Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Understanding Adoption of AI-Based Cybersecurity Systems: The Roles of Cybersecurity Awareness, Trust, and Digital Literacy

Abdulkadir Jeilani Mohamud

a.jeilani@mu.edu.so

Mogadishu University

Abdifatah Nour Rage

Salaam University

Mohamed Adam Isak

Somali National University

Abdisatar Ibrahim Arabow

Mogadishu University

Abdiwahab Osman Siad

Hormuud University

Research Article

Keywords: Artificial Intelligence, Cybersecurity Awareness, Digital Literacy, Trust in AI, Responsible AI, Behavioral Intention, AI-Based Cybersecurity Systems, Cybersecurity Adoption

Posted Date: July 8th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10022929/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Abstract

Artificial Intelligence (AI) has increasingly become a critical component of modern cybersecurity strategies due to its ability to detect, predict, and respond to cyber threats in real time. Despite the growing deployment of AI-based cybersecurity systems, limited understanding exists regarding the factors that drive individuals' intention to adopt such technologies. Therefore, this study develops an integrated research model grounded in technology adoption, cybersecurity awareness, and trust literature to examine the influence of AI-driven cybersecurity awareness on behavioral intention to use AI-based cybersecurity systems. Specifically, the study investigates the mediating roles of trust in AI-based cybersecurity systems and digital literacy while accounting for the effects of responsible AI perception, perceived risk, and prior experience with cybersecurity breaches. Data were collected through a cross-sectional survey and analyzed using Structural Equation Modeling (SEM). The findings reveal that AI-driven cybersecurity awareness significantly enhances behavioral intention to use AI-based cybersecurity systems, trust in AI-based cybersecurity systems, and digital literacy. Furthermore, responsible AI perception positively influences trust, while digital literacy emerges as the strongest predictor of behavioral intention. In contrast, perceived risk negatively affects adoption intentions, whereas prior experience with cybersecurity breaches positively influences users' willingness to adopt AI-based cybersecurity technologies. Interestingly, trust in AI-based cybersecurity systems does not significantly influence behavioral intention and therefore does not mediate the relationship between AI-driven cybersecurity awareness and behavioral intention. However, digital literacy was found to partially mediate this relationship. Overall, the findings underscore the importance of cybersecurity awareness programs and digital literacy development in promoting the adoption of AI-enabled cybersecurity solutions. The study provides valuable theoretical and practical implications for policymakers, cybersecurity practitioners, and organizations seeking to strengthen cyber resilience and encourage the effective utilization of AI-driven cybersecurity technologies.

Introduction

The rapid advancement of artificial intelligence (AI) technologies has significantly transformed the cybersecurity landscape across governments, organizations, and digital platforms worldwide. The increasing sophistication of cyberattacks, ransomware, phishing, data breaches, and AI-enabled cyber threats has compelled organizations to adopt intelligent cybersecurity solutions to strengthen digital protection mechanisms and enhance cybersecurity resilience(Erukude et al., 2025; Yu et al., 2026). AI-based cybersecurity systems have emerged as innovative technological solutions capable of automating threat detection, predicting cyberattacks, identifying vulnerabilities, and improving real-time cybersecurity responses through advanced machine learning and intelligent analytics (Falowo & Bou Abdo, 2026). Consequently, organizations increasingly rely on AI-enabled cybersecurity technologies to improve operational efficiency, strengthen digital security infrastructures, and mitigate cybersecurity risks in highly dynamic digital environments.

Despite the growing adoption of AI-based cybersecurity technologies, several concerns remain regarding users' willingness and readiness to adopt such systems. Existing studies suggest that users' perceptions of trust, risk, digital competency, and awareness significantly influence the adoption of AI-enabled technologies (Hanson & Ott, 2026; Lan et al., 2026). The successful implementation of AI-based cybersecurity systems not only depends on technological capabilities but also on users' understanding, confidence, and acceptance of intelligent cybersecurity technologies. Consequently, understanding the behavioral factors influencing the adoption of AI-driven cybersecurity systems has become an increasingly important research issue in information systems, cybersecurity, and AI governance literature.

Recent developments in cybersecurity research emphasize the strategic importance of AI-driven cybersecurity awareness in enhancing users' preparedness against cyber threats and improving cybersecurity adoption behavior(Bera et al., 2026). AI-driven cybersecurity awareness refers to users' understanding and knowledge regarding AI-enabled cybersecurity threats, intelligent protection systems, cybersecurity risks, and AI-based defensive mechanisms. Individuals with higher levels of cybersecurity awareness are generally more capable of recognizing cybersecurity vulnerabilities, understanding AI functionalities, and adopting appropriate cybersecurity technologies to protect digital assets and information systems. Previous studies further suggest that cybersecurity awareness positively contributes to users' trust, digital competence, and technology adoption intentions (Yu et al., 2026).

In addition, digital literacy has become a critical competency in modern digital environments characterized by increasing dependence on AI-driven technologies. Digital literacy refers to users' ability to effectively access, understand, evaluate, and utilize digital technologies and information systems(Mohammadyari & Singh, 2015). As AI technologies become increasingly integrated into cybersecurity infrastructures, users require adequate digital skills and technological competencies to effectively interact with AI-enabled cybersecurity systems. Existing literature demonstrates that digitally competent individuals are more likely to adopt innovative technologies due to their confidence, technical capability, and ability to understand complex technological systems(Bahçekapili & Boztaş, 2025). Consequently, digital literacy may serve as an important mechanism through which cybersecurity awareness influences users' behavioral intention toward AI-based cybersecurity systems.

Trust also remains one of the most important determinants influencing the adoption of AI-enabled technologies. Trust in AI-based cybersecurity systems refers to users' confidence in the reliability, effectiveness, transparency, and security capabilities of intelligent cybersecurity technologies (Glikson & Woolley, 2020) AI-enabled cybersecurity systems often operate autonomously and manage sensitive organizational and personal information, making trust a critical factor influencing technology acceptance. Existing studies indicate that users are more likely to adopt AI technologies when they perceive such systems as ethical, transparent, explainable, and accountable (Rai, 2020). Therefore, responsible AI perception may significantly contribute to strengthening users' trust in AI-based cybersecurity systems.

At the same time, the increasing use of AI technologies has generated growing concerns regarding cybersecurity risks, privacy protection, algorithmic bias, transparency, and AI governance. Perceived risk has consistently been identified as a major barrier to technology adoption behavior (Lan et al., 2026). Users who perceive AI-enabled cybersecurity systems as risky, uncertain, or unreliable may hesitate to adopt such technologies despite their potential benefits. Furthermore, individuals who previously experienced cybersecurity incidents or data breaches may demonstrate stronger motivation to adopt AI-based cybersecurity technologies to protect themselves against future cyber threats.

Although prior studies have examined AI adoption, cybersecurity awareness, trust, and digital literacy independently, limited research has integrated these constructs into a comprehensive framework explaining behavioral intention toward AI-based cybersecurity systems. Existing studies on AI adoption largely focus on general AI acceptance, fintech, education, healthcare, or organizational AI implementation, while limited attention has been given to AI-enabled cybersecurity adoption behavior (Falowo & Bou Abdo, 2026). Moreover, the mediating roles of trust in AI-based cybersecurity systems and digital literacy in the relationship between AI-driven cybersecurity awareness and behavioral intention remain significantly underexplored in the cybersecurity literature.

Despite the increasing deployment of AI-enabled cybersecurity technologies, two important knowledge gaps remain. First, there is limited empirical understanding regarding the relative influence of awareness-related, trust-related, competency-related, and risk-related factors on users' behavioral intention to adopt AI-based cybersecurity systems.

Second, although cybersecurity awareness has been recognized as a critical antecedent of cybersecurity behavior, little is known about the underlying mechanisms through which awareness translates into actual adoption intentions, particularly through users' trust in AI systems and digital literacy competencies. Addressing these gaps is essential for both theory development and the effective implementation of AI-enabled cybersecurity solutions.

To address these gaps, the present study develops and empirically tests an integrated Trust–Awareness–Competency Framework for explaining behavioral intention to use AI-based cybersecurity systems. Specifically, the study examines the relationships among AI-driven cybersecurity awareness, responsible AI perception, trust in AI-based cybersecurity systems, digital literacy, perceived risk, prior cybersecurity breach experience, and behavioral intention to use AI-enabled cybersecurity technologies. In addition, the study investigates the mediating roles of trust and digital literacy in the relationship between AI-driven cybersecurity awareness and behavioral intention.

Accordingly, this study seeks to answer the following research questions:

RQ1: What are the key factors influencing users' behavioral intention to use AI-based cybersecurity systems?

RQ2: How do trust in AI-based cybersecurity systems and digital literacy mediate the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems?

This research makes several important contributions to the literature. First, the study extends existing AI adoption and cybersecurity behavior literature by integrating awareness, trust, risk, competency, and experience-based perspectives into a unified conceptual framework. Second, the study contributes to the emerging responsible AI and cybersecurity literature by examining the role of responsible AI perception in shaping trust toward AI-based cybersecurity systems. Third, the study empirically validates the mediating role of digital literacy and trust as mechanisms through which cybersecurity awareness influences AI adoption behavior. Fourth, the study provides practical insights for organizations, policymakers, educational institutions, and cybersecurity practitioners regarding the importance of cybersecurity awareness initiatives, digital literacy development, responsible AI governance, and trust-building strategies in facilitating the successful adoption of AI-based cybersecurity systems.

Ultimately, the findings contribute to a deeper understanding of how awareness, trust, digital competency, and risk perceptions interact to influence AI-based cybersecurity adoption behavior, thereby providing a comprehensive framework for advancing both cybersecurity resilience and responsible AI implementation in contemporary digital environments.

Literature Review and Theoretical Framework

2.1 Overview of Prior Research

The increasing sophistication of cyber threats has compelled organizations and individuals to adopt advanced cybersecurity technologies capable of protecting digital infrastructures, sensitive information, and online activities. In recent years, artificial intelligence (AI) has emerged as one of the most transformative technologies in cybersecurity due to its capability to automate threat detection, predict malicious activities, and respond to cyber incidents in real time(Dwivedi, 2025; Kaur et al., 2022). AI-based cybersecurity systems utilize machine learning, predictive analytics, intelligent automation, and behavioral monitoring to improve cybersecurity resilience and operational efficiency.

Despite the technological advancement of AI-driven cybersecurity systems, their successful implementation depends heavily on users' willingness and behavioral intention to adopt such technologies(Chatterjee et al., 2023). Existing studies have primarily focused on the technical efficiency of AI-enabled cybersecurity systems, while limited attention

has been devoted to understanding the behavioral, cognitive, and psychological factors that influence users' acceptance of these technologies (H. A. Aldawood & Skinner, 2018). Consequently, understanding the determinants of behavioral intention toward AI-based cybersecurity systems has become an important research priority.

AI-driven cybersecurity awareness has recently gained substantial scholarly attention as an important determinant of cybersecurity behavior and technology adoption. Cybersecurity awareness refers to users' understanding, knowledge, and perception regarding cybersecurity threats, vulnerabilities, and protective mechanisms (Li et al., 2019). In the context of AI-enabled cybersecurity, awareness enhances users' understanding of how AI technologies improve cybersecurity protection, reduce cyber risks, and automate threat mitigation processes. Individuals with higher AI-driven cybersecurity awareness are therefore more likely to recognize the usefulness and value of AI-based cybersecurity systems.

Trust has also emerged as a central factor influencing users' adoption of AI technologies. AI systems often operate autonomously and rely on complex algorithms that may create uncertainty regarding transparency, reliability, fairness, and accountability (Glikson & Woolley, 2020). Trust in AI-based cybersecurity systems reflects users' confidence that these technologies can effectively protect digital assets and perform cybersecurity functions accurately and ethically. Prior studies indicate that users are more willing to adopt AI systems when they perceive them as trustworthy, reliable, and secure(Kaur et al., 2022).

In addition, digital literacy has become increasingly important in today's digital society. Digital literacy refers to individuals' abilities to effectively access, understand, evaluate, and use digital technologies and online information(Ng, 2012). Digitally literate individuals possess stronger competencies in managing digital tools, understanding cybersecurity risks, and interacting with AI technologies. Existing literature suggests that digital literacy significantly influences technology acceptance, cybersecurity behavior, and users' ability to adapt to emerging technologies(Al-Zahrani & Al-Salloum, 2025).

Perceived risk is another critical factor influencing users' behavioral intention toward AI technologies. Users may perceive various risks associated with AI systems, including privacy violations, data misuse, cybersecurity vulnerabilities, operational failures, and algorithmic bias (Bansal & Axelton, 2024). Such perceived uncertainties may negatively affect users' willingness to adopt AI-based cybersecurity systems. Conversely, prior experiences with cybersecurity breaches can increase users' awareness of cyber threats and motivate them to adopt more sophisticated cybersecurity protection mechanisms(Slavova & Zhauniarovich, 2025).

Although previous studies have separately examined cybersecurity awareness, trust, digital literacy, perceived risk, and AI adoption, limited research has integrated these constructs into a comprehensive framework explaining behavioral intention toward AI-based cybersecurity systems. Furthermore, insufficient empirical evidence exists regarding the mediating mechanisms through which AI-driven cybersecurity awareness influences behavioral intention. Therefore, the present study addresses these gaps by examining the mediating roles of trust in AI-based cybersecurity systems and digital literacy.

The study contributes to the literature in several ways. First, it extends existing AI and cybersecurity adoption research by integrating technological, behavioral, cognitive, and security-related factors into a unified theoretical framework. Second, the study advances understanding of the indirect mechanisms through which AI-driven cybersecurity awareness influences behavioral intention. Third, the study contributes to the emerging responsible AI literature by examining the role of responsible AI perception in building trust toward AI-based cybersecurity systems. Finally, the study provides practical implications for organizations, policymakers, and cybersecurity professionals seeking to improve users' adoption of AI-enabled cybersecurity technologies.

2.2 Theoretical Foundation

This study integrates the Technology Acceptance Model (TAM), Protection Motivation Theory (PMT), Social Cognitive Theory (SCT), Theory of Planned Behavior (TPB), and Trust Theory to explain users' behavioral intention to adopt AI-based cybersecurity systems. The integration of these theories provides a comprehensive explanation of how technological awareness, trust, digital competencies, perceived risks, and prior cybersecurity experiences jointly shape individuals' intentions to use AI-enabled cybersecurity technologies. Theories were selected because no single theoretical perspective sufficiently explains the multidimensional nature of AI-driven cybersecurity adoption behavior. The combination of these theories allows the study to explain cognitive, behavioral, technological, and psychological determinants influencing the adoption of AI-based cybersecurity systems.

2.2.1 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis (1989), is one of the most widely used theories for explaining technology adoption behavior. TAM proposes that users' intention to adopt technology is primarily determined by perceived usefulness and perceived ease of use. The model argues that individuals are more likely to adopt technologies they perceive as beneficial, efficient, and easy to operate. TAM has been extensively applied in studies related to artificial intelligence adoption, cybersecurity technologies, digital transformation, and intelligent systems(Chatterjee et al., 2023; Dwivedi, 2025).

The present study adopts TAM because AI-based cybersecurity systems represent emerging digital technologies that require users' acceptance and behavioral intention for successful implementation. AI-driven cybersecurity awareness, digital literacy, and trust are considered important antecedents that influence users' perceptions regarding the usefulness and effectiveness of AI-enabled cybersecurity systems. Users who possess greater cybersecurity awareness and stronger digital capabilities are more likely to perceive AI-based cybersecurity technologies as useful tools for protecting organizational and personal digital assets. Similarly, trust in AI systems enhances users' confidence regarding the reliability and effectiveness of these technologies, thereby increasing behavioral intention toward adoption.

Recent studies have demonstrated that TAM remains highly relevant in AI adoption research due to the increasing complexity of intelligent technologies and the growing dependence on automated systems (Park & Jones-Jang, 2023). In cybersecurity contexts, users' acceptance of AI-driven security technologies is strongly associated with their perceived usefulness in preventing cyber threats, enhancing security performance, and improving decision-making processes (Zhan et al., 2024). Therefore, TAM provides a strong theoretical foundation for explaining the direct effects of AI-driven cybersecurity awareness, digital literacy, and trust on behavioral intention to use AI-based cybersecurity systems.

2.2.2 Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT), introduced by Rogers (1983), explains how individuals develop protective behaviors when they perceive threats and evaluate coping mechanisms. PMT posits that individuals are motivated to adopt security-related behaviors when they perceive a threat as severe and believe that available protective mechanisms are effective in reducing potential harm. The theory has been widely applied in cybersecurity, information security behavior, and digital risk management studies(Ifinedo et al., 2024).

This study adopts PMT because cybersecurity adoption behavior is strongly associated with users' threat perceptions and risk evaluations. AI-driven cybersecurity awareness and perceived risk are grounded in PMT. Users who are more

aware of cyber threats, cyberattacks, phishing attempts, data breaches, and AI-enabled security mechanisms are more likely to adopt AI-based cybersecurity systems as protective tools against cybersecurity risks. PMT further explains that users evaluate both the severity of cyber threats and the effectiveness of AI-driven cybersecurity systems before deciding whether to adopt such technologies.

The inclusion of perceived risk in this study is strongly supported by PMT because risk perception significantly influences users' security behaviors and technology adoption decisions(Uchendu et al., 2021). Individuals who perceive greater cybersecurity risks may become hesitant to adopt AI systems due to concerns regarding privacy, automation errors, surveillance, or algorithmic bias. Conversely, higher levels of cybersecurity awareness may reduce uncertainty and increase users' confidence in AI-enabled security solutions. Therefore, PMT provides an important theoretical explanation for the relationships between AI-driven cybersecurity awareness, perceived risk, and behavioral intention toward AI-based cybersecurity systems.

2.2.3 Social Cognitive Theory (SCT)

Social Cognitive Theory (SCT), developed by Bandura (1986), emphasizes the importance of self-efficacy, cognitive capability, observational learning, and environmental influences in shaping human behavior. According to SCT, individuals' beliefs about their competencies significantly influence their behaviors, learning processes, and technology adoption decisions. SCT has been extensively utilized in digital literacy, cybersecurity behavior, online learning, and technology adoption studies(Almaiah et al., 2022; Zhao et al., 2025).

This study adopts SCT because digital literacy represents users' knowledge, competencies, and confidence in utilizing digital technologies effectively. Individuals with higher digital literacy are more capable of understanding AI technologies, cybersecurity systems, digital environments, and online security practices. Such individuals possess stronger self-efficacy regarding their ability to interact with AI-enabled systems, interpret cybersecurity information, and manage digital risks effectively.

The theory further explains that digitally literate individuals are more likely to adopt AI-based cybersecurity technologies because they possess stronger confidence in their technological capabilities. Recent studies indicate that digital literacy significantly improves users' technology adoption behavior, cybersecurity readiness, and digital resilience(Neumeyer et al., 2020; Siddiq et al., 2016; Van Deursen & Helsper, 2015). In addition, cybersecurity awareness programs and AI training initiatives enhance users' digital competencies and strengthen their willingness to engage with intelligent cybersecurity systems. Therefore, SCT provides an appropriate theoretical explanation for the relationship between AI-driven cybersecurity awareness, digital literacy, and behavioral intention toward AI-based cybersecurity systems.

2.2.4 Theory of Planned Behavior (TPB)

The Theory of Planned Behavior (TPB), proposed by Ajzen(1991), explains that behavioral intention is determined by attitudes, subjective norms, and perceived behavioral control. TPB suggests that individuals are more likely to perform behaviors when they possess favorable attitudes toward the behavior, perceive social support for the behavior, and believe they have sufficient control over performing the behavior. TPB has been widely used in studies examining cybersecurity behavior, AI adoption, digital technologies, and information systems usage (Al-Emran & Griffy-Brown, 2023; Venkatesh, 2022).

The present study adopts TPB because behavioral intention to use AI-based cybersecurity systems is influenced by users' cognitive evaluations and perceptions regarding AI technologies. Trust, cybersecurity awareness, perceived risk, and digital literacy contribute to users' attitudes and perceived behavioral control toward AI-enabled

cybersecurity systems. Users who trust AI technologies and possess higher cybersecurity awareness are more likely to develop positive attitudes toward adopting AI-based cybersecurity solutions. Similarly, digitally literate users may perceive greater control over using AI systems effectively, thereby strengthening their behavioral intention.

TPB is particularly suitable for this study because AI-based cybersecurity adoption involves voluntary user behavior that is influenced by psychological perceptions and decision-making processes. Recent studies have confirmed that TPB remains highly effective in explaining behavioral intention toward AI-enabled systems, cybersecurity compliance, and digital technology adoption (Milicevic et al., 2024; Salloum et al., 2023). Therefore, TPB provides a robust framework for understanding how trust, perceived risk, and cybersecurity awareness influence users' behavioral intention toward AI-based cybersecurity systems.

2.2.5 Trust Theory

Trust Theory explains that users' willingness to rely on technological systems depends on perceptions of reliability, transparency, competence, integrity, and security (Glikson & Woolley, 2020). Trust becomes particularly important in AI-enabled systems because users often face uncertainty regarding algorithmic decision-making, privacy protection, ethical concerns, and automation reliability. Trust Theory has gained substantial attention in AI adoption, intelligent systems, cybersecurity, and human AI interaction research(Müller et al., 2024; Shin, 2022).

This study adopts Trust Theory because trust is a critical determinant of users' willingness to adopt AI-based cybersecurity technologies. Responsible AI perception and AI-driven cybersecurity awareness are expected to enhance users' trust in AI-based cybersecurity systems. Users are more likely to trust AI systems when they perceive them as ethical, transparent, secure, accountable, and reliable. Responsible AI practices such as fairness, explainability, privacy protection, and algorithmic transparency reduce uncertainty and increase users' confidence in AI-enabled cybersecurity solutions.

Recent studies indicate that trust significantly influences users' adoption of AI technologies, especially in security-sensitive environments where privacy and protection concerns are prominent (Celik, 2023; Choung et al., 2023). Users who trust AI systems are more willing to depend on automated cybersecurity tools for threat detection, risk management, and digital protection. Therefore, Trust Theory provides a strong theoretical basis for explaining the relationships between responsible AI perception, AI-driven cybersecurity awareness, trust, and behavioral intention toward AI-based cybersecurity systems.

2.2.6 Integrated Theoretical Perspective

The integration of TAM, PMT, SCT, TPB, and Trust Theory provides a comprehensive theoretical foundation for understanding the adoption of AI-based cybersecurity systems. TAM explains users' acceptance of AI technologies through perceptions of usefulness and effectiveness. PMT explains how cybersecurity awareness and perceived threats motivate protective behaviors. SCT emphasizes the role of digital literacy and self-efficacy in shaping technology adoption behavior. TPB explains how attitudes, perceptions, and behavioral control influence users' intentions toward AI-based cybersecurity systems. Finally, Trust Theory explains how perceptions of reliability, transparency, and ethical AI practices strengthen users' confidence in intelligent cybersecurity technologies.

The integration of these theories enables the study to explain both the direct and indirect relationships among AI-driven cybersecurity awareness, responsible AI perception, digital literacy, trust, perceived risk, prior cybersecurity experience, and behavioral intention to use AI-based cybersecurity systems. This multidimensional theoretical framework provides a stronger explanation of AI-driven cybersecurity adoption behavior than relying on a single theoretical perspective.

2.3.1 AI-Driven Cybersecurity Awareness and Behavioral Intention to Use AI-Based Cybersecurity Systems

AI-driven cybersecurity awareness refers to individuals' understanding of AI-enabled cyber threats, cybersecurity practices, and the role of artificial intelligence in detecting, preventing, and responding to cyberattacks. With the increasing sophistication of cyber threats, organizations and individuals are increasingly relying on AI-based cybersecurity systems to improve security resilience and threat intelligence (Dwivedi et al., 2023; Uchendu et al., 2021). Existing studies suggest that cybersecurity awareness significantly shapes users' security behaviors and technology adoption intentions (Almaiah et al., 2023).

According to the Technology Acceptance Model (TAM) (Davis, 1989), users are more likely to adopt technologies when they perceive them as useful and beneficial. Individuals with high levels of AI-driven cybersecurity awareness tend to better understand the advantages of AI-enabled cybersecurity tools, including automated threat detection, anomaly identification, predictive analytics, and real-time monitoring. Consequently, awareness positively influences users' behavioral intention to adopt AI-based cybersecurity systems.

Recent studies further indicate that cybersecurity awareness programs improve users' confidence in adopting advanced digital security technologies(Chatterjee & Bhattacharjee, 2020; Kajtazi et al., 2021). Individuals who are knowledgeable about cyber risks are more likely to perceive AI-enabled security solutions as effective protective mechanisms against cyber threats. Therefore, the study proposes the following hypothesis:

H1

AI-driven cybersecurity awareness positively influences behavioral intention to use AI-based cybersecurity systems.

2.3.2 AI-Driven Cybersecurity Awareness and Trust in AI-Based Cybersecurity Systems

Trust is a critical determinant of AI technology adoption, particularly in cybersecurity contexts where users rely on intelligent systems to protect sensitive information and digital assets (Glikson & Woolley, 2020). Trust in AI-based cybersecurity systems refers to users' confidence in the reliability, competence, transparency, and effectiveness of AI-driven security technologies.

Protection Motivation Theory (PMT) (Rogers, 1983) explains that individuals who recognize cybersecurity threats and understand protective technologies are more likely to trust security mechanisms designed to mitigate risks. AI-driven cybersecurity awareness enhances users' understanding of how AI systems function in identifying malicious activities, detecting vulnerabilities, and preventing cyberattacks.

Empirical evidence suggests that cybersecurity awareness significantly improves users' trust in emerging security technologies (Aldawood & Skinner, 2019). When users possess adequate knowledge regarding AI-enabled cybersecurity systems, uncertainty and skepticism toward AI technologies decrease, thereby strengthening trust. Furthermore, awareness helps users understand the benefits and limitations of AI systems, enhancing perceptions of reliability and security effectiveness.

Therefore, the study hypothesizes that:

H2

AI-driven cybersecurity awareness positively influences trust in AI-based cybersecurity systems.

2.3.3 AI-Driven Cybersecurity Awareness and Digital Literacy

Digital literacy refers to individuals' ability to effectively access, understand, evaluate, and use digital technologies and information systems (Ng, 2021). In cybersecurity environments, digital literacy includes competencies related to online safety, cybersecurity practices, digital communication, and technology utilization.

Social Cognitive Theory (SCT) (Bandura, 1986) posits that knowledge acquisition and cognitive learning significantly influence individuals' technological competencies and behaviors. AI-driven cybersecurity awareness contributes to individuals' understanding of digital threats, AI systems, and cybersecurity practices, thereby enhancing their digital literacy capabilities.

Recent studies indicate that cybersecurity awareness initiatives significantly improve digital competencies and technological readiness among users (Abu-Amara et al., 2021; Salloum et al., 2023). Individuals exposed to cybersecurity awareness programs become more knowledgeable about secure digital behaviors, privacy protection, phishing detection, and AI-enabled security tools. Consequently, awareness enhances users' ability to effectively interact with digital systems and cybersecurity technologies.

Moreover, digitally aware individuals are more likely to engage in continuous learning regarding emerging AI technologies and cybersecurity practices. Therefore, the study proposes the following hypothesis:

H3

AI-driven cybersecurity awareness positively influences digital literacy.

2.3.4 Responsible AI Perception and Trust in AI-Based Cybersecurity Systems

Responsible AI perception refers to users' beliefs that AI systems operate ethically, transparently, fairly, securely, and accountably(Floridi et al., 2018). As AI technologies become increasingly integrated into cybersecurity systems, concerns regarding privacy, bias, transparency, and algorithmic accountability have become prominent issues influencing technology trust and adoption.

Trust Theory explains that users are more likely to trust technologies perceived as transparent, ethical, and reliable (Mayer et al., 1995). Responsible AI principles such as fairness, explainability, accountability, and privacy protection reduce uncertainty and enhance users' confidence in AI systems.

Recent studies demonstrate that perceptions of responsible AI significantly influence trust in AI-driven technologies (Shin, 2022; Jöhnk et al., 2023). Users are more likely to trust AI-based cybersecurity systems when they believe these systems make fair decisions, protect user privacy, and operate transparently. Ethical AI practices also minimize fears regarding misuse of personal data and algorithmic bias.

In cybersecurity contexts, trust becomes particularly important because users depend on AI systems to monitor networks, detect threats, and manage sensitive information. Consequently, perceptions of responsible AI positively contribute to trust formation.

Therefore, the study hypothesizes that:

H4

Responsible AI perception positively influences trust in AI-based cybersecurity systems.

2.3.5 Trust in AI-Based Cybersecurity Systems and Behavioral Intention to Use

Trust is widely recognized as a significant predictor of users' intention to adopt AI-enabled technologies (Venkatesh et al., 2022). In cybersecurity environments, users often rely on AI systems to autonomously detect threats, monitor suspicious activities, and secure sensitive information. Consequently, trust becomes a critical factor influencing behavioral intention toward AI-based cybersecurity systems.

The Theory of Planned Behavior (TPB) (Ajzen, 1991) suggests that users' attitudes and beliefs significantly shape behavioral intentions. When individuals trust AI-based cybersecurity systems, they are more likely to develop favorable attitudes toward adoption and continued use.

Existing studies reveal that trust significantly enhances users' willingness to adopt AI-enabled security technologies (Choung et al., 2023; Ameen et al., 2024). Users who perceive AI cybersecurity systems as reliable, accurate, and secure are more likely to depend on these systems for cybersecurity protection. Trust also reduces perceptions of uncertainty and technological complexity associated with AI applications.

Therefore, the study proposes the following hypothesis:

H5

Trust in AI-based cybersecurity systems positively influences behavioral intention to use AI-based cybersecurity systems.

2.3.6 Digital Literacy and Behavioral Intention to Use AI-Based Cybersecurity Systems

Digital literacy plays an essential role in shaping users' readiness and capability to adopt advanced digital technologies, including AI-based cybersecurity systems. Individuals with strong digital competencies are more capable of understanding technological functions, navigating digital environments, and utilizing cybersecurity tools effectively.

Human Capital Theory (Becker, 1964) argues that investments in technological skills and knowledge improve individuals' productivity and technological adaptability. Similarly, SCT suggests that self-efficacy and digital competence significantly influence technology usage behavior.

Prior studies indicate that digital literacy positively affects individuals' acceptance and adoption of AI technologies (van Laar et al., 2021; Reddy et al., 2023). Digitally literate users are more confident in interacting with AI systems, understanding cybersecurity alerts, and managing digital risks. Furthermore, digital literacy reduces technological anxiety and improves perceived ease of use.

In cybersecurity contexts, users with higher digital literacy are better equipped to understand AI-enabled security features and effectively utilize cybersecurity systems. Therefore, the study hypothesizes that:

H6

Digital literacy positively influences behavioral intention to use AI-based cybersecurity systems.

2.3.7 Perceived Risk and Behavioral Intention to Use AI-Based Cybersecurity Systems

Perceived risk refers to users' perceptions of uncertainty, potential losses, privacy concerns, and security threats associated with using AI-based systems (Featherman & Pavlou, 2003). Although AI technologies offer significant cybersecurity benefits, concerns regarding privacy violations, algorithmic errors, data misuse, and automation risks may discourage adoption.

Protection Motivation Theory (PMT) explains that individuals evaluate threats and coping mechanisms before engaging in protective behaviors. While cybersecurity systems aim to reduce cyber risks, users may still perceive risks associated with AI technologies themselves.

Recent studies show that perceived risk negatively influences users' intention to adopt AI-enabled technologies (Baabdullah et al., 2022; Al-Adwan et al., 2023). Users who perceive high levels of technological uncertainty or privacy risks are less likely to trust and adopt AI systems. In cybersecurity settings, concerns regarding AI decision-making accuracy and unauthorized access to sensitive data may further reduce adoption intentions.

Therefore, the study proposes the following hypothesis:

H7

Perceived risk negatively influences behavioral intention to use AI-based cybersecurity systems.

2.3.8 Prior Experience with Cybersecurity Breaches and Behavioral Intention to Use AI-Based Cybersecurity Systems

Prior experience with cybersecurity breaches refers to individuals' previous encounters with cyberattacks, data breaches, phishing incidents, malware infections, or other cybersecurity threats. Such experiences significantly shape users' cybersecurity awareness, risk perceptions, and security behaviors.

Protection Motivation Theory suggests that individuals who have experienced cyber threats are more motivated to adopt protective technologies to prevent future incidents. Prior cybersecurity experiences increase users' perceptions of vulnerability and the importance of effective cybersecurity measures.

Empirical studies indicate that individuals who have previously experienced cyberattacks demonstrate stronger intentions to adopt cybersecurity technologies and protective behaviors (Ifinedo, 2022; Trang et al., 2024). Experiencing cybersecurity breaches often motivates users to seek more advanced and intelligent security solutions, including AI-based cybersecurity systems.

Furthermore, users with prior cyberattack experiences tend to perceive AI-enabled cybersecurity systems as valuable tools for preventing future security incidents. Therefore, the study hypothesizes that:

H8

Prior experience with cybersecurity breaches positively influences behavioral intention to use AI-based cybersecurity systems.

2.3.9 Mediating Role of Trust in AI-Based Cybersecurity Systems

Trust has been widely recognized as a critical mediating mechanism between awareness-related factors and technology adoption behavior. AI-driven cybersecurity awareness enhances users' understanding of AI systems, which subsequently strengthens trust in AI-enabled cybersecurity technologies.

Trust Theory and TPB suggest that users who trust AI systems are more likely to develop favorable behavioral intentions toward adoption. Existing research demonstrates that trust mediates the relationship between awareness, perceptions, and AI adoption behavior (Shin, 2022; Choung et al., 2023).

Users with higher AI-driven cybersecurity awareness are more likely to perceive AI cybersecurity systems as reliable and effective, thereby increasing trust and subsequently enhancing behavioral intention to use such systems.

Therefore, the study proposes the following hypothesis:

H9

Trust in AI-based cybersecurity systems mediates the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems.

2.3.10 Mediating Role of Digital Literacy

Digital literacy also serves as an important mechanism linking cybersecurity awareness and behavioral intention toward AI-based cybersecurity systems. AI-driven cybersecurity awareness contributes to users' digital competencies, technological understanding, and confidence in using AI technologies.

Social Cognitive Theory emphasizes that knowledge and self-efficacy influence behavioral outcomes through enhanced competencies and learning capabilities. Prior research indicates that digital literacy mediates the relationship between awareness and technology adoption behaviors (Reddy et al., 2023; AlMansoori et al., 2024).

Users with strong cybersecurity awareness are more likely to develop digital literacy competencies, which subsequently enhance their confidence and intention to adopt AI-based cybersecurity systems. Consequently, digital literacy acts as a facilitating mechanism through which cybersecurity awareness influences behavioral intention.

Therefore, the study hypothesizes that:

H10

Digital literacy mediates the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems.

2.9 Research Model

Based on the integrated theoretical foundation discussed in the previous sections and the research gaps identified in the literature, this study proposes a conceptual model that examines the influence of AI-driven cybersecurity awareness, responsible AI perception, perceived risk, prior cybersecurity experience, trust in AI-based cybersecurity

systems, and digital literacy on behavioral intention to use AI-based cybersecurity systems (see Fig. 1 and Table 1). The proposed model is grounded in the Technology Acceptance Model (TAM), Protection Motivation Theory (PMT), Social Cognitive Theory (SCT), Theory of Planned Behavior (TPB), and Trust Theory, which collectively explain how technological awareness, cognitive perceptions, digital competencies, and psychological evaluations shape users' intention to adopt AI-enabled cybersecurity technologies.

The Technology Acceptance Model (TAM) provides the primary technological adoption perspective by emphasizing that users' behavioral intention toward adopting new technologies is influenced by their perceptions of usefulness, ease of use, and positive attitudes toward technology (Davis, 1989). Within the context of the present study, AI-driven cybersecurity awareness, trust, and digital literacy represent critical antecedents influencing users' perceptions and behavioral intentions toward AI-based cybersecurity systems. Individuals who understand the benefits and functionalities of AI-enabled cybersecurity tools are more likely to perceive such systems as useful and effective in protecting digital environments.

Protection Motivation Theory (PMT) offers an important security-related perspective by explaining how individuals adopt protective behaviors when they perceive cyber threats and evaluate coping mechanisms (Rogers, 1983). The theory suggests that users who are aware of cybersecurity threats and have prior experiences with cybersecurity breaches are more likely to adopt AI-based cybersecurity systems as protective technologies against cyberattacks. Similarly, perceived risk plays an important role in shaping users' security-related decision-making processes, as higher perceptions of technological or privacy risks may negatively affect adoption intention.

Social Cognitive Theory (SCT) further explains the role of digital literacy in influencing technology adoption behavior (Bandura, 1986). According to SCT, individuals with stronger digital competencies, technological confidence, and self-efficacy are more capable of understanding and effectively using AI-enabled cybersecurity technologies. Consequently, digitally literate users are more likely to adopt AI-based cybersecurity systems and engage in secure digital practices.

In addition, the Theory of Planned Behavior (TPB) explains that users' behavioral intention is shaped by attitudes, perceived behavioral control, and subjective evaluations of technology usage (Ajzen, 1991). In this study, trust in AI-based cybersecurity systems, cybersecurity awareness, and perceived risk contribute to users' attitudes and behavioral evaluations regarding AI-enabled cybersecurity technologies. Trust Theory further complements the model by emphasizing that perceptions of reliability, transparency, ethical responsibility, and system competence significantly influence users' willingness to rely on AI technologies (Glikson & Woolley, 2020). Responsible AI perception is therefore conceptualized as an important determinant of trust in AI-based cybersecurity systems.

Recent studies have reinforced the importance of these factors in AI adoption and cybersecurity contexts. For instance, Dwivedi et al. (2023) and Chatterjee et al. (2024) emphasized that AI awareness and digital competence significantly influence users' adoption of AI-enabled technologies. Similarly, Shin (2022) and Jöhnk et al. (2023) demonstrated that responsible AI practices and trust are critical drivers of AI system acceptance. Existing cybersecurity studies also indicate that prior cybersecurity experiences and risk perceptions significantly shape protective technology adoption behaviors (Ifinedo, 2022; Trang et al., 2024).

In this context, mediation analysis was employed to examine the indirect mechanisms through which AI-driven cybersecurity awareness influences behavioral intention to use AI-based cybersecurity systems via trust and digital literacy. Rather than assuming only direct relationships, this approach captures the indirect effects operating through cognitive and behavioral enablers that facilitate AI adoption behavior. This analytical design aligns with TAM, SCT,

TPB, and Trust Theory, as these theoretical perspectives emphasize that awareness and technological understanding shape behavioral outcomes through intermediate psychological and competency-related mechanisms.

Moreover, the proposed research model integrates both technological and behavioral determinants of AI-based cybersecurity adoption and positions trust and digital literacy as mediating variables that explain how cybersecurity awareness translates into behavioral intention. The model therefore provides a theoretically grounded and empirically testable framework for understanding the factors influencing the adoption of AI-based cybersecurity systems in contemporary digital environments.

Therefore, the conceptual model incorporates seven primary constructs:

1. AI-Driven Cybersecurity Awareness
2. Responsible AI Perception
3. Trust in AI-Based Cybersecurity Systems (Mediator 1)
4. Digital Literacy (Mediator 2)
5. Perceived Risk
6. Prior Experience with Cybersecurity Breaches
7. Behavioral Intention to Use AI-Based Cybersecurity Systems

This model captures both the direct and mediated pathways through which cybersecurity awareness, trust, digital competence, and risk perceptions influence users' intention to adopt AI-based cybersecurity technologies. It also acknowledges the multidimensional nature of AI-enabled cybersecurity environments, where technological awareness, ethical AI perceptions, digital capabilities, and cybersecurity experiences collectively shape users' behavioral adoption decisions (see Table 1).

Table 1
Theoretical Mapping of Influencing Factors and Research Constructs

Identified Factors	Proposed Model Variables	Theoretical Foundation
Limited understanding of AI-enabled cybersecurity threats, low awareness of cybersecurity practices, and inadequate knowledge of AI technologies.	AI-Driven Cybersecurity Awareness	Protection Motivation Theory (Rogers, 1983); Technology Acceptance Model (Davis, 1989)
Ethical concerns regarding AI systems, including transparency, accountability, fairness, and privacy protection.	Responsible AI Perception	Trust Theory (Glikson & Woolley, 2020); Theory of Planned Behavior (Ajzen, 1991)
Confidence in the reliability, competence, and effectiveness of AI-enabled cybersecurity technologies.	Trust in AI-Based Cybersecurity Systems	Trust Theory (Mayer et al., 1995); Technology Acceptance Model (Davis, 1989)
Users' digital competencies, technological self-efficacy, and ability to utilize digital systems effectively.	Digital Literacy	Social Cognitive Theory (Bandura, 1986); Human Capital Theory (Becker, 1964)
Privacy concerns, technological uncertainty, fear of automation errors, and cybersecurity vulnerabilities associated with AI systems.	Perceived Risk	Protection Motivation Theory (Rogers, 1983); Theory of Planned Behavior (Ajzen, 1991)
Previous exposure to cyberattacks, phishing incidents, data breaches, or cybersecurity threats.	Prior Experience with Cybersecurity Breaches	Protection Motivation Theory (Rogers, 1983)
Users' willingness and intention to adopt and use AI-enabled cybersecurity technologies.	Behavioral Intention to Use AI-Based Cybersecurity Systems	Technology Acceptance Model (Davis, 1989); Theory of Planned Behavior (Ajzen, 1991)

Source(s): Authors' own work based on the integration of TAM, PMT, SCT, TPB, and Trust Theory and supporting literature.

Research Methodology

The present study investigates the impact of AI-driven cybersecurity awareness on behavioral intention to use AI-based cybersecurity systems, with the mediating role of trust and digital literacy. The target respondents were professionals and individuals working across different sectors in Somalia, including education, banking and finance, industry, and government/public services. This population was selected because these groups are increasingly exposed to digital systems and AI-enabled cybersecurity solutions in their daily work environments, making them appropriate for examining behavioral intention and trust-related constructs.

Given the absence of a comprehensive sampling frame and the practical constraints in accessing respondents across multiple institutions, a non-probability sampling technique was adopted. Specifically, purposive sampling was used to ensure that only individuals with relevant professional experience and exposure to digital systems were included in the study. The sample was further refined by excluding respondents who did not meet the minimum criteria of being engaged in ICT-related or organizational digital activities.

In determining the minimum required sample size, the study employed G*Power software for power analysis, consistent with prior studies in information systems and behavioral research. The parameters were set at an effect size (f^2) of 0.15, a statistical power of 0.95, an alpha level of 0.05, and six predictors in the model. The analysis indicated a minimum required sample size of 146 respondents, as also reflected in the output results (Critical F =

2.1644, actual power = 0.95). A total of 287 valid responses were ultimately collected and retained after data screening and cleaning procedures. See appendix A and B.

Regarding the demographic profile of the respondents, the majority were male (67.6%), while females represented 32.4%. In terms of age distribution, most respondents were between 26–49 years (59.2%), followed by 18–25 years (31.7%), and 50 years or older (9.1%). With respect to education level, the majority held a Master's degree (75.6%), followed by Bachelor's degree holders (12.2%), PhD holders (6.3%), diploma (4.5%), and high school education (1.4%). Regarding employment sector, respondents were drawn mainly from education (49.5%), banking and finance (32.8%), industry (9.1%), and government/public services (8.7%). The descriptive statistics provide evidence of a highly educated and professionally diverse sample, which strengthens the relevance of the data for examining AI-related behavioral constructs.

For data analysis, the study employed Structural Equation Modeling (SEM), a robust multivariate technique widely used in social science and information systems research (Valaei et al., 2017). SEM is particularly suitable for examining complex relationships among latent constructs, including AI-driven cybersecurity awareness, trust, digital literacy, and behavioral intention. It enables simultaneous assessment of both the measurement model (validity and reliability of constructs) and the structural model (hypothesized relationships among variables), providing comprehensive empirical and theoretical insights. This approach is especially appropriate for behavioral and perceptual studies in emerging digital environments, where constructs are often interrelated and indirectly observed.

Overall, the methodological approach ensures rigorous statistical validation and supports robust inference regarding the relationships among AI cybersecurity awareness, trust, digital literacy, and behavioral intention to use AI-based cybersecurity systems.

Data analysis

Common Method Bias (CMB)

Since the present study employed a cross-sectional survey design and collected self-reported data from a single group of respondents at one point in time, the possibility of common method bias (CMB) was carefully considered. Common method bias refers to systematic measurement error attributable to the measurement method rather than to the constructs represented by the measures themselves, which may artificially inflate or suppress the observed relationships among variables(Podsakoff et al., 2003). This concern is particularly relevant in studies examining behavioral intention, trust, digital literacy, and cybersecurity awareness using perceptual survey instruments.

To reduce the potential influence of CMB, several procedural remedies were implemented during the questionnaire design and data collection stages. Respondents were assured of anonymity and confidentiality, and they were informed that there were no right or wrong answers. Furthermore, the questionnaire items were organized into separate sections according to their constructs to minimize response pattern bias and evaluation apprehension. Clear instructions and simple wording were also used to improve respondents' understanding and reduce ambiguity.

In addition to these procedural measures, Harman's single-factor test was conducted as an initial statistical assessment of common method variance. Following the recommendations of Podsakoff et al. (2003), all measurement items were entered into an exploratory factor analysis using an unrotated principal component approach. The results showed that multiple factors emerged from the analysis, and the first factor accounted for 28.433% of the total variance, which is below the recommended threshold of 50%. This finding indicates that common method bias is unlikely to represent a serious concern in the study.

Furthermore, the full collinearity variance inflation factor (VIF) approach proposed by Kock (2015) was applied to provide a more rigorous evaluation of common method bias. The VIF values for all constructs ranged from 1.133 to 1.639, which are substantially below the conservative threshold value of 3.3 and the commonly accepted threshold of 5. Specifically, the VIF values were 1.554 for Responsible AI, 1.639 for Risk, 1.133 for Trust, 1.238 for Experience, 1.370 for Literacy, and 1.314 for Cybersecurity Awareness. These results suggest the absence of problematic multicollinearity and indicate that common method bias is not likely to significantly affect the study results. The result presented in Table 2.

Additionally, a Common Latent Factor (CLF) analysis was conducted within the Structural Equation Modeling (SEM) framework to further assess the presence of shared variance among the measurement items. A common latent factor was added to the measurement model with paths linked to all observed indicators. The comparison between the original model and the CLF model showed a small chi-square difference ($\Delta\chi^2 = 4.56$, $\Delta df = 1$), where the original chi-square was 1309.314 (df = 758) and the current chi-square was 1304.75 (df = 757). The relatively small difference indicates that the inclusion of the common latent factor did not substantially improve the model fit, suggesting that common method variance does not seriously distort the relationships among the constructs.

Overall, the findings from Harman's single-factor test, the VIF analysis, and the Common Latent Factor approach provide converging evidence that common method bias is not a significant threat to the validity of this study. Therefore, the relationships among AI-driven cybersecurity awareness, trust, digital literacy, and behavioral intention can be interpreted with reasonable confidence.

Table 2
Collinearity variance inflation factor (VIF)

Collinearity Statistics		
Tolerance	VIF	
Responsible	.644	1.554
Risk	.610	1.639
Trust	.882	1.133
Experience	.808	1.238
Literacy	.730	1.370
Cybersecurity	.761	1.314

Note

AICA = AI-Driven Cybersecurity Awareness; TRAI = Trust in AI-Based Cybersecurity Systems; DILI = Digital Literacy; REAI = Responsible AI; PERA = Prior Experience with Breaches; PERI = Perceived Risk; BEIU = Behavioral Intention to Use.

Figure 2. Common method bias

Measurement model assessment

The measurement model was evaluated using Structural Equation Modeling (SEM) with IBM SPSS and AMOS to assess the reliability and validity of the constructs included in the proposed research framework. The assessment involved examining indicator reliability, internal consistency reliability, convergent validity, and discriminant validity following established SEM guidelines. Indicator reliability was assessed through standardized factor loadings. According to Hair et al. (2019), factor loadings above .60 are considered acceptable for confirming item reliability. The results indicated that all measurement items loaded satisfactorily on their respective constructs, with factor loadings ranging from .621 to .930. Since all factor loadings exceeded the recommended threshold, no measurement items were removed from the analysis. The squared multiple correlations (SMC) further demonstrated that the observed variables adequately explained the variance of their corresponding latent constructs. Internal consistency reliability was evaluated using Composite Reliability (CR). As recommended by Fornell & Larcker (1981) and Hair et al. (2019), CR values greater than .70 indicate satisfactory reliability. The CR values for all constructs exceeded the recommended threshold, ranging from .836 to .939. Specifically, Perceived Risk (CR = .939), Responsible AI Perception (CR = .937), AI-driven Cybersecurity Awareness (CR = .936), Trust in AI-based Cybersecurity Systems (CR = .933), Digital Literacy (CR = .918), Behavioral Intention to Use (CR = .905), and Prior Experience with Breaches (CR = .836) demonstrated strong internal consistency reliability. Convergent validity was examined using the Average Variance Extracted (AVE). The AVE values for all constructs exceeded the recommended threshold value of .50 (Fornell & Larcker, 1981), ranging from .563 to .748. These findings confirm that the constructs explain more than 50% of the variance in their respective indicators. Responsible AI Perception recorded the highest AVE value (.748), followed by Trust in AI-based Cybersecurity Systems (.736) and Perceived Risk (.722), indicating strong convergent validity across the constructs. Discriminant validity was assessed using the Fornell–Larcker criterion. The square root of the AVE values for each construct was greater than the correlations between constructs, confirming adequate discriminant validity. For example, the square root of the AVE for Responsible AI Perception (.865) exceeded its correlations with Digital Literacy (.372), AI-driven Cybersecurity Awareness (.109), Trust in AI-based Cybersecurity Systems (.240), and Behavioral Intention to Use (.242). Similarly, the square root of the AVE for Trust in AI-based Cybersecurity Systems (.858) was greater than its correlations with all other constructs. These findings indicate that each construct was empirically distinct from the others. Additionally, the Maximum Shared Variance (MSV) values were lower than the corresponding AVE values for all constructs, further supporting discriminant validity. The MaxR(H) values ranged from .860 to .953, indicating acceptable construct reliability and model stability. Overall, the measurement model demonstrated satisfactory psychometric properties, including adequate indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. Therefore, the measurement model was considered appropriate for proceeding to the structural model analysis.

Table 3
Standardized factor loading, SMC, CR and AVE. Construct

Construct	Items	Factor Loading	SMC
	DILI8	**0.712**	**0.507**
	DILI7	0.884	0.781
	DILI6	0.881	0.776
Digital Literacy (DILI)	DILI5	0.839	0.704
	DILI4	0.781	0.61
	DILI3	0.681	0.464
	DIL2	0.621	0.386
	DILI1	0.677	0.458
	REAI5	0.811	0.658
	REAI4	0.849	0.721
Responsible AI (REAI)	REAI3	0.901	0.812
	REAI2	0.889	0.790
	REAI1	0.870	0.757
	AICA7	0.870	0.757
	AICA6	0.830	0.689
AI – driven Cybersecurity Awareness (AICA)	AICA5	0.837	0.701
	AICA4	0.862	0.743
	AICA3	0.797	0.635
	AICA2	0.840	0.706
	AICA1	0.716	0.513
	TRAI5	0.848	0.719
	TRAI4	0.875	0.766
Trust in AI-based cybersecurity systems (TRAI)	TRAI3	0.918	0.843
	TRAI2	0.849	0.721
	TRAI1	0.796	0.634
	PEBR4	0.632	0.399
	PEBR3	0.865	0.748
Prior experience with breaches (PERA)	PEBR2	0.718	0.516
	PEBR1	0.767	0.588
	BEIU6	0.835	0.697

Construct	Items	Factor Loading	SMC
	DILI8	**0.712**	**0.507**
	BEIU5	0.817	0.667
	BEIU4	0.837	0.701
Behavioral Intention to Use (BEIU)	BEIU3	0.814	0.663
	BEIU2	0.687	0.472
	BEIU1	0.704	0.496
	PERI6	0.693	0.48
	PERI5	0.835	0.697
Perceived risk (PERI)	PERI4	0.930	0.865
	PERI3	0.920	0.846
	PERI2	0.875	0.766
	PERI1	0.822	0.676

Table 4
Discriminant validity

PERI	CR	AVE	MSV	MaxR(H)	PERI	DILI	REAI	AICA	TRAI	PERI	BEIU
	0.939	**0.722**	**0.336**	**0.953**	**0.850**						
DILI	0.918	0.586	0.261	0.935	-0.459	**0.765**					
REAI	0.937	0.748	0.336	0.940	-0.580	0.372	**0.865**				
AICA	0.936	0.678	0.219	0.940	-0.228	0.284	0.109	**0.823**			
TRAI	0.933	0.736	0.058	0.939	-0.077	0.223	0.240	0.230	**0.858**		
PERI	0.836	0.563	0.219	0.860	-0.124	0.236	0.068	0.468	0.155	**0.750**	
BEIU	0.905	0.616	0.261	0.913	-0.350	0.511	0.242	0.425	0.228	0.322	**0.785**

Structural model

The structural model was assessed using Structural Equation Modeling (SEM) to examine the hypothesized relationships among AI-driven cybersecurity awareness, responsible AI perception, trust in AI-based cybersecurity systems, digital literacy, perceived risk, prior experience with cybersecurity breaches, and behavioral intention to use AI-based cybersecurity systems. The results of the hypothesis testing are presented in Table 4 and Fig. 2.

H1 evaluates whether AI-driven cybersecurity awareness positively influences behavioral intention to use AI-based cybersecurity systems. The findings revealed that AI-driven cybersecurity awareness has a significant positive effect on behavioral intention to use AI-based cybersecurity systems ($\beta = .199$, C.R. = 3.961, $p < .001$). Therefore, H1 was supported. This finding suggests that individuals with higher cybersecurity awareness are more likely to adopt AI-based cybersecurity technologies.

H2 evaluates whether AI-driven cybersecurity awareness positively influences trust in AI-based cybersecurity systems. The results indicated that AI-driven cybersecurity awareness has a significant positive effect on trust in AI-based cybersecurity systems ($\beta = .206$, C.R. = 3.405, $p < .001$). Consequently, H2 was supported. This finding implies that increased cybersecurity awareness enhances users' confidence and trust in AI-enabled cybersecurity solutions.

H3 examines whether AI-driven cybersecurity awareness positively influences digital literacy. The results demonstrated that AI-driven cybersecurity awareness has a significant positive effect on digital literacy ($\beta = .282$, C.R. = 4.764, $p < .001$). Hence, H3 was supported. The findings indicate that awareness of AI-driven cybersecurity technologies contributes significantly to the enhancement of users' digital competencies and technological skills.

H4 evaluates whether responsible AI perception positively influences trust in AI-based cybersecurity systems. The results revealed that responsible AI perception significantly and positively influences trust in AI-based cybersecurity systems ($\beta = .149$, C.R. = 3.476, $p < .001$). Therefore, H4 was supported. This finding indicates that users who perceive AI systems as transparent, ethical, and accountable are more likely to trust AI-based cybersecurity technologies.

H5 examines whether trust in AI-based cybersecurity systems positively influences behavioral intention to use AI-based cybersecurity systems. The findings indicated that trust in AI-based cybersecurity systems did not significantly influence behavioral intention to use AI-based cybersecurity systems ($\beta = .051$, C.R. = 1.135, $p = .257$). Therefore, H5 was not supported. This result suggests that although users may trust AI-enabled cybersecurity systems, trust alone may not be sufficient to directly influence their adoption intentions.

H6 evaluates whether digital literacy positively influences behavioral intention to use AI-based cybersecurity systems. The results demonstrated that digital literacy has a significant positive effect on behavioral intention to use AI-based cybersecurity systems ($\beta = .321$, C.R. = 6.775, $p < .001$). Consequently, H6 was supported. The findings indicate that users with higher levels of digital competence are more likely to adopt AI-driven cybersecurity technologies.

H7 examines whether perceived risk negatively influences behavioral intention to use AI-based cybersecurity systems. The results revealed that perceived risk has a significant negative effect on behavioral intention to use AI-based cybersecurity systems ($\beta = -.113$, C.R. = −2.566, $p = .010$). Therefore, H7 was supported. This finding suggests that users who perceive greater uncertainty and risk associated with AI-based cybersecurity systems are less likely to adopt such technologies.

H8 evaluates whether prior experience with cybersecurity breaches positively influences behavioral intention to use AI-based cybersecurity systems. The findings demonstrated that prior experience with cybersecurity breaches has a significant positive effect on behavioral intention to use AI-based cybersecurity systems ($\beta = .140$, C.R. = 2.092, $p = .036$). Hence, H8 was supported. This result indicates that individuals who previously experienced cybersecurity incidents are more inclined to adopt AI-driven cybersecurity solutions as protective mechanisms against future cyber threats.

Overall, the structural model results provide substantial support for the proposed research framework by demonstrating the significant roles of AI-driven cybersecurity awareness, responsible AI perception, digital literacy, perceived risk, and prior cybersecurity breach experience in shaping behavioral intention toward AI-based cybersecurity systems.

Table 2
Results of Hypotheses Testing

Hypothesis	Structural Path	Standardized Estimate (β)	S.E.	C.R.	p-value	Decision
H1	AI-Driven Cybersecurity Awareness → Behavioral Intention to Use	.199	.050	3.961	< .001	Supported
H2	AI-Driven Cybersecurity Awareness → Trust in AI-Based Cybersecurity Systems	.206	.061	3.405	< .001	Supported
H3	AI-Driven Cybersecurity Awareness → Digital Literacy	.282	.059	4.764	< .001	Supported
H4	Responsible AI Perception → Trust in AI-Based Cybersecurity Systems	.149	.043	3.476	< .001	Supported
H5	Trust in AI-Based Cybersecurity Systems → Behavioral Intention to Use	.051	.045	1.135	.257	Not Supported
H6	Digital Literacy → Behavioral Intention to Use	.321	.047	6.775	< .001	Supported
H7	Perceived Risk → Behavioral Intention to Use	−.113	.044	−2.566	.010	Supported
H8	Prior Experience with Cybersecurity Breaches → Behavioral Intention to Use	.140	.067	2.092	`.036	Supported

Note. β = standardized regression coefficient; S.E. = standard error; C.R. = critical ratio.

Mediation Analysis

Lastly, H9 evaluates whether trust in AI-based cybersecurity systems mediates the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems. The results show that the direct effect between AI-driven cybersecurity awareness and behavioral intention to use was found insignificant when the mediator was introduced into the model (β = .047, t = 1.028, p > .05). Furthermore, the indirect effect through trust in AI-based cybersecurity systems was also found insignificant (β = .011, t = 0.917, p > .05), and the confidence interval included zero (Lower Bound = − .005, Upper Bound = .035). Hence, the results reveal no mediation effect. This indicates that trust in AI-based cybersecurity systems does not significantly mediate the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems. Consequently, H9 was not supported.

H10 evaluates whether digital literacy mediates the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems. The results reveal that the total/direct effect of AI-driven cybersecurity awareness on behavioral intention to use was found positive and significant (β = .380, t = 7.900, p < .001). When the mediator was introduced into the model, the direct relationship remained significant, while the indirect effect through digital literacy was also found significant (β = .107, t = 3.821, p < .001). In addition, the bootstrapped confidence interval did not include zero (Lower Bound = .067, Upper Bound = .161), confirming the significance of the mediation effect. Hence, the results reveal a partial complementary mediation. This indicates that

AI-driven cybersecurity awareness influences behavioral intention to use AI-based cybersecurity systems both directly and indirectly through digital literacy. Consequently, H10 was supported (see Table 5 and Fig. 3).

Table 5
Results of Mediation Analysis

Relationship	Direct Effect	S.E.	C.R.	p-value	Indirect Effect	C.R.	95% Confidence Interval	p-value	Mediation Type
AICA → BEIU via TRAI	.047	.046	1.028	.304	.011	0.917	[– .005, .035]	.257	No Mediation (Direct Only)
AICA → BEIU via DILI	.380	.048	7.900	< .001	.107	3.821	[.067, .161]	< .001	Partial Mediation (Complementary)

Note. AICA = AI-Driven Cybersecurity Awareness; TRAI = Trust in AI-Based Cybersecurity Systems; DILI = Digital Literacy; BEIU = Behavioral Intention to Use AI-Based Cybersecurity Systems.

Evaluation model fit indices

The structural model was assessed using Structural Equation Modeling (SEM) through IBM SPSS and AMOS to examine the relationships among the constructs in the proposed integrated Trust–Risk–Competency Framework. The model fit was evaluated using several goodness-of-fit indices, including the chi-square statistic (χ^2), degree of freedom (df), chi-square to degree of freedom ratio (χ^2/df), Goodness-of-Fit Index (GFI), Adjusted Goodness-of-Fit Index (AGFI), Normed Fit Index (NFI), Incremental Fit Index (IFI), Tucker–Lewis Index (TLI), Comparative Fit Index (CFI), and Root Mean Square Error of Approximation (RMSEA), following the recommendations of Hair et al. (2019),Hu & Bentler (1999), and Kline (2018) .

The findings indicated that the structural model demonstrated an acceptable level of fit with the observed data. The chi-square value was significant ($\chi^2 = 1221.875$, $df = 755$, $p < .001$), which is common in SEM studies involving large sample sizes (Kline, 2016). Therefore, additional fit indices were considered to evaluate the adequacy of the model. The normed chi-square value ($\chi^2/df = 1.618$) was below the recommended threshold of 3.0, indicating a good model fit (Hair et al., 2019).

Furthermore, the Incremental Fit Index (IFI = .949), Tucker–Lewis Index (TLI = .944), and Comparative Fit Index (CFI = .939) exceeded the recommended cut-off value of .90, demonstrating satisfactory incremental model fit. Although the Goodness-of-Fit Index (GFI = .831), Adjusted Goodness-of-Fit Index (AGFI = .807), and Normed Fit Index (NFI = .877) were slightly below the recommended threshold of .90, previous studies suggest that values approaching .90 may still indicate acceptable model fit, particularly in complex models with multiple constructs and indicators (Hair et al., 2019; Marsh et al., 2004). In addition, the Root Mean Square Error of Approximation (RMSEA = .065) was below the recommended threshold of .08, indicating a reasonable approximation error and acceptable fit of the model to the data (Hu & Bentler, 1999). Overall, the results suggest that the structural model achieved an acceptable and satisfactory level of goodness-of-fit, supporting the adequacy of the proposed theoretical framework for explaining behavioral intention toward AI-based cybersecurity systems. The result represented in Table 5 and Fig. 4.

Table 5
Goodness fit indices

Fit measure	Recommended Value	Value for the research model
Chi square		1221.875
Degree of freedom (df)		755
X^2/ df	< 3	1.618
p-value	< 0.05	0.000
GFI	>=0.90	0.831
Adjusted GFI	>=0.90	0.807
Normed fit index (NFI)	>=0.90	0.868
Relative fit index (IFI)	>=0.90	0.949
Turker Lewis index (TLI)	>=0.90	0.944
Comparative fit index (CFI)	>=0.90	0.949
Root mean square error of approximation (RMSEA)	< 0.08	0.046
Standardized RMR	< 0.08	0.0490

(χ^2/df), Goodness-of-Fit Index (GFI), Adjusted Goodness-of-Fit Index (AGFI), Normed Fit Index (NFI), Incremental Fit Index (IFI), Tucker–Lewis Index (TLI), Comparative Fit Index (CFI), and Root Mean Square Error of Approximation (RMSEA), following the recommendations of Hair et al. (2019),Hu & Bentler (1999) , and Kline (2018) .

Discussion

The present study set out to examine the relationships among AI-driven cybersecurity awareness, responsible AI perception, trust in AI-based cybersecurity systems, digital literacy, perceived risk, prior cybersecurity breach experience, and behavioral intention to use AI-based cybersecurity systems. The acceptance of most of the proposed hypotheses provides substantial empirical support for the proposed Trust–Awareness–Competency Framework in explaining users' behavioral intention toward AI-enabled cybersecurity technologies. The findings contribute to the growing body of literature on AI adoption, cybersecurity behavior, digital literacy, and responsible AI governance in emerging digital environments.

The study found a significant positive impact of AI-driven cybersecurity awareness on behavioral intention to use AI-based cybersecurity systems. The findings are consistent with recent studies suggesting that awareness and understanding of AI technologies positively influence users' adoption intentions and readiness to engage with AI-enabled systems (Bera et al., 2026; Yu et al., 2026). Users who possess higher awareness regarding AI-driven cybersecurity threats and defensive mechanisms are more likely to recognize the usefulness and strategic importance of AI-based cybersecurity systems in protecting digital assets and reducing cyber threats. Recent studies further indicate that the increasing complexity of AI-related cyber risks has encouraged individuals and organizations to adopt intelligent cybersecurity technologies more proactively (Erukude et al., 2025).

The findings further revealed that AI-driven cybersecurity awareness significantly and positively influences trust in AI-based cybersecurity systems. The results support recent literature emphasizing that awareness and understanding of

AI functionalities enhance users' confidence and trust in AI-enabled technologies (Falowo & Bou Abdo, 2026; Hanson & Ott, 2026). Individuals who understand the operational capabilities of AI-based cybersecurity technologies are more likely to perceive such systems as reliable, effective, and capable of mitigating cybersecurity threats. Recent evidence also suggests that users increasingly associate AI transparency and explainability with higher trustworthiness in cybersecurity applications (Falowo & Bou Abdo, 2026).

The study also found that AI-driven cybersecurity awareness significantly and positively influences digital literacy. This finding indicates that awareness regarding AI-enabled cybersecurity technologies contributes to the enhancement of users' digital competencies and technical capabilities. The result aligns with recent studies demonstrating that AI awareness and AI literacy are closely associated with digital literacy development and responsible AI adoption(Bahçekapili & Boztaş, 2025; Lemay & Doleck, 2020). As AI technologies become increasingly integrated into cybersecurity infrastructures, users are required to develop stronger digital competencies to effectively interact with intelligent systems and cybersecurity platforms.

Furthermore, the findings demonstrated that responsible AI perception significantly and positively influences trust in AI-based cybersecurity systems. The result confirms recent arguments that users are more likely to trust AI systems when they perceive them as ethical, transparent, accountable, and secure (Cetinkaya & Krämer, 2026; Kaur et al., 2022; Shabankareh et al., 2025). Responsible AI governance has become increasingly important in cybersecurity environments because AI systems often operate autonomously and manage sensitive organizational and personal information. Recent reports also suggest that lack of AI governance and transparency remains one of the primary barriers to user trust and organizational AI adoption (Cetinkaya & Krämer, 2026).

The study further revealed that digital literacy significantly and positively influences behavioral intention to use AI-based cybersecurity systems. The findings are consistent with recent studies emphasizing that users with higher levels of digital competence are more likely to adopt AI technologies and effectively engage with digital systems(Bogoslov et al., 2024; Tunmibi, 2024; Vitezić & Perić, 2024). Digitally literate individuals are generally more capable of understanding AI functionalities, evaluating cybersecurity risks, and utilizing intelligent technologies for protection against cyber threats. Recent evidence further suggests that digital literacy remains one of the strongest predictors of AI adoption behavior in modern digital environments (Hanson & Ott, 2026).

Additionally, the findings indicated that prior experience with cybersecurity breaches significantly and positively influences behavioral intention to use AI-based cybersecurity systems. This result suggests that individuals who previously experienced cyberattacks, data breaches, phishing attacks, or other cybersecurity incidents are more inclined to adopt AI-driven cybersecurity technologies as protective mechanisms. Recent cybersecurity studies indicate that growing exposure to AI-powered cyber threats and digital vulnerabilities has increased users' motivation to adopt advanced cybersecurity solutions (World Economic Forum Accenture, 2022). Experiencing cybersecurity incidents may increase users' awareness of digital risks and encourage proactive cybersecurity behavior.

The findings also revealed that perceived risk significantly and negatively influences behavioral intention to use AI-based cybersecurity systems. This finding supports recent literature indicating that concerns regarding privacy, security vulnerabilities, AI misuse, and operational uncertainty negatively affect users' willingness to adopt AI-enabled technologies (Lan et al., 2026; Yu et al., 2026). Users who perceive higher levels of risk associated with AI-based cybersecurity systems may hesitate to adopt such technologies due to concerns regarding data privacy, algorithmic bias, lack of transparency, and potential system failures. Recent research further suggests that trust in AI technologies is still not fully aligned with technological advancement, primarily because users remain concerned about AI governance, security, and accountability(Vitezić & Perić, 2024) .

Interestingly, the study found that trust in AI-based cybersecurity systems does not significantly influence behavioral intention to use AI-based cybersecurity systems. This finding contrasts with several traditional technology adoption studies that identified trust as a direct determinant of adoption intention. One possible explanation is that users may trust AI systems conceptually but still require sufficient digital competence and practical experience before deciding to adopt AI-driven cybersecurity technologies. Recent studies suggest that trust in AI alone may not guarantee adoption unless accompanied by adequate AI literacy, governance, and technical understanding (Falowo & Bou Abdo, 2026).

Finally, the findings provide important empirical insights into the mediating roles of trust in AI-based cybersecurity systems and digital literacy. The results revealed that trust in AI-based cybersecurity systems does not significantly mediate the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems. However, digital literacy was found to significantly mediate the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems. The findings indicate that AI-driven cybersecurity awareness enhances users' digital competencies, which subsequently increases their intention to adopt AI-enabled cybersecurity technologies. Recent studies similarly emphasize that AI literacy and digital literacy are critical mechanisms for translating technological awareness into responsible AI adoption behavior (Memarian & Doleck, 2026; Yu et al., 2026).

Overall, the findings of this study contribute significantly to the contemporary literature on AI adoption and cybersecurity behavior by integrating AI awareness, digital literacy, responsible AI perception, trust, and perceived risk into a unified conceptual framework. The study provides important practical implications for policymakers, cybersecurity practitioners, organizations, and educational institutions. Specifically, the findings suggest that organizations should prioritize cybersecurity awareness initiatives, digital literacy development, responsible AI governance, and transparent AI practices to enhance user confidence and encourage the successful adoption of AI-based cybersecurity systems in increasingly complex digital environments.

Implications

Theoretically, the substantiation of the proposed relationships provides important insights into the role of AI-driven cybersecurity awareness, responsible AI perception, digital literacy, perceived risk, and prior cybersecurity experience in shaping behavioral intention toward AI-based cybersecurity systems. More broadly, the study contributes to the growing literature linking artificial intelligence adoption, cybersecurity behavior, digital literacy, and trust-based technology acceptance frameworks. The findings strengthen existing evidence in the literature suggesting that awareness, competency, and responsible AI governance are critical determinants of users' willingness to adopt emerging AI-enabled technologies (Falowo & Bou Abdo, 2026; Hanson & Ott, 2026).

Additionally, the study contributes to the expanding body of knowledge on AI-based cybersecurity adoption by demonstrating that AI-driven cybersecurity awareness significantly enhances trust in AI-based cybersecurity systems and digital literacy, which subsequently influence behavioral intention to use AI-enabled cybersecurity technologies. This further highlights the importance of cybersecurity awareness as a strategic capability for facilitating technology acceptance in modern digital environments. The findings also extend previous studies on responsible AI by empirically confirming that users' perceptions regarding transparency, fairness, accountability, and ethical AI governance positively influence trust in AI-based cybersecurity systems(Alqahtani et al., 2026; Shabankareh et al., 2025).

Furthermore, the study contributes to the literature on digital literacy and AI adoption by validating the significant mediating role of digital literacy in the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems. The findings indicate that awareness alone may not be sufficient to drive AI adoption unless users possess adequate digital competencies and technological skills. This contribution is particularly important because recent studies have increasingly emphasized that AI literacy and digital literacy are essential for responsible and effective adoption of intelligent technologies (Memarian & Doleck, 2026; Yu et al., 2026). Therefore, the study extends current technology adoption theories by integrating competency-based perspectives into AI-enabled cybersecurity adoption research.

The findings also contribute to cybersecurity behavior literature by confirming the significant negative influence of perceived risk on behavioral intention to use AI-based cybersecurity systems. This demonstrates that concerns regarding privacy, security vulnerabilities, transparency, and operational uncertainty remain important barriers to AI adoption. In addition, the positive influence of prior cybersecurity breach experience on behavioral intention suggests that cybersecurity incidents increase users' motivation to adopt advanced protective technologies, supporting the assumptions of Protection Motivation Theory and cybersecurity awareness frameworks.

Importantly, the study provides empirical evidence that trust in AI-based cybersecurity systems does not significantly mediate the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems. This finding contributes to the ongoing debate regarding the role of trust in AI adoption by suggesting that trust alone may not directly translate into behavioral intention in cybersecurity contexts without sufficient digital competence and technological understanding. Hence, the study offers a nuanced perspective on the complex interaction between trust, awareness, and digital capability in AI-enabled cybersecurity adoption.

Practically, understanding the factors that directly and indirectly influence behavioral intention toward AI-based cybersecurity systems can help organizations, policymakers, educational institutions, and cybersecurity practitioners improve AI adoption strategies and strengthen cybersecurity resilience. The validation of the proposed model demonstrates the importance of investing in AI-driven cybersecurity awareness programs, responsible AI governance practices, and digital literacy development initiatives to encourage users' acceptance of AI-enabled cybersecurity technologies.

The findings suggest that organizations should align their cybersecurity strategies with awareness-building initiatives and digital competency development programs to enhance users' readiness to adopt AI-based cybersecurity systems. Since digital literacy emerged as one of the strongest predictors of behavioral intention, organizations and educational institutions should prioritize digital skill development and AI literacy training to improve users' confidence and competence in interacting with intelligent cybersecurity technologies.

Furthermore, the significant influence of responsible AI perception on trust suggests that organizations implementing AI-driven cybersecurity systems should focus on ethical AI governance, transparency, explainability, and accountability to strengthen users' confidence in AI-enabled technologies. Developers and cybersecurity practitioners should also reduce users' perceived risks by implementing robust privacy protection mechanisms, transparent AI decision-making processes, and effective cybersecurity policies.

Given the substantial influence of AI-driven cybersecurity awareness and digital literacy on behavioral intention to use AI-based cybersecurity systems, the findings emphasize the strategic importance of continuous cybersecurity education, AI literacy development, and awareness campaigns in modern digital environments. Such initiatives may significantly improve users' acceptance of AI-enabled cybersecurity technologies and enhance organizational cybersecurity preparedness in response to evolving cyber threats.

Conclusion

The literature on artificial intelligence adoption and cybersecurity behavior demonstrated the growing importance of AI-driven cybersecurity awareness, responsible AI perception, trust, and digital literacy in influencing users' acceptance of AI-based cybersecurity systems. However, limited studies have integrated these constructs into a comprehensive framework to explain behavioral intention toward AI-enabled cybersecurity technologies. This paper presents one of the early attempts to develop and empirically test an integrated Trust–Awareness–Competency Framework that links AI-driven cybersecurity awareness, responsible AI perception, digital literacy, perceived risk, prior cybersecurity breach experience, and behavioral intention to use AI-based cybersecurity systems.

This research contributes to the artificial intelligence, cybersecurity, and technology adoption literature by demonstrating that AI-driven cybersecurity awareness significantly enhances trust in AI-based cybersecurity systems, improves digital literacy, and positively influences behavioral intention to use AI-enabled cybersecurity technologies. The findings further reveal that digital literacy plays a significant mediating role in strengthening the relationship between AI-driven cybersecurity awareness and behavioral intention to use AI-based cybersecurity systems. In contrast, perceived risk negatively influences users' adoption intentions, while trust in AI-based cybersecurity systems does not directly predict behavioral intention.

The findings of this research indicate that cybersecurity awareness and digital literacy are critical capabilities for the successful adoption of AI-based cybersecurity systems. The study further demonstrates that responsible AI perception is essential for building users' trust in AI-enabled cybersecurity technologies. These findings reinforce the importance of integrating responsible AI governance, digital competency development, and cybersecurity awareness initiatives into organizational cybersecurity strategies.

Policymakers, cybersecurity practitioners, educational institutions, and organizational managers should develop deliberate strategies to foster AI-driven cybersecurity awareness and strengthen digital literacy among users and employees. Organizations should also promote responsible AI practices by ensuring transparency, accountability, fairness, and ethical governance in AI-enabled cybersecurity systems. Furthermore, leadership and top management should provide a clear vision regarding the strategic importance of AI-based cybersecurity technologies and encourage continuous cybersecurity education and AI literacy development programs. Such initiatives may significantly enhance users' confidence, reduce perceived risks, and improve the successful adoption of AI-driven cybersecurity systems in increasingly complex digital environments.

Research Limitations and Future Research Directions

The present study has several limitations that should be acknowledged. First, the data were collected from users and professionals within a specific technological and cybersecurity context; therefore, the generalizability of the findings may be limited. Future studies should replicate the proposed model across different countries, industries, organizational settings, and cultural environments to validate the consistency and applicability of the findings in diverse contexts.

Second, the current study examined selected determinants of behavioral intention to use AI-based cybersecurity systems, including AI-driven cybersecurity awareness, responsible AI perception, trust, digital literacy, perceived risk, and prior cybersecurity breach experience. Future research should investigate additional factors that may influence AI-based cybersecurity adoption, such as perceived usefulness, perceived ease of use, AI explainability, cybersecurity culture, organizational support, regulatory compliance, privacy concerns, and technology readiness.

Third, the present study adopted a cross-sectional research design, which limits the ability to establish causal relationships among the study variables over time. Future studies are encouraged to employ longitudinal research designs to examine how users' perceptions, trust, awareness, and behavioral intentions toward AI-based cybersecurity systems evolve over time as AI technologies become more advanced and widely adopted.

Fourth, although the study examined the mediating roles of trust in AI-based cybersecurity systems and digital literacy, future studies may explore additional mediating and moderating variables such as AI literacy, cybersecurity resilience, organizational trust, self-efficacy, perceived transparency, and ethical AI governance mechanisms. Such investigations may provide a deeper understanding of the mechanisms through which AI awareness influences cybersecurity technology adoption behavior.

Finally, future research may apply alternative theoretical perspectives and advanced analytical techniques to further extend the understanding of AI-based cybersecurity adoption. Researchers may integrate theories such as the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), Protection Motivation Theory (PMT), Diffusion of Innovation Theory (DOI), or Artificial Intelligence Acceptance Models into future studies. In addition, future studies may employ mixed-method approaches, multi-group analysis, machine learning techniques, or longitudinal SEM approaches to provide richer empirical insights into users' adoption behavior toward AI-based cybersecurity systems.

Declarations

Conflict of Interest

The authors declare that they have no competing interests.

Ethical Approval

This study was reviewed and approved by the Research Ethics Committee of Salaam University, Mogadishu, Somalia. The research was conducted in accordance with applicable ethical principles and institutional guidelines for research involving human participants.

Consent to Participate

Participation in this study was voluntary. Informed consent was obtained from all participants prior to their involvement in the survey. Participants were informed about the purpose of the study, the confidentiality of their responses, and their right to withdraw from the study at any time without any consequences.

Consent to publish

Not applicable

Funding

The authors received no specific funding for this research from any public, commercial, or not for profit funding agency.

Author Contribution

Abdulkadir Jeilani Mohamud conceptualized the study, designed the research framework, performed data analysis, interpreted the findings, and drafted the manuscript. Abdifatah Nour Rage contributed to the research design, literature review, methodology development, and manuscript revision. Mohamed Adam Isak participated in data analysis, validation of results, and critical review of the manuscript. Abdisatar Ibrahim Arabow contributed to the theoretical framework, interpretation of findings, and manuscript editing. Abdiwahab Osman Siad assisted with data validation, methodological review, and critical revisions of the manuscript. All authors reviewed, revised, and approved the final version of the manuscript.

Acknowledgements

The authors would like to express their sincere appreciation to all individuals who contributed to the successful completion of this study. We are particularly grateful to the employees who dedicated their time and effort to provide valuable information. We also extend our gratitude to colleagues and academic peers who provided valuable comments, suggestions, and constructive feedback during the development of the manuscript. Finally, the authors acknowledge the support provided by their respective institutions, which facilitated the completion of this research.

Data Availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

References

1. Abu-Amara F, Almansoori R, Alharbi S, Alharbi M, Alshehhi A. A novel SETA-based gamification framework to raise cybersecurity awareness. Int J Inform Technol. 2021;13(6):2371–80. https://doi.org/10.1007/s41870-021-00760-5.
2. Ajzen I. (1991). The theory of planned behavior. In *Handbook of Theories of Social Psychology: Volume 1* (pp. 438–459). https://doi.org/10.4135/9781446249215.n22
3. Al-Emran M, Griffy-Brown C. The role of technology adoption in sustainable development: Overview, opportunities, challenges, and future research agendas. Technol Soc. 2023;73:102240.
4. Al-Zahrani AA, Al-Salloum OI. Success factors in achieving excellence in cybersecurity (a case study of the Kingdom of Saudi Arabia). Int J Res Stud Publishing. 2025;6(68):59–87.
5. Aldawood HA, Skinner G. (2018). A critical appraisal of contemporary cyber security social engineering solutions: measures, policies, tools and applications. *2018 26th International Conference on Systems Engineering (ICSEng)*, 1–6.
6. Aldawood H, Skinner G. Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. Future Internet. 2019;11(3). https://doi.org/10.3390/fi11030073.
7. Almaiah MA, Alfaisal R, Salloum SA, Hajjej F, Shishakly R, Lutfi A, Alrawad M, Al Mulhem A, Alkhdour T, Al-Maroof RS. Measuring Institutions' Adoption of Artificial Intelligence Applications in Online Learning Environments: Integrating the Innovation Diffusion Theory with Technology Adoption Rate. Electron (Switzerland). 2022;11(20):1–19. https://doi.org/10.3390/electronics11203291.
8. Alqahtani A, Yan J, Vlahu-Gjorgievska E, Cao C. Factors Influencing Citizens' Adoption of AI-Enabled Public Services in Saudi Arabia: The Role of Cybersecurity, Privacy, and Trust. Digit Government: Res Pract. 2026;7(2):1–24.

9. Ammah LNA, Lütge C, Kriebitz A, Ramkissoon L. AI4people – an ethical framework for a good AI society: the Ghana (Ga) perspective. J Inform Communication Ethics Soc. 2024;22(4):453–65. https://doi.org/10.1108/JICES-06-2024-0072.
10. Bahçekapili E, Boztaş GD. (2025). Generative AI and digital literacy: Unravelling user intentions through PLS-SEM and machine learning. J Inform Sci, 01655515251396900.
11. Bandura A. (1986). *SOCIAL FOUNDATIONS Of THOUGHT AND ACTION A Social Cognitive Theory*. http://ereserve.library.utah.edu/Annual/PSY/3960/Gelfand/social1.pdf
12. Bansal G, Axelton Z. Impact of cybersecurity disclosures on stakeholder intentions. J Comput Inform Syst. 2024;64(1):78–91.
13. Bera S, Bera I, Rahut D. (2026). AI adoption among young Indians: an analysis using a MIMIC model. *Humanities and Social Sciences Communications*.
14. Bogoslov IA, Corman S, Lungu AE. Perspectives on artificial intelligence adoption for European union elderly in the context of digital skills development. Sustainability. 2024;16(11):4579.
15. Celik I. Exploring the determinants of artificial intelligence (AI) literacy: Digital divide, computational thinking, cognitive absorption. Telematics Inform. 2023;83:102026.
16. Cetinkaya NE, Krämer N. Between transparency and trust: Identifying key factors in AI system perception. Behav Inform Technol. 2026;45(5):840–54.
17. Chatterjee S, Bhattacharjee KK. Adoption of artificial intelligence in higher education: a quantitative analysis using structural equation modelling. Educ Inform Technol. 2020;25(5):3443–63. https://doi.org/10.1007/s10639-020-10159-7.
18. Chatterjee S, Chaudhuri R, Kamble S, Gupta S, Sivarajah U. Adoption of artificial intelligence and cutting-edge technologies for production system sustainability: a moderator-mediation analysis. Inform Syst Front. 2023;25(5):1779–94.
19. Chedrawi C, Haddad G, Tarhini A, Osta S, Kazoun N. Exploring the impact of responsible AI usage on users' behavioral intentions. J Innov Knowl. 2025;10(6):100813. https://doi.org/10.1016/j.jik.2025.100813.
20. Choung H, David P, Ross A. Trust in AI and its role in the acceptance of AI technologies. Int J Human–Computer Interact. 2023;39(9):1727–39.
21. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly: Manage Inform Syst. 1989;13(3):319–39. https://doi.org/10.2307/249008.
22. de Bruin M. (2022). Individual and Contextual Variables of Cyber Security Behaviour. *ArXiv.Org*, *190230551*.
23. Dwivedi YK. Generative Artificial Intelligence (GenAI) in entrepreneurial education and practice: emerging insights, the GAIN Framework, and research agenda. Int Entrepreneurship Manage J. 2025;21(1):82.
24. Dwivedi YK, Kshetri N, Hughes L, Louise E, Jeyaraj A, Kumar A, Baabdullah AM, Koohang A, Raghavan V, Ahuja M, Albanna H, Ahmad M, Al-busaidi AS, Balakrishnan J, Barlette Y, Basu S, Bose I, Brooks L, Buhalis D, Wright R. International Journal of Information Management Opinion Paper : So what if ChatGPT wrote it ? Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy . Int J Inf Manag. 2023;71(March). https://doi.org/10.1016/j.ijinfomgt.2023.102642.
25. Elmy J, Jizat M. (2012). *Investigating ICT-literacy assessment tools : Developing and validating a new assessment instrument for trainee teachers in Malaysia*. *August*.
26. Erukude ST, Marella VC, Veluru SR. (2025). AI-Driven Cybersecurity Threats: A Survey of Emerging Risks and Defensive Strategies. *International Conference on Data Science and Applications*, 185–197.

27. Falowo OI, Bou Abdo J. Empirical study on automation, ai trust, and framework readiness in cybersecurity incident response. Algorithms. 2026;19(1):62.
28. Featherman MS, Pavlou PA. Predicting e-services adoption: a perceived risk facets perspective. Int J Hum Comput Stud. 2003;59(4):451–74. https://doi.org/https://doi.org/10.1016/S1071-5819(03)00111-3.
29. Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, Luetge C, Madelin R, Pagallo U, Rossi F, Schafer B, Valcke P, Vayena E. AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Mind Mach. 2018;28(4):689–707. https://doi.org/10.1007/s11023-018-9482-5.
30. Fornell C, Larcker DF. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. J Mark Res. 1981;18(1):39. https://doi.org/10.2307/3151312.
31. Fraillon J, Duckworth D. (2025). *Computer and Information Literacy Framework BT - IEA International Computer and Information Literacy Study 2023: Assessment Framework* (J. Fraillon & M. Rožman, editors; pp. 21–34). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61194-0_2
32. Gefen D, Karahanna E, Straub DW. Trust and TAM in Online Shopping: An Integrated Model1. Manage Inform Syst Q. 2003;27(1):51–90. https://doi.org/10.2307/30036519.
33. Glikson E, Woolley AW. Human trust in artificial intelligence: Review of empirical research. Acad Manag Ann. 2020;14(2):627–60.
34. Hair JF, Risher JJ, Sarstedt M, Ringle CM. When to use and how to report the results of PLS-SEM. Eur Bus Rev. 2019;31(1):2–24. https://doi.org/10.1108/EBR-11-2018-0203.
35. Hanson TA, Ott C. Trust in Financial Technology: The Role of Financial Literacy, Digital Financial Literacy, Technological Literacy, and Trust in Artificial Intelligence. J Risk Financial Manage. 2026;19(2):97.
36. Hu LT, Bentler PM. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Struct Equ Model. 1999;6(1):1–55. https://doi.org/10.1080/10705519909540118.
37. Ifinedo P, Vachon F, Ayanso A. Reducing data privacy breaches: an empirical study of relevant antecedents and an outcome. Inform Technol People. 2024;38(4):1712–34. https://doi.org/10.1108/ITP-07-2022-0516.
38. Kajtazi M, Sarker S, Johansson B, Holmberg N, Keller C, Tona O. Toward a Unified Model of Information Security Policy Compliance: A Conceptual Replication Study. AIS Trans Replication Res. 2021;7:1–15. https://doi.org/10.17705/1atrr.00067.
39. Kaur D, Uslu S, Rittichier KJ, Durresi A. Trustworthy artificial intelligence: a review. ACM Comput Surv (CSUR). 2022;55(2):1–38.
40. Kim DJ, Ferrin DL, Rao HR. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decis Support Syst. 2008;44(2):544–64. https://doi.org/https://doi.org/10.1016/j.dss.2007.07.001.
41. Kline RB. (2018). Response to Leslie Hayduk's review of principles and practice of structural equation modeling,1 4th edition. *Canadian Studies in Population*, *45*(3–4), 188–195. https://doi.org/10.25336/csp29418
42. Kock N. Common method bias in PLS-SEM: A full collinearity assessment approach. Int J E-Collaboration. 2015;11(4):1–10. https://doi.org/10.4018/ijec.2015100101.
43. Kruger H, Drevin L, Steyn T. (2006). A framework for evaluating ICT security awareness. Issa, 1–11. icsa.cs.up.ac.za
44. Lan Y, Liu S, Chen H, Xia L. (2026). Configurational effects of personal innovativeness, self-efficacy, and perceived risk on AI adoption in media students. Sci Rep.

45. Lemay DJ, Doleck T. Constructivist educational technology: Re-examining the foundations and state of the literature. Br J Edu Technol. 2020;51(6):1905–6. https://doi.org/10.1111/bjet.13042.
46. Li L, He W, Xu L, Ash I, Anwar M, Yuan X. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. Int J Inf Manag. 2019;45:13–24. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.10.017.
47. McKnight DH, Choudhury V, Kacmar C. Developing and validating trust measures for e-commerce: An integrative typology. Inform Syst Res. 2002;13(3):334–59. https://doi.org/10.1287/isre.13.3.334.81.
48. Milicevic N, Kalas B, Djokic N, Malcic B, Djokic I. Students' intention toward artificial intelligence in the context of digital transformation. Sustainability. 2024;16(9):3554.
49. Mohammadyari S, Singh H. Understanding the effect of e-learning on individual performance: The role of digital literacy. Comput Educ. 2015;82:11–25. https://doi.org/https://doi.org/10.1016/j.compedu.2014.10.025.
50. Müller LS, Nohe C, Reiners S, Becker J, Hertel G. Adopting information systems at work: a longitudinal examination of trust dynamics, antecedents, and outcomes. Behav Inform Technol. 2024;43(6):1096–128.
51. Neumeyer X, Santos SC, Morris MH. Overcoming barriers to technology adoption when fostering entrepreneurship among the poor: The role of technology and digital literacy. IEEE Trans Eng Manage. 2020;68(6):1605–18.
52. Ng W. Can we teach digital natives digital literacy? Comput Educ. 2012;59(3):1065–78.
53. Park YJ, Jones-Jang SM. Surveillance, security, and AI as technological acceptance. AI Soc. 2023;38(6):2667–78.
54. Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers Secur. 2017;66:40–51. https://doi.org/https://doi.org/10.1016/j.cose.2017.01.004.
55. Podsakoff PM, Lee MKSB J. Y., Podsakoff NP. Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. J Appl Psychol. 2003;88(5):879–903.
56. Rogers RW. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Social Psychology: Source Book, 153–76.
57. Salloum SA, Bettayeb A, Salloum A, Aburayya A, Khadragy S, Hamoudi R, Alfaisal R. Novel machine learning based approach for analysing the adoption of metaverse in medical training: A UAE case study. Inf Med Unlocked. 2023;42:101354.
58. Shabankareh M, Sahne K, Nazarian SS, A., Foroudi P. (2025). The impact of AI perceived transparency on trust in AI recommendations in healthcare applications. Asia-Pacific J Bus Adm.
59. Shin D. The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. Int J Hum Comput Stud. 2021;146:102551. https://doi.org/10.1016/j.ijhcs.2020.102551.
60. Shin D. How do people judge the credibility of algorithmic sources? AI Soc. 2022;37(1):81–96.
61. Siddiq F, Hatlevik OE, Olsen RV, Throndsen I, Scherer R. Taking a future perspective by learning from the past–A systematic review of assessment instruments that aim to measure primary and secondary school students' ICT literacy. Educational Res Rev. 2016;19:58–84.
62. Slavova S, Zhauniarovich Y. We Really Need the Help of AI: A Case Study of AI Adoption in Cybersecurity. ACM Transactions on Internet Technology; 2025.
63. Tunmibi S. (2024). Digital competence as predictor for the motivation to use artificial intelligence technologies among librarians in Edo and Delta States, Nigeria. J Technol Innovations Energy.
64. Uchendu B, Nurse JRC, Bada M, Furnell S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers and Security*, *109*. https://doi.org/10.1016/j.cose.2021.102387

65. Valaei N, Rezaei S, Ismail WKW. Examining learning strategies, creativity, and innovation at SMEs using fuzzy set Qualitative Comparative Analysis and PLS path modeling. J Bus Res. 2017;70:224–33.
66. Van Deursen AJAM, Helsper EJ. (2015). *The third-level digital divide: Who benefits most from being online?*.
67. Venkatesh V. Adoption and use of AI tools: a research agenda grounded in UTAUT. Ann Oper Res. 2022;308(1):641–52.
68. Vitezić V, Perić M. The role of digital skills in the acceptance of artificial intelligence. J Bus Industrial Mark. 2024;39(7):1546–66.
69. World Economic Forum Accenture. (2022). Global cybersecurity outlook 2022. In *Insight Report* (Issue Cybersecurity Outlook 2022). https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
70. Yu S, Carroll F, Bentley BL. Rethinking AI literacy education in higher education: Bridging risk perception and responsible adoption. Social Sci Humanit Open. 2026;13:102751.
71. Zhan Y, Ahmad SF, Irshad M, Al-Razgan M, Awwad EM, Ali YA, Ayassrah AY. A. B. A. (2024). Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. *Heliyon*, *10*(1).
72. Zhao X, Tong Y, Lee H, Shahzad U. The role of artificial intelligence in enhancing corporate environmental information disclosure: Implications for energy transition and sustainable development. Energy Econ. 2025;148(April):108680. https://doi.org/10.1016/j.eneco.2025.108680.

Figures

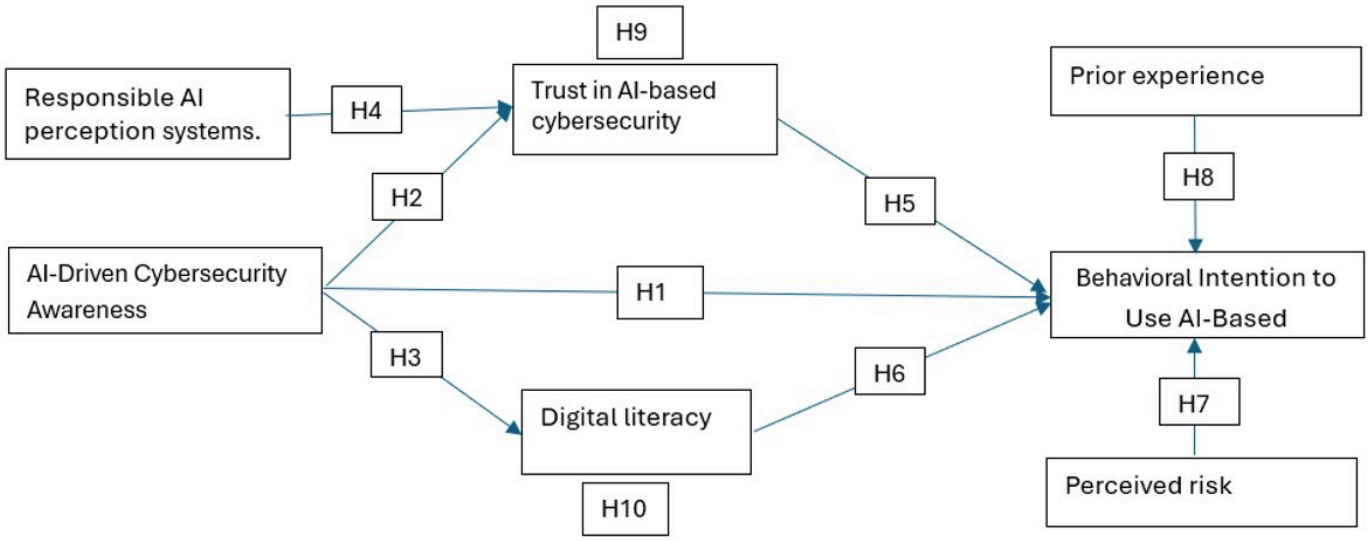


Figure 1

Research Model

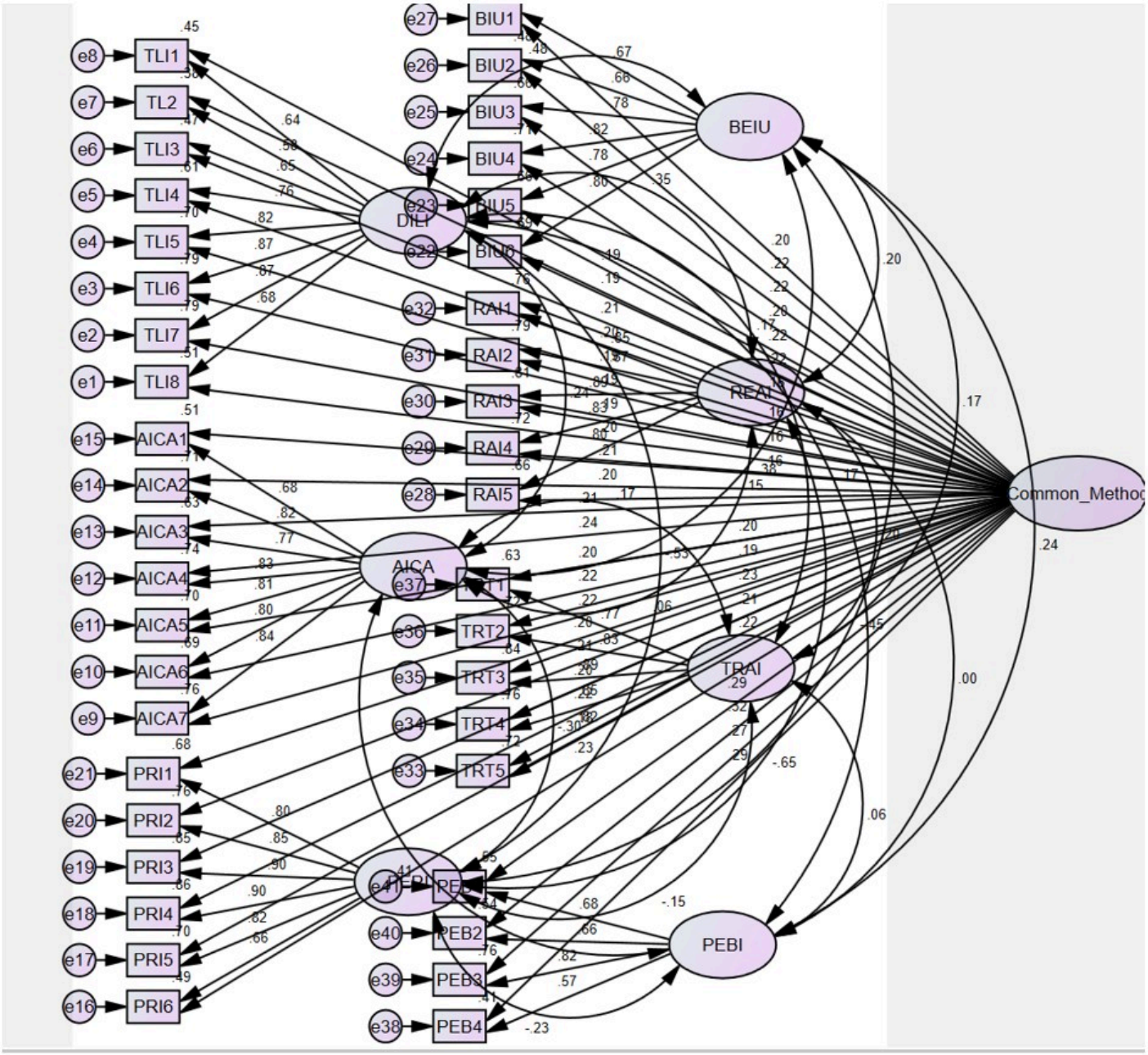


Figure 2

Common method bias

Note: AICA = AI-Driven Cybersecurity Awareness; TRAI = Trust in AI-Based Cybersecurity Systems; DILI = Digital Literacy; REAI = Responsible AI; PERA = Prior Experience with Breaches; PERI = Perceived Risk; BEIU = Behavioral Intention to Use.

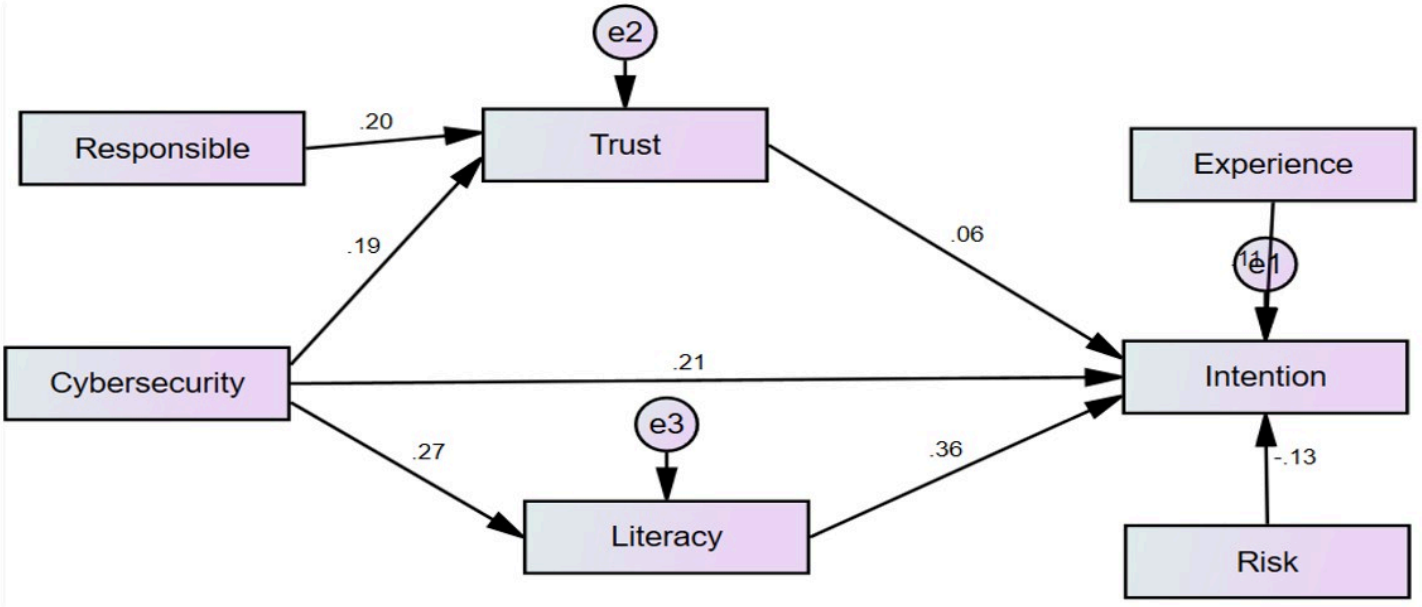


Figure 3

Figure 2. Results of the hypotheses

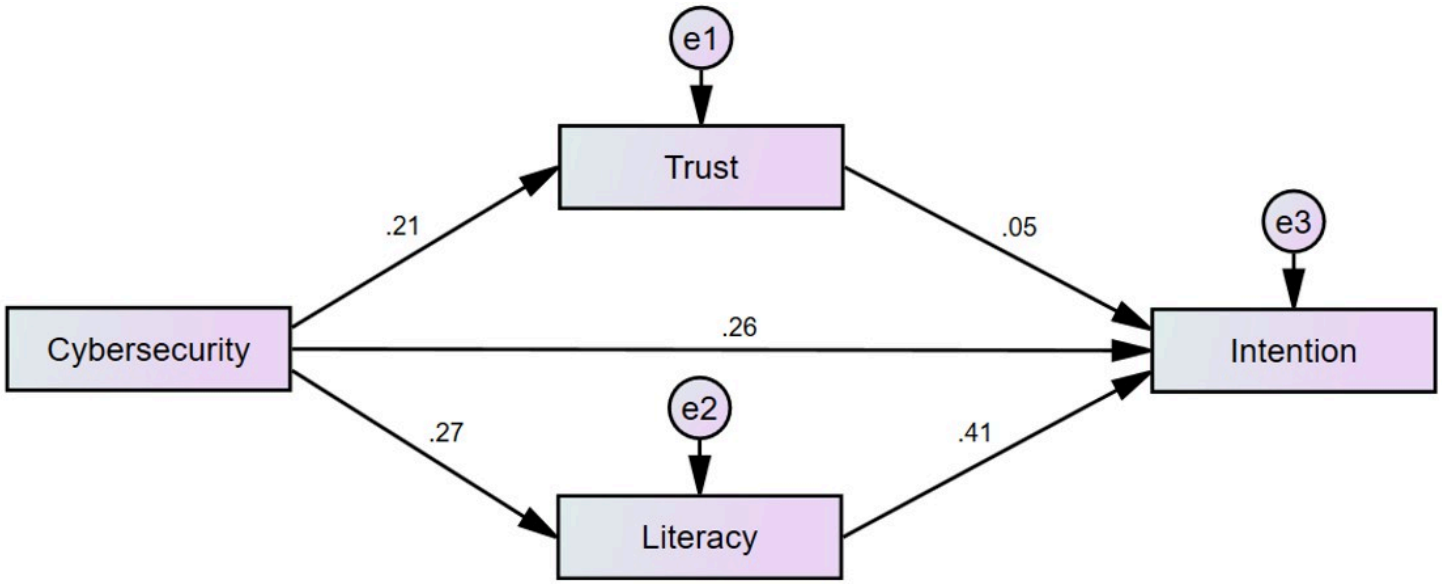


Figure 4

Figure 3. Mediation analysis

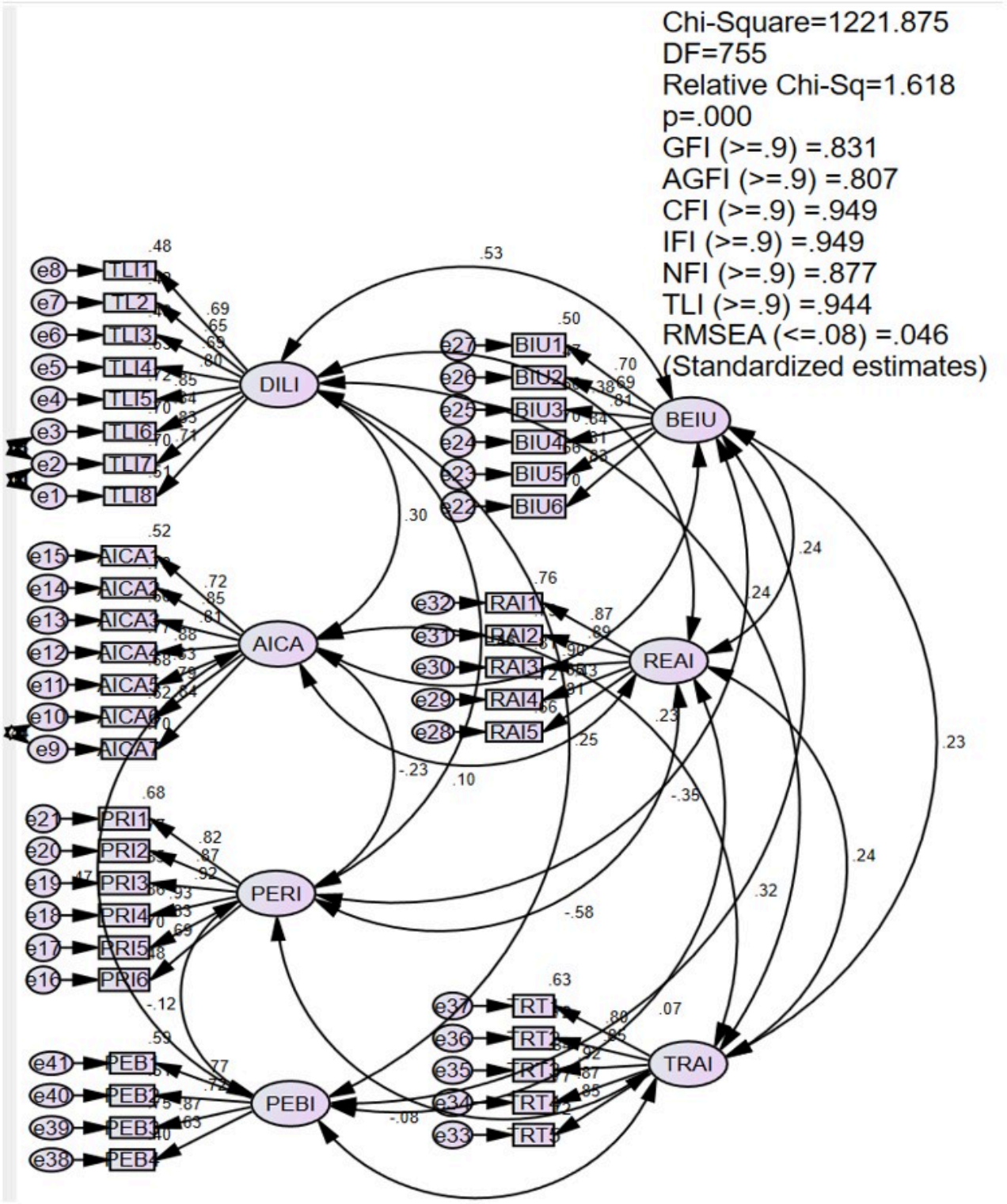


Figure 5

Figure 4. Goodness fit index

Note: AICA = AI-Driven Cybersecurity Awareness; TRAI = Trust in AI-Based Cybersecurity Systems; DILI = Digital Literacy; REAI = Responsible AI; PERA = Prior Experience with Breaches; PERI = Perceived Risk; BEIU = Behavioral Intention to Use.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Appendices.docx