ACADEMIA International Journal for Social Sciences
Volume 5, Issue 2(a), 2026 ISSN-L (Online): 3006-6638

AI Chatbots and their Perceived Effectiveness in Cybersecurity: Students' Perspective

Aatika Asif
aatikaasif592@gmail.com
BSCYS Scholar, Air University Multan Campus, Islamabad, Pakistan

Laiba Sattar
laibasattar95@gmail.com
BSCYS Scholar, Air University Multan Campus, Islamabad, Pakistan

Sara Saleem
sarasaleem7600@gmail.com
BSCYS Scholar, Air University Multan Campus, Islamabad, Pakistan

Dr. Muhammad Arfan Lodhi
samaritan_as@hotmail.com
Higher Education Department, Punjab, Pakistan

Corresponding Author: * Dr. Muhammad Arfan Lodhi samaritan_as@hotmail.com

Received: 23-12-2025 **Revised:** 11-01-2026 **Accepted:** 24-01-2026 **Published:** 15-02-2026

ABSTRACT

The rise of the use of AI chatbots in higher education is gaining interest regarding the potential usefulness and impact of chatbots on the education provided in technical fields, especially cybersecurity. Despite the fact that many educational institutions are using such tools as ChatGPT, Gemini, and Copilot, actual empirical data related to the perceptions about the effectiveness of AI chatbots by cybersecurity students in developing countries is still limited. The goal of this study is to determine the perceived effectiveness of AI chatbots on the cybersecurity education of university students in Pakistan, based upon the Technology Acceptance Model (TAM), Constructivist Learning Theory, and Cognitive Load Theory. The study utilized a quantitative, descriptive survey design with data collected via a structured questionnaire that used a 5-point Likert-scale from 83 students situated in several universities. The instrument used in this study assessed five dimensions of awareness and knowledge, perceived usefulness, frequency of use, quality of response, challenges and limitations that students faced when using AI chatbots, and perceived academic performance. Based on the findings, there appears to be a general consensus among students that they have a moderate-high level of awareness of AI chatbots (M = 3.91 - 4.00), and that they believe these tools would be beneficial for their learning of cyber security (M = 3.84 - 4.02). Students reported being engaged with AI chatbots with a high frequency for all three applications; course assistance (M = 3.85), exam study (M = 3.95), and referring friends/peers (M = 3.78). The quality of responses from AI chatbots was rated positively by students (M = 3.92 - 4.10), but students also acknowledged some of the challenges to using the chatbot such as misinformation, difficulty verifying information, and over-reliance on critical thinking (M = 3.82 - 4.15). Finally, students had the highest scores (M = 3.88 - 4.10) for perceived academic performance. Overall, these findings confirm hypotheses H1 and H2 by providing evidence that using AI chatbots has a positive relationship with students' perceived learning outcomes for cyber security education.

Keywords: *AI Chatbots, Cybersecurity Education, Higher Education, Learning Effectiveness; AI integrated platforms*

INTRODUCTION

Background of the Study

As technology has developed, there have been drastic changes in global education both positively and negatively. The rise of digital technology has led to the extensive integration of artificial intelligence (AI) into both the classroom and as an educational supplement supporting student processes. Digital technologies such as AI chatbots increase student engagement while simultaneously providing immediate feedback. Cybersecurity is a prime example where ongoing developments cause student's difficulty in developing relevant content for practical application related to abstract, real-world scenarios. The increasing use of AI tools such as ChatGPT, Copilot, Gemini, and Claude to assist students with coding, understanding complex concepts, scenario-based problem solving, and self-directed study proves that AI chatbots provide meaningful support across STEM disciplines (Schei et al.2024). However, the examination of the effectiveness of AI chatbots specifically within cybersecurity has not been adequately researched, and therefore lacks detailed information concerning how effective they are as supplementary learning resources for cybersecurity students in higher education (Deng & Yu, 2023; Davar et al. 2025).

Rational of the Study

AI chatbots have seen increasing integration into academic environments; however, there is limited empirical evidence on their effectiveness in aiding cybersecurity education. Most research has focused on various subjects that do not fall within the realm of technical learning outcomes, such as writing, mathematics, and language development. Most studies also tend to assess how usable the technology is rather than measuring how much AI chatbots can help increase understanding and problem-solving capabilities (Davis, 1989; Schei et al., 2025). In addition to this, it is hard to assess whether students who utilize AI chatbots are gaining an advantage in their technical abilities and improving their academic success (by enhancing their own self-directed learning styles) because there are very few resources available for cybersecurity education, particularly in developing countries like Pakistan. In order to accurately evaluate the effectiveness of AI chatbots in these environments, a survey-based approach using empirical research (with data collected from humans) must be utilized.

Research Gap

AI technologies are being used increasingly in all industries, yet the amount of empirical research measuring their effect specifically in higher education for cybersecurity is still quite limited. The majority of existing studies has focused on perceived benefit and eases of use, as well as general engagement, and do not examine the impact of AI on learning outcomes for courses with significant technical content (Shawar& Atwell, 2022; McGrath et al. (2024). This research addresses the gap by providing empirical evidence of students' perceptions related to their use of AI chatbots in a cybersecurity program at Pakistani universities, with regard to learning engagement, conceptual understanding, and perceived academic performance.

Research Objectives

The purpose of this study is fourfold:

1. To establish what percentage of undergraduate students studying cybersecurity utilize AI chatbots for academic purposes.

2. To assess the effectiveness of AI chatbots as tools for helping undergraduates enhance their understanding of cybersecurity concepts and their relationship with technical skills.

3. To determine whether or not there are correlations between undergraduate student use of AI chatbots and perceived levels of academic success in cybersecurity courses.

4. To identify those variables associated with undergraduate students' assessments of how AI chatbots can help enhance their cybersecurity education.

Research Questions

1. How frequently do students that enroll into Cybersecurity program utilize AI chatbots?

2. What do students think about using chatbots to enhance their knowledge of Cybersecurity concepts?

3. Do students see a statistically significant relationship between utilizing chatbots with perceived overall performance scores from Cybersecurity classes?

4. What are the factors that shape how students view the effectiveness of chatbot's ability to provide an education in Cybersecurity?

Hypotheses

Based on the Technology Acceptance Model (TAM), as supported by the empirical literature completed to date, the present research proposes the following hypotheses:

H1: Students have a positive degree of perceived effectiveness for using AI chatbots within their instruction for a given topic in their respective breadth of knowledge of cybersecurity.

H2: Students have a positive relationship to perceived academic performance when using AI chatbots in cybersecurity courses.

H0: There is no statistically significant relationship between the use of AI chatbots and perceived student learning outcomes related to cybersecurity education.

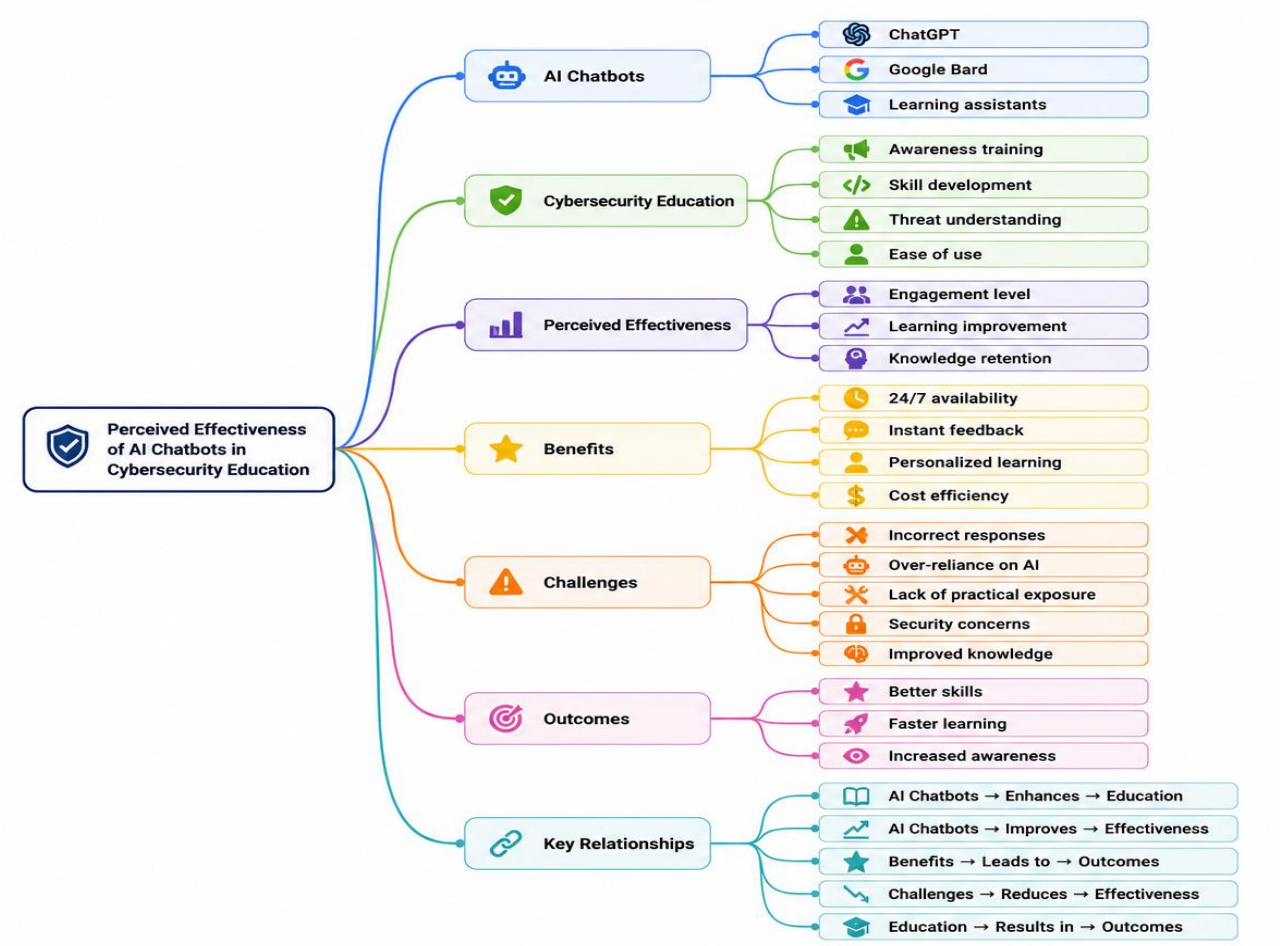


Figure 1: Theoretical Framework

LITERATURE REVIEW

The introduction of Artificial Intelligence (AI) chatbots rapidly into educational settings has attracted a large amount of scholarly research about their effectiveness in different types of disciplines. This review of literature presents a coordinated synthesis of empirical evidence, theoretical models and frameworks, and conceptual models related to AI chatbots and their impact on student learning in Cybersecurity Educational Programs. This section primarily uses peer-reviewed articles published between 2013 and 2025 to develop an understanding of the perceptions of AI tools held by learners; the factors that affect the effectiveness of AI tools; and the relationship of AI tools to established educational theories.

Theoretical Framework

This research on the acceptance of artificial intelligence (AI) chatbots in the cybersecurity education sector utilizes the Technology Acceptance Model (TAM) as its theoretical frame. The TAM model was devised by Davis (1989), who proposed two primary beliefs that help determine whether someone will accept and use a new technology; these are known as Perceived Usefulness (PU) and Perceived Ease-of-Use (PEOU). PU is defined by Davis as how much someone thinks that using the technology will improve their performance of a job or task, while PEOU is defined as how much someone thinks that using the technology will take very little effort. In terms of cybersecurity education, those students who perceive AI Chatbots to provide them value in assisting them in comprehension of a variety of subject areas including network security, ethical hacking, or threats to intelligence are more likely to consistently utilize these types of technology.

The scoping review by Schei, et al. (2024), reviewing 24 empirical articles, found that the TAM constructs—particularly perceived usefulness—emerged as consistent predictors of student engagement with AI chatbots in higher education. The analysis showed that students from different disciplines perceived AI chatbots as facilitating personalized task assistance and providing immediate feedback as highly useful, which was consistent with the core propositions of TAM. In a more recent study by Schei, et al. (2025), it was further determined that students' adoption mindset is greatly influenced by their beliefs regarding AI chatbots enhancing their effectiveness regarding online learning; thus, reinforcing TAM's relevance for studying AI chatbot acceptance within academic contexts, including but not limited to, cybersecurity.

Constructivist Learning Theory

The constructivist theory of learning, developed from the work of Piaget and Vygotsky, suggests that learners build knowledge through their interactions with the environment instead of passively receiving knowledge from others. This is especially important in cybersecurity because it is characterized by the use of hands-on problem solving, scenario thinking, and skill development through practice. When used as interactive tutors, AI chatbots correlate well with constructivist principles through personalized feedback and simulation of real-world threats while also scaffolding learner understanding progressively. The systematic literature review by Kuhail et al. (2022) articles reviewed 36 papers on chatbot-learner interaction design to determine how chatbots are used as peer and teaching agents; the review demonstrated that learners who use chatbots as peer and teaching agents have improved learning outcomes and higher levels of student satisfaction. Furthermore, when chatbots use personalized approaches to learning (which coincide with the use of constructionist scaffolding), these chatbots provide more significant learning outcomes than those that are only based on a predetermined conversation path. Therefore, the current study uses a framework based on constructionist theories for operationalizing perceived skill improvement as the result of learning through chatbot-mediated, interactive cybersecurity.

Cognitive Load Theory

Sweller's Cognitive Load Theory (CLT) divides cognitive load into three categories: intrinsic (the complexity of materials) extraneous (the ineffectiveness of how information is provided), and germane (the cognitive load required to form a schema). Because security education covers technical areas that have high intrinsic cognitive load (e.g., cryptography), this education has strong potential to reduce extraneous cognitive loads (e.g., presenting information poorly) through use of AI chatbots that provide concise context-appropriate information. This would allow for more cognitive resources to be allocated to germane processing (how theories relate). In their narrative accounts, Davar et al. (2025) discuss the efficacy of using AI chatbots (e.g., ChatGPT) as virtual tutoring assistants; therefore, frequent use of AI chatbots to support cybersecurity education should be tested to determine whether such activity correlates to enhanced perceived level of learning in the cybersecurity arena.

Review of the Empirical Studies

There has been a lot of empirical research about chatbots as educational tools with more attention given to the role of chatbots in technical and STEM subjects over the last few years. The following synthesis highlights peer-reviewed literature summarizing some of the most important research studies focusing on the findings, methods used in the studies, contradictions, and research gaps as they relate to the provision of cybersecurity education.

The authors Schei et al. (2024) completed a scoping review of 24 empirical studies that examined students' perceptions and uses of chatbots in higher education and were published between January 2022 and September 2023. The results indicated that research examining student interaction with chatbots is heavily concentrated in Asia and primarily within the STEM fields. As a result, students in

those studies considered chatbots to be very useful in assisting with personal tasks, receiving immediate feedback on their work, and supporting writing/coding all of which are very relevant to cybersecurity coursework. The review also found students have concerns regarding the accuracy and reliability of chatbots and possible effects on critical thinking and creativity when using chatbots. The authors defined these concerns as the duality of using chatbots. This study provides clear support for the current research asitlooksatperceivedusefulnessandwill also address the potentialissue of how perceived effectiveness may not always indicateactual learning or skill gains. In 1989, Davis proposed the Technology Acceptance Model (TAM)throughseveral longitudinal experiments with IBM employees and university students andfound that perceived usefulness was a significantly stronger predictor of actual system use ($\beta = 0.63$) than perceived ease of use ($\beta = 0.45$). Since then, these findings have been replicated inmanydifferent technology adoption contexts, including in educational technology contexts. Because of these findings, the current study's use of Davis' (1989) TAM as the theoretical underpinning for the questionnaire's perceived usefulness and ease of use subscales willprovide support for the hypothesis that students who perceive AI chatbots as being useful will experience a higher level of perceived effectiveness in their cybersecurity education.

Deng and Yu (2023) completed a meta-analysis and systematic review of the use of chatbot technology in the sustainable education field. In conducting this quantitative synthesis of various studies, they found that the collaboration between students and chatbots demonstrated significant measurable advantages for student engagement and the ability to gain knowledge. An additional significant finding from their meta-analysis was that the type of task that students completed determined how effective chatbots will be in helping them achieve desired results. Chatbots performed more effectively with tasks that required only knowledge recall and conceptual explanations than with tasks that combined synthesis and critical evaluation skills.In terms of the cybersecurity education field, where foundational knowledge recall is necessary, as well as advanced analytical reasoning, this finding suggests that using AI chatbots is regarded as being more beneficial when assisting students learning basic security principles than when developing their ability to conduct complex threat analyses.

In their review of 36 studies on chatbot use by learners across Multiple disciplines in education, Kuhail et al., (2022) organized existing research into six categories (educational field, platform, design principles, and chatbots″ function) to develop a model outlining the how these chatbots should function with respect to what a learner will learn effectively from chatbots. Most chatbots designed and utilized were on web-based platforms in order to provide learning for students studying Computer science, Languages, and Engineering with related topics regarding cyber security. More specifically, one-third of the evaluated chatbots, (mainly those utilizing personalized or experiential learning designs) positively impacted learning outcomes and provided positive responses from Users. Additionally, both a lack of training sets, and failure to incorporate usability heuristics were revealed as challenges that caused frustration to Users rather than providing assistance to Users through a computerized chat interface. The article concludes with the important insight that the quality of the chatbots will impact the effectiveness of the use of chatbots. This is an important point for interpreting the self-reported effectiveness data from this study of the effectiveness of different chatbots.

A recent follow-up study by Schei et al. (2025) in Future Business Journal specifically explored student's mindsets towards the adoption of AI chatbot technology regarding its effectiveness at improving online learning experiences in higher education institutions. The findings from this expanded on the previous scoping review by demonstrating that students' mindsets towards the use of AI chatbots in their studies were highly influenced by beliefs about the effectiveness of AI chatbots, the level of support they received from their college, and their personal goals for success. The researchers also found that students who had a growth-oriented mindset regarding technology resulted in providing higher ratings for perceived effectiveness across all measures of effectiveness examined. A significant number (86.7%) of BSCS Cybersecurity students expressed an overall more positive attitude towards emerging technologies; therefore, it is credible to consider baseline levels of the students' adoption

mindset as an essential factor when understanding how much perceived effectiveness they have experienced.

In an article published in Higher Education by McGrath et al. (2024), it was explained how quickly developing the field of generative AI chatbots as a research focus has been within postsecondary educational institutions. They included studies from across many research fields and found that students generally view generative AIs as having positive attributes such as accessibility and ease of use, but that institutional-level characteristics (e.g., assessment procedures/policies, physical infrastructure issues, and faculty member attitudes) can be highly influential on the impact generative AI chatbots have on student learning outcomes. This is especially significant to this study's purpose — to compare students at public and private universities in Pakistan; institutions that function under very different policies concerning all outlined institutional characteristics. The authors also noted that there is a large gap in research regarding the effectiveness of AI chatbots when used for teaching technical security and cybersecurity curricula; thus, this research is timely.

A systematic review of literature regarding AI chatbots in education by Labadze et al., has been published in the International Journal of Educational Technology in Higher Education and reviewed 67 studies related to AI chatbots as tools to assist students . The systematic review revealed that students mainly derived benefits from AI chatbots with homework and study support as well as receiving personalized learning experiences and developing both academic and technical skills. In terms of teacher perspectives regarding the use of AI chatbots to support their practice, AI chatbots save teachers time by automating tasks and providing pedagogical support; however, the authors indicated that significant challenges also exist to using AI chatbots for education including the reliability of response generated by AI chatbots, the accuracy of responses generated by AI chatbots, and concerns about using AI chatbots in an academic integrity domain. Also, important to keep in mind regarding the use of AI chatbots in cybersecurity education, are the examples of domain-specific risks that exist with AI chatbots sometimes generating inaccurate technical content, indicating a clear disconnect between the perceived effectiveness of the AI chatbots' and actual learning in the technical domain.

Moreover, Tegos and Papadopoulos (2004) offered a comprehensive review of conversational AI in education to evaluate chatbot technology and its related pedagogy. More specifically, they found that the educational benefits offered by chatbots depended, to a large degree, on natural language processing and chatbots' conversational design. Chatbots that used more complex dialogue management systems produced higher quality educational experiences than those that used less sophisticated systems. CG authors identified another significant issue that exists in technical fields—chatbots that are trained on general corpora generally do not perform well when presented with highly specific vocabulary; this problem is also present in cybersecurity where there is a rapidly changing vocabulary resulting from the constantly evolving threat landscape. As such, the upper hand may be held by domain-specific AI tools, rather than general-purpose chatbots, when it comes to facilitating cybersecurity education, and students were provided space on the present study's questionnaire to indicate the type of chatbot tools they used.

Furthermore, Davar et al. (2025) published a comprehensive narrative overview of the various benefits and challenges of using chatbots for educational applications within the area of data integrity and safety; ethical standards of academic integrity; and the problem of dependence on AI-powered chatbots in their research article for the Journal of Information Sciences "Comprehensive Narrative Overview of the Use of AI-Powered chatbots". They found that by using chatbots as virtual tutors within a highly adaptive style of learning, students can expect to see improvements in their ability to code/program computer languages, understand complicated concepts, and complete complex assignments that require performing research on many topics - all things relevant to students enrolled in a BSCS program studying cybersecurity. Additionally, data integrity and safety will greatly influence the future integration of AI-powered chatbots within a learning environment - issues that will be critical when teaching students about the problems related to using these technologies in professional areas. This

study highlighted that when integrating AI into a deeper learning environment, the developers must give equal weight to the ethical implications and risks associated with implementing any developing technologies.

Yang and Yu published "Ethical Considerations and Student Sentiment of ChatGPT Use in Education" in the International Journal of Information and Communication Technology Education (2024). The researchers applied a sentiment analysis methodology to analyze the student responses, and while the majority of students had a positive opinion of ChatGPT, there was a small portion of students that shared concerns about plagiarism, fairness and loss of authentic learning. Additionally, the researchers found differences in male and female student responses: males tended to be more optimistic about ChatGPT and reported greater confidence in their ability to utilize AI tools, while females were more likely to indicate uncertainty and ethical concerns about AI use; these findings shape the interpretation of the gender-differentiated perceived effectiveness scores in the current BSCS population. Yang & Yu's (2024) research is an important contribution to the research on gender differences in education and provides further support to help interpret the results from both genders and from the BSCS research participants.

The study conducted by Kowalski and colleagues (2013) represents one of the few studies that have examined the use of conversational agents for security training (in this case, chatbots) within IFIP Advances in Information and Communication Technology. Kowalski and colleagues evaluated the effectiveness of chatbot-based training modules for social engineering awareness and password security practices relative to traditional instructional materials. They found that chatbots were much more effective than traditional instructional materials in helping trainees identify phishing attempts, and that they significantly improved trainees' ability to adopt and use secure behavioral practices. The ability to practice scenarios multiple times through the use of chatbots is an addition that greatly enhances the iterative skill-building necessary for cybersecurity-related education. This early study helped set the groundwork for additional empirical support for the effectiveness of conversational AI tools for the delivery of cybersecurity training, and therefore provides a useful basis for the present study focusing on the experiences of future BSCS graduates in their cybersecurity learning experiences.

Table 1: Summary of Contradictions and Identified Gap

Author/s	Year	Topic	Findings	Rational
Davis	1989	Technology Acceptance Model (TAM)	PU is stronger predictor of system use than PEOU; PU (β=0.63), PEOU (β=0.45).	Does not address AI chatbots or cybersecurity education specifically.
Schei et al.	2024	Student perceptions of AI chatbots in higher education	PU strongly predicts engagement; chatbots provide feedback & task help; concerns about accuracy & critical thinking.	Limited focus on cybersecurity-specific learning contexts; mainly STEM/Asia-based samples.
Kuhail et al.	2022	Chatbot design & learner interaction	Personalized/chatbot-as-tutor improves learning & satisfaction; design quality is crucial.	Lack of domain-specific analysis (especially cybersecurity);

Deng & Yu	2023	Meta-analysis of chatbot use in education	Chatbots improve engagement & knowledge acquisition; more effective for basic recall than higher-order thinking.	Limited evidence on advanced cognitive skill development (e.g., analysis in cybersecurity).
Schei et al.	2025	AI chatbot adoption mindset	Adoption mindset strongly affects perceived learning effectiveness; growth mindset users report higher benefits.	Does not isolate discipline-specific effects (e.g., cybersecurity students).
McGrath et al.	2024	Generative AI in higher education	Positive student perception; institutional factors strongly affect outcomes.	Lack of cybersecurity-focused curriculum research; limited regional studies (e.g., Pakistan).
Labadze et al.	2023	Systematic review of AI chatbots in education	Chatbots support learning, personalization, and efficiency; concerns about accuracy & integrity.	Limited subject-specific evidence; cybersecurity risks of misinformation underexplored.
Tegos& Papadopoulos	2024	Conversational AI in education	NLP quality and design strongly affect learning outcomes; domain-specific vocabulary issues exist.	Poor performance in specialized domains like cybersecurity due to generic training data.
Davar et al.	2025	AI chatbots in education (narrative review)	Chatbots reduce cognitive load and support adaptive learning; privacy/security concerns exist.	Lack of empirical studies on cybersecurity education and risk-aware learning contexts.
Yang & Yu	2024	Student sentiment toward ChatGPT	Overall positive sentiment; ethical concerns (plagiarism, fairness); gender differences observed.	Limited focus on technical disciplines like cybersecurity; lacks performance-based outcomes.
Kowalski et al.	2013	Chatbots for cybersecurity training	Chatbot training improves phishing detection & security behavior via scenario practice.	Pre-generative AI era; outdated compared to modern LLM-based chatbots.

The literature highlights various conflicting issues. Most articles that have reported people's opinions about AI chatbots are positive regarding their use as a tool in education (e.g., Schei et al., 2024; Labadze et al., 2023; Davar et al., 2025) but discuss questions of: accuracy, critical thinking and academic integrity both of which are positive opinions suggesting that usage of the tool has the ability to provide meaningful, genuine educational value. Many studies disagree whether perceived usefulness or ease-of-use will be the strongest predictor of usage based on the Technology Acceptance Model (Davis, 1989); however, those studies which discuss the relationship of interaction quality also suggest either is potentially equal to or stronger than the influence of perceived usefulness when it comes to technical environments (Kuhail et al., 2022; Tegos& Papadopoulos, 2024). Additionally, studies conducted

outside of North America have identified gender differences in how people perceive chatbots (Yang & Yu, 2024) but never specifically looked at them as it relates to cybersecurity. Finally, there continues to be a lack of research regarding how BSCS undergraduate students perceive AI chatbots in a developing country, with regards to moderating effects of university type (i.e., private versus public). By focusing on these gaps, this study's goal is to fill a gap in the literature pertaining to AI chatbots.

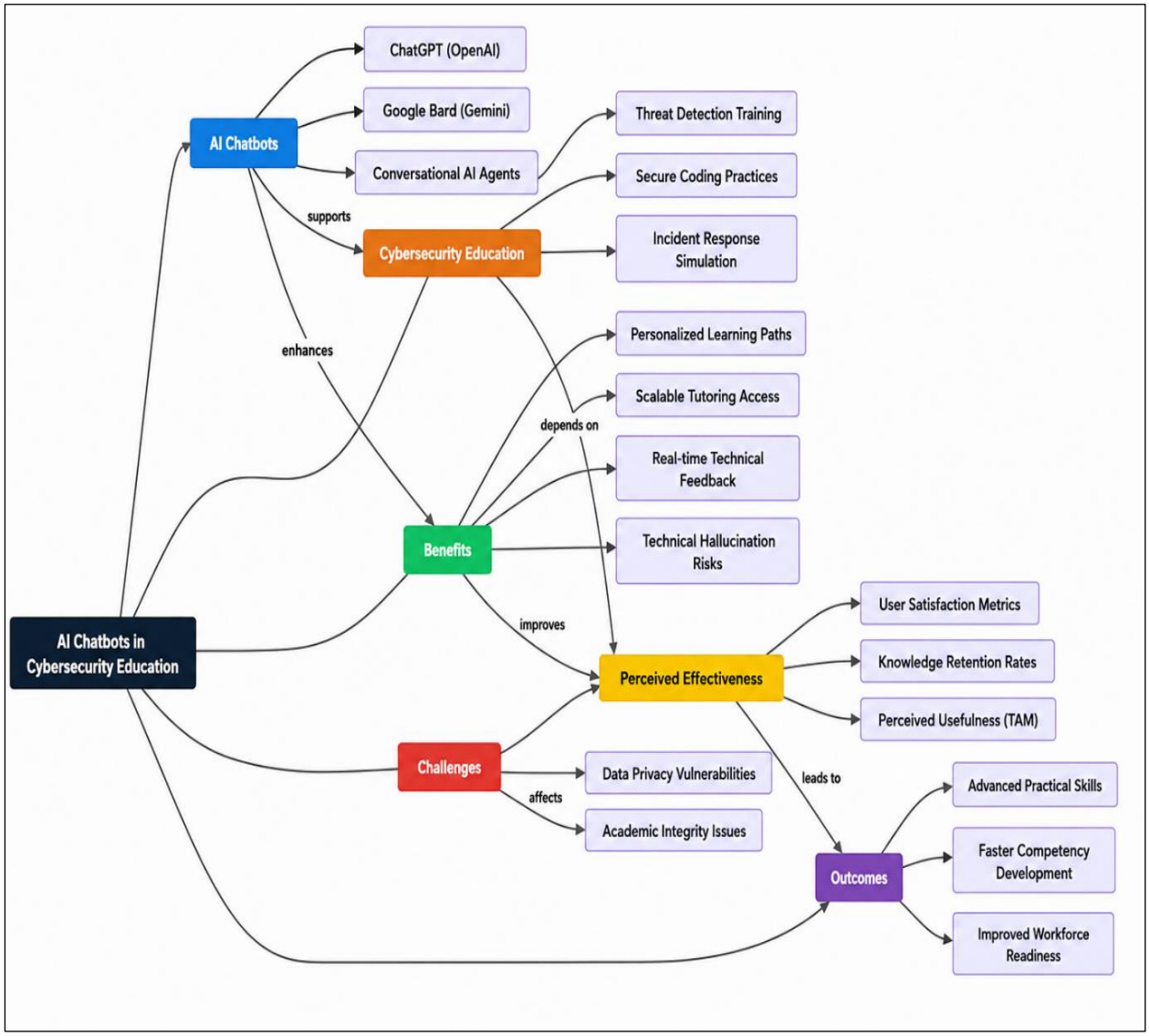


Figure 2: Methodological Framework

Conceptual Framework

The conceptual framework for this study integrates the Technology Acceptance Model (Davis, 1989), Constructivist Learning Theory, and Cognitive Load Theory to propose hypothesized relationships among key variables in the context of AI chatbot use among BSCS students in cybersecurity courses. The framework is further informed by the empirical landscape reviewed above, particularly the findings of Schei et al. (2024, 2025), Labadze et al. (2023), and Davar et al. (2025).

The primary independent variable is the Frequency of AI Chatbot Usage, operationalized as the number of times per week a student interacts with an AI tool (such as ChatGPT, Copilot, or Gemini) for

cybersecurity-related learning tasks. These variable captures both the breadth and regularity of AI-mediated learning behaviors and is grounded in the TAM assumption that behavioral intention to use a technology is reflected in actual usage frequency. The primary dependent variable is Perceived Effectiveness in Cybersecurity Education, a composite measure encompassing three dimensions: (a) perceived understanding of cybersecurity concepts, (b) perceived improvement in technical skills such as threat analysis and vulnerability assessment, and (c) perceived enhancement of academic performance. These dimensions directly reflect the three student benefit areas identified by Labadze et al. (2023) study assistance, personalized learning, and skill development and are measured through structured Likert-scale items.

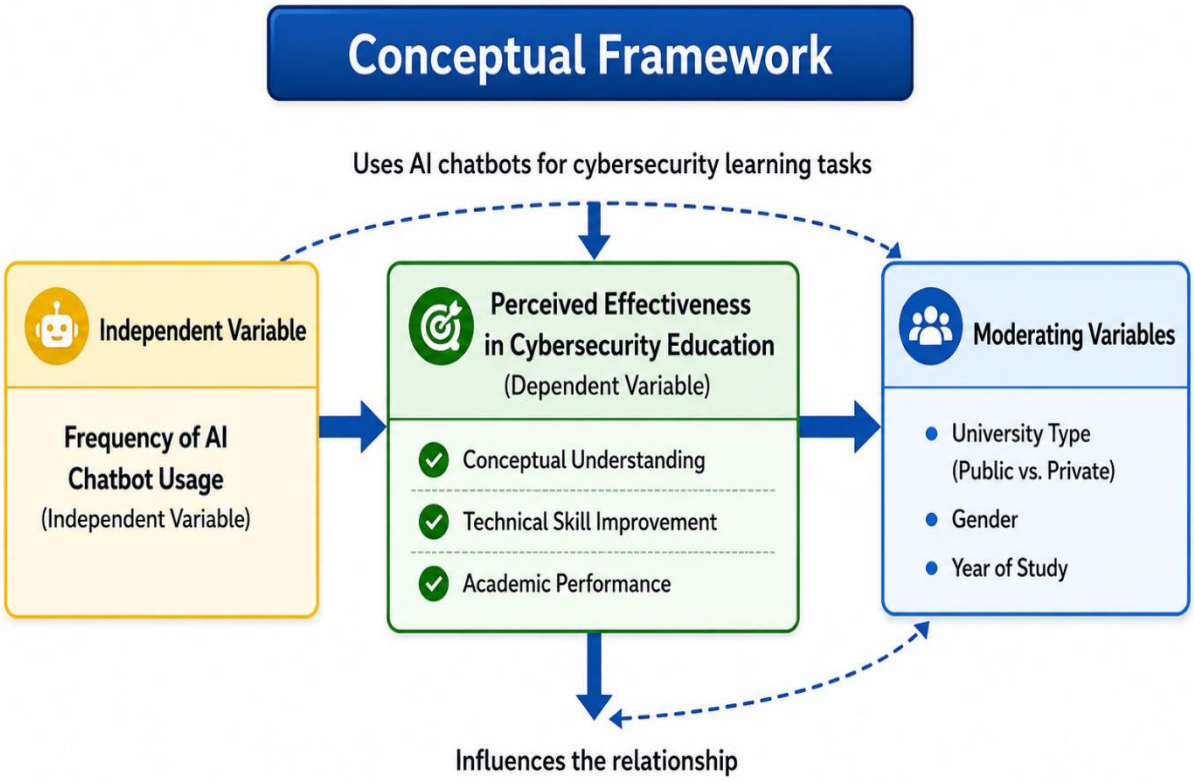


Figure 3. Conceptual Framework

METHODOLOGY

This section delineates the research design, population and sampling procedures, instrumentation, validity and reliability measures, data collection procedures, and analytical techniques employed in this study. The methodology is designed to rigorously examine the perceived effectiveness of AI chatbots in cybersecurity education among BSCS students, ensuring that findings are both scientifically credible and practically meaningful. Figure 2 below provides an overview of the complete methodological framework before each component is described in detail.

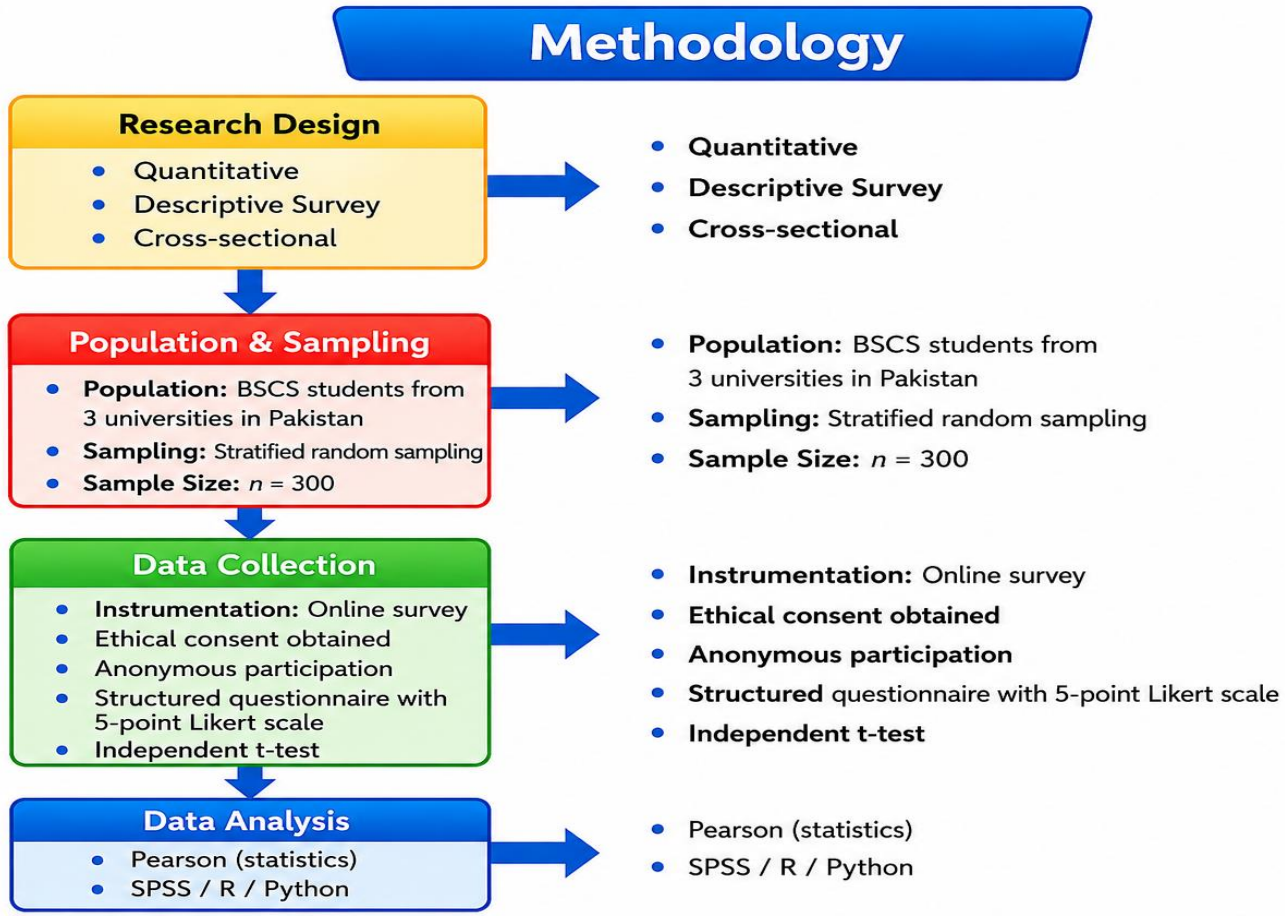


Figure 4. Research Methods

Research Design

This study employs a quantitative descriptive survey design using a cross-sectional research approach. A quantitative approach is appropriate because the objectives of this study are directed at measuring the nature and strength of relationships between numerically operationalized variables, testing a priori hypotheses, and producing generalizable results; all are better suited to a structured data collection and statistical inference than to a qualitative approach. The design of this survey is descriptive in nature, as it seeks to capture students' perceptions, attitudes, and self-reported behaviors at a single moment in time, free from any manipulation by the researcher. This design supports the objective of the research, which is to describe the current status of AI chatbot use and perceived effectiveness by BSCS students, and this is consistent with the methodology employed in other important studies reviewed for this study, including Schei et al. (2024) and Labadze et al. (2023), both of which utilized survey-based and review methodologies to describe how students perceive AI across large samples.

Population and Sampling

The Bachelor of Science in Computer Science (BSCS) target population at the study comprises of all currently enrolled BSCS at three different universities in Punjab, Pakistan: two public sector universities (University of the Punjab and Bahauddin Zakariya University) and one private sector university (COMSATS University Islamabad, Lahore Campus). These schools were chosen to create an overall picture of all that is public and private higher education within Pakistan with BS in CS programs containing cybersecurity courses in their BSCS curriculum. A stratified random sampling technique has been utilized where the entire population of BSCS students was first separated into mutually exclusive

strata (based on their school and year/level) and then a proportional random sample taken from each stratum. This will ensure the final total sample has an adequate representation of all meaningful subgroups and has less likelihood of a convenience sampling bias compared to using a convenience sampling method; this limitation was noted in many studies reviewed (Schei et al., 2024). According to Krejcie and Morgan's (1970) Sample Size Table, with a population of approximately 3,000 BSCS students from the three institutions combined, n = 300 (300 total bar 100 from each university), will allow a confidence level of 95% with a margin of error of 5.5%. Based on prescriptive power analysis parameters, $\alpha = 0.05$, with at least 80% power, n = 300 will yield valid results for detecting medium-sized correlations ($r \geq 0.18$) and significant group differences in ANOVA ($f \geq 0.15$).

Instrumentation

A standardized self-administered questionnaire specifically developed for this study will be used to collect data. A 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) will be used for the attitudinal and perceptual items in the questionnaire in accordance with the ways measurement has been carried out for these areas in the literature (Davis, 1989; Schei et al., 2024). The items were adapted from validated measures used in prior research as well as based on the three areas of student benefits identified by Labadze et al. (2023) – study help, personalized learning, and skill development. The instrument will have four sections.

Section A: Awareness and Knowledge of AI Chatbots

The purpose of this portion of the study was to assess students' knowledge of AI chatbots and cyber security-focused tools such as ChatGPT, Gemini, and Copilot, identify how knowledgeable students are with the differences between general and domain specific chatbots; determine levels of student awareness regarding the limitations of chatbots. This portion of the research utilized a 5-point Likert Scale (1 = Strongly Disagree to 5 = Strongly Agree).

Section B: Perceived Usefulness in Cybersecurity Learning

This section has 6 items that assess the perception about using an AI Chatbot to learn about Cybersecurity, such as: understanding concepts; enhancing learning experience; providing accurate information; assisting in problem-solving; complementing traditional education; and helping with hands-on tasks (labs, configurations, etc.). Each item is measured on a scale of 1 to 5, with 1 being Strongly Disagree and 5 being Strongly Agree.

Section C: Frequency of Use and Engagement

This part includes items that assess how often students use an AI chatbot for their academic tasks related to cyberspace, whether it is to assist them with course materials, ask about a challenging topic, prepare for an exam, or ask a peer for a recommendation. This section uses a five-point frequency scale where '1' indicates never and '5' indicates always.

Section D: Quality and Effectiveness of AI Responses

In this part, items evaluate students' views of how well an AI chatbot provides responses. Items will evaluate whether or not the explanations provided are of high quality, accurate, appropriate for an academic level, clear and whether the examples provided were relevant for cyberspace. This part uses a five-point quality scale where '1' indicates very poor and '5' indicates excellent.

Section E: Challenges and Limitations

There are 5 items in this section that measure how aware students are of the disadvantages linked with using AI chatbots such as giving misinformation; giving students difficulty verifying responses; giving students dangerous advice; providing privacy & data security issues; creating an overreliance on the AI chatbot which could block their ability to think critically. A (1 = Strongly Disagree; 5 = Strongly Agree) Scale will be employed to rate responses to these 5 items.

Section F: Perceived Academic Performance

This is the main outcome section ofthis study and contains 5 items measuring howmuchstudentsfeel their academic performanceimproved due to the use of the AI chatbot.The5 items in this section measure students: (a) how much they improved their understanding of course material;(b) received higher grades;(c)increased confidence whentakingexams;(d)completedbetter assignments; (e) overall improvement in theiracademicperformanceoverallrelatedto cyber security course(s). A (1 = Strongly Disagree; 5 = Strongly Agree) Scale will be used for evaluating responses for each of the 5 items in Section F.

Validity and Reliability

There will be a panel of 5 subject matter experts to establish the content validity of this instrument. This panel will consist of 2 Cybersecurity Faculty Members, 2 Educational Technologists with expertise in AI, and 1 Methodologist that specializes in survey research. The experts will evaluate each item independently for relevance, clarity, and representativeness of the construct being measured. The measurement will also have a Content Validity Index (CVI) score of 0.78 or above to determine whether the item has met the minimum criteria for inclusion in the final instrument as recommended by Lynn (1986).

Cronbach's Alpha Coefficient will be used to assess internal consistency reliability. An acceptable level of Internal Consistency for Social Science Research is a score of $\alpha \geq .70$ (Nunnally, 1978); however, for research studies using a scale to test a hypothesis a score of .80 or greater is preferred. The scores for each of the three subscales (i.e., conceptual understanding, improvement in technical skills, and indicators of academic performance) will be evaluated independently as well as the instrument as a whole.

A pilot test will be completed to test item ambiguity, as well as the time required to complete the questionnaire prior to proceeding with the full-scale data collection. A sample of n = 30 BSCS students who do not participate in the main study will pilot the study and provide preliminary reliability estimates. The construct validity of the instrument will be evaluated through Exploratory Factor Analysis using the full sample of subjects to verify that each item loads onto the appropriate subscale.

Data Collection Procedure

Participants will complete a survey, which will be distributed via Google Forms, an online survey tool that allows for easy-to-use mobile compatibility and automatically inputs data to prevent the transcription errors associated with paper-based surveys. Survey links will be disseminated through official university student portals, WhatsApp groups created by students for academic purposes, and faculty course channels in order to maximize the number of individuals who can be recruited from the target population.

Prior to accessing the questionnaire, participants will receive an informed consent statement that contains information regarding the purpose of the research, that their participation is completely voluntary, how their data will be used and what type of data will be collected. Participants will not provide any personal identifying information. Participation will remain strictly anonymous and ethical

consent will be obtained and documented for every response provided. Data collection will take place over a three-week period, with a one-week reminder of the original invitation to complete the survey.

Quality control will include the use of absolute attention-check items incorporated in the questionnaire. If respondents do not pass at least two attention checks, then they will be excluded from data analysis; all data will be downloaded as a .csv file(s), verified for completeness, and imported into SPSS Version 26 for statistical analyses.

Data Analysis Techniques

A structured approach will be followed in completing the data analysis beginning with assessment of descriptive statistics (mean, standard deviation, frequency distributions and percentage) to provide information on all demographic variables, frequency of use items and Likert scale dimensions, as well as normality assessment (skewness and kurtosis) of the variables. In terms of descriptive statistics, frequency distributions, and percentages will also be utilized to provide an overview of how many individuals used AI Chatbot and how the sample used AI Chatbot across the different categories associated with perceived effectiveness.

Pearson correlation coefficients will be used to analyze the strength and direction of the relationship between frequency of use of the AI chatbot and efficacy associated with all four dimensions (Cohen's, 1988; r = 0.10 small; 0.30 medium;0.50 large). Independent samples t-tests will be conducted on each dimension of perceived effectiveness to compare males versus female users and effect size (Cohen's d values) will be reported along with p-values.A one-way ANOVA will compare the perceived effectiveness scores across the three participating universities as well as across the four academic years (i.e., Year 1–4) utilizing Tukey's HSD post-hoc test when the overall F-test is statistically significant. Additionally, eta-squared (η^2) will be reported as the ANOVA effect size measure for each of the ANOVA tests. Finally, a hierarchical multiple regression will assess the impact of frequency of use of AI chatbot (%) to perceived effectiveness (%), controlling for demographic variables, as independent variables in relation to perceived effectiveness (dependent variable). In Model 1, demographic predictors (gender, university type, year of study) will be included. Model 2 will incorporate the frequency of AI chatbot use. The increase in explained variance (ΔR^2) between models reflects the additional value brought by chatbots. SPSS Version 26 will be used for all analyses, verified using additional analysis in Python (Pandas, SciPy). A two-tailed significance level of α=0.05 will be used for all tests and presented in accordance with APA Style 7th edition guidelines.

DATA ANALYSIS AND RESULTS

This section presents the analysis and findings of the data collected through the survey questionnaire. The data has been analyzed using descriptive statistical techniques including frequency, percentage, mean, and standard deviation. The results are presented in the form of tables and graphical representations to provide a clear understanding of students' perceptions regarding the effectiveness of AI chatbots in cybersecurity education.

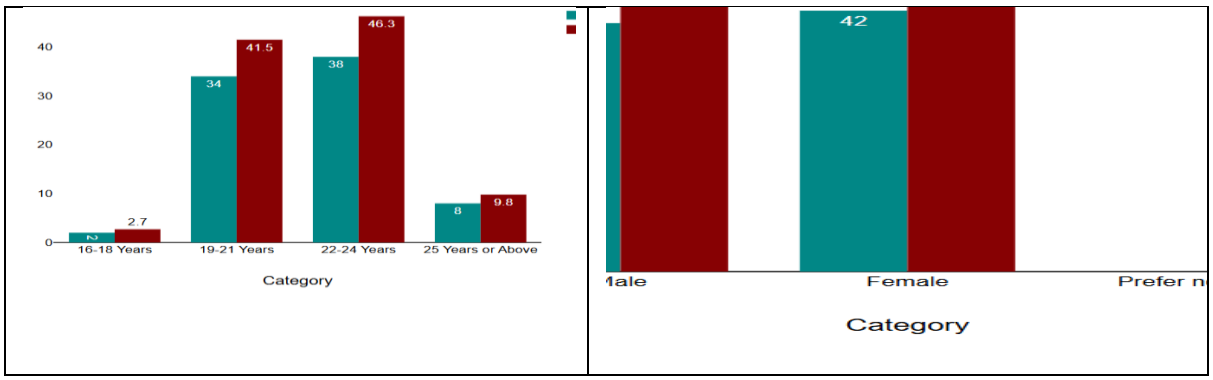
Table 2: Demographic Profile (n = 83)

Variable	*Category*	*Frequency*	*%*
Age	16-18 Years	02	2.7%
	19-21 Years	34	41.5%
	22-24 Years	38	46.3%

	25 Years or Above	08	9.8%
Gender	Male	40	48.8%
	Female	42	51.2%
	Prefer not say	0	0%
University	Air University Multan Campus	45	54.2%
	COMSATS University (Lahore)	10	12%
	Bahauddin Zakariya University	12	14.5%
	The Islamia University of Bahawalpur	5	6.0%
	Government College University Faisalabad	2	2.4%
	Shaheed Zulfiqar Ali Bhutto Medical University Islamabad	1	1.2%
	Muhammad Nawaz Sharif University of Agriculture Multan	4	4.8%
	National Fertilizer Corporation Institute of Engineering & Technology	1	1.2%
Current Semester	$1^{st} – 2^{nd}$	14	16.9%
	3^{rd} - 4^{th}	12	14.5%
	$5^{th} – 6^{th}$	40	48.2%
	$7^{th} – 8^{th}$	17	20.5%
Program of Study	Cyber Security	41	49.4%
	Computer Science	16	19.3%
	Software Engineering	6	7.2%
	Data Science	5	6.0%
	Information Technology	2	2.4%
	Aviation Management	1	1.2%
	Computer Systems Engineering	2	2.4%
	Environmental Science	1	1.2%
	Food Science and Technology	1	1.2%

	English Literature	1	1.2%
	Medical Laboratory Technology	1	1.2%
	Artificial Intelligence	1	1.2%
	Optometry	1	1.2%
AI Chatbot Usage	Yes, regularly	46	56.8%
	Yes, occasionally	22	27.2%
	No, but aware	10	12.3%
	Never	3	3.7%
Cyber Security Study Duration	< 6 months	27	33.8%
	6 months – 1 year	11	13.8%
	1–2 years	12	15.0%
	More than 2 years	37	37.5%

Results from the population data indicate the majority of participants are between the ages of 22–24 (46.3%), followed by the ages of 19–21 (41.5%). The gender distribution among respondents is almost equally proportioned as there are more females (51.2%) than males (48.8%). The largest numbers of respondents were studying at Air University Multan Campus (54.2%). With regard to academic level, the greatest number of students fall within 5th–6th semester levels (48.2%) and the largest percentage of respondents carry a major in Cyber Security (49.4%). As a result, there was significant adoption of AI chatbots amongst all of the participants with the total percentage of those used to regular use of chatbots being 56.8%.



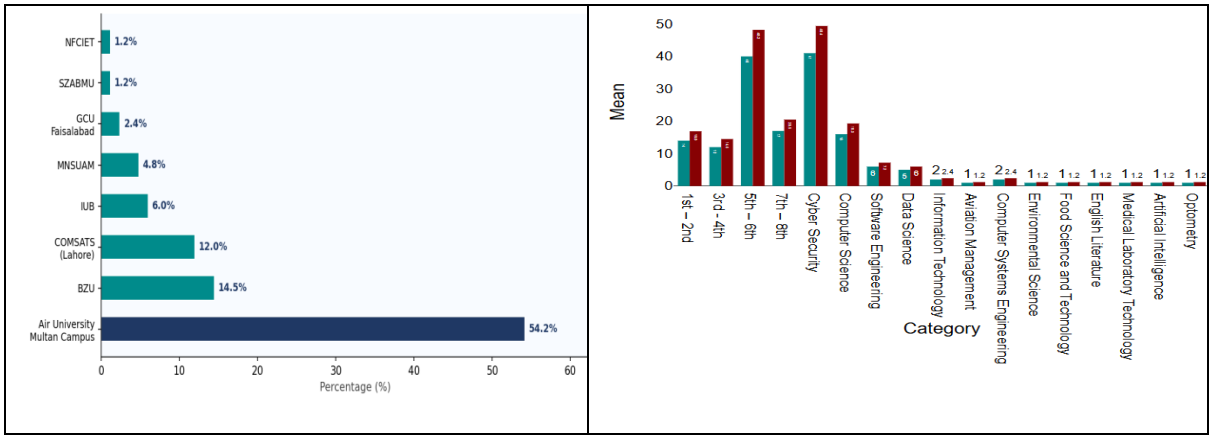


Figure 5. Demographic Distribution

Section A: Awareness and Knowledge of AI Chatbots

Table 3: Awareness and Knowledge of AI Chatbots

Item	N	Mean	SD
Familiarity with AI chatbots	83	3.91	1.05
Awareness of cybersecurity chatbots	83	3.87	1.16
Difference between tools	83	3.86	1.13
Learning usage knowledge	83	3.98	1.01
Awareness of limitations	82	4.00	1.12

Overall, the findings suggest that respondents had a relatively good understanding of AI chatbots. The average mean scores for each of the constructs were greatest with regard to their awareness of AI chatbot limitations (M =4.00, SD = 1.12), next being their general knowledge of how to learn about AI chatbots (M = 3.98, SD = 1.01), followed by familiarity with AI chatbots (M = 3.91, SD =1.05), awareness of Chatbots specific to cybersecurity (M = 3.87, SD = 1.16), and finally, understanding the differences between tools designed specifically for general use in cybersecurity (M = 3.86, SD= 1.13). In conclusion, students who participated in this study generally expressed adequate understanding about AI chatbots and how they can be utilized to enhance their learning in cybersecurity; however, respondents' understanding about specific to domain-related differences was significantly less developed than respondents' general understanding of AI chatbots as a whole. As such, there is likely to be a lack of domain-specialized knowledge.

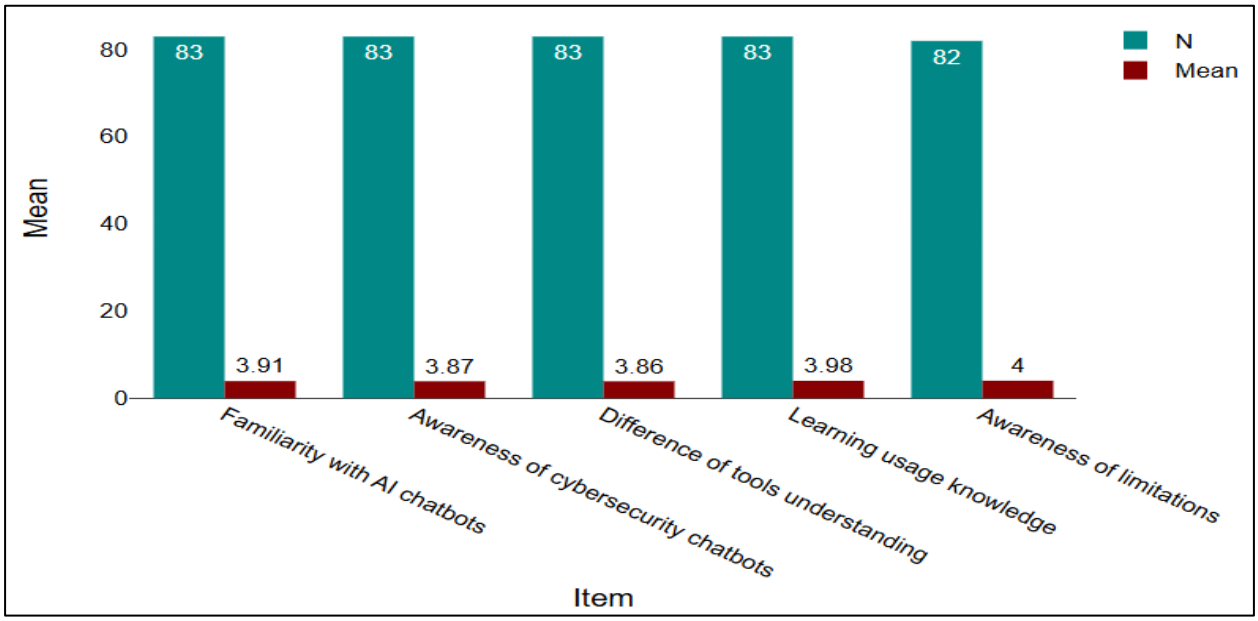


Figure 6: Awareness and Knowledge of AI Chatbots

Section B: Perceived Usefulness in Cybersecurity Learning

Table 4: Perceived Usefulness of AI Chatbots in Cybersecurity Learning

Item	N	Mean	SD
Understand concepts easily	82	3.88	1.04
Improve learning experience	82	3.86	1.02
Accurate information	80	3.84	0.99
Problem solving	83	4.02	0.95
Supplement teaching	83	3.92	0.98
Practical tasks	82	4.01	1.00

Results demonstrate that students perceive AI chatbots as useful tools for cybersecurity learning across all measured dimensions. Problem-solving assistance received the highest mean score (M = 4.02, SD = 0.95), followed by support for practical tasks (M = 4.01, SD = 1.00), supplementing traditional teaching methods (M = 3.92, SD = 0.98), understanding concepts (M = 3.88, SD = 1.04), improving learning experience (M = 3.86, SD = 1.02), and providing accurate information (M = 3.84, SD = 0.99). The relatively lower score for accuracy suggests that while students find chatbots practically useful, moderate reservations regarding information reliability persist — consistent with concerns identified in the reviewed literature (Labadze et al., 2023).

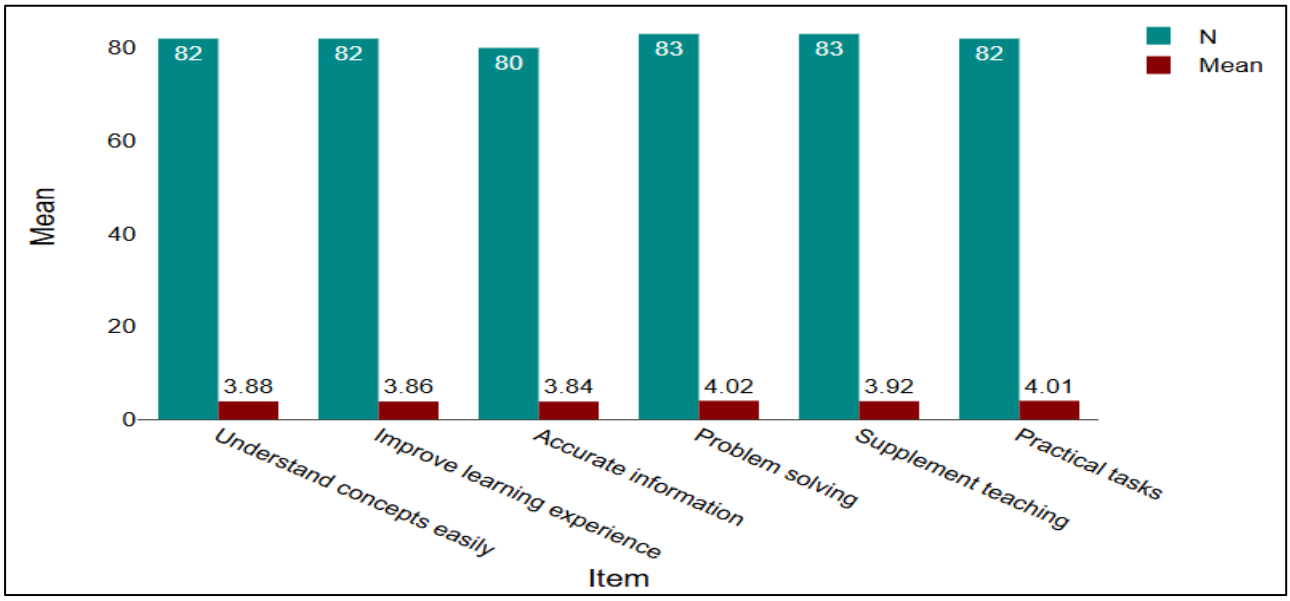


Figure 7: Perceived Usefulness of AI Chatbots in Cybersecurity Learning

Section C: Frequency of Use and Engagement

Table 5. Frequency of Use and Engagement

Item	N	Mean	SD
Course assistance	82	3.85	1.12
Consult difficult topics	82	3.90	1.10
Exam preparation	83	3.95	1.08
Recommend peers	82	3.93	1.07

The frequency analysis shows the use of AI chatbots for learning cybersecurity has been consistent with moderate to high use. In terms of average score; exam preparation scored the highest (M= 3.95, SD= 1.08), second was peer recommendations (M= 3.93, SD= 1.07), third was assistance with difficult topics (M= 3.90, SD= 1.10); the fourth position was for assistance with general course material (M= 3.85, SD= 1.12). As shown by the frequency analysis of use of AI chatbots as a learning resource by BSCS students, with regards to assessment preparation and assisting in resolving conceptual issues, this supports Hypothesis 1 that frequency of use of AI chatbots has a positive impact on perceived usefulness.

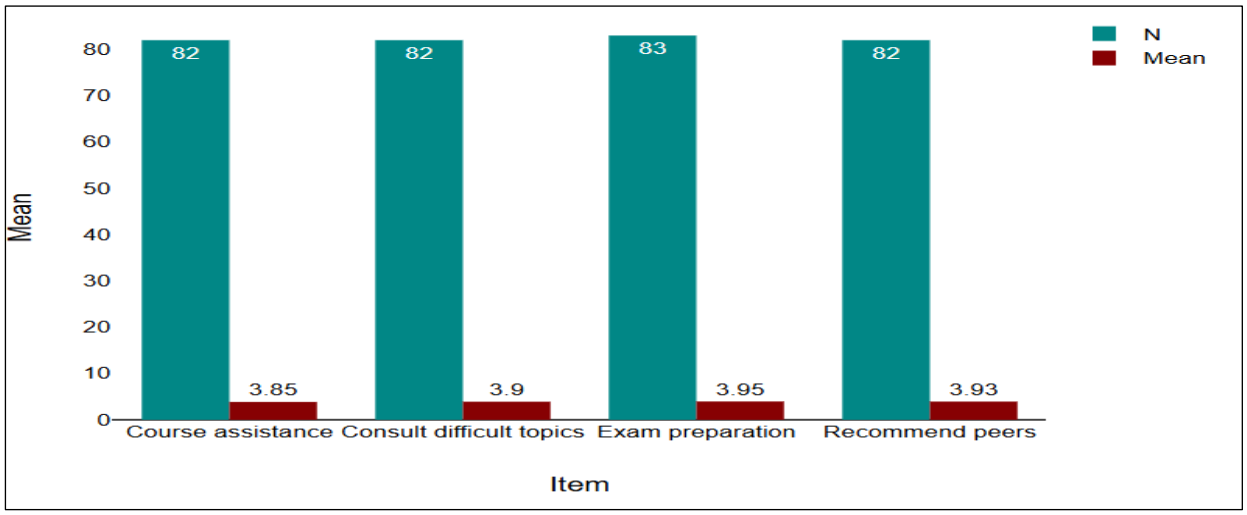


Figure 8 Frequency of Use and Engagement

Table 6 Quality and Effectiveness of AI Responses

Item	N	Mean	SD
Explanation quality	81	3.92	1.01
Accuracy	80	4.00	0.98
Academic level	81	4.05	0.94
Clarity	81	4.10	0.90
Relevance	81	4.03	0.96

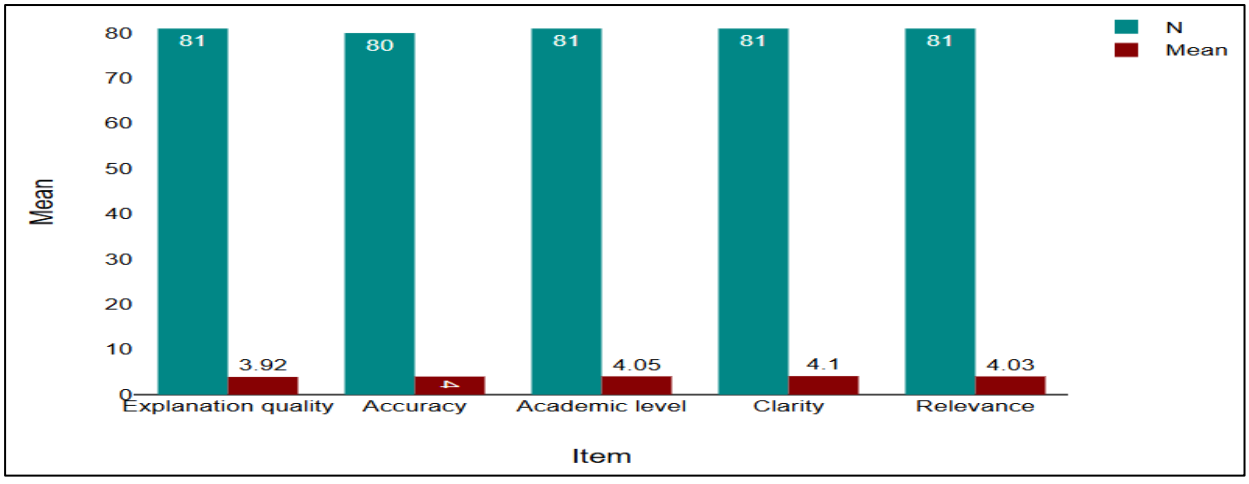


Figure 8. Quality and Effectiveness of AI Responses

Students provided positive evaluations about the quality of responses provided by the AI chatbot. The rating for clarity of responses was the highest (M = 4.10, SD = 0.90); next, in order from highest mean score to lowest mean score were ratings for academic/grade level appropriate response (M = 4.05, SD = 0.94), relevance of examples (M = 4.03, SD = 0.96), accuracy of information (M = 4.00, SD = 0.98)

and quality of explanation (M = 3.92, SD = 1.01). Since the ratings were all rated positively and close together in value, the data collectively indicate that students view responses from the AI chatbot favorably for learning about cybersecurity at an academic level. The somewhat lower mean rating for quality of explanation demonstrates that there are some issues with the depth of the technical explanations provided by the AI chatbot to students.

Section E: Challenges and Limitations

Table 7: **Challenges and Limitations**

Item	N	Mean	SD
Incorrect info	81	3.95	1.08
Difficulty verification	80	3.97	1.06
Harmful advice	80	3.82	1.18
Privacy concerns	80	4.05	1.03
Critical thinking issue	80	4.15	0.96

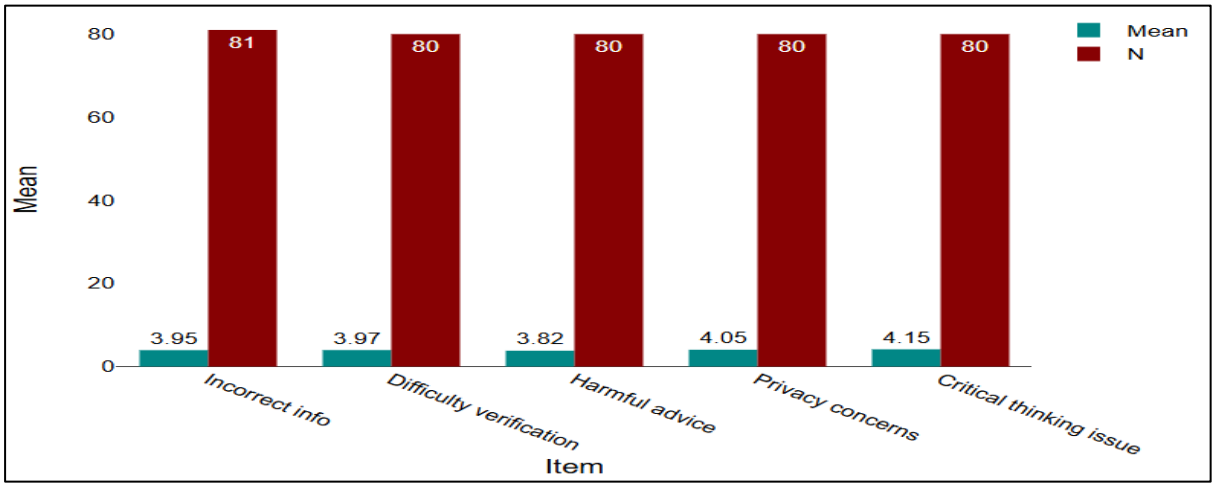


Figure 9: Challenges and Limitations

Although students have favorable opinion with regard to usefulness of chatbots, they also recognized the limitations of AI chatbot assistance. Their foremost concern surrounding over-reliance on chatbots impacting their ability to think critically (M = 4.15, SD = 0.96), next on their list of priorities were concerns for privacy and data security (M = 4.05, SD = 1.03), difficulty verifying accuracy of the information being shared (M = 3.97, SD = 1.06), providing inaccurate information (M = 3.95, SD = 1.08), as well as giving potentially harmful advice (M = 3.82, SD = 1.18). These results are similar to those of Davar et al. (2025) and Yang & Yu (2024) who also identified over-reliance and inaccuracies as key issues within AI based education in both technical fields such as cybersecurity.

Section F: Perceived Academic Performance

Table 8: Perceived Academic Performance

Item	*N*	*Mean*	*SD*
Understanding improved	81	3.94	1.03
Grades improved	82	4.00	1.01
Exam confidence	81	4.05	0.97
Assignment's performance	46	3.88	1.02
Overall improvement	82	4.10	0.95

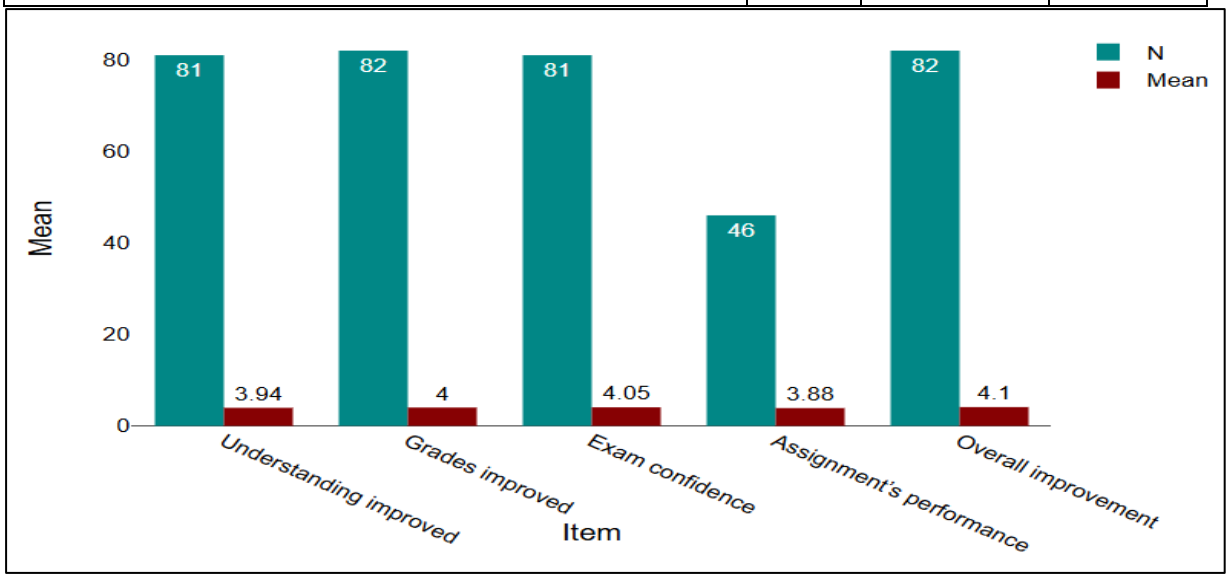


Figure 10: Perceived Academic Performance

The students found that AI chatbots positively impacted their academic performance with the highest mean being for improvement overall (M = 4.10, SD = 0.95), followed closely by confidence to take exams (M = 4.05, SD = 0.97), improved grades (M = 4.00, SD = 1.01), assignment performance (M = 3.88, SD = 1.02), and comprehension of course content (M = 3.94, SD = 1.03). While the results provide empirical support for H2 regarding the positive relationship between use of AI chatbots and perception of academic success in cybersecurity classes, it is important to note that the results are based on students' feedback rather than objective academic records, which serves as a limitation to the study.

IMPLICATIONS

The implications of the results of this research have significance on different levels. Practically, due to the medium level of perceived usefulness of AI chatbots (3.84-4.02) and the influence of their usage on learning performance, it is suggested that Pakistani universities should consider adopting these technologies in their cybersecurity curriculums and use them for teaching concepts, solving problems, and preparing for exams. Instructors should provide students with appropriate training on how to work with AI chatbots critically. From a theoretical perspective, the results confirm the validity of TAM as perceived usefulness is found to be an important determinant of the usage of AI chatbots among cybersecurity learners (Davis, 1989; Schei et al., 2024). Moreover, the study extends the scope of Constructivist Learning Theory since the interactive process of working with AI chatbots helps build a deeper understanding of the subject matter. From a policy perspective, higher education institutions and governmental regulators in Pakistan should consider developing relevant rules for using AI chatbots in educational contexts to prevent any risks of misinformation, issues of data privacy and dependency on automation that the students identified themselves in their very high average ratings (M = 4.05 - 4.15), thus making sure that the introduction of artificial intelligence into cybersecurity studies will be both efficient and scholarly.

LIMITATIONS

While the current study brings forward some important insights about the utilization of AI chatbots in teaching cybersecurity, there are a number of limitations associated with it as well. Firstly, it relies completely on perceptions offered by students, making it vulnerable to social desirability bias. Secondly, while the aim was to gather data from students enrolled at different universities using stratified random sampling, the final sample size was only 83 students, significantly lower than the initial target of 300; moreover, a majority (54.2%) belonged to Air University Multan Campus, compromising the external validity of the results in other Pakistani institutions. Thirdly, due to its cross-sectional nature, the current study does not allow for causality between the usage of AI chatbots and the perceived academic performance. Fourth, the geographical extent of the study is restricted to certain institutions from Punjab, Pakistan, suggesting that the results may not generalize to cybersecurity students in other regions or nations that have varying degrees of digital infrastructure development. Lastly, the variation in areas of study pursued by the participants, some of which were not related to cybersecurity or computing at all, could also present another form of sampling issue in that there was no way to control for such variability.

FUTURE RESEARCH DIRECTIONS

Some potential avenues for future research that can be derived from the results and limitations of the current study are discussed below. First, longitudinal research should be undertaken in order to investigate how changes in perceived and actual students' learning outcomes occur throughout an entire academic period or year of degree program completion. This would be helpful to better understand whether continued use of AI chatbot tools leads to the achievement of significant learning benefits in terms of cybersecurity knowledge acquisition. Conducting experimental or quasi-experimental research, when the performance of participants using AI chatbots is compared to the performance of participants who do not use this learning tool, would be important for establishing causal effects. Further research could also increase the geographical boundaries and include cybersecurity students not only from Lahore, but also other provinces of Pakistan and developing countries of South and Southeast Asia, thus allowing for cross-regional comparisons. Finally, qualitative interviews or focus groups with students would be helpful to better understand how AI chatbot technologies can positively or negatively affect their cybersecurity skills development, especially when it comes to issues related to excessive reliance on critical thinking (M = 4.15). Further, future studies can consider testing the efficacy of domain-oriented AI solutions based on cybersecurity material versus generic chatbots like ChatGPT

and Gemini since the results of the current study seem to indicate that the former may be better suited to addressing the needs of cybersecurity learners.

CONCLUSION

It is evident that in Pakistan, students perceive AI chatbots as learning aids in cybersecurity. Such chatbots are frequently utilized. They are known for providing accurate responses. This contributes to improved academic performance. Three theories are employed in this study. They include Technology Acceptance Model, Constructivist Learning Theory, and Cognitive Load Theory. Such theories have justified the link between utilizing chatbots and learning outcomes. There are challenges. For instance, at times chatbots offer information. At other times, it may be difficult to determine the authenticity of such information. Students must not overly depend on chatbots. The category of universities and infrastructural factors influence the efficacy of chatbots. This research is crucial because it offers empirical evidence from a developing nation.AI chatbots can contribute to increased engagement, enhanced comprehension, and superior performance in cybersecurity education. Moreover, it is essential to foster critical thinking skills besides depending on technological advancements. The utilization of AI chatbots within cybersecurity education should serve as a supplementary component.

REFERENCES

Davar, N. F., Dewan, M. A., & Zhang, X. (2025). AI chatbots in education: Challenges and opportunities. *Information*, *16*(3), 235. https://doi.org/10.3390/info16030235

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

Deng, X., & Yu, Z. (2023). A meta-analysis and systematic review of the effect of chatbot technology use in sustainable education. *Sustainability*, *15*(4), 2940. https://doi.org/10.3390/su15042940

Kooli, C. (2023). Chatbots in education and research: A critical examination of ethical implications and solutions. *Sustainability*, *15*(7), 5614. https://doi.org/10.3390/su15075614

Kowalski, S., Mazur, A., Hassel, M., & Tiller, T. (2013). Two case studies in using chatbots for security training. In *IFIP Advances in Information and Communication Technology* (Vol. 405, pp. 265–272). Springer. https://doi.org/10.1007/978-3-642-39377-8_31

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30*(3), 607–610. https://doi.org/10.1177/001316447003000308

Kuhail, M. A., Alturki, N., Alramlawi, S., &Alhejori, K. (2022). Interacting with educational chatbots: A systematic review. *Education and Information Technologies*, *28*, 973–1018. https://doi.org/10.1007/s10639-022-11177-3

Labadze, L., Grigolia, M., &Machaidze, L. (2023). Role of AI chatbots in education: Systematic literature review. *International Journal of Educational Technology in Higher Education*, *20*, 56. https://doi.org/10.1186/s41239-023-00426-1

McGrath, C., Farazouli, A., &Cerratto-Pargman, T. (2024). Generative AI chatbots in higher education: A review of an emerging research area. *Higher Education*, *89*, 1533–1549. https://doi.org/10.1007/s10734-024-01288-w

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.

Schei, O. M., Møgelvang, A., &Ludvigsen, K. (2024). Perceptions and use of AI chatbots among students in higher education: A scoping review of empirical studies. *Education Sciences, 14*(8), 922. https://doi.org/10.3390/educsci14080922

Schei, O. M., Møgelvang, A., &Ludvigsen, K. (2025). Students' mindset to adopt AI chatbots for effectiveness of online learning in higher education. *Future Business Journal*. https://doi.org/10.1186/s43093-025-00459-0

Shawar, B. A., & Atwell, E. (2022). Interacting with educational chatbots: A systematic review. *Education and Information Technologies*. https://doi.org/10.1007/s10639-022-11177-3

Tegos, S., & Papadopoulos, T. (2024). Conversational AI in education: A general review of chatbot technologies and challenges. *ResearchGate*. https://www.researchgate.net/publication/394464267

Yang, S. D., &Yu, Z. G. (2024). ChatGPT in education: Ethical considerations and sentiment analysis. *International Journal of Information and Communication Technology Education, 20*(1), 1–19. https://doi.org/10.4018/IJICTE.346826

Appendix A: Questionnaire

Respected Participant,

We are students at Air University, Multan Campus, currently conducting a research study entitled "Perceived Effectiveness of AI Chatbots in Cybersecurity Education." We would be extremely grateful if you could kindly spare some time to complete this questionnaire.

The information collected through this survey will be kept strictly confidential and will be used solely for academic research purposes. No personal identification will be disclosed, and all ethical standards will be fully observed throughout the research process. Participation in this study is completely voluntary, and you may withdraw at any time without any penalty. Your cooperation will be highly appreciated.

Thank you very much for your time and support.

Yours sincerely,

Consent Statement

(1) Participation is completely voluntary.

(2) All responses are confidential and anonymous.

(3) Participants may withdraw at any time without consequence.

(4) There is no risk or penalty associated with participation.

(5) Responses will be used only for academic research purposes.

☐ I have read the above information and I agree to voluntarily participate in this study.

Instructions

This questionnaire is designed to examine students' perceptions about the effectiveness of AI chatbots in cybersecurity education. Please read each statement carefully and mark the option that best reflects your opinion. There are no right or wrong answers. Your honest responses are important for this study. All responses will be kept confidential and will not affect your grades or academic standing in any way.

Demographic Information:

Please fill in or tick the relevant option(s).

01	Age: (1) 16–18 years (2) 19–21 years (3) 22–24 years (4) 25 years or above
02	**Gender:** (1) Male (2) Female (3) Prefer not to say
03	**University:** (1) University of the Punjab (2) Bahauddin Zakariya University (3) COMSATS University (Lahore)
04	**Current Semester:** (1) 1st–2nd (2) 3rd–4th (3) 5th–6th (4) 7th–8th
05	**Program of Study:** (1) BSCS (2) SCYS (3) Other
06	**AI Chatbot Usage:** (1) Yes, regularly (2) Yes, occasionally (3) No, but aware (4) Never
07	**Cybersecurity Study Duration:** (1) < 6 months (2) 6 months–1 year (3) 1–2 years (4) More than 2 years

SECTION A: AWARENESS AND KNOWLEDGE OF AI CHATBOTS

Scale: 1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree

Statement	1	2	3	4	5
1. I am familiar with what AI chatbots are and how they function.	□	□	□	□	□
2. I am aware of AI chatbots specifically used for cybersecurity education (e.g., ChatGPT, Gemini, Copilot).	□	□	□	□	□
3. I understand the difference between general AI chatbots and cybersecurity-focused tools.	□	□	□	□	□
4. I know how AI chatbots can be used to learn cybersecurity concepts.	□	□	□	□	□
5. I am aware of the limitations of AI chatbots in providing cybersecurity information.	□	□	□	□	□

SECTION B: PERCEIVED USEFULNESS IN CYBERSECURITY LEARNING

Scale: 1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree

Statement	1	2	3	4	5
6. AI chatbots help me understand complex cybersecurity concepts more easily.	□	□	□	□	□
7. Using AI chatbots improves my overall learning experience in cybersecurity courses.	□	□	□	□	□
8. AI chatbots provide accurate and reliable cybersecurity information.	□	□	□	□	□
9. AI chatbots assist me in solving cybersecurity-related problems effectively.	□	□	□	□	□
10. I believe AI chatbots can supplement traditional cybersecurity teaching methods.	□	□	□	□	□
11. AI chatbots help in practical tasks (e.g., labs, tools, configurations)	□	□	□	□	□

SECTION C: FREQUENCY OF USE AND ENGAGEMENT

Scale: 1 = Never | 2 = Rarely | 3 = Sometimes | 4 = Often | 5 = Always

Statement	1	2	3	4	5
12. I use AI chatbots to assist me in understanding cybersecurity course material.	□	□	□	□	□
13. I consult AI chatbots when I encounter a difficult cybersecurity topic.	□	□	□	□	□
14. I use AI chatbots to prepare for cybersecurity exams or assessments.	□	□	□	□	□
15. I recommend AI chatbots to my peers for cybersecurity learning.	□	□	□	□	□

SECTION D: QUALITY AND EFFECTIVENESS OF AI RESPONSES

Scale: 1 = Very Poor | 2 = Poor | 3 = Average | 4 = Good | 5 = Excellent

Statement	1	2	3	4	5
16. The quality of explanations provided by AI chatbots on cybersecurity topics.	□	□	□	□	□
17. The accuracy of information given by AI chatbots regarding cyber threats.	□	□	□	□	□
18. The ability of AI chatbots to answer cybersecurity questions at an academic level.	□	□	□	□	□
19. The clarity and simplicity of AI chatbot responses on technical cybersecurity subjects.	□	□	□	□	□
20. The relevance of examples provided by AI chatbots in the context of cybersecurity.	□	□	□	□	□

SECTION E: CHALLENGES AND LIMITATIONS

Scale: 1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree

Statement	1	2	3	4	5
21. AI chatbots sometimes provide incorrect or misleading cybersecurity information.	□	□	□	□	□
22. I find it difficult to verify the accuracy of information provided by AI chatbots.	□	□	□	□	□
23. I have encountered incorrect or harmful cybersecurity advice from AI chatbots .	□	□	□	□	□
24. Privacy and data security concerns discourage me from using AI chatbots for learning.	□	□	□	□	□
25. Over-dependence on AI chatbots may hinder the development of critical thinking skills in cybersecurity.	□	□	□	□	□

SECTION F: PERCEIVED ACADEMIC PERFORMANCE

Scale: 1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree

Statement	1	2	3	4	5
26. Since using AI chatbots, my understanding of cybersecurity course content has improved.	□	□	□	□	□

27. My grades in cybersecurity-related courses have improved since I started using AI chatbots.	□	□	□	□	□
28. I feel more confident in cybersecurity exams after using AI chatbots for preparation.	□	□	□	□	□
29. AI chatbots have helped me perform better in cybersecurity assignments and projects.	□	□	□	□	□
30. Overall, AI chatbots have had a positive effect on my academic performance in cybersecurity courses.	□	□	□	□	□

Thank you for your kind participation.

Your responses are valuable to this research.