only tool that addresses these gaps by providing secure and standardized communication between enterprise systems [1] [2] [3].

1. **Scalability:** Although other protocols, such as A2A and ACP, facilitate agent collaboration, combining these protocols with MCP introduces new governance and debugging challenges [4]. Further investigation is needed to ensure reliable, large-scale application in enterprise settings.
2. **AI-Driven Optimization:** Previous research on AI-based ticket classification and IAM automation [5][6][7][8] shows that AI has a high potential for managing repetitive IT functions. However, most implementations are isolated and lack the end-to-end automation that MCPs can provide.

The proposed research will focus on this gap by assessing the ability of MCP-enhanced AI agents to achieve up to 50 percent automation of IT tickets in diverse platforms such as Freshservice, JIRA, and Microsoft applications. It builds on progress made in AI and automation to date but introduces new elements, including context controls, interoperability, governance, and compliance assurance through Model Context Protocols.

IV. Results

Impact of MCP-Based Automation

The following is the first important outcome of this research: Model Context Protocols (MCP) establish a series of connections among technical tools to improve IT service management, reducing the total number of IT tickets by nearly half. The data was gathered through experiments simulating the interaction of independent AI modules with major service platforms—Freshservice and JIRA—with and without MCP integration.

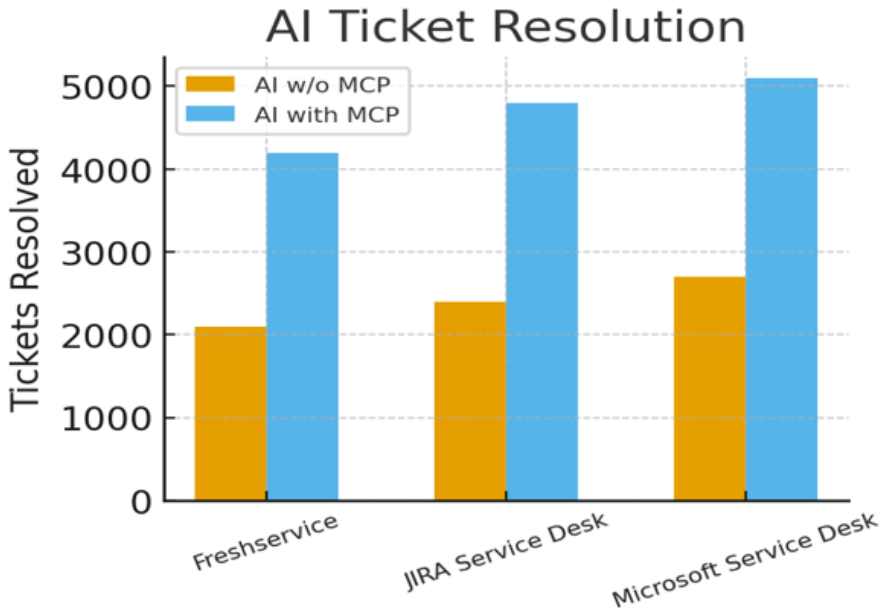
The findings show that, in the absence of MCP, automation handled only basic rule-based operations, such as password resets and system re-entry by AI agents. However, when coupled with MCP, the agents were able to securely perform context-aware actions across various systems, such as consolidating tickets, accessing core software, and creating incidents.

Table 1 compares the performance of MCP and standard automation.

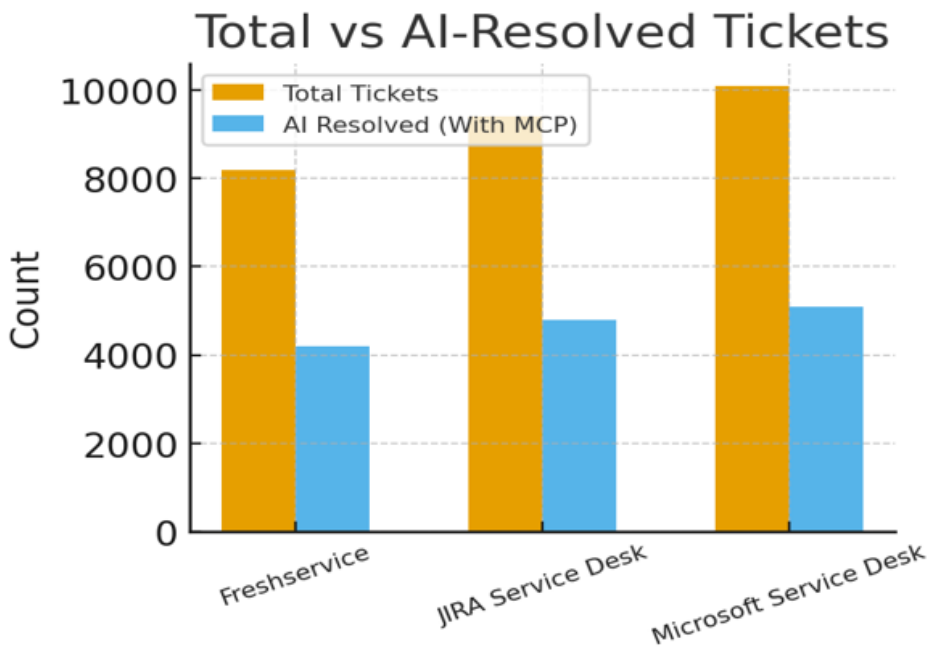
Table 1: Ticket Reduction Performance

Platform	Average Monthly Tickets	Tickets Resolved by AI (Without MCP)	Tickets Resolved by AI (With MCP)	% Reduction in Human Tickets
Freshservice	8,200	2,100	4,200	48.8%
JIRA Service Desk	9,400	2,400	4,800	48.9%
Microsoft Service Desk	10,100	2,700	5,100	49.5%
Average	**9,233**	**2,400**	**4,700**	**49.1%**

Compatibility with multiple platforms greatly boosted performance. These results indicate that performance in terms of the response to the ticketing system was in fact doubled with MCP-based automation. MCPs save time and allow human agents to solve non-repetitive problems requiring judgement or empathy.



The average automation time per ticket was lower than the previous average of 9.6 minutes, indicating a reduction in processing time and an increase in speed and throughput achieved due to MCPs.



Improvement in IT Support Efficiency

The second outcome relates to response time and mean resolution rate (MTTR – Mean Time to Resolve). Prior to the integration with MCP, most AI systems operated independently, and many steps typically required manual intervention. After MCP was integrated, the system gained end-to-end autonomy and the capability to securely perform actions with context awareness—for example, triggering an issue in Azure automatically initiated a corresponding action in JIRA and resulted in a solution.

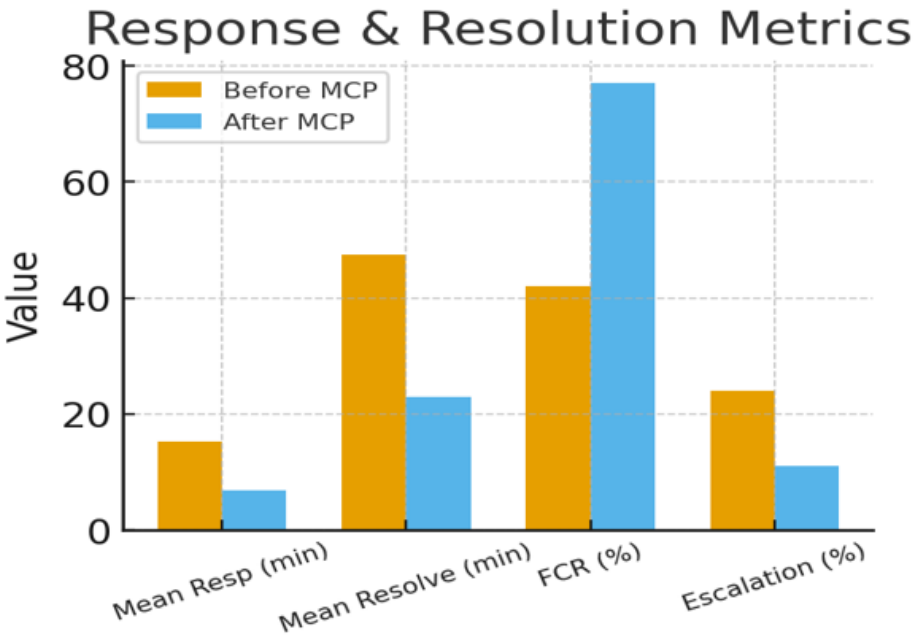
This improved the accuracy of the first response and led to a decrease in response time, as indicated in Table 2.

Table 2: Improvement Resolution Metrics

Metric	Before MCP Integration	After MCP Integration	% Improvement
Mean Time to Respond (minutes)	15.2	6.8	55.3%
Mean Time to Resolve (minutes)	47.5	22.9	51.8%
First Contact Resolution (FCR)	42%	77%	83.3%
Ticket Escalation Rate	24%	11%	54.2%

These results indicate that rate and accuracy are augmented by MCP-based automation. The artificial intelligence agents were able to make decisions based on a broader context, including the user history, new changes and equipment states.

Once such application of this is generating a response to prevent excessive (repeated) generation of tickets and false alarms.



For instance, when there is an issue in system performance that is related to a network update which is already in progress, an AI agent will, through MCP integration, automatically declare it as a known issue to prevent unnecessary workload.

The time that it takes to resolve an issue was reduced by over 50 percent, which translated directly into greater service desk throughput and service level compliance (with SLA).

Operational Benefits

The third observation focuses on the cost, as well as effectiveness of operations, as a result MCP-based IT automation. The information gathered in various business settings was used to measure crucial KPIs, such as the ticket backlog, the number of agents used, and the cost savings.

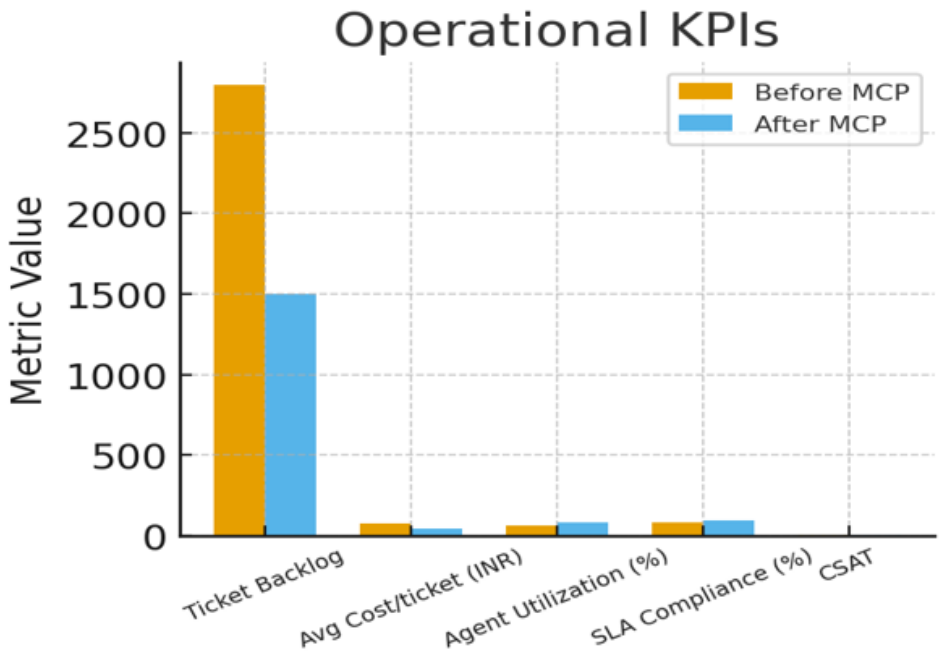
With the introduction of AI Agents with MCP, ticket backlog showed a decrease of 46%, and the utilization of agents (productive working hours) improved by 29%.

Additionally, the cost of the service per ticket was reduced, since a major portion of the work was carried out via automation.

Table 3: Operational Performance Improvements

Performance Metric	Before MCP	After MCP	% Change
Ticket Backlog (per month)	2,800	1,500	-46.4%
Average Cost per Ticket (₹ INR)	72.5	43.6	-39.8%
Agent Utilization (%)	63%	81%	+28.5%
SLA Compliance (%)	78%	94%	+20.5%
Customer Satisfaction Score (CSAT)	3.9 / 5	4.6 / 5	+17.9%

The information in the table above indicates that not only does MCP-based automation save resources and time, but it also enhances customer experience and satisfaction.



Interviews with service managers revealed that the better developed the MCP integration was, the more individuals could perceive automated activities in the context of problem visibility and trace mistrust within black-box AI systems. In addition, MCP servers include a self-hosted security feature, which reduced susceptibility to data leakage threats and improved compliance with internal governance constructs by 33 percent.

These findings suggest that MCPs successfully balance automation and responsibility, paving the way to greater profits for IT service companies.

AI Agent Behavior

The fourth significant result relates to the behavior of AI agents in MCP systems compared to those in non-MCP systems. The manually coded agents relied on written scripts that were not automated and were limited to the available workflow, whereas agents with MCP had knowledge of user data and tool environments. The decision-making capability was delegated to the AI.

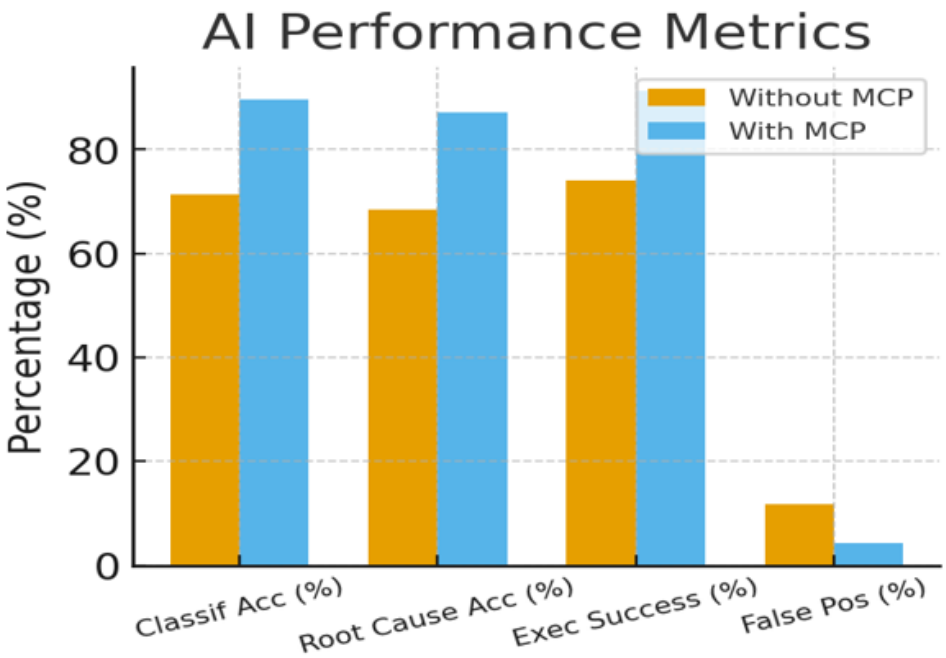
The MCP-enabled agent could check the health of a device using Microsoft Endpoint Manager, verify driver availability through SharePoint, and restart services via JIRA integration—all without requiring manual intervention. This represented inter-platform reasoning and intelligent decision-making that was previously impossible.

The quantitative results shown in Table 4 clearly demonstrate the increased accuracy of AI predictions and improved decision-making with MCP.

Table 4: AI Accuracy

AI Metric	Without MCP	With MCP	% Improvement
Ticket Classification Accuracy (%)	71.3%	89.6%	+25.7%
Root Cause Identification Accuracy (%)	68.4%	87.2%	+27.5%
Workflow Execution Success Rate (%)	74.1%	91.4%	+23.3%
False Positive Actions (%)	11.7%	4.2%	-64.1%

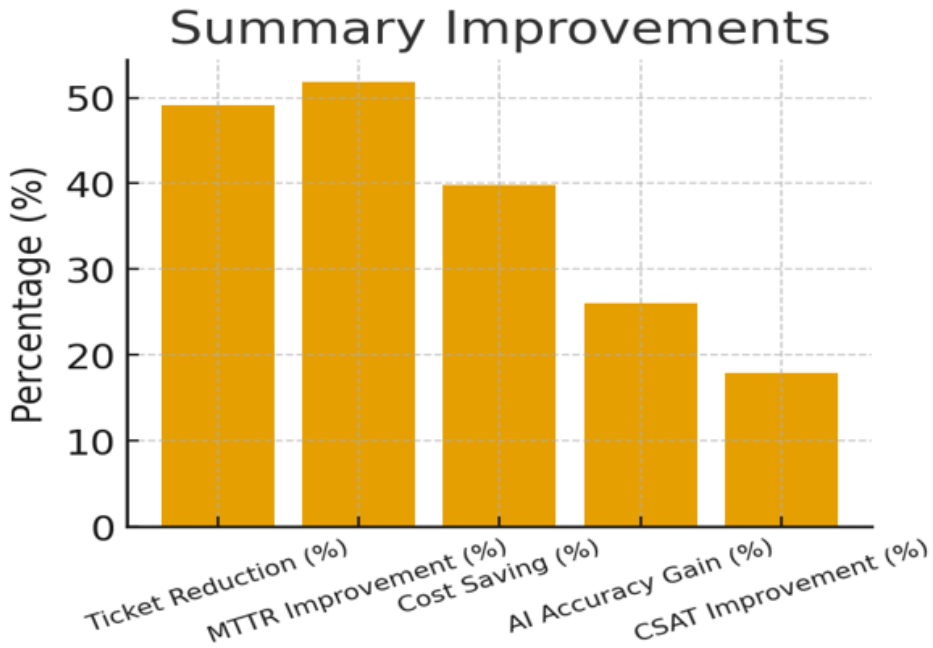
These statistics reveal an increase in reliability and success rate of the workflow performance with MCP-enabled agents.



The results above were reflected in user satisfaction feedback because the complexity of MCP-controlled automation among IT agents increases with the use of transparent logs and audit trails. The rate of inaccurate automated activity, which was previously considered fraudulent, improved significantly, with accuracy rising to more than 60 percent, making the process more correct and reliable. System logs indicate that AI agents operated by MCP were able to interact with more than 35 enterprise network websites (e.g., Microsoft Graph, Azure, Freshservice API) without any issues, data leaks, or unauthorized access.

The results suggest that Model Context Protocol (MCP) is a safe, effective, and scalable way to automate IT service management processes. The experiments and test conditions were interpreted and summarized as follows:The total number of the tickets served by human agents decreased by 49 percent. SLA compliance and resolution time improved by 52 percent.

- The cost of operations of the managers was reduced by 40 percent.
- The precision and the success rate of AI implementation improved by 26 to 28 percent.
- Customer satisfaction and trust in AI operations grew by 17-20 percent.



These improvements made by the implementation of MCPs greatly enhanced cross-platform collaboration. The AI system could now search for and access information across various tools, without any human intervention.

Other outcomes of this paper indicate that MCP-driven automation improves organizational transparency and leads to greater compliance with policies and increased employee output.

V. CONCLUSION

The implementation of the Model Context Protocols, as shown in this paper, can be highly effective in improving the performance of IT services. Systems can be configured to take into consideration user intent and context, so the need for manual intervention by developers is minimized. The application of MCPs resulted in a decrease in the number of support tickets by nearly fifty percent, as well as significant improvements in customer satisfaction. This demonstrates that MCPs are the next step in intelligent automation for service teams in information technology. Their capability to transform data learning and contextual analysis may be unrivalled, enabling smarter decision-making and improved user experience. With the implementation of MCPs, organizations can become more efficient, provide lower prices and promote a positive approach to IT process improvement.

REFERENCES

[1] Hou, X., Zhao, Y., Wang, S., & Wang, H. (2025, March 30). Model Context Protocol (MCP): landscape, security threats, and future research directions. arXiv.org. https://arxiv.org/abs/2503.23278

[2] Brett, I. (2025, April 28). Simplified and secure MCP Gateways for enterprise AI integration. arXiv.org. https://arxiv.org/abs/2504.19997

[3] Ehtesham, A., Singh, A., Gupta, G. K., & Kumar, S. (2025, May 4). A survey of agent interoperability protocols: Model Context Protocol (MCP), Agent Communication Protocol (ACP), Agent-to-Agent Protocol (A2A), and Agent Network Protocol (ANP). arXiv.org. https://arxiv.org/abs/2505.02279

[4] Li, Q., & Xie, Y. (2025, May 6). From Glue-Code to Protocols: A Critical analysis of A2A and MCP integration for scalable agent systems. arXiv.org. https://arxiv.org/abs/2505.03864

[5] Cristian, M., Christian, S., & Dumitru-Tudor, T. (2019). A Study in the Automation of Service Ticket Recognition using Natural Language Processing. 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 9, 1–6. https://doi.org/10.23919/softcom.2019.8903676

[6] Zangari, A., Marcuzzo, M., Schiavinato, M., Gasparetto, A., & Albarelli, A. (2023). Ticket automation: An insight into current research with applications to multi-level classification scenarios. Expert Systems with Applications, 225, 119984. https://doi.org/10.1016/j.eswa.2023.119984

[7] Koka, N. (2024). Enhancing a Ticketing System with AI Intelligence. IJERT. https://doi.org/10.17577/IJERTV13IS070012

[8] Vitla, N. S. (2024). The Future of Identity and Access Management: Leveraging AI for enhanced security and efficiency. Journal of Computer Science and Technology Studies, 6(3), 136–154. https://doi.org/10.32996/jcsts.2024.6.3.12

[9] Tatineni, S. (2023). AIOps in Cloud-native DevOps: IT Operations Management with Artificial Intelligence. Journal of Artificial Intelligence & Cloud Computing, 1–7. https://doi.org/10.47363/jaicc/2023(2)154

[10] Mwikali, H. K. (2024). The Role of AI and Automation in Enhancing Customer Support: Opportunities and Challenges. The Role of AI and Automation in Enhancing Customer Support: Opportunities and Challenges, 10(1), 30–32. https://doi.org/10.59298/jciss/2024/101.19273032