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

Assessing the Effectiveness of Artificial Intelligence Techniques in Mitigating Cyber security Risks

Chennu Naga Venkata Sai*[1], Rangu Jaswanth[2], Avula Manasa[3], Yaramakula Sai Pranathi Reddy[4], Suryakanth V. Gangashetty[5], D. Govind[6]

Submitted: 10/05/2023 **Revised**: 15/07/2023 **Accepted**: 09/08/2023

Abstract: The goal of the research was to determine whether or whether dangers to cyber security might be mitigated using approaches based on machine learning, with a particular focus on Iraq. The main data and the qualitative research approach were the ones that were chosen. The information needed for the study was collected from members of staff working in the information technology department. The sample size for this particular investigation was 468, and the researchers performed confirmation factor analysis of discriminant validity, basic analysis of models, and assessment of the hypotheses. All of the P-values were determined to be significant, with the only exception being the expert system, which did not demonstrate any association with machine learning and cyber security. Accessibility, geographical location, the size of the sample, and the number of components comprised the majority of the most critical variables.

Keywords: *Machine Learning Techniques, Cyber security Threats, Qualitative Study, Information Technology Personne*

1. Introduction

The significance and salience of safeguarding computer systems against potential cyber threats have witnessed a notable escalation within the contemporary global landscape. In reference to, White posits that the United States' Federal Bureau of Investigations (FBI) delineates a cyber-attack as an act of aggression propelled by political motivations, executed by subnational entities, targeting computer systems, information repositories, software applications, and data sets, ultimately leading to the infliction of harm upon non-combatant entities. Technological progress requires the creation of new preventative measures due to the rise in cyber risks. Cyber-attacks are becoming more frequent in the industrial sector, where they can seriously harm structures and cause financial losses in the millions of dollars, according to Huang et al. in Because businesses are relying more and more on digital technology, which contains sensitive financial and personal data, cyber-attacks against them are becoming more frequent. As a result, it is considered to be one of the major problems in today's world because it exposes personal information while also resulting in financial loss.

According to, cyber-attacks can involve hacking, virus infections, spyware, denial-of-service assaults, and other actions that could have an impact on the entire country. As a result of the attacks, cyber-attack victims frequently endure severe psychological repercussions, such as dissatisfaction, tension, and anxiety. Taddeo suggests using artificial intelligence (AI) to lessen the effects of cyber-attacks. In accordance with Bha-tele et al.'s definition in, AI is machine intelligence that performs tasks usually done by intelligent beings?

In order to make decisions based on knowledge and gain insights from knowledge, decision-making processes use the expertise of human specialists. Taddeo has shown that AI can have both beneficial and detrimental consequences on cyber security, with one of the latter being the potential for attacks to escalate and become faster and more destructive. As a result of AI's promotion of cyberspace security and improvement of defensive strategies, cyber security has substantially improved. Additionally, according to Conti et al. , the application of AI makes it easier for security experts to find signs of a cyber-threat. The utilisation of machine learning techniques has witnessed a notable surge in its application within the domains of malware analysis and network anomaly detection, primarily attributable to the advancements in artificial intelligence (AI). Identifying cyber security concerns in Iraq using artificial intelligence approaches

[1] *Student, Department of Computer Science and Engineering, KL Deemed to be university, Green Fields vaddeswaram-522302, INDIA, 2000031637@kluniversity.in, https://orcid.org/0009-0000-8252-8682*
[2] *Student, Department of Computer Science and Engineering, KL Deemed to be university, Green Fields vaddeswaram-522302, INDIA, 2000031268@kluniversity.in, https://orcid.org/0009-0003-5493-9339*
[3] *Student, Department of Computer Science and Engineering, KL Deemed to be university, Green Fields vaddeswaram-522302, INDIA,2000030076@kluniversity.in, https://orcid.org/0009-0003-3524-0573*
[4] *Student, Department of Computer Science and Engineering, KL Deemed to be university, Green Fields vaddeswaram-522302, INDIA,2000031848@kluniversity.in, https://orcid.org/0009-0003-7685-2066*
[5] *Professor, Department of Computer Science and Engineering, KL Deemed to be university, Green Fields vaddeswaram-522302, INDIA,svg@kluniversity.in,https://orcid.org/0000-0001-6745-4363*
[6]*Professor, Department of Computer Science and Engineering, KL Deemed to be university, Green Fields vaddeswaram-522302, INDIA,d_govind@kluniversity.in*
** Corresponding Author Email: 2000031637@kluniversity.in*

would be the focus of the upcoming study, according to the literature. According to studies by , for instance, AI can either enhance the assault process by delivering speedier and more painful strikes or it can enhance cyber security. As a result, the study's main goal is to determine how AI might assist Iraq in enhancing cyber security by fending off cyber-attacks. The report's importance stems from the fact that it emphasises how crucial AI technologies are to IT specialists in averting hacks.

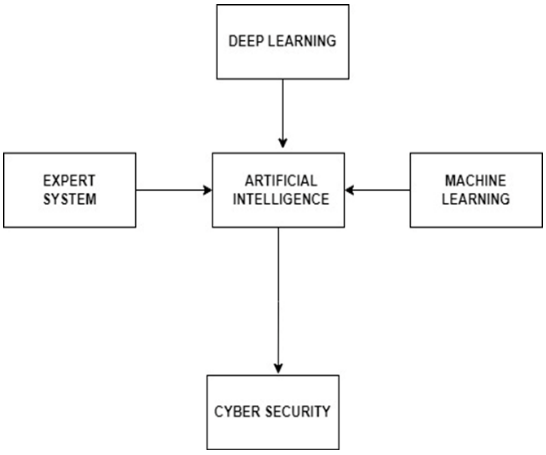


Fig 1: Framework

2. Reviewing the Literature

The focal point of this scholarly investigation revolves around the amalgamation of artificial intelligence and cyber security, with particular emphasis on its intersection with the realm of social media. This study delves into the potential applications of artificial intelligence (AI) tools in addressing the security implications associated with the utilization of social media platforms. The present study endeavor's to delve into a diverse array of technologically advanced artificial intelligence (AI) systems, encompassing the realms of natural language processing (NLP) and machine learning (ML). The overarching objective of this research endeavor is to meticulously discern and subsequently alleviate potential perils that may arise within the aforementioned AI-driven technologies. These hazards primarily encompass the domains of unsolicited electronic communications (commonly referred to as spam), unauthorized seizure of user accounts (commonly known as account hijacking), and the dissemination of erroneous or misleading information (commonly referred to as false information). The primary objective of this project is to enhance the efficacy of cyber security protocols within the perpetually evolving digital landscape. This shall be achieved through the utilization of artificial intelligence (AI) in the comprehensive examination of vast volumes of data sourced from social media platforms [1]. The primary objective of this scholarly investigation is to furnish a comprehensive examination of contemporary advancements, challenges, and prospects within the realm of artificial intelligence as it pertains to the domain of cyber security. This scholarly article critically examines a diverse range of artificial intelligence (AI) methodologies, including but not limited to machine learning, deep learning, and natural language processing. The primary focus lies in evaluating the practical applications of these approaches in the realm of cyber threat detection and response. The aforementioned research further emphasizes the paramount importance of artificial intelligence (AI) systems that possess the capacity for explication, as well as models that can be comprehended, in order to enhance the transparency and dependability of AI-driven cyber security systems. The present study offers a valuable contribution to the advancement of AI-driven cyber security methodologies through the identification of existing lacunae and the proposition of prospective avenues for exploration [2]. This chapter undertakes a comprehensive examination of the intricate interconnection between artificial intelligence (AI) and the realm of cyber security, shedding light on the immense potential for AI to fundamentally transform the landscape of cyber risk detection and prevention. The present study underscores the significance of artificial intelligence (AI) in the realm of automating the surveillance of threats, detecting anomalies, and predicting potential attacks. The present discourse additionally delves into the exploration of the potentialities and predicaments entailed in the utilization of artificial intelligence (AI) as a means to enhance the cyber security stance, with particular emphasis on the occurrence of adversarial assaults. The aforementioned study provides valuable insights into the dynamic landscape of AI-driven cyber security practices. The elucidation of these profound insights is facilitated through the meticulous analysis of empirical case studies and the astute examination of practical applications derived from the tangible realm of reality [3].

In this particular section of the book, the authors delve into the examination of artificial intelligence and machine learning methodologies as they pertain to the domain of cyber security. The present research endeavor's to explore the latent capacity of artificial intelligence (AI) in enhancing the security of information and communication technology (ICT) systems. This scholarly discourse encompasses a range of topics, including but not limited to intrusion detection, malware analysis, and threat intelligence. It elucidates the potential of AI-driven systems in the realm of promptly identifying and mitigating cyber threats. In addition to the aforementioned subjects, the curriculum encompasses the domain of threat intelligence. This paper delves into the intricacies surrounding data quality, model robustness, and ethical considerations within the realm of artificial intelligence-enhanced cyber security [4]. The multifarious applications of artificial intelligence that have been investigated in this scholarly inquiry are intricately intertwined with the domain of cyber security. This scholarly inquiry delves into the potentiality of enhancing threat detection, response, and mitigation strategies through the utilization of methodologies driven by artificial intelligence. The present study endeavor's to examine the efficacy of a diverse array of artificial intelligence (AI) technologies, encompassing machine learning algorithms, neural networks, and anomaly detection, in the realm of identifying and mitigating cyber-attacks. This scholarly article provides valuable insights into the pragmatic implementation of artificial intelligence (AI) in fortifying cyber security protocols through an exhaustive examination of existing literature and a comprehensive analysis of pertinent case studies [5].

The primary objective of this scholarly investigation is to explore the potential impact of artificial intelligence on enhancing the realm of cyber security within the domain of cyber-physical systems (CPS). This scholarly inquiry delves into the exploration and application of artificial intelligence methodologies in the realm of monitoring and safeguarding interconnected constituents of cyber-physical systems, encompassing domains such as industrial control systems and intelligent infrastructure, among various other illustrative instances. The research elucidates the paramount importance of incorporating AI-powered anomaly detection, predictive modeling, and real-time monitoring as fundamental constituents of an all-encompassing cyber security framework for Cyber-Physical Systems (CPS) in order to effectively counter emerging manifestations of cyber threats. The present study endeavor's to make a noteworthy contribution towards enhancing the resiliency and dependability of critical infrastructure, with a specific emphasis on the intricate challenges entailed in safeguarding Cyber-Physical Systems (CPS) [6]. The present comprehensive analysis provides a delineation of the intricate interplay between the domains of artificial intelligence and cyber security. Within the realm of scholarly inquiry, the present investigation delves into the domain of artificial intelligence (AI) and its various methodologies, such as data mining and machine learning, with the aim of exploring their prospective utility within the discipline of cyber security. The subject matter encompasses a diverse array of topics, spanning from the analysis of network traffic and assessment of vulnerabilities, to the detection of intrusions and analysis of malicious software. The present report offers valuable insights pertaining to the nascent realm of AI-driven cyber security solutions, meticulously examining the merits and demerits of diverse techniques propelled by artificial intelligence [7]. The authors embark upon a thorough and exhaustive examination of the current state of artificial intelligence and its myriad applications within the realm of computer and network security. The present investigation undertakes a comprehensive exploration of the foundational principles underlying artificial intelligence (AI)-enabled cyber security methodologies, meticulously scrutinizing pivotal concepts, methodologies, and nascent developments. This scholarly article delves into the exploration of machine learning algorithms, neural networks, and deep learning architectures in the realm of identifying and mitigating cyber threats. This study contributes to the existing body of knowledge regarding the multifaceted involvement of artificial intelligence (AI) in safeguarding digital assets, by undertaking a comprehensive evaluation of the efficacy of AI in the realm of cyber security, while concurrently addressing the inherent challenges it encounters [8]. This scholarly article presents a comprehensive investigation into the multifaceted applications of artificial intelligence in enhancing the realm of cyber security. The present study endeavor's to explore a multitude of artificial intelligence (AI)-based methodologies, encompassing anomaly detection, behavioral analysis, and threat intelligence. Furthermore, it aims to assess the capacity of these aforementioned techniques in fortifying the existing cyber security protocols. The present discourse delves into the profound import of artificial intelligence (AI) in the realm of automating the identification and subsequent counteraction of cyber threats. Considerable emphasis is duly accorded to the imperative of incorporating adaptive and self-learning systems as a means to effectively safeguard against the emergence of nascent attack vectors [9]. The focal point of this study lies in the utilization of artificial intelligence within the realm of cyber threats intelligence. The present study endeavor's to explore the potential utilization of artificial intelligence methodologies in the analysis and prediction of potential cyber threats, with the ultimate objective of enhancing the proactive identification and mitigation of impending cyber-attacks. This scholarly article provides valuable insights into the domain of AI-driven threat intelligence, thereby contributing to the enhancement of cyber security practices. The paper extensively delves into the utilization of machine learning algorithms for the purpose of analyzing vast volumes of data, with the objective of identifying discernible patterns and anomalies associated with cyber threats [10].

The primary objective of this research endeavor is to thoroughly examine and scrutinize the plausible utilization of artificial intelligence within the realm of cyber security, with a specific focus on its practical implications. The present study centers its attention on the various modalities through which artificial intelligence (AI)-based methodologies can be harnessed to augment the efficacy of cyber security protocols and effectively respond to emerging threats. This scholarly manuscript delves into the utilization of artificial intelligence (AI) techniques, encompassing machine learning and deep learning, within contemporary cyber security frameworks, with the aim of enhancing the efficacy of threat identification, incident response, and vulnerability management [11]. The primary focus of this study pertains to the applications of explainable artificial intelligence (XAI) within the realm of cyber security research. The present study offers a comprehensive examination of the contemporary landscape within the domain of enhancing transparency and interpretability in AI-driven cyber security systems. The primary objective of this endeavor is to enhance user confidence, accountability, and understanding pertaining to AI-generated insights through the examination and elucidation of strategies and techniques employed in expounding upon AI-driven judgments within the realm of cyber security scenarios [12]. In this scholarly investigation, a novel framework is posited, drawing inspiration from biological systems, to address the intricate challenge of cyber security. The primary objective of this study is to explore the potential of bio-inspired artificial intelligence (AI) methodologies in enhancing the security of critical systems. The discourse elucidates the potential of swarm intelligence, genetic algorithms, and neural networks in addressing cyber threats and vulnerabilities, thereby fostering the development of innovative and flexible cyber security solutions [13].

Chapter delves into the comprehensive examination and evaluation of the utilization of artificial intelligence techniques for the purpose of network intrusion detection within the realm of cyber security. Within the realm of this particular field of inquiry, the examination primarily revolves around the exploration and analysis of artificial intelligence (AI) techniques, specifically focusing on machine learning algorithms. The overarching objective is to ascertain the viability of these aforementioned methodologies as efficacious instruments in the identification and prevention of network-centric cyber-attacks. The present analysis delves into the utilization of artificial intelligence (AI)-powered intrusion detection systems (IDS) as a means to enhance the security of digital networks. This investigation also explores the inherent possibilities and challenges entailed in this endeavor [14]. The present research endeavor’s to examine the phenomenon of black box attacks on explainable artificial intelligence (XAI) methodologies within the domain of cyber security. This scholarly inquiry delves into the intricacies surrounding the inherent deficiencies and potential perils associated with cyber security solutions propelled by artificial intelligence. The aforementioned discourse underscores the imperative of fortifying the resilience and countering adversarial incursions within artificial intelligence (AI)-driven cyber security systems. It elucidates the potentiality of malevolent agents to exploit vulnerabilities inherent in AI models, thereby surmounting extant security protocols. The discourse centers upon the manner in which artificial intelligence models can be leveraged to circumvent security mechanisms [15].

3. Structure Built on Ideas:

In order to conduct a comprehensive investigation, the researcher has chosen to utilize primary data collection methods and employ a quantitative analytical approach. The assigned researcher was tasked with conducting an evaluation of the efficacy of artificial intelligence (AI) tools in mitigating vulnerabilities within the realm of cyber security, with a specific focus on the unique context of Iraq. The data was meticulously gathered by the diligent researcher from a cohort of highly knowledgeable Iraqi IT industry experts who possess a profound understanding of state-of-the-art methodologies, encompassing the realm of artificial intelligence (AI) and the intricate landscape of cyber security challenges. The rationale behind the selection of a sample size of 468 for this study is rooted in the notion that larger sample sizes tend to enhance the validity, reliability, and accuracy of empirical investigations. The present article can function as an initial reference for fellow researchers seeking to embark upon investigations pertaining to a relevant subject matter. Nevertheless, it is imperative to acknowledge that limited sample sizes are frequently deemed unfavorable and fail to guarantee the veracity and reliability of the obtained results (Fig.1).

To find the required respondents, they were asked questions and given a self-administered survey questionnaire constructed on the Likert scale. The participants received the questionnaire, which they were instructed to fill out with their opinions and experiences and then return. The participant might return the survey whenever it was convenient for them.

The data were initially assessed using the following methods: The proposed research methodology entails the utilization of confirmatory factor analysis (CFA) as a statistical technique to assess the measurement models fit to the observed data. CFA serves as a rigorous approach to evaluate the construct validity and reliability of the measurement instrument. Discriminant validity will be examined to ensure that the constructs under investigation are distinct from one another, thereby establishing their unique contributions to the research model.

Furthermore, The SEM approach and multiple regression models were used to ascertain the link between variables because the study's goal was to evaluate the relationship and mediation between components. The hypotheses were labeled as "accepted" or "rejected" based on the results.

4. Result:

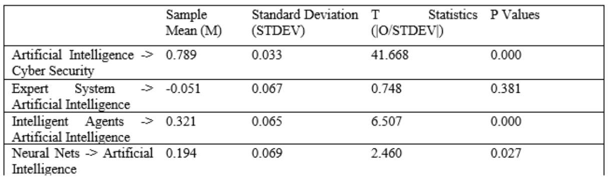
4.1. Confirming factor analysis

A confirmatory factor analysis was employed to evaluate the comprehensive validity of the model. The empirical assessment of the appropriateness of the study's variables was conducted, yielding a determined value of 0.6, which was deemed to possess the requisite level of adequacy. The table below presents a concise summary of the factor loadings, Cronbach's alpha, composite reliability, and AVE (Average Variance Extracted) values.

In accordance with the findings presented in Table 1, it is observed that all factor loadings surpass the threshold of 0.7. This noteworthy observation suggests that the factors under investigation exert a substantial influence on the variables in question. The aforementioned are the three pivotal constructs: Cronbach's Alpha, Composite Reliability, and Average Variance Extracted (AVE). The aforementioned indicators serve as a means of assessing the suitability of the model for further utilization in subsequent testing endeavors. The Cronbach Alpha coefficient, a widely used measure of internal consistency reliability, is considered to be a reliable indicator of the dependability of the underlying structures when it exceeds the threshold of 0.70. The results presented in Table 1 exhibit a remarkable consistency, with all values surpassing the threshold of 0.7. This noteworthy observation underscores the inherent reliability and promising utility of the aforementioned findings.

Composite reliability, akin to Cronbach's alpha, serves as an additional metric for assessing the reliability of the data. It provides insight into the internal consistency of the underlying constructs. In order to ensure a robust level of internal consistency within structures, it is imperative that the composite dependability values attain a minimum threshold of 0.70. The examination of the residual variance's explained variation by the predictors is conducted through the utilization of the Average Variation Extracted (AVE). Given the ubiquity of the 0.5 benchmark, it is imperative that the value of a variable surpasses the threshold of 0.5 in order to attain consideration. Table 1 exhibits the potential of the variables to be employed for subsequent hypothesis testing and model evaluation, while also indicating the internal consistency of the data. Coefficients of composite dependability found to be more than 0.70 suggest an adequate degree of internal consistency. Similarly, the average variance extracted coefficients surpass the criterion of 0.5, signifying a substantial amount of shared variance captured by the latent constructs.

Table 1: presents the coefficients derived from the model.

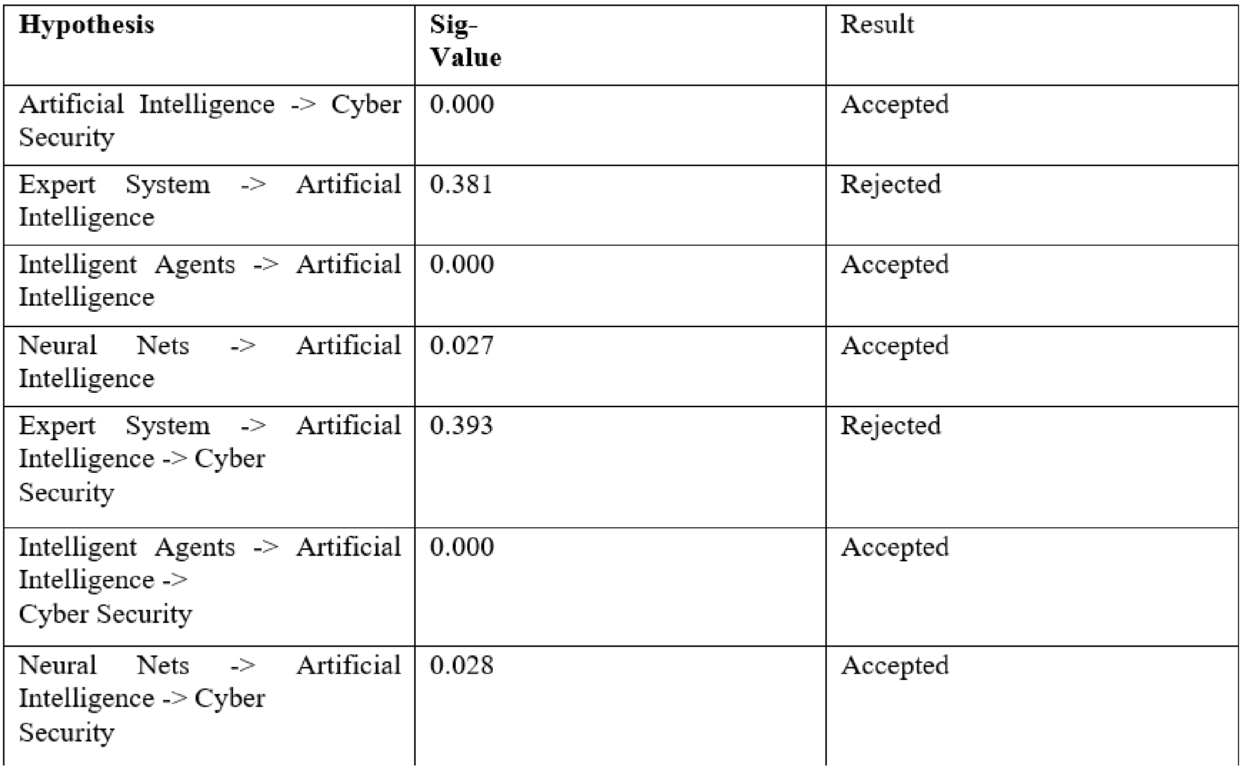


	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Artificial Intelligence -> Cyber Security	0.789	0.033	41.668	0.000
Expert System -> Artificial Intelligence	-0.051	0.067	0.748	0.381
Intelligent Agents -> Artificial Intelligence	0.321	0.065	6.507	0.000
Neural Nets -> Artificial Intelligence	0.194	0.069	2.460	0.027

4.2. Diverse Validity:

The subsequent phase of this investigation aims to evaluate the discriminant validity. The present inquiry aims to ascertain the veracity of the study's variables through the utilization of discriminant validity. Furthermore, this study delves into the profound implications of a variable's enduring interplay with other variables. The tabular representation presented below elucidates the interconnections and associations between the various conceptual entities. The utilization of the heterotrait-monotrait ratio (HTMT ratio) for the evaluation of discriminant validity is demonstrated. The models of Partial Least Squares (PLS) and Structural Equation Modeling (SEM), which serve as the foundation for evaluating and assessing models, can have their discriminant validity evaluated through a distinctive technique known as Heterotrait-Monotrait Ratio of Correlations (HTMT). Any variable that exceeds the predetermined threshold of 0.90, whether in terms of theoretical or empirical accuracy, can be considered erroneous. The requisite HTMT ratio exhibits a value of 0.90. The demonstration of conceptual and statistical precision of all variables and sub variables is evidenced by the observation that all HTMT values fall below the threshold of 0.90. The objective of the conducted experiments was to validate the veracity of the reflective constructs elucidated within this scholarly manuscript, thereby establishing a robust association or correlation with the indicators outlined in the path model as referenced by the citation.

Table 2: Evaluation of Hypotheses



Hypothesis	Sig- Value	Result
Artificial Intelligence -> Cyber Security	0.000	Accepted
Expert System -> Artificial Intelligence	0.381	Rejected
Intelligent Agents -> Artificial Intelligence	0.000	Accepted
Neural Nets -> Artificial Intelligence	0.027	Accepted
Expert System -> Artificial Intelligence -> Cyber Security	0.393	Rejected
Intelligent Agents -> Artificial Intelligence -> Cyber Security	0.000	Accepted
Neural Nets -> Artificial Intelligence -> Cyber Security	0.028	Accepted

4.3. Simple kind:

The present study incorporates a comprehensive model analysis encompassing the dependent variable of cyber security, the mediating variable of artificial intelligence (AI), and the independent variables of expert systems, neural networks, and intelligence agents. The inclusion of these variables allows for a thorough examination of their interrelationships and their respective impacts on the overall research framework. The tables presented below serve to elucidate the profound significance and distinctive characteristics inherent in the model under scrutiny.

The R square values for AI and cyber security. In contrast, it is noteworthy to mention that the recalibrated R square coefficients for the domains of artificial intelligence and cyber security exhibit values of 0.233 and 0.635%, respectively. The R-squared values serve to quantify the extent to which the variations in the dependent variables can be attributed to the independent variables. On the other hand, the adjusted R-squared is employed as a means to assess potential discrepancies or deficiencies in the data or findings.

The table 1 presents the inclusion of significant values (P-values) as they pertain to the study's incorporation of a mediating variable. In order to attain statistical significance, it is imperative that the observed outcomes exhibit a level of significance below the threshold of 0.05 ($P < 0.05$), as prescribed by the established standard value of P. Any quantity surpassing this threshold is deemed inconsequential and devoid of correlation. The statistical analysis reveals that the computed P value for the integration of artificial intelligence (AI) with cyber security is 0.000. This exceedingly small P value, which falls below the conventional threshold of significance (typically set at 0.05), suggests a strong indication of a meaningful relationship between AI and cyber security. It is worth noting that such a finding aligns with previous research, which has consistently demonstrated the substantial impact of AI in this domain. The observed significance levels pertaining to the expert system, intelligence agents, and neural agents are 0.492, 0.000, and 0.017, correspondingly. All the remaining values, with the exception of the expert system, pertain to the domain of artificial intelligence.

4.4. Evaluating the theories:

The meticulous scrutiny of hypotheses constitutes an indispensable phase within the analytical framework. Following the completion of the requisite examinations aimed at ascertaining the interrelationship between the variables, as well as their dependability and internal coherence, the investigator proceeds to assess the extent to which the hypothesis has been substantiated.

All alternative hypotheses were determined to be valid, except for the hypothesis pertaining to the expert system, as evidenced by the empirical findings presented in Table 2.

The obtained P-value of 0.000 signifies strong statistical evidence in favour of the initial hypothesis positing that artificial intelligence (AI) exerts a substantial and advantageous influence on the domain of cyber security. This inference is substantiated by a considerable corpus of empirical data. The obtained P-value of 0.492 indicates that there was no statistically significant influence observed in the analysed data. It is important to note that in order for an effect to be deemed significant, the P-value must be below the conventional threshold of 0.05. The empirical findings of this study have unequivocally established a noteworthy and affirmative influence of intelligent agents on the field of artificial intelligence, as evidenced by the remarkably low P-value of 0.000. The present study reveals a noteworthy observation, namely that the utilisation of expert systems exerts a substantial and favourable influence on the domain of artificial intelligence.

Moreover, a noteworthy correlation can be observed between neural networks and artificial intelligence, as evidenced by the derived P-value of less than 0.05. The P-value of the expert system, quantified at 0.49, surpasses the conventional significance level of 0.05. This observation indicates that the two variables under consideration exhibit independence, thereby influencing the domains of artificial intelligence and cyber security. The subsequent variable under investigation, namely intelligence agents equipped with artificial intelligence and focused on the domain of cyber security, exhibited a remarkably low p-value of 0.000.

Furthermore, an intriguing and noteworthy finding emerged from our investigation, revealing a statistically significant and positively inclined correlation coefficient of 0.018 between the domains of neural networks, artificial intelligence (AI), and cyber security.

5. Discussion:

The comprehensive analysis of the survey's results revealed that the utilization of artificial intelligence (AI) emerges as a pivotal asset for enterprises seeking to enhance their effectiveness in the realm of cyber security. In light of the substantial quantities of data and personal information that are susceptible to compromise by malevolent actors operating in the digital realm, the prevailing circumstances have unequivocally underscored the criticality of cyber security as an indispensable facet necessitating meticulous attention and management within the purview of every enterprise. Due to the rapid pace of globalization and the continuous advancements in technology, enterprises are progressively opting to store their clientele's financial and personal data within cloud-based infrastructures with greater frequency. Due to the escalating dependence on digital technology, there has been a concomitant surge in the occurrence of cyberattacks. Based on the findings of the study, it can be observed that all independent variables, with the exception of the expert system, exhibited significant and positive correlations. Notwithstanding the prevailing dissent among individuals towards this particular study, as well as numerous other studies that espouse the significance of expert systems, it is regrettable to report that this investigation failed to yield any statistically significant findings.

4.1. Limitations and potential outcomes:

The researcher claimed that a number of issues complicated the investigation. Two of the main problems were accessibility and the size of the response sample. The COVID issue prevented the researcher from contacting respondents one at a time; as a result, meetings were scheduled, and small groups filled out the surveys. Second, there weren't enough respondents; it is proposed that more data gathered from a bigger population might reinforce future findings.

Being confined to the Iraqi IT business was the researcher's only area of interest, which also constrained the study's geographic scope. Therefore, future studies could be improved by including additional Middle Eastern comparisons or by including more variables to measure the effects.

6. Conclusion

The researcher used a quantitatively analytical approach to the problem, using primary data gathered from people working in the information technology industry in Iraq. The thorough research that was carried out as part of this study yielded empirical data that unambiguously illustrate that the use of neural networks and intelligence agents has a significant and noticeable impact on the field of artificial intelligence. It should come as no surprise that there is an urgent need for data security to advance in tandem with the exponential growth of data storage made possible by advances in technology.

Acknowledgements

No funding sources.

Author contributions

All authors are equally contributed in preparing, experimenting and reviewing the article.

Conflicts of interest

The authors declare no conflicts of interest.

Reference:

[1] B. Thuraisingham, "The Role of Artificial Intelligence and Cyber Security for Social Media," *2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, New Orleans, LA, USA, 2020, pp. 1-3, doi: 10.1109/IPDPSW50202.2020.00184.

[2] Zhang, Z., Ning, H., Shi, F. *et al.* Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artif Intell Rev* **55**, 1029–1053 (2022). https://doi.org/10.1007/s10462-021-09976-0

[3] Bhatele, Kirti Raj, et al. "The Role of Artificial Intelligence in Cyber Security." *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems,* edited by S. Geetha and Asnath Victy Phamila, IGI Global, 2019, pp. 170-192. https://doi.org/10.4018/978-1-5225-8241-0.ch009

[4] Prasad, R., Rohokale, V. (2020). Artificial Intelligence and Machine Learning in Cyber Security. In: Cyber Security: The Lifeline of Information and Communication Technology. Springer Series in Wireless Technology. Springer, Cham. https://doi.org/10.1007/978-3-030-31703-4_16]

[5] Abbas, N.N., Ahmed, T., Shah, S.H.U. *et al.* Investigating the applications of artificial intelligence in cyber security. *Scientometrics* **121**, 1189–1211 (2019). https://doi.org/10.1007/s11192-019-03222-9

[6] H. Sedjelmaci, F. Guenab, S. -M. Senouci, H. Moustafa, J. Liu and S. Han, "Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems," in IEEE Network, vol. 34, no. 3, pp. 6-7, May/June 2020, doi: 10.1109/MNET.2020.9105926.
Li, Jh. Cyber security meets artificial intelligence: a survey. *Frontiers Inf Technol Electronic Eng* **19**, 1462–1474 (2018). https://doi.org/10.1631/FITEE.1800573

[7] Okutan and C. Eyüpoğlu, "A Review on Artificial Intelligence and Cyber Security," 2021 6th International Conference on Computer Science and Engineering (UBMK), Ankara, Turkey, 2021, pp. 304-309, doi: 10.1109/UBMK52708.2021.9558949.

[8] S. B.S., N. S., N. Kashyap and S. D.N., "Providing Cyber Security using Artificial Intelligence – A survey," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 717-720, doi: 10.1109/ICCMC.2019.8819719.

[9] R. Trifonov, O. Nakov and V. Mladenov, "Artificial Intelligence in Cyber Threats Intelligence," 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Mon Tresor, Mauritius, 2018, pp. 1-4, doi: 10.1109/ICONIC.2018.8601235.

[10] Ali, A. W. Septyanto, I. Chaudhary, H. A. Hamadi, H. M. Alzoubi and Z. F. Khan, "Applied Artificial Intelligence as Event Horizon Of Cyber Security," 2022 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2022, pp. 1-7, doi: 10.1109/ICBATS54253.2022.9759076.

[11] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," in IEEE Access, vol. 10, pp. 93104-93139, 2022, doi: 10.1109/ACCESS.2022.3204051.

[12] Demertzis, K., Iliadis, L. (2015). A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security. In: Daras, N., Rassias, M. (eds) Computation, Cryptography, and Network Security. Springer, Cham. https://doi.org/10.1007/978-3-319-18275-9_7

[13] Khan, S.U., Eusufzai, F., Azharuddin Redwan, M., Ahmed, M., Sabuj, S.R. (2022). Artificial Intelligence for Cyber Security: Performance Analysis of Network Intrusion Detection. In: Ahmed, M., Islam, S.R., Anwar, A., Moustafa, N., Pathan, AS.K. (eds) Explainable Artificial Intelligence for Cyber Security. Studies in Computational Intelligence, vol 1025. Springer, Cham. https://doi.org/10.1007/978-3-030-96630-0_6

A. Kuppa and N. -A. Le-Khac, "Black Box Attacks on Explainable Artificial Intelligence(XAI) methods in Cyber Security," 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 2020, pp. 1-8, doi: 10.1109/IJCNN48605.2020.9206780.

[14] Andraško, J., Mesarčík, M. & Hamuľák, O. The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. *AI & Soc* **36**, 623–636 (2021). https://doi.org/10.1007/s00146-020-01125-5

[15] S. Merat and W. Almuhtadi, "Artificial intelligence application for improving cyber-security acquirement," 2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE), Halifax, NS, Canada, 2015, pp. 1445-1450, doi: 10.1109/CCECE.2015.7129493.

[16] Mrs. Leena Rathi. (2014). Ancient Vedic Multiplication Based Optimized High Speed Arithmetic Logic . International Journal of New Practices in Management and Engineering, 3(03), 01 - 06. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/29

[17] Jaruwatcharaset, C. . (2023). Effects of Using a Temperature Control System in Bandicota indica Stalls with Internet of Things Technology. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 166–170. https://doi.org/10.17762/ijritcc.v11i4s.6324