Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, May : 2023

APPLICATION OF IT INDUSTRY AND THE EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE APPROACHES AGAINST CYBER SECURITY THREATS

[1]Dr. Anjaiah Adepu, Professor, CSE, St. Peter's Engineering College(A), Telangana, India
[2]Chennaiah Kate, Assistant Professor, IT, St. Peter's Engineering College(A), Telangana, India

[3]Chinni Krishnaiah.G. Assistant Professor CSE-AIML,Mallareddy University,Telangana,India

[4]Sreekanth Kottu, Assistant Professor IT, St. Peter's Engineering College(A), Telangana, India

[1]anjaiah@stpetershyd.com,[2]chennaiah@stpetershyd.com, [3]chinnikrishnaiahg@mallareddyuniversity.ac.in, [4]sreekanthkottu@gmail.com

ABSTRACT

The researcher chose a quantitative way of study design together with primary data in order to assess the efficiency of artificial intelligence solutions against cyber security issues, specifically in the instance of Iraq. The data was gathered by the researcher from IT industry workers. The study's sample size was 468, and its methods included confirmatory factor analysis, discriminant validity testing, basic model analysis, and hypothesis testing. Except for the expert system, which had no meaningful relationship to artificial intelligence or cyber security, all variables' P-values were found to be significant. Accessibility, geographic region, sample size, and the number of variables were the key problems.

KEYWORDS: Intelligent machines, Expert systems, Neural agents, agents for cyber-security intelligence

INTRODUCTION

The prevention of cyberattacks has emerged as a crucial and urgent issue in the modern world, entailing safeguarding the computer system from potential dangers [1]. According to White's depiction in [2], a cyberattack is a politically motivated attack against computer systems, information, programmes, and data that ends in violence being committed against non-combatant targets by sub-national parties. The development of new preventive measures is necessary due to the increased cyber dangers brought on by technological advancement. According to Huang et al. in [3], cyberattacks are becoming more frequent in the industrial sector, which results in physical damage to the facilities and the possible loss of millions of dollars in value. The fundamental cause of the rise in cyberattacks against businesses is the growing reliance on digital technology, which results in the storage of financial and personal data. Due to the fact that it not only results

in financial loss but also causes the leakage of sensitive information, it is thus regarded as one of the most significant difficulties in the contemporary environment.

According to [4], cyberattacks may affect everyone in the nation and include hacking, denial of service assaults, spyware infections, and malware infections. Cyberattacks also have a significant psychological impact on victims, leading to dissatisfaction, tension, and anxiety.

Artificial intelligence (AI) is a useful tool for lessening the damage of cyberattacks, as Taddeo noted in [5]. According to Bhatele et al. in [6,] AI is defined as machine intelligence that carries out activities normally associated with intelligent beings.

When making decisions, such as when conducting medical diagnoses or drawing conclusions from knowledge, the expertise of human specialists is incorporated. In terms of cyber security, Taddeo in [5] has shown that AI has both positive and negative consequences, with the negative implications being that it may facilitate the escalation of assaults, leading to faster and more damaging attacks. Moving in the right direction, AI enhances defensive strategies, fosters security in cyberspace, and dramatically improves cyber security. Additionally, Conti et al. state in [7] that AI helps security experts recognize signs of a cyberthreat. Due to AI, the use of machine learning for malware analysis and network anomaly detection has increased. According to the literature, the major goal of the study is to evaluate the efficacy of artificial intelligence approaches for increasing defenses against cyber security threats, notably in Iraq. For instance, the research done by [5] has shown that AI may either intensify the process of assaults by producing faster and more painful attacks or it can result in the enhancement of cyber security. Therefore, the main goal of the research is to ascertain how AI may be used in Iraq to defend against cyberattacks, which would improve cybersecurity. The report is significant because it highlights the value of AI technology to IT workers for adopting preventive measures against cyberattacks.

2. LITERATURE REVIEW

The percentage of internet users in Iraq has climbed from 47% in 2011 to 74.9% in 2016, indicating that 24 million people use the internet for social media, online games, and other purposes. For the most part, Iraq Telecom is in charge of providing internet access to users. However, the rise in internet usage has also contributed to an uptick in computer crimes.

Regarding cybercrime, Iraq has seen three significant examples in particular. The State Oil Company was the target of the first significant incident in 2012, when a virus struck and destroyed computer drives and information with the intention of halting oil production. The second significant incident included the hacking of Baghdad University, while the last big incident involved government administration and the interruption of government activities [8–14]. Additionally, research by [15] showed that cybercrimes are spreading around the world, making it essential for nations to maintain robust cybersecurity. By creating rules and regulations and putting an emphasis on improving cyber-security, Iraq has taken the initiative to increase cyber-security.

The fundamental goal of AI in Iraq was to generate intelligence that was comparable to or superior to that of humans in order to improve the cognitive system. Healthcare, robotics, retail, and the insurance business are just a few of the sectors that AI has begun to permeate. The AI revolutions have not yet been completely accepted by Iraq, though. It has been determined that the nation is investing significantly in artificial intelligence by concentrating on the communication network, availability of mentors, finance, development of the infrastructure, and manufacturers [16–20]. Similar to this, research by [21] shown that the rise of AI, notably in Saudi Arabia's higher education, has helped to advance educational quality and learning outcomes. AI integration has benefited information technology (IT) in other ways as well, including critical thinking, communication, problem-solving, technological literacy, and creativity. The second significant incident included the hacking of Baghdad University, while the last big incident involved government administration and the interruption of government activities [8–14]. Additionally, research by [15] showed that cybercrimes are spreading around the world, making it essential for nations to maintain robust cybersecurity. By creating rules and regulations and putting an emphasis on improving cyber-security, Iraq has taken the initiative to increase cyber-security.

The fundamental goal of AI in Iraq was to generate intelligence that was comparable to or superior to that of humans in order to improve the cognitive system. Healthcare, robotics, retail, and the insurance business are just a few of the sectors that AI has begun to permeate.

H1: Cybersecurity is significantly improved by artificial intelligence, which lessens the impact of cyberattacks.

The expert system, which is used to recognize questions supplied by clients or software, is the most widely used AI technique. Expert systems are offered in a variety of configurations, from compact systems to hybrid systems used for diagnostics. The system is also employed to provide security for cyber defense [28–31]. Similar to this, the work by [32] showed how expert systems use input data to assess vulnerabilities and the amount of hazard associated to transactions on e-commerce platforms. In light of this, the expert system has formed the following hypothesis.

H2: Expert systems play a big, helpful function in artificial intelligence.

H3: Cybersecurity and expert systems are significantly mediated by artificial intelligence.

Neural nets, commonly referred to as deep learning, are a further cutting-edge aspect of AI technology. It was primarily influenced by how the human brain worked, which has many neurons that are capable of learning any kind of material. When used in conjunction with cyber security, the system can assist in determining if a file is harmful or valid without the involvement of a person. In contrast to the traditional machine learning method, neural nets produce a strong performance in identifying harmful threats [33–36]. Additionally, [37] has similarly illustrated how a neural network enables easy monitoring of the computer's security as well as corrective action. In light of this, the following neural network assumptions are built.

H4: Neural networks play a big part in artificial intelligence's ability to defend against cyberattacks.

H5: Cybersecurity and artificial intelligence are significantly mediated by each other.

According to a research by [33], an intelligent agent is a separate entity of AI that primarily recognises movement through sensors while paying attention to the environment's actual cues, or agents, and focuses its own activity towards the accomplishment of objectives. The main purpose of intelligent agents is to defend against distributed denial of service (DDoS) assaults. The technologies also offer proactive measures, mobility, and a language for agent communication, among other benefits. According to a research by [28], intelligent agents are independent computer systems that cooperate with one another to defend against online attacks. The study also acknowledges that the intelligent agent is primarily created to counteract DDoS by assisting cyber agents in communication and mobility.

H6: Intelligence agents play a big part in artificial intelligence's ability to defend against cyberattacks.

H7: Cybersecurity and artificial intelligence work well together thanks to artificial intelligence.

2.1 Theoretical framework

The researcher chose a quantitative approach of research design combined with primary data for the subsequent complete investigation. The study wanted to see how well artificial intelligence methods protected against cyber security dangers, specifically in the situation of Iraq. The data was gathered by the researcher from workers in Iraq's IT sector who were well-versed in cutting-edge techniques including artificial intelligence (AI) and cyber security challenges. The sample size for this study was 468 because larger samples provide for more accurate, trustworthy, and authentic results. This research article can be used as a starting point for other researchers who want to do research in a related field.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, May : 2023

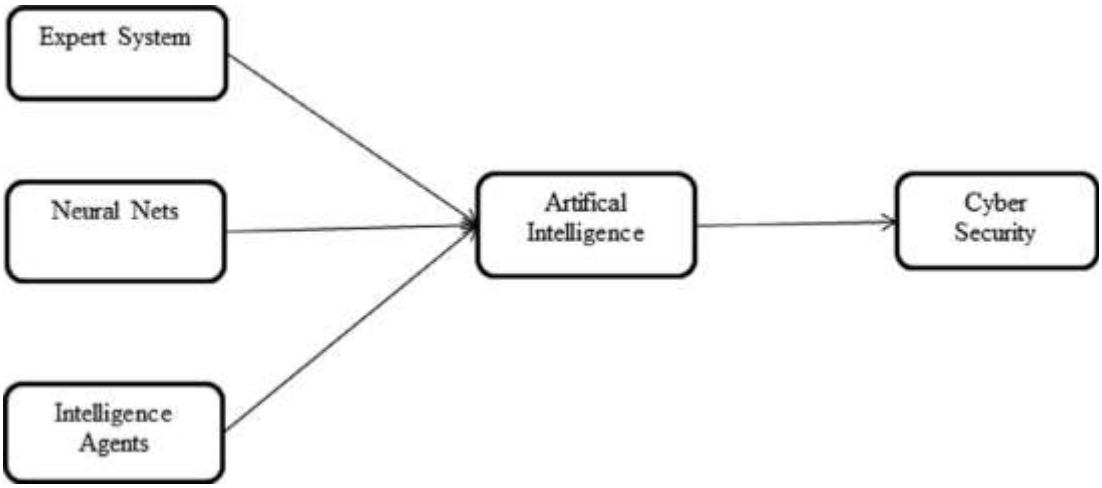

Fig 1. Conceptual Framework.

A lower sample size, however, is usually a drawback and does not ensure the validity of the findings [38] (Fig. 1). In order to reach the required respondents, a survey questionnaire based on a Likert scale was employed, and it was delivered to them for self-administering in the event of any questions. The questionnaire was filled out by the respondents based on their opinions and experiences, and they were invited to provide feedback. The questionnaire was returned at the respondent's convenience.

After that, Smart PLS was used to assess the data. Confirmatory factor analysis, discriminant validity, basic model analysis, and finally hypothesis assessment were the data analytic approaches used. The variables constructions were first examined to see if they are linked to one another or not using the data. Multiple regression models were employed to identify the association between variables since the researcher's goal was to investigate the relationship as

well as whether or not mediation existed between the variables. The created hypotheses were classified as "accepted" or "rejected" based on the outcomes.

3. RESULT

3.1. Confirmatory factor analysis

Confirmatory factor analysis was utilized to determine the model's overall fitness. The proper value of 0.6 was chosen in order to assess the fitness of the study's variables. The values acquired from factor loadings, Cronbach's alpha, composite reliability, and AVE (Average Variance Extracted) are summarized in the table below.

Table 1

	Factor Loadings	Cronbach Alpha	Composite Reliability	AVE
AI1	0.835	0.896	0.928	0.762
AI2	0.870			
AI3	0.886			
AI4	0.900			
CSY1	0.656	0.790	0.851	0.540
CSY2	0.637			
CSY3	0.611			
CSY4	0.868			
CSY5	0.859			
ES1	0.881	0.861	0.915	0.782
ES2	0.907			
ES3	0.865			
IA1	0.883	0.874	0.923	0.799
IA2	0.921			
IA3	0.877			
NN1	0.799	0.817	0.891	0.733
NN2	0.894			
NN3	0.871			

All factor loading values in Table 1 above are more than 0.7, indicating that factors have a significant impact on the variables. Cronbach Alpha, Composite reliability, and AVE are the following significant values that are displayed above. These metrics demonstrate the model's fitness and whether or not they are suitable for additional testing. Cronbach Alpha measures the constructions' dependability, and a desired or ideal value should be more than 0.7. All results are above 0.7, as shown in Table 1, indicating their reliability and potential for further application.

Similar to Cronbach Alpha, composite reliability is a different metric for evaluating the data's dependability and it shows how consistently the constructs are expressed inside. To guarantee excellent internal consistency in constructions, the minimal values of composite reliability should be greater than 0.7. The variation that is explained by residual variance predictors, on the other hand, is examined using AVE (Average variation Extracted). Its established benchmark value is 0.5, therefore for the variables to be considered significant, their values must be more than 0.5. The fact that Table 1 above's AVE values are greater than 0.5 and the composite reliability values are greater than 0.7 indicates that the data are internally consistent in addition to demonstrating that the variables are appropriate for further testing of hypotheses and model evaluation.

3.2. Discriminant validity

Discriminant validity is tested in this study article's second testing phase. Discriminant validity is a technique used to assess the precision of the study's variables. It also indicates how much a variable affects whether or not it is connected to other variables overall. The findings below demonstrate whether or not the constructions are connected to one another.

The HTMT ratio (Heterotrait -Monotrait Ratio), which is demonstrated in Table 2, is used to evaluate discriminant validity. Another innovative technique for evaluating the discriminant validity in the PLS, SEM approach that serves as the foundation for model evaluation and assessment, is HTMT. Any variable whose values surpass the benchmark value of 0.90 indicates that it is conceptually or statistically inaccurate. The HTMT ratio must be 0.90. All of the HTMT values produced, as seen in Table 2 above, are less than 0.90, indicating conceptual and statistical accuracy for all variables and sub-variables. Applying these tests was done to make sure that the route model's indicators and the reflective constructs in this article had a significant relationship or link [39].

3.3. Basic model

Expert systems, neural networks, and intelligence agents are the independent variables in this article's model analysis, together with AI as the mediating variable and cyber security as the dependent variable. The significance of the model and key model attributes are displayed in the tables below.

According to Table 3 above, the model's R square value for AI and cyber security, respectively, is 0.238 and 0.636. On the other side, for AI and cyber security, the corrected R square values are 0.233 and 0.635, respectively. This shows that R square values reveal the differences in the data produced by the independent variables in the dependent, whereas R square adjusted is used to evaluate any inconsistencies or inaccuracies in data or outcomes. The model's coefficients are displayed in the following Table 4 above.

The significant values (P-value) are also shown in the above table since the research also includes a mediating variable. The required findings should be less than 0.05 (P 0.05), according to the conventional value of P, in order to be considered significant. Any value over it is regarded as being irrelevant and having no relationship. The P value for AI with cyber security is 0.000, which is quite important, as was previously mentioned. Following this are the significance values for the expert system, intelligence agents, and neural agents, which are 0.492, 0.000, and 0.017, respectively. Only one of these values—the expert system—does not relate to artificial intelligence, but the others do.

3.4. Evaluation of hypotheses

The next crucial step in the analysis process is the evaluation of the hypotheses. The researcher now assesses whether the hypothesis was true or not after performing all necessary tests to determine the link between variables and their reliability and internal consistency.

Apart from the expert system, it is clear from the data in Table 5 above that all other hypotheses were accepted.

The initial hypothesis was that AI has a large and beneficial influence on cyber security. It was discovered that since the P-value was 0.000, a significant impact does indeed exist.

The P-value was 0.492, therefore there is no significant influence since the P value should be less than 0.05, according to the research on expert systems' significant and positive effects on artificial intelligence. As a result of the P-value being 0.000, it was determined that intelligent agents had a large and beneficial influence on artificial intelligence.

Furthermore, there is a substantial relationship between neural networks and artificial intelligence, as evidenced by the P-value of 0.017, which is less than 0.05. The expert system came next, which has an influence on both artificial intelligence and cyber security. It achieved a P-value of 0.493, which is larger than 0.05, indicating that there is no correlation between these factors. The following variable, intelligence agents with cyber security and artificial intelligence, had a P value of 0.000.

Similar to this, a significant and favorable influence was shown since the correlation between neural networks, artificial intelligence, and cyber security was 0.018.

					Nets
Artificial Intelligence					
Cyber Security	0.889				
Expert System	0.350	0.440			
Intelligent Agents	0.529	0.585	0.730		
Neural Nets	0.413	0.562	0.684	0.625	

Table 3 Model.

	R Square	R Square Adjusted
Artificial Intelligence	0.238	0.233
Cyber Security	0.636	0.635

DISCUSSION

The study's overall findings suggested that AI has emerged as one of the key resources for businesses looking to increase their performance in terms of cyber security. Because there is a potential that enormous amounts of data and sensitive information may be targeted by online hackers, the current scenario has demonstrated that cyber security is one of the crucial elements that any organization must assure. The personal and financial information of businesses is saved in the cloud as a result of fast globalization and technological progress, and as a result of this greater reliance on digital technology, cyberattacks have risen in frequency. The study's conclusions showed that, with the exception of the expert system, all independent variables exhibited meaningful and favorable relationships.

Table 4
Model Coefficients.

	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)
Artificial Intelligence -> Cyber Security	0.797	0.023	34.668
Expert System -> Artificial Intelligence	0.041	0.065	0.688
Intelligent Agents -> Artificial Intelligence	0.411	0.062	6.607
Neural Nets -> Artificial Intelligence	0.164	0.068	2.390

Table 5
Hypothesis Assessment.

S. NO	Hypothesis	Sig-Value	Result
1	Artificial Intelligence -> Cyber Security	0.000	Accepted
2	Expert System -> Artificial Intelligence	0.492	Rejected
3	Intelligent Agents -> Artificial Intelligence	0.000	Accepted
4	Neural Nets -> Artificial Intelligence	0.017	Accepted
5	Expert System -> Artificial Intelligence -> Cyber Security	0.493	Rejected
6	Intelligent Agents -> Artificial Intelligence -> Cyber Security	0.000	Accepted
7	Neural Nets -> Artificial Intelligence -> Cyber Security	0.018	Accepted

4.1 Limitation and potential future implications

The researcher encountered a lot of obstacles while working on this investigation. Accessibility and the size of the responder sample was one of the main problems. The researcher was unable to

personally contact the respondents due to the present COVID situation, but meetings were set up and questionnaires were filled out in small groups. The results might be even better in the future, it is proposed, if additional information is gathered from a big number of individuals due to the limited number of respondents.

Additionally, because the study was geographically constrained by the researcher's only emphasis on the IT sector in Iraq, it may be enhanced in the future by doing additional comparisons with other Middle Eastern nations or by including other factors in the analysis.

CONCLUSION

In conclusion, it can be said that the researcher conducted a quantitative study using primary data gathered from workers in Iraq's IT industry. Intelligence agents and neural nets have a major influence on artificial intelligence, according to the results of the hypothesis testing. Technology development has resulted in more data being stored, which calls for higher levels of data security.

REFERENCES

[1] M. Komar et al., ‘‘High performance adaptive system for cyber-attacks detection,” in 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017, vol. 2, pp. 853–858.
[2] J. White, Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies, Glob. Secur. Stud., 7 (4) (2016).
[3] K. Huang, C. Zhou, Y.-C. Tian, S. Yang, Y. Qin, Assessing the physical impact of cyberattacks on industrial cyber-physical systems, IEEE Trans. Ind. Electron. 65 (10) (2018) 8153–8162.
[4] M. Bada, J.R.C. Nurse, The social and psychological impact of cyberattacks, in Emerging Cyber Threats and Cognitive Vulnerabilities, Elsevier, 2020, pp. 73– 92.
[5] M. Taddeo, Three ethical challenges of applications of artificial intelligence in cybersecurity, Minds Mach. 29 (2) (2019) 187–191.
[6] K.R. Bhatele, H. Shrivastava, N. Kumari, The Role of Artificial Intelligence in Cyber Security, in Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems, IGI Global, 2019, pp. 170–192.
[7] M. Conti, T. Dargahi, A. Dehghantanha, Cyber threat intelligence: challenges and opportunities, Cyber Threat Intelligence, Springer (2018) 1–6.
[8] S. Alshathry, Cyber attack on saudi aramco, Int. J. Manag., 11 (5) (2016).
[9] S. Al Amro, Cybercrime in Saudi Arabia: fact or fiction?, Int. J. Comput. Sci. Issues 14 (2) (2017) 36.
[10] H.J. Mohammed, H.A. Daham, Analytic hierarchy process for evaluating flipped classroom learning, Comput. Mater. Contin. 66 (3) (2021) 2229– 2239.

[11] H.J. Mohammed, I.A. M. Al-Jubori, M.M. Kasim, Evaluating project management criteria using fuzzy analytic hierarchy Process, AIP Conf. Proc., 2138 (1) (2019) 040018(1–6).

[12] H.J. Mohammed, M.M. Kasim, I.N. Shaharanee, Selection of suitable e-learning approach using TOPSIS technique with best ranked criteria weights, AIP Conf. Proc., 1905 (2017) 040019(1–6).

[13] H.J. Mohammed, M. Kasim, I.N. Shaharanee, Evaluation of e-learning approaches using AHP- TOPSIS technique, J. Telecommun. Electron. Comput. Eng. 10 (1–10) (2018) 7–10.

[14] S. Hashemi, A. Marzuki, H.J. Mohammed, S. Kiumarsi, The effects of perceived conference quality on attendees' behavioural intentions, Anatolia 31 (3) (2020) 360–375.

[15] T.S. Alshammari, H.P. Singh, Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index, Arch. Bus. Res., 6 (12) (2018).

[16] S.M. Ahmed, Artificial intelligence in Saudi Arabia: Leveraging entrepreneurship in the Arab markets, 2019 Amity International Conference on Artificial Intelligence (AICAI) (2019) 394–398.

[17] B. Alhayani, M. Rane, Face recognition system by image processing, Int. J. Electron. Commun. Eng. Technol. 5 (5) (2014) 80–90.

[18] B. Alhayani, H. Ilhan, Hyper spectral image classification using dimensionality reduction techniques, Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng. 5 (4) (2017) 71–74.

[19] B. Alhayani, A. Abdallah, Manufacturing intelligent corvus corone module for a secured two way image transmission under WSN, Eng. Comput. 37 (9) (2020) 1–17.

[20] B. Alhayani, H. Ilhan, Visual sensor intelligent module based image transmission in industrial manufacturing for monitoring and manipulation problems, J. Intell. Manuf. 4 (2020) 1–14.

[21] M. Elhajji, A.S. Alsayyari, A. Alblawi, Towards an artificial intelligence strategy for higher education in Saudi Arabia, in: 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), 2020, pp. 1–7.

[22] S. Zeadally, E. Adi, Z. Baig, I.A. Khan, Harnessing artificial intelligence capabilities to improve cybersecurity, IEEE Access 8 (2020) 23817– 23837.

[23] I.Z. Chaloob, R. Ramli, M.K.M. Nawawi, A new multi-interval weights approach in fuzzy goal programming for a multi-criteria problem, Int. J. Math. Oper. Res. 9 (2) (2016) 214–229.

[24] I.Z. Chaloob, R. Ramli, M.K.M. Nawawi, Measuring economic and environmental efficiency for agricultural zones in Iraq using data envelopment analysis, Int. J. Inf. Decis. Sci. 10 (3) (2018) 235–248.

[25] I.Z. Chaloob, R. Ramli, M.K.M. Nawawi, Using simulation and data envelopment analysis to evaluate Iraqi regions in producing strategic crops, AIP Conf. Proc. 1635 (1) (2014) 525–529.

[26] E. Madhok, A. Gupta, N. Grover, Artificial Intelligence Impact on Cyber Security, IITM J. Manag. IT 7 (1) (2016) 100–107.
[27] A. Szychter, H. Ameur, A. Kung, H. Daussin, The Impact of Artificial Intelligence on Security: a Dual Perspective, Taylor & Francis Taylor & Francis Group http://taylorandfrancis. com, 2018.
[28] A. Anwar, S.I. Hassan, Applying artificial intelligence techniques to prevent cyber assaults, Int. J. Comput. Intell. Res. 13 (5) (2017) 883–889.
[29] H.J. Mohammed, M.M. Kasim, A.K. Hamadi, E.A. Al-Dahneem, Evaluating of collaborative and competitive learning using MCDM technique, Adv. Sci. Lett. 24 (6) (2018) 4084–4088.
[30] H.J. Mohammed, M.M. Kasim, I.N. Shaharanee, Multi-criteria evaluation of elearning approaches, in Proceedings of the 6th International Conference on Computing and Informatics, 2017, no. May.
[31] H.J. Mohammed, M.M. Kasim, E.A. AL-Dahneem, A.K. Hamadi, An analytical survey on implementing best practices for introducing e-learning programs to students, J. Educ. Soc. Sci., 5 (2) (2016) 191–196.
[32] K. Pal, R. Tiwari, S. Maheshwary, Implementation of artificial intelligence methods to curb cyber assaults: A review, Int. Res. J. Eng. Technol. (2018) 1466–1469.
[33] A. Panimalar, G. Pai, S. Khan, Artificial intelligence techniques for cyber security, Int. Res. J. Eng. Technol. 5 (3) (2018) 122–124.
[34] H.J. Mohammed, E. AL-dahneem, A. Hamadi, A comparative analysis for adopting an innovative pedagogical approach of flipped teaching for active classroom learning, J. Glob. Bus. Soc. Entrep., 3 (5) (2016) 86–94.
[35] J.S. Ahmed, H.J. Mohammed, I.Z. Chaloob, Application of a fuzzy multiobjective defuzzification method to solve a transportation problem, Mater. Today Proc. (2021).
[36] H.A. Daham, H.J. Mohammed, An evolutionary algorithm approach for vehicle routing problems with backhauls, Mater. Today Proc. (2021).
[37] A. Magcale, D. Kekai, Artificial intelligence with cyber security, Google Patents (2018).
[38] N. Blaikie, Confounding issues related to determining sample size in qualitative research, Int. J. Soc. Res. Methodol. 21 (5) (2018) 635–641.
[39] M.R. Ab Hamid, W. Sami, M.H.M. Sidek, Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion, J. Phys. Conf. Ser. 890 (1) (2017) 12163.