JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

AI-BASED CYBERSECURITY SOLUTIONS: SECURING INFORMATION AND PRIVACY IN THE EVOLVING DIGITAL AGE

Fahad Amin [1], Dr. Ihsan Said [2]

Affiliations

[1] Department of Computer Science, Cybersecurity North American University, Stafford, TX, USA
Email: famin1@na.edu

[2] Department of Computer Science, Chair, Assistant Professor of Computer Science, North American University, Stafford, TX, USA
Email: isaid@na.edu

Corresponding Author's Email

[1]famin1@na.edu

Article History
Received on 16.10.2025
Accepted on 20.11.2025
Published on 31.12.2025

Abstract
The fast development of digital technologies has caused the volume and complexity of cyber threats to become very serious risk to information security and user privacy. Traditional methods of cybersecurity are becoming insufficient to handle advanced and emerging attacks.
The purpose of the present study is to assess the level of success of Artificial Intelligence (AI)-based cybersecurity solutions and to determine the main obstacles to their adoption and how they affect the privacy of data and the evolution of security practices in the future.
The research design was that of quantitative research through the use of a structured questionnaire that was administered to IT professionals, cybersecurity experts, academic researchers, and students. There were 250 valid responses, which were collected using convenience sampling. Descriptive statistical methods, such as frequencies, percentages, mean, and standard deviation, were used to analyze the data.
The findings show that most of the respondents believe that AI is more efficient than conventional approaches to threat detection and prevention. Awareness was found to be high, and moderate levels of adoption of AI tools were observed. Nevertheless, the implementation cost, shortage of skills as well as privacy were noted to be major challenges. Moreover, the majority of respondents admitted that AI brings both new risks and advantages with it.
The paper summarizes that AI is a key to improving cybersecurity through proactive and intelligent threat management. Although it has its merits, effective implementation involves technical, ethical, and organizational challenges that need to be addressed.
It has also been suggested that organizations should invest in skills, find cost-effective AI solutions, enhance data governance processes, and implement regulatory frameworks to ensure secure and ethical use of AI in cybersecurity.
Keywords: Artificial Intelligence, Cybersecurity, Threat Detection, Data Privacy, Machine Learning, Digital Security

I. INTRODUCTION

The rapid pace of the digital technology revolution in the recent past has altered the way individuals and organizations and governments transact their business and communicate with one another that has brought about unprecedented connectivity, efficiency and data exchanges [1]. However, the digital revolution has come with complex problems of cybersecurity whereby sensitive information is fast going into the wrong hands through cyber-attacks [2, 3]. It is evident that overuse of digital platforms, cloud computing and interconnected systems has increased the attack surface to a very huge extent, data protection, and confidentiality are becoming a concern in the contemporary era [4]. Cybercriminals have also been updating

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

their techniques over time; and are employing emerging techniques, such as ransomware, phishing, zero-day attacks and advanced persistent threats that circumvent the traditional security infrastructure [5-7].

The traditional cybersecurity systems, which are predominantly rule-based systems and signature detection systems, become ineffective in responding to the current cyber threat [8]. These types of systems highly rely on patterns that are pre-established and the human factor that makes them non-relevant to dynamic and previously unknown attacks [9]. This brings into consideration the fact that the organizations are now more likely to resort to the implementation of Artificial Intelligence (AI) as the tool of intensifying their cybersecurity operations [10]. Through the assistance of AI technologies, machine learning, deep learning, and natural language processing, it can be capable of processing large data, identifying anomalies, as well as responding to threats in real time [11-14].

Cybersecurity tools based on AI represent a proactive system of detection and prevention of threats since they deliver pattern detection and anticipation of future attacks before they begin [15]. In comparison to the traditional systems, AI is capable of learning continuously and changing according to the new threats and thus it is a highly successful tool of addressing the new cyber threats [16]. To illustrate this, AI can be programmed to scan network traffic, user activities, and system activities to identify patterns of anomalies that may indicate a security attack. These functions have the capacity to dramatically reduce the response time and improve upon the overall resilience within the system [17, 21].

The other significant use of AI in cybersecurity is in phishing and social engineering attacks. Through the implementation of natural language processing AI systems are able to analyze email text, identify malicious links and even learn to recognize suspicious patterns of communication [18]. Also, AI-based authentication systems, including behavioral biometrics, increase identity verification by examining user behaviors, which reduces the possibility of unauthorized access [19-21]. The innovation helps in enhancing data security and reducing human error, which is a significant contributor of security breach.

Although AI has some benefits, there are a few issues with its implementation in cybersecurity. The development of the adversarial AI is one of the most significant issues, as cybercriminals can utilize the AI technologies to build more sophisticated and unpreventable attacks [22]. The AI models may be manipulated by techniques including data poisoning and evasion attacks, resulting in false threat detection and greater vulnerability [23]. Also, AI systems need access to massive amounts of data, which raises serious privacy and ethical issues related to data collection, storage, and use.

The regulatory frameworks including the data protection laws highlight the importance of transparency and accountability in AI applications [24]. Organizations should make sure that the AI systems do not violate these guidelines and find a balance between security and the privacy of the users [25]. Explainable AI and privacy-preserving methods represent important approaches that can be used to foster trust and responsible implementation.

In the future, AI will most likely be used in cybersecurity through the creation of autonomous and adaptive security frameworks that can learn and respond to threats on their own [26]. Shared threat intelligence among organizations can further promote worldwide cybersecurity through collaborative AI systems [27]. Nevertheless, this necessitates ongoing innovation, cross-disciplinary synergy, and good governance [28].

To sum up, AI-based cybersecurity solutions are the first step in the digital era of information and privacy protection. Although AI has considerable benefits in threat detection and response, these issues are important in order to implement it safely and ethically.

B. Problem Statement

Modern society is rapidly becoming digitalized, and the number of cyber threats is growing significantly, becoming a critical threat to information security and privacy of users. Traditional cybersecurity systems which operate using fixed rules and through human intervention can no longer be used to fight these advanced and sophisticated cyberattacks like ransomware, phishing, and zero-day attacks. The advent of the Artificial Intelligence promises to improve threat detection and threat response but there are also new problems that come with the implementation of the AI such as the adversarial attacks, high costs to implement, and shortage of trained professionals, and concerns regarding data privacy. In addition, since AI systems require

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

large amounts of data, they introduce ethical and legal issues regarding data security and integrity. Organizations are grappling with the benefits of AI-based security and the threat of risks and limitations. Therefore, the effectiveness, challenges, and ethical issues of AI-based cybersecurity devices are acutely requiring scrutiny to advance safe, reliable, and privacy-conscious online space.

II. LITERATURE REVIEW

A. Evolution of Cybersecurity Threats

The advancement of the digital technologies has significantly contributed to the sophistication and intensity of the cyber threats [29]. The rule-based and signature-based traditional cybersecurity tools such as firewalls and anti-virus software cannot handle new attacks like zero-day attacks and polymorphic malwares [30]. The accelerated progress in cloud computing, the Internet of Things, and decentralized networks also enhanced vulnerabilities and conventional approaches are no longer sufficient [31]. Researchers emphasize the need to have intelligent and dynamic security systems in order to overcome such threats that are continually evolving.

B. Role of AI in Threat Detection and Prevention

Artificial Intelligence has reshaped threat detection where large amounts of data are utilized by systems to extract patterns associated with malicious activities [32]. Machine learning models can classify network traffic and help detect anomalies that indicate a potential threat [33]. Behavioral analytics also plays a critical role in identifying insider threats and unauthorized activity, through the continual monitoring of user behavior [34]. Deep learning applications enhance malware detection through file and execution behavior analysis, even when the attackers are attempting to conceal malicious code.

C. AI in Automated Incident Response

Cybersecurity AI-based solutions are highly beneficial in improving the incident response process through automated threat detection and mitigation processes [35, 45]. Security orchestration and automated response (SOAR) systems focused on priority of threats according to their severity and implement some set response to contain the threats [36]. Predictive analytics can also enable business organizations to be aware of the vulnerability and detect an attack before it strikes [37]. Furthermore, the use of AI makes digital forensics more effective, as it processes information on various sources to recreate attack patterns, as well as identify threat agents.

D. Challenges and Limitations of AI in Cybersecurity

Despite its good features, AI-based cybersecurity is characterized by a number of limitations. There are adversarial attacks, e.g., data poisoning and model evasion, which can compromise AI systems and impair their performance [38]. False positives are also a significant problem since the systems that are over sensitive would produce too many alerts hence become inefficient [39, 46]. Additionally, AI requires massive data or quality data to train, which is not necessarily objective and available. These complications highlight the need to continually improve and strong framework development [40].

E. Ethical and Privacy Concerns

When it comes to AI in cybersecurity, human privacy and ethical matters are of paramount importance. Artificial intelligence may need to access sensitive data, and this brings about the possibility of abuse or unauthorized access [41]. The regulatory systems focus on the information security and openness of AI applications [42]. In order to be held accountable, explainable AI is necessary so that the stakeholders are able to know how the decision will be made [43, 47]. Privacy sensitive federated learning can as well be employed to minimize risks as the information can be analyzed without exposing the raw data [44, 48].

F. Future Directions in AI-Based Cybersecurity

The future of cybersecurity lies in the development of self-directed AI systems that can adjust and decide in real-time. Reinforcement learning can be used to make systems responsive to the threat, and generative AI can be used to simulate cyberattacks to find vulnerabilities. Collaboration among AI ecosystems and blockchain integration can also enhance data security and integrity. However, such advances are impossible to achieve without collaboration among scientists, industry players and policymakers.

G. Research Questions

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

1. How effective are AI-based cybersecurity solutions compared to traditional methods?
2. What are the major challenges in adopting AI for cybersecurity?
3. How does AI impact data privacy and ethical considerations?
4. What is the level of awareness and adoption of AI in cybersecurity?
5. What future trends are expected in AI-based cybersecurity systems?

H. Research Objectives

1. To evaluate the effectiveness of AI-based cybersecurity solutions
2. To identify challenges in AI adoption for cybersecurity
3. To analyze ethical and privacy concerns
4. To examine awareness and usage trends
5. To propose recommendations for secure AI implementation

III. METHODOLOGY

A. Research Design

The research design adopted in the study was a quantitative research design to test the effectiveness, challenges and perception of Artificial Intelligence (AI) in the field of cybersecurity. The survey-based method was also employed to gather systematic data concerning the respondents, which made it possible to analyze it and interpret the findings objectively.

B. Population of the Study

The target audience was IT professionals, experts in cybersecurity, faculty in computer science, and computer science researchers, as well as technology-related employees, graduate and final-year students. The reason why these participants were chosen was that these individuals have some direct or indirect experience with cybersecurity practices and AI technologies.

C. Sample Size and Sampling Technique

There were 250 valid responses obtained in the study. Convenience sampling was used as a non-probability sampling strategy because of the availability and the desire of respondents. This was the best method that the researcher used to collect the relevant data in a manner that was efficient to people that had sufficient knowledge of the subject matter.

D. Data Collection Instrument

The structured questionnaire created in this study was used to collect data. The questionnaire was made up of two major sections:

Section A: Demographic data (e.g., role, experience level, awareness)

Section B: AI-related cybersecurity statements, such as effectiveness, challenges, adoption, risks, and future trends.

The perceptions and attitudes of respondents were measured on a 5-point Likert scale (Strongly Agree-Strongly Disagree).

E. Data Collection Procedure

The questionnaire was administered using online services, such as email and online survey instruments. The study purpose was explained to the respondents and participation was voluntary. Anonymity and confidentiality were observed to promote honest and unbiased responses.

F. Data Analysis Techniques

Descriptive statistical analysis was employed in the analysis of the data collected. Demographic variables were analyzed using frequencies and percentages and the study variables were analyzed using mean and standard deviation. The findings have been in tables and figures to enable easier interpretation and understanding.

G. Ethical Considerations

The research was conducted in adherence to ethical research standards. The participants were made aware of the research objective and they agreed to take part in the research. Privacy and confidentiality of data were highly taken care of and the information gathered was utilized in academic purposes only.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

IV. RESULTS/FINDINGS OF THE STUDY

Findings of the study are the most important results or findings of the collected data after the analysis. They provide the factual information, patterns, relationships, and trends that were identified in the course of research. The results are typically obtained through statistical analysis or qualitative interpretation and directly answer the research questions or objectives. They provide the foundations of discussion, conclusions and recommendations in a study.

FIGURE 1
ROLE OF RESPONDENTS

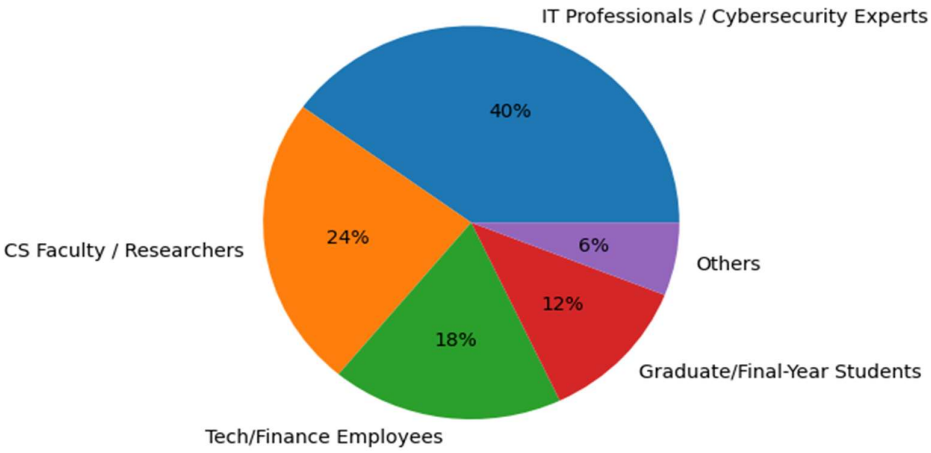


Figure 1 demonstrates the distribution of respondents is highly concentrated by the technically specialized respondents. The most numerous segments of the target audience is IT professionals and cybersecurity experts (40%), which implies that the dataset is significantly informed by those who have direct experience in the industry and understand the domain well. This increases the technical validity and practical applicability of the results.

The second-largest segment (24%), which provides an academic and research-oriented perspective, is constituted by the CS faculty and researchers. Their inclusion would make sure that the data covers both the theoretical knowledge and the trends in the field.

Tech/finance workers of the population (18%) provide an inter-industry perspective, which is especially important in the context of the application of technology in financial and corporate settings. In the meantime, graduate and final-year students (12%) offer the perspectives of new professionals, which represents the current exposure of education and the future trends of the workforce.

The Others (6%), category reflects a very low percentage indicating there is not much impact of non-core or unrelated backgrounds.

On the whole, the sample is relatively balanced but is biased towards more experienced professionals (64% of them were IT experts and faculty members), which enhances the credibility of expert-driven sources but also reduces the generalizability of results to non-technical sets.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

FIGURE 2
LEVEL OF EXPERIENCE

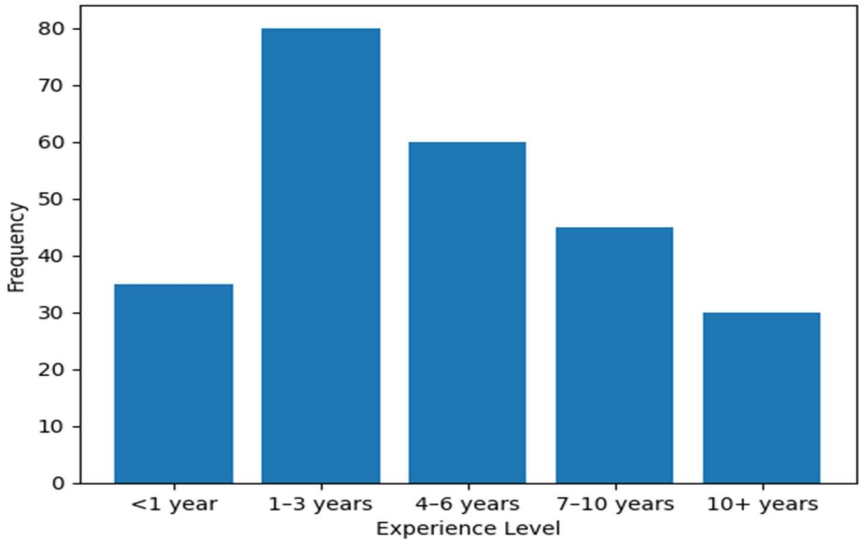
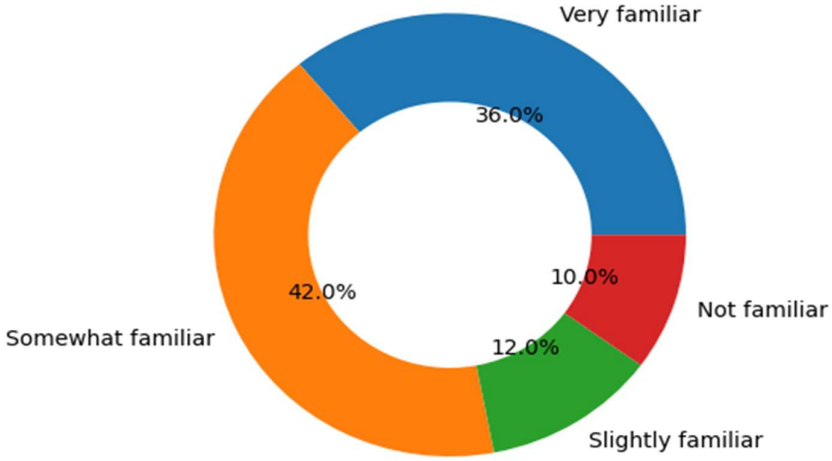


Figure 2 shows the respondent experience profile is of a moderately experienced and professionally diverse sample. The highest percentage is represented in the 1-3 years category (32%), and it suggests that there exists a substantial number of new professionals that might be actively involved in the newest technologies and industry practices. Respondents that reported 4-6 years of experience are 24%, which comprises mid-level professionals that are exposed with a lot of fieldwork. On the same note, individuals with experience of 7-10 years (18%) and over 10 years (12%) years respectively, are combining to provide 30% of the sample, providing the sample with a representation of senior level experience as well as strategic knowledge. The sample under 1 year of experience (14%) constitutes entry-level opinions and indicates the current academic education and background knowledge. The distribution is generally even with a mild bias in the early and middle career respondents (56% between 1 and 6 years). This makes the dataset more relevant to the present-day industry dynamics yet the inclusion of the viewpoints of the experienced individuals adds depth and reliability to the dataset.

FIGURE 3
AWARENESS OF AI IN CYBERSECURITY



The statistics of figure 3 reveal that the general awareness of AI in cybersecurity among surveyed individuals is high. A large proportion (78%) of the sample is represented as somewhat familiar (42%) and very familiar (36%). It shows that the majority of the project participants have a good grasp of AI use in cybersecurity and are well exposed to the modern technological trends.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

The percentage of respondents who are slightly familiar (12%) is also lower, indicating that the awareness is limited, although it does exist, and presumably is the sign of those who engage indirectly or with emerging interest in the field. In the meantime, the proportion of those who are not familiar reminds low (10%), which means that there is little level of ignorance in the sample.

All in all, there is a strong distribution of an informed base of respondents, with a significant concentration in moderate to high awareness rates. This contributes to the plausibility of the responses on AI in cybersecurity because they are, by a big part, informed by those who are knowledgeable and yet, includes a small portion of people who do not know a lot to provide a wider view.

TABLE 1
AI IMPROVES THREAT DETECTION VS TRADITIONAL METHODS

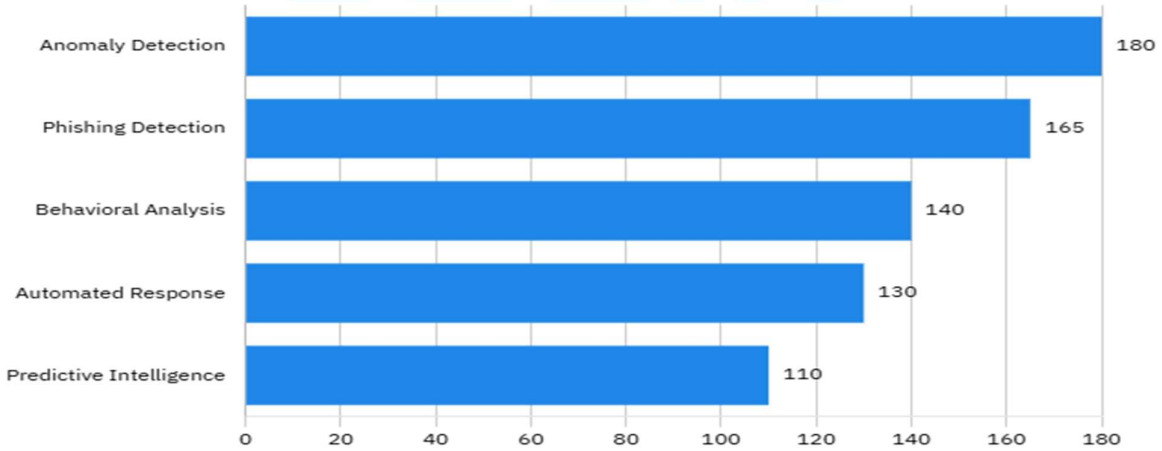
S. No	Response	Frequency	Percentage
1	Strongly Agree	100	40%
2	Agree	80	32%
3	Neutral	35	14%
4	Disagree	20	8%
5	Strongly Disagree	15	6%
	Total	**250**	**100%**

The results of table 1 are highly suggestive of the positive view of AI in threat detection over the conventional approach. A large proportion of the respondents (40%) strongly agree and 32% agree and this The results of Table 1 are highly suggestive of the positive view of AI in threat detection over the results of Table 1 are highly suggestive of the positive view of AI in threat detection over the conventional approach. A large proportion of the respondents (40%) strongly agree and 32% agree and this is a total of 72% of the sample size. It proves that AI-based cybersecurity solutions have a high level of confidence and are better in detecting and preventing threats.

The moderate part of the respondents is neutral (14%), which would indicate certain hesitation or the absence of direct interaction with AI-based systems. Meanwhile the lesser proportion of the results are the disagreements with 8% disagreeing and 6% strongly disagreeing, amounting to 14%. This implies a low level of skepticism, which may be because of the fears of implementation issues, reliability, or unfamiliarity.

In general, the distribution indicates a definite agreement on the problem as AI-enhanced threat detection is supported by a significant majority over the opposition. This further intensifies the feeling that AI is an important addition to the field of cybersecurity, however, a small portion of respondents still has reservations that could be explored further.

FIGURE 4
AI APPLICATION AWARENESS



JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

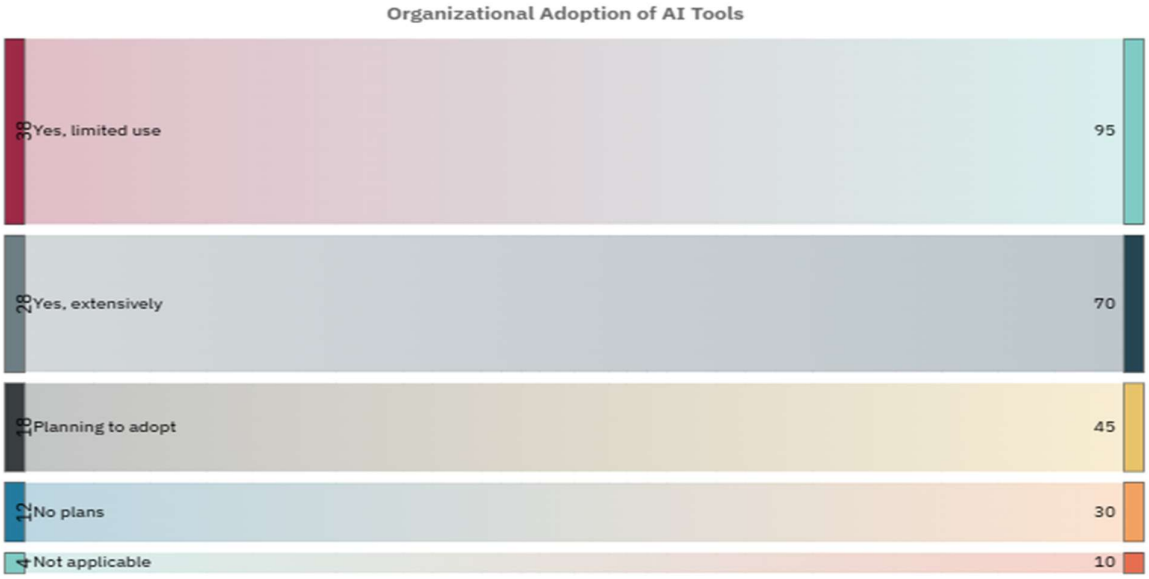
The results in figure 4 indicate that the familiarity of the various AI applications in cybersecurity is high with substantial variations in specific areas. The most common usage (72%) which is an anomaly detection application is a typical knowledge application and is likely to be the most common usage example of the respondents. Nevertheless, on the same note, phishing detection is very much conscious (66%), which also shows its critical importance in fighting typical cyber threats.

Behavioral analysis (56%), automated response (52%), have moderate levels of awareness and this is to say that these applications are often relatively familiar, not as prominently utilized or comprehended as anomaly and phishing detection.

The lowest awareness (44%), which represents a relatively low familiarity, is the case with predictive intelligence. It can be attributed to the fact that it is more sophisticated and data-driven and is less noticeable in everyday cybersecurity activity.

On the whole, the findings indicate that the respondents are usually highly knowledgeable with regards to fundamental AI applications, especially those that are directly connected to immediate threat recognition. Nevertheless, there is less awareness of more sophisticated and proactive use, which may indicate a lapse in exposure or knowledge of new AI capabilities in cybersecurity.

FIGURE 5
ORGANIZATIONAL ADOPTION OF AI TOOLS



The findings in figure 5 demonstrate an increased yet still developing use of AI tools in organizations. The highest percentage of respondents (38%), indicate that they use AI limitedly, indicating that although most organizations have initiated the implementation of AI technologies, it is in the initial or partial stages.

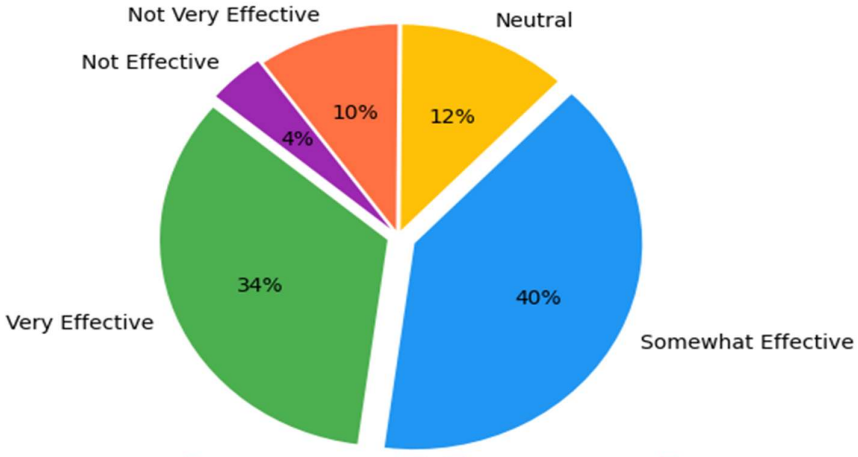
A significant proportion of 28% report extensive usage, which shows that a considerable portion of the organizations have adopted AI-based solutions more comprehensively in their businesses. Put together, 66% of those who confirmed any degree of AI adoption show a high level of overall adoption.

Moreover, 18% of the respondents report that their organizations are considering the use of AI tools, which means that there can be further expansion of AI adoption and growth in the future. However, conversely, a lower percentage (12%) indicate they do not intend to adopt, implying some resistance or perhaps limited access to adoption, like cost, expertise, and infrastructure. The not applicable category (4%) does not have much overall interpretation influence.

Generally, the results arise to indicate that although the adoption of AI in organizations is not new, it is largely in a transitional stage wherein many of the organizations are in a process of leaving the scope of limited implementation to more broad uses of AI.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

FIGURE 6
EFFECTIVENESS OF AI IN PREVENTING ATTACKS

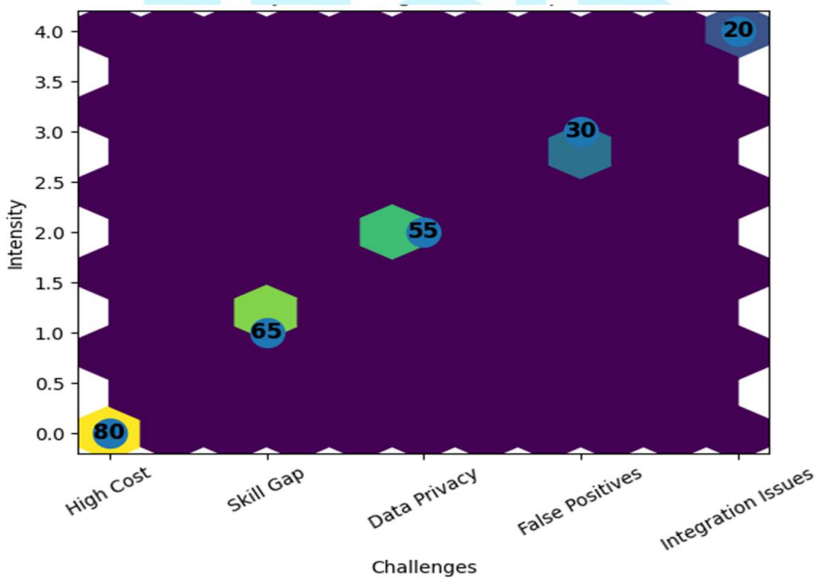


The results in figure 6 reflect that the perception of AI as an effective tool in cyberattack prevention is generally positive. A full majority of the respondents perceive AI to be effective, of which 40% is somewhat effective, and 34% very effective, which is 74% of the sample. This indicates great trust in the idea of AI in supporting proactive cybersecurity actions.

Only a smaller proportion are indifferent (12%), meaning that they are not certain or do not have much direct experience with AI-based prevention systems. Meanwhile, 10% of the respondents believe that AI is not very effective, with only 4% not considering it effective, creating 14% of the negative respondents. Minorities may be employed to symbolize accuracy concerns, implementation challenges, or the complicacies of the threat.

In general, the distribution reveals that AI is perceived as a largely effective practice as far as prevention of attacks is concerned with a large majority of respondents considering it an effective tool. However, the neutral and skeptical reactions indicate that further efforts should be made to continue enhancing, confirming, and creating awareness to increase the level of confidence in AI-powered cybersecurity solutions even more.

FIGURE 7
MAJOR CHALLENGES IN AI ADOPTION



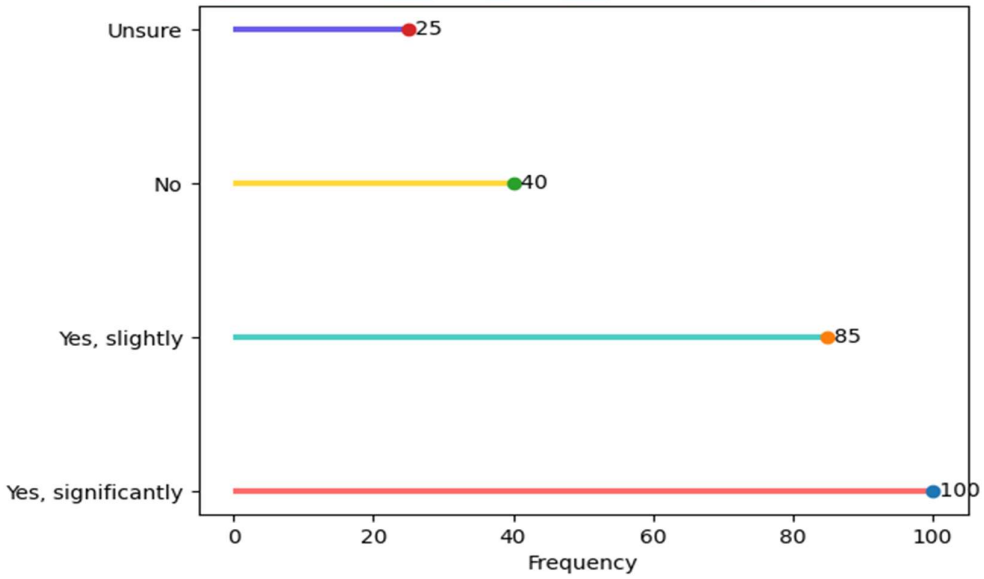
JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

The figure 7 statistics indicate some of the challenges that are likely to prevent the successful implementation of AI in cybersecurity, and two most critical challenges are the financial and human resources. High cost (32%), is the most widespread issue, indicating that even the large size of the organization does not imply that there is much money invested in AI technologies, infrastructure, and maintenance.

The second most apparent issue is the gap in skills (26%), meaning the inability to find skilled professionals capable of designing, implementing, and utilizing AI-based systems. This emphasizes the value of special training and capacity building. The issue of data privacy (22%) also represents a burning point, which presupposes the fear of mismanagement, security, and ethical use of sensitive data to the AI system. Meanwhile, there are false positives (12%) that indicate inefficiencies in action since AI systems presume the presence of innocent actions as being a threat to the system, which potentially leads to less trust and effectiveness.The least popular challenge is integration issues (8%), which still remains relevant and implies the problem with integrating AI-based solutions into the existing organizational structures and processes.

In general, the results indicate that the AI adoption process is ongoing, but it is limited mainly by economic, technical, and ethical factors with cost and expertise being the most prominent hindrances.

FIGURE 8
AI INTRODUCES NEW RISKS



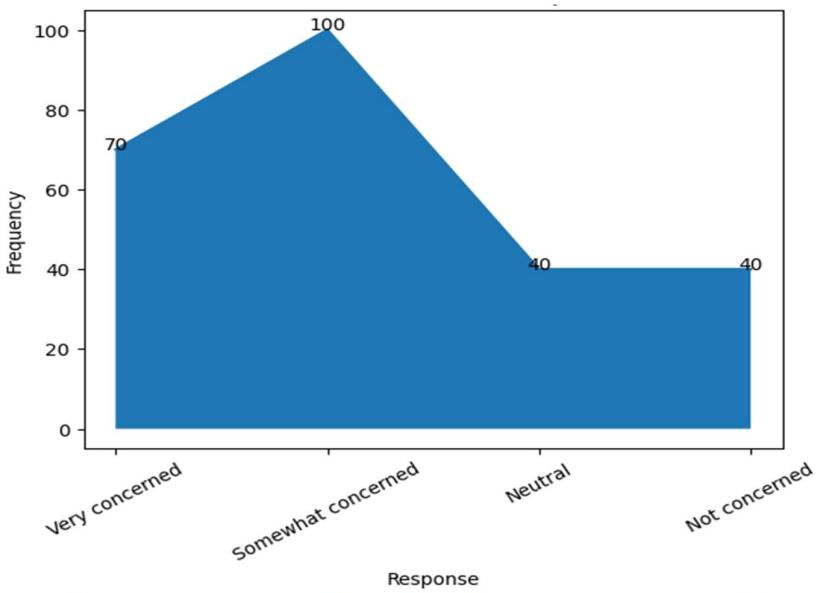
The analysis as has shown in figure 8 shows that a significant majority of the respondents believe that AI poses a novel threat to cybersecurity. In particular, 40% think it creates risks that are significant, and 34% say the impact is slight, which adds up to 74% acknowledging some level of risk. This shows a high level of understanding that, although it has advantages, AI also has other vulnerabilities and difficulties.

Only a smaller percentage of respondents 16%, think that AI poses no new risks, indicating that respondents are either confident that current controls are sufficient or that risks related to AI can be handled within current systems. In the meantime, 10% are uncertain, which implies a lack of confidence or less awareness of the possible dangers of AI technologies.

In general, the distribution indicates a careful attitude to the respondents, in which the benefits of AI are identified, but it is offset with the threats of the system, the vulnerabilities of the system, and the unintended consequences. This highlights the need to develop effective risk management and governance systems and AI integration in cybersecurity.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

FIGURE 9
CONCERNS ABOUT PRIVACY



The statistics shows that privacy is one of the concerns of the respondents in relation to AI in cybersecurity. A majority of them 68% (28% very concerned and 40% somewhat concerned) are concerned about the implication to privacy to some extent, making data protection another key element of AI implementation.

A smaller portion is neutral (16%), or no concern or no knowledge, and the same (16%), or no concern is possibly explained by trust in organizational safeguarding or unawareness concerning the danger of privacy.

Overall, the results point to the fact that the implementation of AI is increasing, and the question of privacy has become a major concern. These concerns are pivotal to implementing AI responsibly with robust data governance, transparency and ethical behaviors to maintain trust.

TABLE 2
NEED FOR AI REGULATIONS

S. No	Response	Frequency	Percentage
1	Strongly Agree	130	52%
2	Agree	60	24%
3	Neutral	30	12%
4	Disagree	20	8%
5	Strongly Disagree	10	4%

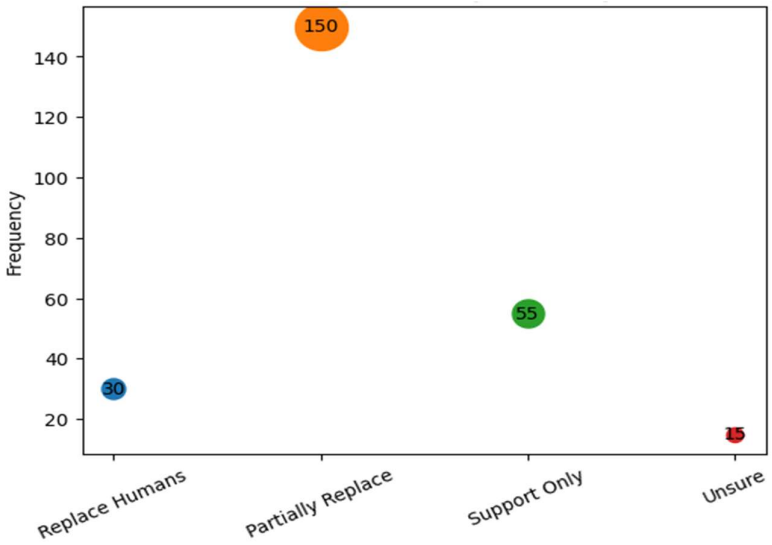
As shown in table 2, the respondents are highly agreeing on the issue of the necessity to regulate AI in relation to cybersecurity. Most of the respondents, 76% (52% strongly agree, 24% agree) are in favor of the use of regulatory frameworks, meaning that a large proportion of the respondents are knowledgeable of the role of regulation, ethical oversight, and standard to AI use.

The smaller percentage (12%) is a neutral one, i.e. they do not know or are not very aware of the extent or need of regulations. Regulatory measures are supported by only 12% (8% disagree and 4% strongly disagree), which means that not a large number of people are opposed to regulation.

Altogether, the information indicates that the vast majority of the respondents support the idea of regulatory mechanisms designed and implemented to make AI applications in the cybersecurity domain safe, responsible, and accounted.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

FIGURE 10
FUTURE ROLE OF AI IN CYBERSECURITY



The data reflects what individuals think about the changing role of AI in the field of cybersecurity. Most of the respondents (60%) are of the opinion that AI is going to partially substitute human labor, i.e. it will substitute some work, but still human laborers will have to have the specialized knowledge in making more complicated decisions and oversight. The minor group (22%) perceives AI as an assistant technology that does not eliminate human skills but only supplements them. Only 12% of people believe that AI will replace all the human functions indicating that people do not believe in the wholesale automation idea. The remaining 6% are uncertain, that reflects no definite way on AI.

Generally, the results indicate that the respondents present AI as something supporting and partly automating in cybersecurity, which could optimize effectiveness and threat prevention, but there are still several crucial and strategic tasks to be done by humans.

TABLE 3
FUTURE FOCUS AREAS OF AI

S. No	Area	Frequency	Percentage
1	Real-time Threat Detection	90	36%
2	Automated Response	75	30%
3	Social Engineering Defense	45	18%
4	Zero-day Prevention	25	10%
5	Compliance Automation	15	6%

The information indicates the future focus of AI in cybersecurity. The highest priority (36%), which is a reflection of the urgent need to detect and mitigate cyber threats immediately in dynamic environments, is real-time threat detection. This is followed by automated response (30%), as a result of the increasing role of AI-based interventions in minimizing response time and minimizing the harm caused by attacks.

Social engineering defense (18%), and zero-day prevention (10%) show focused interest in combating advanced and emerging threats, but are currently given relatively less attention. Compliance automation (6%) is the lowest, implying that regulatory and procedural uses of AI are not perceived as a key concern in relation to operational security.

All in all, the strategic direction of AI in cybersecurity is influenced by expectations of respondents that AI is mainly interested in improving proactive and automated threat management, and more on new attack vectors and regulatory assistance.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 3, Issue 2, 2025
https://jecir.com/

TABLE 4
CONFIDENCE IN AI FOR FUTURE SECURITY

S. No	Response	Frequency	Percentage
1	Very Confident	60	24%
2	Confident	115	46%
3	Neutral	45	18%
4	Not Confident	30	12%
	Total	**250**	**100%**

Based on the findings, the future of AI in cybersecurity is perceived as positive in general. Most of the respondents (70%), including 46 and 24% who are confident and very confident respectively, indicate confidence in the potential of AI to improve security and deal with changing threats.

A smaller percentage is neutral (18%), indicating that they are not sure of what AI can do or how difficult it can be to implement. Only 12% say that they are not confident, which means that they have a low level of doubt about its effectiveness.

On balance, the data shows that most respondents place a lot of confidence in AI as a trusted means of future cybersecurity, and optimism is dominant but a minor segment of cautious or uncertain perspectives.

V. DISCUSSION

According to the findings of this paper, it is a promising sign of the growing involvement of Artificial Intelligence (AI) in the enhancement of cybersecurity practices. A vast majority of interviewees claimed that AI-related systems tend to be more effective in threat detection compared to conventional security measures, and 72% of respondents agreed with this statement. This is after the previous study that identified the inefficiency of the rule-based systems and the strength of AI to highlight complex and previously unseen threats as a result of adaptive learning strategies [8], [32]. The findings can also be justified by the fact that the high awareness level was also observed among the respondents (78% somewhat familiar or very familiar), which is an indication of the increased pervasion of AI technologies in cybersecurity domains.

This research also indicates that AI applications, including anomaly detection and phishing identification, are well-known and this finding aligns with the literature that highlights their usefulness in real-time threat detection and prevention [18], [33]. Nevertheless, the relative lack of understanding of predictive intelligence implies that the advanced capabilities of AI are still developing and are not completely known or adopted in organizations. This implies that there is a gap between basic AI use and more complex predictive algorithms.

Regarding organizational adoption, the results indicate that 66% of the organizations have been adopting AI to some level, but most were at the transition level with minimal adoption. This confirms previous studies which otherwise refer to cost and infrastructure constraints as obstacles to full-scale adoption [22], [38]. The high cost (32%), and skill gaps (26%) as the key challenges identified only confirm issues discussed in previous literature on the resource-intensive character of AI implementation and the lack of experienced personnel [23], [40].

Also, the study indicates extensive ethical and privacy consideration because 68 percent of participants indicated that they were concerned with data privacy. This is consistent with the existing literature that highlights the importance of transparency, explainability and compliance with regulations in AI-based systems [24], [43]. The consensus with the argument of the necessity of AI regulations is high (76%), which underlines the significance of the governance frameworks in the responsible and safe adoption.

Finally, the respondents expressed optimism on the future of AI in cybersecurity with 70% of them expressing that they believed in its potential. However, the perception that AI poses new threats (74%) suggests a responsible attitude, which demonstrates the idea of the new form of a Cold War between AI-based offenses and defenses [42]. Overall, the discussion confirms that despite the fact that AI is a useful tool that

can make cybersecurity more effective, there must be a need to address the technical, ethical, and operational concerns associated with it to make the use of this tool sustainable.

VI. CONCLUSION & RECOMMENDATIONS

The paper concludes that Artificial Intelligence has emerged as one of the transformational factors in cybersecurity and has made a massive impact in the potential of organizations to detect, prevent and respond to the evolving cyber threat. These findings indicate that the attitude toward AI-based solutions is high and favorable, particularly in improving the quality of threat recognition and proactive security. The fact that many of the respondents are rather well informed is another indication that AI is no longer a futuristic concept, it is now a component of modern cybersecurity networks. Nevertheless, the articles also indicate that even though there are benefits of using AI, the use of AI is not balanced, and most organizations are in their initial or intermediate levels of applying AI. It implies that the potential of AI is not a brand-new concept anymore, but the practice is conditioned by numerous organizational and technical limitations.

Along with the problems listed, there are also serious issues that are discussed in the paper that cannot be overlooked. The obstacles to its extensive adoption are the high cost of implementation, lack of access to professional assistance and the problem of data privacy and ethical utilization. In addition, the concept according to which AI is a novel type of risk also means that the introduction of intelligent systems into the security infrastructure will be challenging. The worries raise the question that AI is not an isolated system, but a part of the bigger system of cybersecurity, which needs to be designed, controlled, and unmanageable. The importance of responsibility and innovativeness ratio is also confirmed by the need of regulatory frameworks and ethical provisions.

Some key points can be given in regard to the major recommendations based on these conclusions. In order to optimize capacity building the organization should incorporate special training and education to produce a competent workforce that can operate AI-based systems comfortably. The financial obstacle can be addressed by investing strategically in scalable and low-cost AI solutions to the small and medium-sized businesses. Aggressive privacy protection, transparency, and value creation as part of data governance practices must be strengthened to achieve confidence in the AI application. Industry, academia and policymakers' collaboration needs to matter in order to ensure that knowledge sharing and innovation as well as practice standardization are facilitated.

Additionally, the adoption of AI in companies cannot be a quick process and the simplest way of implementing this technology, which is threat detection, comes first, followed by the more advanced applications such as predictive analytics and automated response system. Another reason is that AI models should be updated and revised in order to be relevant to new threats. Finally, the safe, responsible, and sustainable use of AI in cybersecurity will depend on the establishment and implementation of large-scale regulatory frameworks. Overall, although the possibilities of AI in improving cybersecurity are enormous, the implementation process will be successful, only when the challenge is approached with the assistance of strategic, ethical, and collaborative actions.

REFERENCES

[1] N. G. Camacho, "The role of AI in cybersecurity: Addressing threats in the digital age," *J. Artif. Intell. Gen. Sci. (JAIGS)*, vol. 3, no. 1, pp. 143–154, 2024.

[2] H. Rehan, "AI-driven cloud security: The future of safeguarding sensitive data in the digital age," *J. Artif. Intell. Gen. Sci. (JAIGS)*, vol. 1, no. 1, pp. 132–151, 2024.

[3] M. Aslam, "AI and cybersecurity: An ever-evolving landscape," *Int. J. Adv. Eng. Technol. Innov.*, vol. 1, 2024.

[4] A. Shahana, R. Hasan, S. F. Farabi, J. Akter, M. A. A. Mahmud, F. T. Johora, and G. Suzer, "AI-driven cybersecurity: Balancing advancements and safeguards," *J. Comput. Sci. Technol. Stud.*, vol. 6, no. 2, pp. 76–85, 2024.

[5] J. N. Chukwunweike, M. Yussuf, O. Okusi, and T. Oluwatobi, "The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions," *World J. Adv. Res. Rev.*, vol. 23, no. 2, p. 2550, 2024.
[6] Z. B. Akhtar and A. T. Rawol, "Enhancing cybersecurity through AI-powered security mechanisms," *IT J. Res. Dev.*, vol. 9, no. 1, pp. 50–67, 2024.
[7] M. Mahfuri, S. Ghwanmeh, R. Almajed, W. Alhasan, M. Salahat, J. H. Lee, and T. M. Ghazal, "Transforming cybersecurity in the digital era: The power of AI," in *2024 2nd Int. Conf. Cyber Resilience (ICCR)*, IEEE, pp. 1–8, Feb. 2024.
[8] S. Rangaraju, "Secure by intelligence: Enhancing products with AI-driven security measures," *EPH-Int. J. Sci. Eng.*, vol. 9, no. 3, pp. 36–41, 2023.
[9] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions," *Front. Big Data*, vol. 7, p. 1497535, 2024.
[10] I. O. Owolabi, C. K. Mbabie, and J. C. Obiri, "AI-driven cybersecurity in FinTech & cloud: Combating evolving threats with intelligent defense mechanisms," *Int. J. Multidiscip. Res. Sci. Eng. Technol.*, vol. 7, p. 12, 2024.
[11] V. Baladari, "Adaptive cybersecurity strategies: Mitigating cyber threats and protecting data privacy," *J. Sci. Eng. Res.*, vol. 7, no. 8, pp. 279–288, 2020.
[12] A. Tanikonda, B. K. Pandey, S. R. Peddinti, and S. R. Katragadda, "Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems," *J. Sci. Technol.*, vol. 3, no. 1, 2022.
[13] A. S. George, "Riding the AI waves: An analysis of artificial intelligence's evolving role in combating cyber threats," *Partners Univ. Int. Innov. J.*, vol. 2, no. 1, pp. 39–50, 2024.
[14] V. Kolluri, "An extensive investigation into guardians of the digital realm: AI-driven antivirus and cyber threat intelligence," *Int. J. Adv. Res. Interdiscip. Sci. Endeav.*, vol. 1, no. 2, pp. 71–77, 2024.
[15] M. Z. Afshar and M. H. Shah, "Performance evaluation using balanced scorecard framework: Insights from a public sector case study," *Int. J. Hum. Soc.*, vol. 5, no. 1, pp. 40–47, 2025.
[16] Z. B. Akhtar, "Artificial intelligence (AI) within the realm of cyber security," *Insight Electr. Electron. Eng.*, vol. 1, no. 1, pp. 1–11, 2024.
[17] J. Singh, "The evolution of cybersecurity in the big data era: Moving beyond data protection to data-driven security," in *2023 IEEE Int. Conf. ICT in Bus. Ind. & Gov. (ICTBIG)*, IEEE, pp. 1–6, Dec. 2023.
[18] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: An overview, security intelligence modeling and research directions," *SN Comput. Sci.*, vol. 2, no. 3, p. 173, 2021.
[19] M. Z. Afshar and M. H. Shah, "Examining the role of change management in enhancing organizational resilience in public sector entities," *Center Manage. Sci. Res.*, vol. 3, no. 3, pp. 931–942, 2025.
[20] A. Karunamurthy, R. Kiruthivasan, and S. Gauthamkrishna, "Human-in-the-loop intelligence: Advancing AI-centric cybersecurity for the future," *Quing: Int. J. Multidiscip. Sci. Res. Dev.*, vol. 2, no. 3, pp. 20–43, 2023.
[21] D. Mohiuddin, "Consumer perceptions and trust in AI-generated advertising: An experimental study in the Pakistani context," *Apex Journal of Social Sciences*, vol. 3, no. 1, pp. 53–68, 2024.
[22] S. Thapaliya and A. Bokani, "Leveraging artificial intelligence for enhanced cybersecurity: Insights and innovations," *Sadgamaya*, vol. 1, no. 1, pp. 46–52, 2024.
[23] G. V. S. Meghana, S. S. Afroz, R. Gurindapalli, S. Katari, and K. Swetha, "A survey paper on understanding the rise of AI-driven cyber crime and strategies for proactive digital defenders," in *2024 4th Int. Conf. Pervasive Comput. Soc. Netw. (ICPCSN)*, IEEE, pp. 25–30, May 2024.
[24] K. Kaushik, A. Khan, A. Kumari, I. Sharma, and R. Dubey, "Ethical considerations in AI-based cybersecurity," in *Next-Generation Cybersecurity: AI, ML, and Blockchain*, Singapore: Springer Nature, pp. 437–470, 2024.

[25] N. Arshad, M. U. Baber, and A. Ullah, "Assessing the transformative influence of ChatGPT on research practices among scholars in Pakistan," *Mesopotamian J. Big Data*, pp. 1–10, 2024.
[26] Aurangzeb, M. Asif, and M. K. Amin, "Resources management and SME's performance," *Humanities & Social Sciences Reviews*, vol. 9, no. 3, pp. 679–689, 2021, doi: 10.18510/hssr.2021.9367.
[27] M. Asif, A. Khan, and M. A. Pasha, "Psychological capital of employees' engagement: Moderating impact of conflict management in the financial sector of Pakistan," *Global Social Sciences Review*, vol. 4, no. 3, pp. 160–172, 2019, doi: 10.31703/gssr.2019(IV-III).15.
[28] N. A. A. H. Nahid, T. Islam, H. A. Rube, and M. I. H. Tusar, "Circular economy models for urban logistics: The role of bio-based packaging in sustainable transportation networks," in *Proc. IISE Annu. Conf.*, Institute of Industrial and Systems Engineers (IISE), pp. 1–6, 2025.
[29] M. R. Islam, M. M. Islam, I. A. Badhan, and M. N. Hasnain, "The role of artificial intelligence in carbon pricing policies: Economic and environmental implications," *J. Eng. Comput. Intell. Rev.*, vol. 3, no. 2, pp. 1–19, 2025.
[30] S. Akter, T. S. Turja, A. Hossain, S. A. Eshra, and I. Rasul, "AI in business analytics for financial risk assessment: Survey insights from the banking and insurance industries," *Int. J. Bus. Manag. Sci.*, vol. 5, no. 3, pp. 1–30, 2025.
[31] M. Asif and M. S. Sandhu, "Social media marketing revolution in Pakistan: A study of its adoption and impact on business performance," *Journal of Business Insight and Innovation*, vol. 2, no. 2, pp. 67–77, 2023, doi: 10.52783/eel.v13i5.901.
[32] S. S. A. Rahman, "A HIPAA-compliant web application design framework for next-generation telehealth systems," *Int. J. Res. Technol.*, vol. 12, no. 4, pp. 166–184, 2024.
[33] A. Dash, F. Amin, S. K. Sahoo, and S. K. Mishra, "Secure comparative evaluation of Alzheimer MRI classification models using blockchain," in *Proc. 13th Int. Conf. Intell. Syst. Embedded Design (ISED)*, 2025, pp. 905–911.
[34] U. Twaha and Y. Arfin, "An AI-driven framework for real-time fake news detection: Developing a machine learning-based filter for news platforms in the United States," 2025, doi: 10.54660/IJFEI.2025.2.4.158-169.
[35] S. M. H. Shah, F. Amin, and A. Khan, "Cyber-resilient mobile edge computing: A deep neural approach for secure and efficient task offloading," *Asian Bull. Big Data Manag.*, vol. 5, no. 1, pp. 200–215, 2025.
[36] I. A. Badhan, M. N. Hasnain, and M. H. Rahman, "Advancing operational efficiency: An in-depth study of machine learning applications in industrial automation," *Policy Res. J.*, vol. 1, no. 2, pp. 21–41, 2023.
[37] M. A. Hasan, M. T. R. Mazumder, M. C. Motari, M. S. H. Shourov, and M. J. Howlader, "A data-centric evaluation of AI-powered fraud detection and BI dashboards in strengthening trust and ROI in US e-commerce," *Spanish J. Innov. Integr.*, vol. 49, pp. 157–175, 2025.
[38] N. Sultana, M. A. Nasir, C. Majumder, and A. H. K. Choain, "Exploring AI-driven approaches for safeguarding sensitive ERP, HR, and defense data within US organizations," *J. Bus. Insight Innov.*, vol. 3, no. 2, pp. 43–59, 2024.
[39] M. Asif and R. J. Asghar, "Managerial accounting as a driver of financial performance and sustainability in small and medium enterprises in Pakistan," *Center for Management Science Research*, vol. 3, no. 7, pp. 150–163, 2025, doi: 10.5281/zenodo.17596478.
[40] F. Jimmy, "Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses," *Valley Int. J. Digit. Libr.*, vol. 1, pp. 564–574, 2021.
[41] J. P. Bharadiya, "AI-driven security: How machine learning will shape the future of cybersecurity and Web 3.0," *Am. J. Neural Netw. Appl.*, vol. 9, no. 1, pp. 1–7, 2023.
[42] G. Waizel, "Bridging the AI divide: The evolving arms race between AI-driven cyber-attacks and AI-powered cybersecurity defenses," in *Int. Conf. Mach. Intell. & Security Smart Cities (TRUST) Proc.*, vol. 1, pp. 141–156, Jul. 2024.
[43] E. O. Abolaji and O. T. Akinwande, "AI powered privacy protection: A survey of current state and future directions," *World J. Adv. Res. Rev.*, vol. 23, no. 3, pp. 2687–2696, 2024.

[44] I. H. Sarker, *Introduction to AI-driven cybersecurity and threat intelligence*, Cham: Springer Nature, pp. 3–19, 2024.
[45] M. Asif and A. Shaheen, "Creating a high-performance workplace by the determination of importance of job satisfaction, employee engagement, and leadership," *Journal of Business Insight and Innovation*, vol. 1, no. 2, pp. 9–15, 2022.
[46] D. Mohiuddin, "HR tech adoption in digital banking: Implications for workforce development and financial sector growth in emerging economies," *Journal of Business Insight and Innovation*, vol. 4, no. 2, pp. 77–90, 2025.
[47] D. Mohiuddin and D. N. Farhan, "Artificial intelligence in marketing: Ethical challenges and solutions for consumers and society," *Journal of Business Insight and Innovation*, vol. 4, no. 1, pp. 73–87, 2025.
[48] D. Mohiuddin, "Algorithmic hyper-personalization: The double-edged sword of predictive personalization—An empirical investigation," *Journal of Engineering and Computational Intelligence Review*, vol. 2, no. 2, pp. 82–94, 2024.