# ASSESSING IT PROFESSIONALS' PERCEPTIONS OF AI-DRIVEN PATCH MANAGEMENT IN ENTERPRISE IT SYSTEMS

by

ALEXANDER M. ELLIOTT

B.S., University of Maryland Global Campus, 2011

M.S., University of Maryland Global Campus, 2018

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2025

# Assessing IT professionals' perceptions of AI-driven patch management in enterprise IT systems

**Alexander Elliott,** *Middle Georgia State University*, *alexander.elliott@mga.edu*

## Abstract

The increasing complexity of enterprise IT systems and evolving cybersecurity threats necessitate efficient vulnerability management. Traditional patch management methods are slow and prone to errors, positioning AI-driven patch management systems as a viable solution through the automation of vulnerability detection, prioritization, and remediation. This quantitative study applies the Technology Acceptance Model (TAM) to examine how perceived usefulness (PU), perceived ease of use (PEOU), and attitude toward use (ATU) influence behavioral intention (BI) to adopt AI-driven solutions. Findings reveal that attitude toward use (ATU) is the strongest predictor of adoption, followed by perceived usefulness (PU), while perceived ease of use (PEOU) has no significant impact. These results underscore the importance of organizations in fostering positive user attitudes and effectively communicating the benefits of AI to drive adoption. These findings advance the literature on AI adoption in cybersecurity by clarifying the roles of user perception and attitude in shaping adoption behavior within enterprise IT settings.

**Keywords**: AI-driven patch management, vulnerability management, cybersecurity, Technology Acceptance Model, enterprise IT systems, behavioral intention

## Introduction

Managing security patches in enterprise IT environments is a cornerstone of cybersecurity. However, it remains a persistent challenge due to increasingly complex infrastructures and rapidly evolving cyber threats. Wong (2024) highlights that traditional patch management methods, which rely heavily on manual processes, often fail to scale with modern demands, exposing organizations to risks such as security breaches and operational disruptions. To address these limitations, Artificial Intelligence (AI) presents a transformative approach to patch management. Wong (2024) states that AI-driven patch management systems enhance speed, accuracy, and scalability by automating vulnerability identification, prioritization, and remediation tasks. These systems also reduce manual workloads, enabling IT professionals to focus on proactive threat mitigation and other strategic cybersecurity initiatives.

This study examines IT professionals' perceptions of AI-driven patch management systems through the lens of the Technology Acceptance Model (TAM). Developed by Davis (1989), TAM outlines how perceived usefulness (PU), perceived ease of use (PEOU), and attitude toward use (ATU) influence behavioral intention (BI). The findings from this study will offer insights into the key factors driving AI adoption in enterprise IT environments.

Traditional cybersecurity vulnerability management methods are often inefficient and labor-intensive, leading to delays that increase the risk of cyber threats, security breaches, and data loss. Wong (2024) explains that manual processes struggle to keep pace with the rapid emergence of new vulnerabilities, making it difficult for organizations to maintain effective cybersecurity defenses. To mitigate these challenges, Jawaid (2023) highlights the potential of AI-driven patch management systems, which automate vulnerability identification and prioritization, enabling faster and more efficient threat response. Similarly, Goswami (2019) emphasizes that AI enhances scalability by intelligently prioritizing and remediating vulnerabilities based on their criticality and impact, allowing organizations to allocate resources more

effectively. Furthermore, Harshith et al. (2024) highlight AI's role in automating routine security tasks, improving operational efficiency, and enabling security teams to focus on more complex threat detection and response strategies. By integrating AI-driven automation, organizations can significantly enhance their cybersecurity resilience and improve overall threat management capabilities.

This study aims to assess how three predictor variables — perceived usefulness, perceived ease of use, and attitude toward use — influence the dependent variable, behavioral intention, among IT professionals who adopt AI-driven patch management systems. By examining these relationships, the study aims to address inefficiencies in traditional patching methods and provide insights into the factors that influence the adoption of AI in large-scale IT environments. The findings will contribute to developing more effective and scalable patch management strategies, ultimately enhancing security and operational efficiency in enterprise IT environments. The purpose of this research is to answer the following research question:

RQ1: Which of the three predictor variables (i.e., perceived usefulness, perceived ease of use, and attitude toward use) significantly influences IT professionals' behavioral intention to adopt AI-driven patch management solutions?

### Research objectives

This study aims to identify the predictor variables —specifically, perceived usefulness, perceived ease of use, and attitude toward use — that significantly impact IT professionals' behavioral intention to adopt AI-driven patch management systems. By exploring the role of these factors in AI adoption for vulnerability remediation, the research will enhance the understanding of how AI-based patch management strategies can address current inefficiencies, ultimately improving security practices in enterprise IT environments.

## Review of Literature

### Challenges of traditional patch management

Traditional patch management processes face several limitations, including reliance on periodic scans and manual processes that are inherently reactive, time-consuming, and prone to human error (Wong, 2024). These inefficiencies result in delays in addressing newly discovered vulnerabilities, increasing the risk of exploitation by attackers. Wong (2024) highlights how AI-driven systems address these limitations by automating vulnerability identification, prioritization, and remediation tasks. This approach accelerates responses and reduces the likelihood of overlooking critical vulnerabilities, improving operational efficiency. Additionally, AI's scalability makes it suitable for large and complex IT environments, enabling organizations to proactively and adaptively address cybersecurity challenges (Wong, 2024).

One critical limitation is dependence on manual processes. Wong (2024) notes that analyzing scan reports to prioritize vulnerabilities often overwhelms security teams, particularly in large-scale environments with high volumes of vulnerabilities. Similarly, Sontan and Samuel (2024) argue that manual patch deployment introduces risks, such as errors in patch application or incompatibilities with existing systems, which can potentially cause service disruptions or introduce new vulnerabilities. The growing complexity of IT infrastructures and the overwhelming number of alerts generated by traditional tools exacerbate these challenges. Conventional methods also struggle to keep pace with the rapidly evolving threat landscape, leaving organizations vulnerable to exploitation (Goswami, 2019).

Another significant challenge is the time-intensive nature of traditional patch management. Wong (2024) explains that fixed-interval vulnerability scans leave gaps during which newly emerging threats can remain undetected for weeks or months. Additionally, the lengthy process of testing and deploying patches across diverse IT environments delays remediation, increasing the exposure of critical systems to potential threats.

Scalability issues further hinder traditional patch management practices. Sontan and Samuel (2024) emphasize that resource-intensive manual processes cannot meet the demands of large, interconnected IT infrastructures. As vulnerabilities increase and IT systems become more complex, traditional methods fail to provide adequate coverage, exposing organizations to heightened risk.

Traditional patch management methods face significant limitations, including reliance on manual processes, scalability issues, and delays in addressing vulnerabilities. These inefficiencies expose organizations to evolving cyber threats, highlighting the need for automation. Wong (2024) and Sontan and Samuel (2024) emphasize that AI-driven systems can overcome these challenges by improving efficiency, reducing human error, and ensuring timely responses to emerging risks.

**AI-driven patch management systems**

AI-driven patch management systems offer advanced solutions to address the inefficiencies of traditional patch management methods. Goswami (2019) explains that these systems prioritize patches by evaluating criticality, potential impact, and compatibility with existing infrastructure. This targeted approach minimizes operational disruptions while effectively addressing vulnerabilities. Organizations can proactively schedule patches by analyzing extensive datasets, including historical attack patterns and real-time threat intelligence, reducing their exposure to emerging threats.

Recent innovations, particularly those in generative AI, have significantly enhanced the capabilities of these systems. Wong (2024) describes how AI models leverage machine learning (ML) and deep learning (DL) techniques to optimize patch management and vulnerability remediation. AI-generated synthetic data can assist in training security models to identify emerging threats and test patch effectiveness in controlled environments. Harshith et al. (2024) further demonstrate that AI-powered automation improves efficiency by reducing the manual workload associated with patch prioritization, scheduling, and deployment tasks. By automating these processes, cybersecurity professionals can focus on proactive threat hunting and strategic incident response.

AI-driven automation also plays a key role in vulnerability remediation. Samtani et al. (2020) highlight the role of AI in cyber threat intelligence and adversarial machine learning, emphasizing its ability to analyze vast amounts of security data and improve decision-making in security operations. However, AI-based remediation requires ongoing monitoring to mitigate risks associated with false positives and adversarial threats. Wong (2024) supports this by explaining how ML models continuously refine cybersecurity defenses through adaptive learning.

Generative AI's ability to create predictive threat models based on simulated data offers additional benefits. Harshith et al. (2024) discuss how AI-driven simulations enhance security planning by predicting potential attack vectors and proactively mitigating risks. Organizations that integrate AI-driven automation into their patch management strategies can significantly reduce downtime, optimize resource allocation, and enhance security posture.

Organizations can enhance accuracy, reduce operational disruptions, and proactively address zero-day vulnerabilities by adopting generative AI and automated patch management. Harshith et al. (2024) and Wong (2024) emphasize the integration of AI-driven automation to optimize patch deployment and ensure robust cybersecurity defenses.

**Benefits of AI and ML in patch management**

Integrating AI and ML into patch management significantly improves efficiency, accuracy, and scalability. Harshith (2024) explains that AI systems apply advanced behavioral analysis and anomaly detection to

identify real-time vulnerabilities, quickly neutralizing potential risks. By automating these processes, organizations minimize downtime and maintain operational continuity.

AI's speed and accuracy in detecting and addressing vulnerabilities are key advantages. Jawaid (2023) explains that AI algorithms rapidly analyze network traffic to identify unusual behaviors or security flaws, prioritizing critical vulnerabilities for immediate remediation. This capability reduces the risk of exploitation and enables a faster response to threats than traditional methods.

AI-driven automation also enhances patch deployment processes. Sontan and Samuel (2024) note that AI systems can autonomously analyze security alerts and execute predefined patching actions, reducing the time required to address vulnerabilities. These systems consistently apply standardized protocols, minimizing the likelihood of human error and ensuring accurate remediation. Moreover, automation allows security teams to focus on more strategic tasks, improving overall efficiency.

Another significant benefit of ML models is their adaptability. Harshith (2024) notes that ML techniques enable systems to predict vulnerabilities based on historical data, facilitating preemptive patching. Similarly, Jawaid (2023) highlights that continuous learning enhances the resilience of AI systems, ensuring they remain effective against evolving threats. AI's scalability also ensures that patch management processes can accommodate increasing data volumes and IT complexities, as Harshith (2024) and Sontan and Samuel (2024) noted.

Integrating AI and ML in patch management enhances efficiency, scalability, and accuracy. With capabilities such as real-time vulnerability detection and predictive modeling, these technologies reduce downtime and improve operational resilience. Harshith (2024) and Jawaid (2023) illustrate how AI-driven automation enables organizations to address vulnerabilities preemptively, supporting a more proactive approach to cybersecurity.

**Challenges of AI and ML in patch management**

Despite AI and ML's benefits in patch management, their adoption presents unique challenges. Goswami (2019) emphasizes the importance of robust training data, noting that insufficient or low-quality datasets can result in inaccurate vulnerability assessments. Addressing this challenge requires comprehensive and diverse datasets to improve algorithm reliability.

Bias in AI systems is another concern. Harshith et al. (2024) and Muthuraj and Singla (2023) highlight that biases in training data can lead to inconsistent prioritization of vulnerabilities, potentially leaving critical security gaps unresolved. Transparent model development practices and regular evaluations are necessary to mitigate these biases.

Transparency and accountability are critical for building trust in AI-driven systems. Sontan and Samuel (2024) emphasize the importance of Explainable AI (XAI) in cybersecurity, arguing that straightforward interpretability techniques are necessary to clarify the decision-making process behind patch prioritization and deployment. They highlight approaches such as feature importance analysis, which provides insights into AI-driven processes and enables better oversight (Sontan & Samuel, 2024).

Other challenges include the accuracy of AI systems. Harshith et al. (2024) caution that AI may misinterpret benign configurations as vulnerabilities or fail to detect novel threats, resulting in false positives or negatives. Continuous refinement of AI models is essential for improving their performance (Muthuraj & Singla, 2023). Data privacy concerns also arise, as AI training often requires sensitive data, increasing the risk of breaches (Sontan & Samuel, 2024). Employing data anonymization techniques can help address these risks.

Integrating AI into patch management necessitates overcoming challenges such as ensuring compatibility with legacy systems and addressing the shortage of skilled professionals. Workforce development and educational programs are essential for ensuring the effective implementation and maintenance of AI-driven systems (Muthuraj & Singla, 2023).

Adopting AI and ML in patch management presents several challenges, including ensuring the availability of high-quality training data and mitigating biases that can impact vulnerability prioritization (Goswami, 2019; Harshith et al., 2024). Transparency through Explainable AI (XAI) and regular evaluations are crucial for building trust (Sontan & Samuel, 2024). Additional hurdles include false positives, data privacy risks, and workforce development to address legacy system compatibility and skill gaps (Muthuraj & Singla, 2023).

**Perceptions of AI adoption in cybersecurity**

Perceptions of artificial intelligence (AI) play a pivotal role in shaping its adoption and success within cybersecurity applications. Organizations widely regard the deployment of AI in cybersecurity as a critical advancement that boosts operational efficiency and alleviates repetitive tasks. AI-driven systems streamline processes, enhance productivity, and deliver scalable solutions for vulnerability management at the enterprise level (Radebe et al., 2022). Automation enables cybersecurity professionals to focus on high-priority issues rather than routine operational tasks. These systems also reduce false positives, allowing the teams to prioritize genuine threats and actionable insights, enhancing their overall effectiveness (Radebe et al., 2022).

User attitudes and behavioral intentions influence the adoption of AI tools, as these are core components of the Technology Acceptance Model (TAM) (Davis, 1989). TAM suggests that perceived usefulness—the extent to which a user believes that technology will enhance job performance—and perceived ease of use—the extent to which a user thinks the technology will be effortless—are primary determinants of user acceptance (Davis, 1989). These constructs directly influence attitudes toward technology use and behavioral intention, predicting usage (Davis, 1989).

In cybersecurity, perceived usefulness is critical in shaping attitudes toward AI adoption. AI-enabled systems streamline data collection and incident investigation, significantly reducing response times and improving operational efficiency (Radebe et al., 2022). The study by Radebe et al. (2022) highlights that AI tools enhance productivity by automating security tasks, minimizing manual workload, and improving response times, all of which contribute to their perceived usefulness. Similarly, perceived ease of use influences behavioral intention by reducing resistance to new technology. Systems that integrate seamlessly into workflows and require minimal training enhance users' confidence and willingness to adopt them (Davis, 1989).

TAM emphasizes that positive attitudes toward using technology directly influence behavioral intention. Users are more likely to exhibit a firm intention to adopt and continue using AI systems when they perceive them as valuable and easy to use (Davis, 1989). In cybersecurity, this relationship highlights the importance of designing AI tools with user-centered features that address specific challenges, such as reducing false positives and improving data analysis efficiency (Radebe et al., 2022). Providing adequate training and demonstrating the practical benefits of AI systems further strengthens the user's intention to adopt such technologies (Davis, 1989; Radebe et al., 2022).

## Methodology

### Instrument

This study employs a survey instrument based on the Technology Acceptance Model (TAM), first introduced by Davis (1989), a foundational model for understanding technology adoption. TAM identifies perceived usefulness (PU) and perceived ease of use (PEOU) as primary factors influencing behavioral intention (BI) to use technology. Attitude toward use (ATU) is a mediating factor that captures users' affective responses toward system adoption (Davis, 1989).

The study defines and measures the TAM constructs as follows:

1. PU is measured using four items that assess participants' perceptions of how AI-driven patch management systems enhance job performance, streamline tasks, and improve security. These items align with Davis's (1989) definition of PU as a key determinant of BI.
2. PEOU assesses participants' perceptions of how easily they can learn, integrate, and use AI-driven patch management systems through four evaluation items. Davis (1989) demonstrated that PEOU directly influences BI and indirectly affects PU by shaping perceptions of usability.
3. ATU assesses participants' confidence, enthusiasm, and attitude toward adopting AI-driven patch management systems through four items. In Davis's (1989) original TAM model, ATU mediates the relationship between PU, PEOU, and BI, reflecting the role of user perceptions in technology adoption.
4. BI is measured using three items that assess participants' willingness to support and adopt AI-driven patch management systems within their organizations. Davis (1989) identified BI as the strongest predictor of actual technology use.

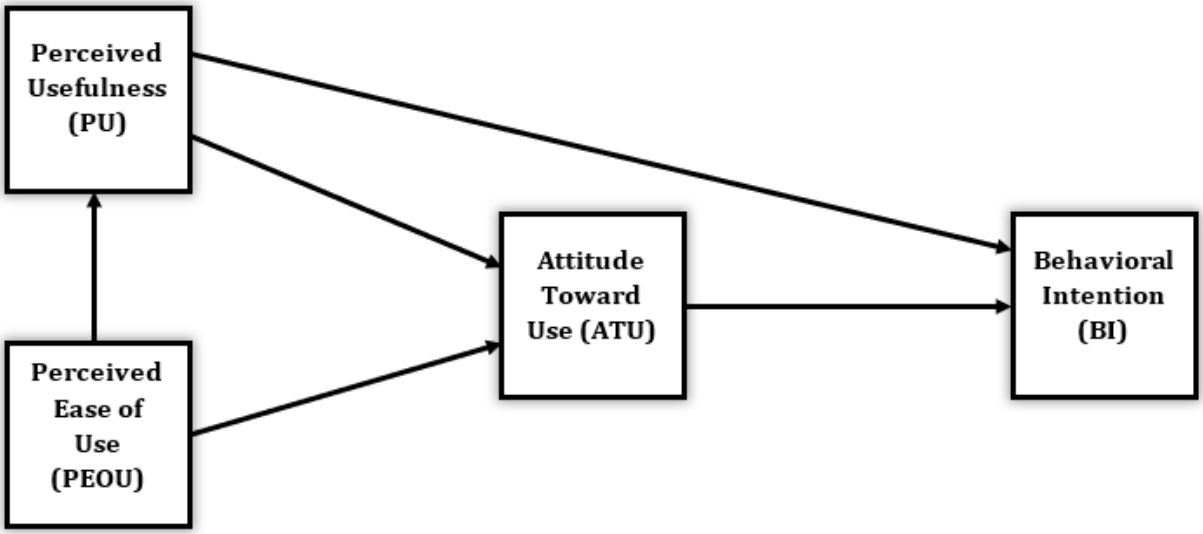
### Survey Design

The survey employs a 7-point Likert scale, where participants rate their level of agreement with each statement, ranging from 1 (Strongly Disagree) to 7 (Strongly Agree). This scaling method is commonly used in TAM-based research to capture user perceptions and adoption intentions with greater granularity (Davis, 1989).

The survey is designed for IT professionals and aligns with TAM's core constructs: PU, PEOU, ATU, and BI, ensuring relevance to AI-driven patch management systems. The Appendix contains a complete list of survey items. Figure 1 presents TAM, illustrating the relationships among these constructs and serving as the foundation for this study.

**Figure 1**

*Technology Acceptance Model (TAM) For Assessing IT Professionals' Perceptions of AI-Driven Patch Management*




*Note.* Adapted from Davis (1989). The TAM model illustrates how perceived usefulness (PU) and perceived ease of use (PEOU) influence attitude toward use (ATU), which, in turn, affects behavioral intention (BI).

**Subjects and procedure**

The researcher administered the survey electronically through SurveyMonkey, ensuring that all questions were mandatory to obtain a complete dataset. SurveyMonkey enables researchers to efficiently create and distribute customized surveys via email or websites, facilitating data collection through descriptive statistics, graphical reports, and exportable spreadsheets (Creswell & Creswell, 2018).

Of the 123 individuals who accessed the survey, 120 provided electronic consent and completed the questionnaire as the informed consent process required. The final dataset includes these 120 valid responses, excluding those who did not consent or complete the survey.

Data cleaning procedures were performed before analysis to ensure data accuracy and consistency. The researcher:

1. Removed responses from participants who did not consent to comply with ethical research guidelines.
2. Checked for incomplete responses and excluded cases with missing data affecting key variables.
3. Verified response consistency to ensure data validity.

The researcher employed a non-probability convenience sampling approach, selecting respondents based on availability rather than systematic randomization. This method aligns with the quantitative research guidelines Creswell and Creswell (2018) outlined. Additionally, purposive sampling was applied to target individuals in Information Technology roles within the United States, ensuring alignment with the study's objectives, as described by Etikan et al. (2015).

To ensure ethical compliance, the researcher obtained Institutional Review Board (IRB) approval and provided participants with details about the study's purpose, confidentiality measures, and their right to withdraw before obtaining electronic consent. Data collection was conducted securely through SurveyMonkey, and responses were automatically anonymized following best practices for online research (Roberts & Allen, 2015).

The final sample of 120 IT professionals meets the recommended sample-to-variable ratio guideline of 20:1 for factor analysis (Rahman, 2023). Since this study examined four constructs (PU, PEOU, ATU, and BI), the minimum required sample size was 80 participants. Exceeding this threshold enhances the reliability and robustness of the data analysis.

**Data analysis**

The researcher analyzed the survey data using SPSS version 29 to examine relationships between PU, PEOU, ATU, and BI in adopting AI-driven patch management systems.

Before conducting statistical analyses, the researcher cleaned the dataset by removing responses from participants who did not consent or failed to complete the survey. This process ensured that the final dataset included 120 valid responses, improving the accuracy and reliability of the results.

The researcher used descriptive statistics to summarize responses for each construct, providing measures of central tendency (mean) and variability (standard deviation). To assess the internal consistency of the measurement scales, the researcher calculated Cronbach's alpha for each construct.

The researcher conducted a multiple regression analysis to evaluate the impact of PU, PEOU, and ATU on BI. This analysis assessed the overall goodness of fit of the model and the statistical significance of individual predictors, adhering to established guidelines for SPSS data analysis. The researcher tested the assumptions of multiple regression by examining the normality of residuals using histograms, P-P plots, and scatterplots.

## Results

This section presents the results of the data analysis, following the order of statistical tests conducted. These tests include descriptive statistics, reliability analysis, multiple regression analysis, and diagnostics for regression assumptions. The multiple regression analysis examines the extent to which perceived usefulness (PU), perceived ease of use (PEOU), and attitude toward use (ATU) predict behavioral intention (BI) to adopt AI-driven patch management solutions.

**Descriptive and reliability analysis**

The survey data were analyzed using SPSS to explore relationships between PU, PEOU, ATU, and BI in adopting AI-driven patch management systems. The researcher computed descriptive statistics to summarize participant responses and provide insights into central tendencies and variability. Knapp (2017) emphasizes the importance of descriptive statistics in survey data analysis, highlighting how measures such as means, standard deviations, and ranges offer a comprehensive view of participant perceptions.

Table 1 presents the descriptive statistics, including each construct's mean, standard deviation, minimum, and maximum values. The results indicate that participants generally held positive perceptions of AI-driven patch management solutions:

- PU_Avg had a mean of 4.79 (SD = 1.40), indicating that respondents found the system beneficial for enhancing job performance and security.

- PEOU_Avg had a mean of 4.30 (SD = 1.29), showing slightly more significant variability in how easily participants believed they could integrate the system into existing workflows.
- ATU_Avg had a mean of 4.58 (SD = 1.53), indicating a generally favorable attitude toward adopting AI-driven patch management systems.
- BI_Avg had a mean of 4.49 (SD = 1.60), indicating a moderate to high likelihood of adoption if implemented in organizations.

**Table 1**

*Descriptive Statistics for Key Study Constructs*

*Descriptive Statistics*

| | N | Minimum | Maximum | Mean | Std. Deviation |
|---|---|---|---|---|---|
| SMEAN(PU_Avg) | 120 | 1.00 | 7.00 | 4.7857 | 1.40351 |
| SMEAN(PEOU_Avg) | 120 | 1.00 | 7.00 | 4.2983 | 1.29084 |
| SMEAN(ATU_Avg) | 120 | 1.00 | 7.00 | 4.5798 | 1.53493 |
| SMEAN(BI_Avg) | 120 | 1.00 | 7.00 | 4.4902 | 1.60055 |
| Valid N (listwise) | 120 | | | | |

*Note.* PU = perceived usefulness; PEOU = perceived ease of use; ATU = attitude toward use; BI = behavioral intention.

A reliability analysis using Cronbach's Alpha assessed the internal consistency of each construct, with all values exceeding the recommended threshold of 0.70. Taber (2017) explains that Cronbach's alpha values above 0.70 indicate strong reliability. Table 2 presents Cronbach's alpha values for each construct, confirming the internal consistency of the measures.

**Table 2**

*Cronbach's Alpha for Reliability Analysis*

| Construct | Cronbach's Alpha (α) | Interpretation |
|---|---|---|
| **Perceived Usefulness (PU)** | .923 | Excellent |
| **Perceived Ease of Use (PEOU)** | .870 | Good |
| **Attitude Toward Use (ATU)** | .950 | Excellent |
| **Behavioral Intention (BI)** | .933 | Excellent |

*Note.* Cronbach's Alpha values of 0.70 or higher indicate acceptable reliability, values of 0.80 or higher indicate good reliability, and values of 0.90 or higher indicate excellent reliability (Taber, 2017).

**Multiple regression analysis**

The researcher conducted a multiple regression analysis regarding the research question (RQ1), examining which of the three predictor variables—PU, PEOU, and ATU—significantly influence IT professionals' BI to adopt AI-driven patch management solutions.

The researcher mitigated multicollinearity by creating composite scores for PU_Avg, PEOU_Avg, and ATU_Avg, following Frost's (n.d.) recommendation to reduce the risk of inflated $R^2$ values when including multiple predictors.

***Model fit***

The model summary in Table 3 indicates a strong positive relationship between the predictor variables and BI_Avg, with:

- R = 0.910, indicating a high correlation between predictors and Behavioral Intention.
- $R^2$ = 0.828, showing that PU, PEOU, and ATU explain 82.8% of the variance in BI_Avg.
- Adjusted $R^2$ = 0.824, suggesting the model generalizes well without overfitting.

Frost (n.d.) cautions that unnecessary variables may artificially inflate $R^2$, but the slight difference between $R^2$ and Adjusted $R^2$ indicates that the model maintains strong predictive integrity. The standard error of the estimate (SEE) is 0.675, indicating the degree to which predicted values align with the observed data (Frost, n.d.).

**Table 3**

*Model Summary for Multiple Regression Predicting Behavioral Intention (BI)*

*Model Summary*[b]

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .910[a] | .828 | .824 | .67521 |

[a]. Predictors: (Constant), ATU_Avg, PEOU_Avg, PU_Avg

[b]. Dependent Variable: BI_Avg

*Note.* PU = perceived usefulness; PEOU = perceived ease of use; ATU = attitude toward use; BI = behavioral intention.

***Model significance***

The ANOVA results (Table 4) confirm that the regression model is statistically significant:

- F (3, 115) = 184.553, $p < .001$, indicating that the predictor variables, as a group, significantly explain variance in BI_Avg.
- ANOVA uses the F-statistic and p-value to determine whether the model fits better than one without predictors. Knapp (2017) notes that p-values below .05 indicate statistical significance, supporting the model's validity.

**Table 4**

*ANOVA for Multiple Regression Model*

*ANOVA*[a]

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 252.420 | 3 | 84.140 | 184.553 | <.001[b] |
| | Residual | 52.430 | 115 | .456 | | |
| | Total | 304.850 | 118 | | | |

a. Dependent Variable: BI_Avg

b. Predictors: (Constant), ATU_Avg, PEOU_Avg, PU_Avg

*Note.* PU = perceived usefulness; PEOU = perceived ease of use; ATU = attitude toward use; BI = behavioral intention. $p < .001$.

***Predictor significance and effect sizes***

As shown in Table 5, the regression coefficients provide insights into the individual impact of each predictor on BI_Avg:

**Table 5**

*Coefficients of Predictors on Behavioral Intention*

*Coefficients*[a]

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. | Collinearity Statistics | |
|---|---|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | | Tolerance | VIF |
| 1 | (Constant) | -.290 | .240 | | -1.212 | .228 | | |
| | PU_Avg | .263 | .098 | .231 | 2.679 | .008 | .201 | 4.964 |
| | PEOU_Avg | .125 | .067 | .101 | 1.873 | .064 | .517 | 1.935 |
| | ATU_Avg | .652 | .093 | .625 | 7.031 | <.001 | .189 | 5.280 |

a. Dependent Variable: BI_Avg

*Note.* PU = perceived usefulness; PEOU = perceived ease of use; ATU = attitude toward use; BI = behavioral intention. $p < .001$.

Among the predictors, ATU had the most substantial effect on BI (B = 0.652, p < .001), indicating that a positive attitude toward AI-driven patch management significantly increases the intention to adopt it. PU also showed a significant positive effect (B = 0.263, p = .008), suggesting that IT professionals are more likely to adopt the solution if they perceive it as useful. In contrast, PEOU had a weaker, non-significant

effect (B = 0.125, p = .064), indicating that ease of use is not a primary factor in adoption decisions. The p-values indicate the statistical significance of these results, with values below .05 representing significant relationships (Knapp, 2017).

### *Multicollinearity assessment*

The researcher examined the Variance Inflation Factor (VIF) values to assess potential multicollinearity. Knapp (2017) states that VIF values above 5 indicate possible multicollinearity, while values exceeding 10 suggest severe collinearity issues. As shown in Table 5:

- PU_Avg: VIF = 4.964
- ATU_Avg: VIF = 5.280
- PEOU_Avg: VIF = 1.935

These values indicate moderate multicollinearity for PU and ATU, whereas PEOU does not raise concerns. However, no corrective action was necessary, as the VIF values remained below the severe threshold of 10.

### *Regression assumption diagnostics*

To validate the assumptions of multiple regression, the researcher examined a histogram, a P-P plot, and a scatterplot following recommendations by Laerd Statistics (n.d.).

- The histogram of standardized residuals suggests an approximately normal distribution, forming a roughly symmetric, bell-shaped curve.
- The P-P plot of standardized residuals indicates that the data follows the expected normal distribution, with points aligning along the diagonal.
- The scatterplot of standardized predicted values versus standardized residuals shows no discernible pattern or funneling, confirming homoscedasticity and the assumption of constant variance.

These results support the regression model's validity, ensuring its findings' reliability.

## Discussion

The findings of this study demonstrate that ATU is the most significant predictor of IT professionals' behavioral intentions (BI) to adopt AI-driven patch management systems, with a beta coefficient of 0.652 and a p-value of less than 0.001 (see Table 5). This result aligns closely with Davis's (1989) Technology Acceptance Model (TAM), which highlights attitudes as critical predictors of technology adoption. High mean scores on survey items measuring ATU (Appendix, Items 10–13) confirmed strong positive sentiments among IT professionals toward adopting AI-driven systems. Specifically, participants expressed enthusiasm for the potential benefits of these systems, such as improved cybersecurity and more efficient vulnerability management.

PU also significantly influenced BI, although less prominently than ATU (B = 0.263, p = .008; see Table 5). Survey responses (Appendix, Items 1–4) revealed that IT professionals recognize AI's practical advantages, including the automation of routine tasks and more effective vulnerability management, which aligns with existing cybersecurity literature (Harshith et al., 2024; Jawaid, 2023). Despite acknowledging these benefits, the lower predictive power of PU relative to ATU indicates that positive attitudes toward AI may play a more decisive role in adoption decisions.

Interestingly, PEOU did not significantly influence BI (B = 0.125, p = .064; see Table 5). Survey responses (Appendix, Items 5–8) indicated that although IT professionals believed they could quickly learn and

operate AI-driven patch management systems, ease of use alone was not a strong driver of their adoption intentions. This aligns partially with Radebe et al. (2022), who suggest experienced cybersecurity professionals value system functionality and automation capabilities above ease of use. However, this contrasts with Geddam et al. (2024), whose findings indicate that both PU and PEOU significantly influence BI directly and indirectly via ATU. Differences in context, precisely the expertise level and familiarity with sophisticated technologies among IT professionals, may explain this divergence.

These insights collectively emphasize the importance of strategically addressing user attitudes through training, clear communication of operational benefits, and prioritizing robust, reliable performance in AI tool design. Organizations can significantly boost AI adoption rates and strengthen cybersecurity resilience by adopting these strategic approaches.

## Implications of findings

### *The importance of attitude toward AI adoption*

This study highlights the critical role of ATU in the adoption of AI-driven patch management systems. Davis (1989) identifies attitudes toward technology as key drivers of BI, a position reinforced by this study's findings ($B = 0.652$, $p < .001$; see Table 5). Similarly, Geddam et al. (2024) indicate that PU and PEOU directly and indirectly influence BI through ATU. The strong predictive power of ATU suggests that organizations should invest in targeted training programs that emphasize the practical benefits of AI, such as reducing manual workloads and improving accuracy. Addressing user concerns, providing hands-on experience, and ensuring transparent communication can strengthen positive attitudes toward AI adoption.

### *Perceived usefulness as a secondary adoption factor*

PU also significantly influenced adoption ($B = 0.263$, $p = .008$; see Table 5), supporting Davis's (1989) assertion that usefulness is a key determinant of technology adoption. Geddam et al. (2024) note that when users recognize how AI enhances job performance, their willingness to adopt the technology increases. Therefore, organizations should focus on demonstrating the impact of AI on streamlining cybersecurity operations and improving efficiency. By clearly communicating these benefits, organizations can build user confidence and encourage broader adoption.

### *Minimal impact of perceived ease of use*

In this study, PEOU did not significantly influence BI ($B = 0.125$, $p = .064$; see Table 5). Although Geddam et al. (2024) found significant direct and indirect effects of both PU and PEOU on BI through ATU, contextual differences might explain the differing results of the current study. Specifically, the sample of experienced IT professionals in the current study may prioritize system functionality, performance, and security benefits over ease of use. Therefore, organizations targeting skilled cybersecurity professionals should emphasize system robustness and performance over simplistic interfaces when implementing AI-driven solutions.

### *Evaluating TAM's role in AI-driven patch management*

The high $R^2$ value of 0.828 (see Table 3) confirms TAM's effectiveness in explaining AI adoption within cybersecurity contexts. Knapp (2017) emphasizes that high $R^2$ values indicate a strong model fit, thereby reinforcing the validity of TAM in understanding AI-driven adoption behaviors. This study extends previous TAM research by demonstrating that ATU is the strongest predictor of adoption, while PEOU is

not a significant factor. These findings suggest that IT professionals prioritize system functionality and security over ease of use when assessing AI-driven solutions.

Additionally, a multicollinearity assessment (see Table 5) showed that PU_Avg (VIF = 4.964) and ATU_Avg (VIF = 5.280) exhibited moderate multicollinearity but remained below the severe threshold (VIF > 10) (Knapp, 2017). This indicates that the predictors in this model are sufficiently independent, justifying their inclusion in the regression analysis.

***Practical implications***

Based on these findings, organizations should:

- Develop strategies to foster positive attitudes toward AI adoption by highlighting AI's practical benefits, providing comprehensive training, and transparently addressing user concerns.
- Communicate AI's operational benefits, emphasizing its capacity to streamline cybersecurity operations and enhance job performance.
- Integrating robust and high-performing AI tools within cybersecurity frameworks is a priority for IT professionals, who prioritize functionality and performance over simplicity.

By applying these strategies, organizations can boost AI adoption and fortify their cybersecurity posture.

## Limitations

This study presents several limitations. First, using a non-probability convenience sampling method limits external validity due to the non-random selection of participants. As Andrade (2021) explains, convenience sampling draws participants from accessible sources; however, such samples may not accurately represent the broader population, thereby restricting generalizability.

Additionally, this study relied on an opt-in panel for data collection, which introduces the potential for measurement errors due to participant misreporting (Bailey & Brick, 2024). Opt-in panel respondents may provide inaccurate responses intentionally to qualify for additional surveys or unintentionally due to survey fatigue. These factors can affect data accuracy and introduce response bias (Bailey & Brick, 2024).

This study's sample was collected using SurveyMonkey's Audience feature, which operates as an opt-in panel by recruiting self-selected participants. Although this panel provided access to IT professionals in the United States, its self-selected nature introduces selection bias, as participants voluntarily join rather than being randomly chosen (Bailey & Brick, 2024). While weighting adjustments can sometimes mitigate these biases, their effectiveness depends on strong assumptions about the underlying population (Bailey & Brick, 2024).

Finally, while the final sample size of 120 participants exceeds the minimum threshold for factor analysis, its relatively homogeneous composition and geographic limitation may restrict the generalizability of the findings. Andrade (2021) suggests that future research should focus on increasing sample size and enhancing diversity to improve overall validity and broaden applicability.

## Recommendations for future research

Future research should investigate the long-term effects of AI-driven patch management on an organization's cybersecurity posture. Specifically, studies should examine how AI enhances vulnerability assessment by improving the rapid identification, prioritization, and remediation of vulnerabilities across diverse IT environments (Goswami, 2019). Additionally, research should investigate the adoption of AI within managerial decision-making processes, focusing on the factors that influence its acceptance and integration. Marocco et al. (2024) highlight that organizational readiness, ethical considerations, and managerial perceptions play a critical role in AI adoption, emphasizing the need for trust, transparency, and alignment with existing decision-making structures. Understanding these factors would provide a more comprehensive view of AI adoption challenges and opportunities.

Future studies should also investigate effective user training methods to facilitate the implementation of AI. Palade and Carutasu (2021) propose a six-factor AI readiness model encompassing resource, cultural, strategic, IT, partnership, and cognitive readiness. Integrating these readiness factors into training programs could enhance decision-making, promote AI ethics, strengthen management support, and increase stakeholder engagement. Developing tailored training programs that address these factors may improve user attitudes and encourage the widespread adoption of AI-driven patch management systems.

Moreover, future research should develop robust metrics and frameworks to assess the effectiveness of AI-driven patch management. Dissanayake et al. (2022) emphasize the need for evaluation frameworks that measure technical performance and organizational impacts, including operational efficiency and enhanced security posture. Similarly, Wen et al. (2024) emphasize the importance of integrating AI into security assurance frameworks to ensure compliance with evolving regulatory standards, thereby enhancing the transparency and interpretability of AI-driven security models. Future studies should investigate methods for adapting these security assurance frameworks to diverse IT environments, particularly in complex infrastructures that require real-time threat mitigation.

Finally, research should investigate how scalable and adaptable AI frameworks, such as those proposed by Kansal and Prasad (2024), can enhance cybersecurity resilience across diverse organizational infrastructures. As AI-driven security solutions evolve, developing scalable implementation strategies will ensure sustainable, long-term advancements in cybersecurity.

# Conclusion

This study investigated IT professionals' perceptions of AI-driven patch management systems in enterprise IT environments, utilizing the Technology Acceptance Model (TAM). The findings indicate that attitude toward use (ATU) is the strongest predictor of adoption ($B = 0.652$, $p < .001$), highlighting the critical role of user perceptions in AI adoption. Perceived usefulness (PU) also significantly influences behavioral intention (BI) ($B = 0.263$, $p = .008$), reinforcing the importance of effectively communicating AI's operational benefits. However, perceived ease of use (PEOU) was not a significant predictor ($B = 0.125$, $p = .064$), suggesting that IT professionals prioritize functionality over usability when evaluating AI-driven security solutions.

These findings underscore the importance of cultivating positive user attitudes when implementing AI-driven patch management through strategic communication, targeted training, and transparent AI decision-making processes. Simply improving ease of use may not drive adoption; organizations must demonstrate AI's effectiveness in reducing workloads, enhancing security, and optimizing operational efficiency to build trust and encourage widespread adoption.

This study contributes to the growing body of research on AI adoption in cybersecurity by validating the applicability of TAM in enterprise IT settings. The model's high explanatory power ($R^2 = 0.828$) underscores its relevance in understanding BI within cybersecurity, particularly regarding AI-driven automation tools.

Future research should investigate the long-term effects of AI-driven patch management, including its sustained efficacy in mitigating security risks and its impact on overall cybersecurity resilience. Additionally, studies should examine organizational readiness and managerial perceptions to understand better the barriers and facilitators of AI adoption across diverse IT environments.

Ultimately, the successful adoption of AI-driven patch management solutions requires a user-centric approach that fosters trust and engagement and communicates the tangible benefits of AI. By addressing these factors, organizations can maximize adoption rates, strengthen cybersecurity resilience, and ensure a proactive defense against evolving cyber threats.

## References


Andrade, C. (2021). The inconvenient truth about convenience and purposive samples. *Indian Journal of Psychological Medicine*, *43*(1), 86–88. https://doi.org/10.1177/0253717620977000

Bailey, M., & Brick, J. M. (2024). Probability and nonprobability samples in surveys: opportunities and challenges (OPRE Report 2024-182). *U.S. Department of Health and Human Services.* https://acf.gov/opre/report/probability-and-nonprobability-samples-surveys-opportunities-and-challenges

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Ali Babar, M. (2022). *Software security patch management—A systematic literature review of challenges, approaches, tools, and practices. Information and Software Technology*, 144, 106771. https://doi.org/10.1016/j.infsof.2021.106771

Etikan, I., Musa, S. A., & Alkassim, R. S. (2015). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Frost, J. (n.d.). How to interpret adjusted R-squared and predicted R-squared in regression analysis. *Statistics by Jim*. https://statisticsbyjim.com/regression/interpret-adjusted-r-squared-predicted-r-squared-regression/

Frost, J. (n.d.). How to interpret R-squared in regression analysis. *Statistics by Jim.* https://statisticsbyjim.com/regression/interpret-r-squared-regression/

Geddam, S. M., Nethravathi, N., & Hussian, A. A. (2024). Understanding AI adoption: The mediating role of attitude in user acceptance. *Journal of Informatics Education and Research, 4*(2), 1664–1672. https://doi.org/10.52783/jier.v4i2.975

Goswami, M. J. (2019). Utilizing AI for automated vulnerability assessment and patch management. *EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal, 8*(2), 54–59. https://eduzonejournal.com/index.php/eiprmj/article/view/571/502

Harshith, V., Bapuji, V., Siri, C., & Bathini, N. (2024). Artificial intelligence paradigms in cybersecurity. *Journal of Systems Engineering and Electronics, 34*(5), 508–513. https://jseepublisher.com/wp-content/uploads/49-JSEE2274.pdf

Jawaid, S. A. (2023). Artificial intelligence with respect to cybersecurity. *Journal of Advances in Artificial Intelligence, 1*(2), 96–102. https://doi.org/10.18178/JAAI.2023.1.2.96-102

Kansal, S., & Prasad, M. S. R. (2024). AI-driven vulnerability detection and resolution frameworks for enhanced security posture. *Integrated Journal for Research in Arts and Humanities, 4*(6), 444–458. https://www.ijrah.com/index.php/ijrah/article/view/666

Knapp, H. (2017). *Intermediate statistics using SPSS*. SAGE Publications.

Laerd Statistics. (n.d.). *Multiple regression analysis using SPSS Statistics.* https://statistics.laerd.com/spss-tutorials/multiple-regression-using-spss-statistics.php

Marocco, S., Barbieri, B., & Talamo, A. (2024). Exploring facilitators and barriers to managers' adoption of AI-based systems in decision making: A systematic review. *AI*, *5*(4), 2538–2567. https://doi.org/10.3390/ai5040123

Muthuraj, & Singla, S. (2023). Artificial intelligence and machine learning. *Medico-Legal Update, 23*(Special Issue), 1–5. https://doi.org/10.37506/mlu.v23i5.3458

Palade, M., & Carutasu, G. (2021). Organizational readiness for artificial intelligence adoption. *Scientific Bulletin of the Politehnica University of Timişoara, Transactions on Engineering and Management*, *7*(1&2), 30–35. https://doi.org/10.59168/FDMS6321

Radebe, M., Tsibolane, P., & Hart, M. (2022). Perceptions of AI tools for cybersecurity in large enterprises. *Proceedings of the 8th International Conference on Decision Support System Technology (ICDSST 2022)*. https://www.researchgate.net/publication/364899781

Rahman, M. (2023). Sample size determination for survey research and non-probability sampling techniques: A review and set of recommendations. *Journal of Entrepreneurship, Business and Economics, 11*(1), 42–62. https://scientificia.com/index.php/JEBE/article/view/201

Roberts, L. D., & Allen, P. J. (2015). Exploring ethical issues associated with using online surveys in educational research. *Educational Research and Evaluation*, *21*(2), 95–108. https://doi.org/10.1080/13803611.2015.1024421

Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap. *ACM Transactions on Management Information Systems, 11*(4), Article 17, 1-19. https://doi.org/10.1145/3430360

Sontan, A. D., & Samuel, S. V. (2024). The intersection of artificial intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews, 21*(2), 1720–1736. https://doi.org/10.30574/wjarr.2024.21.2.0607

Taber, K. S. (2017). The use of Cronbach's Alpha when developing and reporting research instruments in science education. *Research in Science Education, 48*(6), 1273–1296. https://doi.org/10.1007/s11165-016-9602-2

Wen, S.-F., Shukla, A., & Katt, B. (2024). Artificial intelligence for system security assurance: A systematic literature review. *International Journal of Information Security*, *24*(43), 1–42. https://doi.org/10.1007/s10207-024-00959-0

Wong, E. (2024). Optimizing vulnerability management through artificial intelligence. *MZ Computing Journal, 5*(2), 1–7. https://mzjournal.com/index.php/MZCJ/article/view/188

# Appendix

## Survey Instrument

The following survey items assessed IT professionals' perceptions of AI-driven patch management systems. These items are based on the Technology Acceptance Model (TAM) and adapted from Davis (1989).

**Perceived Usefulness (PU)**

1. Using an AI-driven patch management system would enhance my job performance.
2. AI-driven patch management systems would improve the overall security of the IT environment.
3. AI-driven patch management systems would simplify the process of identifying and prioritizing vulnerabilities.
4. AI-driven patch management systems would allow me to spend more time on strategic tasks by reducing time spent on manual patching.

**Perceived Ease of Use (PEOU)**

5. I believe learning to use an AI-driven patch management system would be straightforward.
6. Integrating an AI-driven patch management system into existing workflows would be easy.
7. I expect that using an AI-driven patch management system would not require significant effort.
8. I anticipate that AI-driven patch management systems would be intuitive for IT professionals to use.

**Attitude Toward Use (ATU)**

9. I feel positively about our organization's potential use of AI-driven patch management.
10. I am confident that AI-driven patch management systems could significantly benefit our cybersecurity efforts.
11. I am enthusiastic about adopting AI-driven technology for managing security patches.
12. I believe that AI-driven patch management systems represent an innovative solution to cybersecurity challenges.

**Behavioral Intention (BI)**

13. I intend to use an AI-driven patch management system if it becomes available in my organization.
14. I would actively support the adoption of AI-driven patch management systems within my organization.
15. I would be open to replacing traditional patch management methods with AI-driven systems in the near future.