Research Article

Advances in Machine Learning & Artificial Intelligence

Reviewing Effectiveness of Artificial Intelligence Techniques Against Cyber Security Risks: In Case of It Industry in Saudi Arabia

Mohammed I Alghamdi*

Department of Computer Science, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

***Corresponding author**
Mohammed I Alghamdi, Department of Computer Science, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

Submitted: 20 Oct 2020; **Accepted:** 26 Oct 2020; **Published:** 05 Nov 2020

Summary

Aim: *The aim of the researcher was to determine the effectiveness of artificial intelligence techniques against cyber security risks particularly in case of Saudi Arabia*

Method: *Researcher has opted for quantitative method of research design along with primary data. The researcher collected the data from employees working in this I.T industry of Saudi Arabia. The sample size for this study was 468 and confirmatory factor analysis, discriminant validity, basic analysis of model and lastly, hypothesis assessment was carried out.*

Findings: *The P-values of all variables were obtained as significant apart from expert system which had no significant relation with artificial intelligence and cyber security.*

Limitations: *Geographical area, sample size, less variables and accessibility was the main issue.*

Keywords: Artificial intelligence, Cyber-security, Expert system, Intelligence agents, Neural agents,

Introduction

In the contemporary environment, the protection against cyber-attacks has become a vital and urgent issue which involves protecting the computer system from possible threats [1]. White has depicted that the term cyber-attack defined by the U.S Federal Bureau Investigations is a politically involved attack against computer systems, information, program and data that results in causing violence against non-combatant targets by sub-national groups [2]. Advancement in technology is also leading to higher cyber threats which requires in developing new preventive measures. Huang, Tariq has indicated that cyber-attacks are increasing in the industrial area that leads towards physical damages to the facilities that leads to potential loss of million-dollar worth [3, 4]. The rationale behind the increase of cyber-attacks among companies is mainly due to the increasing dependence on digital technology which causes the financial and personal information to be stored. Thus, it is considered as the most important challenges in the current scenario as it not only leads to financial loss but also causes leakage to sensitive information.

According to Bada and Nurse the cyber-attacks range from hacking, denial of services, spyware and malware infections that can result in affecting everyone in the country [5]. Cyber-attacks also result in causing major psychological effects among the individuals resulting in frustration, stress and anxiety.

Taddeo pointed out that the artificial intelligence (AI) is an effective activity for reducing the impact of cyber-attacks [6]. Bhatele, Sharivastava and Kumari have defined AI as the machine intelligence that performs tasks that are associated with the intelligence being [7]. The knowledge of human experts is embedded for the decision making such as for conducting medical diagnosis and gaining insights from knowledge in making a decision. In respect to cyber security, Taddeo has demonstrated that AI causes both bad and good effects in which the bad effects of AI are that it has a risk of facilitating the escalation process of the attacks for causing faster and more impactful attacks [6]. Moving towards good effect, AI leads to significantly improving the cyber security along with enhancing defensive measures and fostering security in cyberspace. In addition, Conti, Dehghantanha and Dargahi that AI provides the security professionals for identifying cyber threat indicators [8]. AI has led to increasing usage of machine learning for conducting malware analysis along with network anomaly detection.

With respect to the literature, the following study is mainly conducted to analyze the effectiveness of artificial intelligence

techniques for enhancing against cyber security risks particularly in Saudi Arabia. For instance, the study conducted by Taddeo has depicted that AI has both good and bad effect on cyber-security as it can either escalate the process of attacks of causing faster and painful attacks or can result in enhancing the cyber security [6]. Hence, the primarily objectives of the research are to determine the role of artificial intelligence in Saudi Arabia in countering against the cyber-attacks that leads to enhancing cyber-security. The significance of the study is that it provides the importance of AI technologies among the IT professionals for taking preventive measure against cyber-attacks.

Literature Review

In Saudi Arabia, the admittance of internet in 2016 has increased to 74.9% from 47% in 2011 where it illuminates that 24 million individuals are utilizing the internet for social media, internet-based games and other. Saudi Telecom is mainly responsible for the distribution of the internet to the customers. However, with the incline of internet usage has also led to the increase of computer crimes. There are particularly three major cases that have occurred in Saudi Arabia regarding cybercrime. The first major case is reflected to the State oil company Aramco where it was hit by virus in 2012 that resulted in causing demolition to information and drives to computer which was aimed to stopping the oil production. The second major case is related with King Saud University which was hacked where the last major case is reflected to government administration that led to the disruptions on operations of government [9-11]. In addition, study conducted by Alshammari and Singh (2018) has depicted that cyber-crimes are increasing around the globe where it is critical for the countries to have strong cyber-security. Saudi Arabia has been taking initiative for enhancing the cyber-security by developing laws and regulation along with focusing on enhancing cyber-security [12].

The main idea of AI in Saudi Arabia was to enhance the cognitive system by developing similar or better intelligence than humans. AI technology has started to infiltrate various industries which comprises of healthcare, robotics, retail and insurance industry. However, Saudi Arabia has not yet fully embraced the AI revolutions. It is identified that the country is making significant investment on the artificial intelligence by focusing on communication network, accessibility to mentors, funding, infrastructure development and manufacturers [13]. Similarly, study conducted by Elhajji, Alsayyari and Alblawi has indicated that the emergence of AI particularly in the higher education of Saudi Arabia has contributed towards promoting educational quality and learning outcome [14]. The incorporation of AI has also contributed towards the information technology (IT) in respect to critical thinking, communication, problem solving, technological literacy and creativity.

In the past few years, many of the researchers have started exploring the approaches of AI for enhancing the cyber-security. The term cyber-security is referred to the processes, system and human behaviour that supporting in safeguarding the electronic resources. AI has been identified as a versatile technique for determining false information along with evaluating large amount of data [15]. Similarly, the study conducted by Maddox, Gupta and Grover has depicted that the artificial intelligence is getting strong recognition towards assisting the users for fighting crime and resolving problems in cyber space [16]. AI mainly supports in identifying the viruses, designing solutions and deploying solutions that support in countering against the cyber-crime. Szychter has also that many organizations are incorporating AI as it can enhance the security of internet of things (IoT) by predicting or detecting malicious activities. In the basis of the literature, the following hypothesis has been developed [17].

H1: *Artificial intelligence has a significant and positive effect on cyber-security which reduces the impact of cyber-attack*

The most common tool that is used for the AI is the expert system which utilized for identifying inquiries that are presented by client or software. Expert systems are provided in different forms which ranges from small system to hybrid system that is utilized for diagnostic purposes. In addition, the system is utilized for providing security in the cyber defense [18]. Similarly, the study conducted by Pal, Tiwari and Maheshwary has depicted that expert system utilizes the input data for identifying vulnerability along with the threat level related to the transaction on E-commerce websites. Hence, in this manner, the following hypothesis has been developed for expert system.

H2: *Expert system has a significant and positive role on the artificial intelligence.*

H3: *Artificial intelligence has a significant mediating effect between the expert system and cyber-security.*

Another effective technology and advanced branch for the AI is the neural nets which is also known as the deep learning. It was mainly inspired by the functions of the human brain that was associated with several neurons that can learn any type of data. When applied with the cyber-security, the system can support in identifying whether there is a file malicious or legitimate without the interference of human. Neural nets yield a strong result in determining the malicious threats in comparison with the classical machine learning system [19]. In addition, Magcale and Kekai has similarly depicted that neural network allows in easily monitoring the security of the computer while also taking remedial action [20]. Hence, in this perspective, the following hypotheses are designed in respect to neural nets:

H4: *Neural nets has a significant role on the artificial intelligence for countering against cyber-attacks.*

H5: *Artificial intelligence has a significant mediating effect between the Neural Nets and cyber-security.*

As per the study conducted by Panimalar, Pai and Khan intelligent agent is an independent entity of the AI where it mainly recognizes the movement through sensors while following the environment

actual indication i.e. an agent and directs its overlay activity towards the achievement of goals [19]. Intelligent agent is mainly created for countering against the distributed denial of services (DDoS) attacks. The tools also have several advantages as it provides with proactive measures, mobility and agent communication language. In respect to study of Anwar and Hassan [18], intelligent agents are self-sufficient computer system that shares information with each other while fighting cyber assaults. Moreover, the study also recognizes that the intelligent agent is mainly designed for countering against the DDoS through the support of cyber agent's communication and movement. In this manner, the following hypotheses are designed for the study that concentrates on intelligence agent:

3.0 Conceptual Framework

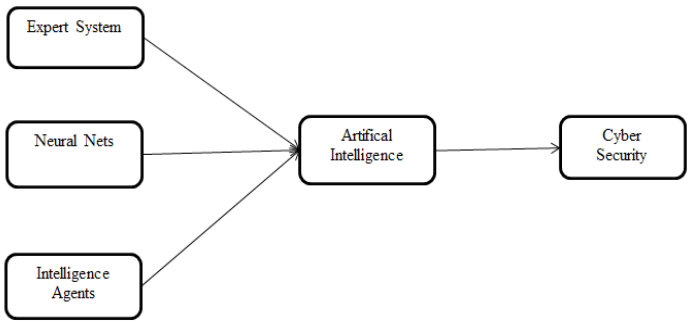

Figure 1: Conceptual Framework

Methodology

For the following comprehensive study, the researcher has opted for quantitative method of research design along with primary data. The aim of the researcher was to determine the effectiveness of artificial intelligence techniques against cyber security risks particularly in case of Saudi Arabia. The researcher collected the data from employees working in this I.T industry of Saudi Arabia who possess thorough knowledge about advanced methods such as artificial intelligence technology and cyber security issues. The sample size for this study was 468 because with increased sample size, the study becomes more accurate, reliable and authentic. Other researchers who wish to conduct study in similar domain can use this research article as a base paper. However, a smaller sample size is always a limitation and does not guarantees the authenticity of the results [21].

A survey questionnaire was used based on Likert scale for reaching out to the desired respondents and was distributed among them by self-administering in case of any queries. The respondents filled the questionnaire as per their opinion and experiences and were asked to share to return back. Based on the respondents own convenience, the questionnaire was returned. The data was then analysed through the use of Smart PLS. The data analysis techniques adopted were confirmatory factor analysis, discriminant validity, basic analysis of model and lastly, hypothesis assessment. The data was first tested for determining whether the variables constructs are related to each other or not. Since the aim of the researcher was to examine the relationship as well as the mediation between the variables or not therefore, SEM technique was used and through multiple regression models, the relationship between variables was identified. Based on the results obtained, the hypothesis formed were declared as "accepted" or "rejected".

Results

Confirmatory Factor Analysis

In order to find out the overall fitness of the model, confirmatory factor analysis was used. To determine the fitness of variables used in the study, the appropriate value of 0.6 was set. The table below provides overview of the values obtained through factor loadings, Cronbach Alpha, Composite reliability and AVE (Average Variance Extracted).

	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			

Table 1: Confirmatory Factor Analysis

The table 1 above shows that all values of factor loadings are above 0.7 which indicates that factors influence the variables strongly. The next important values shown above are Cronbach Alpha, Composite reliability and AVE. These metrics show the fitness of the model and whether they can be used further for testing or not. Cronbach Alpha shows the reliability of the constructs and desired or optimum value should be above 0.7. The table above clearly indicates that all values are above 0.7 which means that they are reliable and can be used further.

Composite reliability is another measure for assessing the reliability of the data and it indicates the internal consistency of the constructs similar to like Cronbach Alpha. The minimum values of composite reliability should exceed 0.7 in order to ensure high internal consistency in constructs. On the other hand, AVE (Average Variance Extracted) is used to examine the variance that is explained through the predictors of residual variance. The accepted benchmark value for it is 0.5 which means that for the variables to be deemed as significant, their values should exceed 0.5. As shown by table 1 above that AVE values exceed 0.5 and composite reliability values also exceed 0.7 indicating that there is internal consistency in data as well as shows that variables are suitable for further testing of hypothesis and model assessment.

Discriminant Validity

The second phase of testing in this research article includes of discriminant validity. The purpose of using discriminant validity is to find out the accuracy of the variables used in the study. It also explains the overall magnitude of whether a variable is related with other variables or not. The results below show whether the constructs are related to each other or not:

	Artificial Intelligence	Cyber Security	Expert System	Intelligent Agents	Neural 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 2: Discriminant Validity

The table 2 above show that discriminant validity is assessed through HTMT ratio (Heterotrait-Monotrait Ratio). HTMT is another new method of assessing the discriminant validity in PLS, SEM method that forms the basis for model evaluation and assessment. The HTMT ratio needs to be 0.90 and any variable that has values exceeding benchmark of 0.90 indicate that the variables are not accurate conceptually or statistically. As shown in table 2 above, all the values obtained of HTMT are less than 0.90 which means that all variables and sub-variables are accurate conceptually and statistically. The purpose of applying these test was to ensure that reflective constructs of this article has strong relationship or association with its indicators in the path model [22].

Basic Model

The model analysis of this article includes the independent variables that are expert system, neural nets and intelligence agents along with mediating variable that was artificial intelligence and dependent variable that was cyber security. The tables below show the model significance as well as important characteristics of the model:

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

Table 3: Model

The table 3 above shows that the model has R square value as 0.238 and 0.636 of artificial intelligence and cyber security respectively. On the other hand, the adjusted R square values are 0.233 and 0.635 of artificial intelligence and cyber security respectively. This indicates that R square adjusted is used for evaluating any discrepancies or errors in data or results whereas, R square values show the variations in the data caused by the independent variables in the dependent variables.

	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Artificial Intelligence -> Cyber Security	0.797	0.023	34.668	0.000
Expert System -> Artificial Intelligence	-0.041	0.065	0.688	0.492
Intelligent Agents -> Artificial Intelligence	0.411	0.062	6.607	0.000
Neural Nets -> Artificial Intelligence	0.164	0.068	2.390	0.017

Table 4: Model Coefficients

The next table 4 above shows the coefficients of the model. Since the research has a mediating variable too therefore, the table above shows the significance values (P-value) as well. The standard value of P shows that the desired results should be less than 0.05 ($P < 0.05$) in order to indicate it as significant. Any value exceeding it is considered to be insignificant and has not relationship. As shown above, the P value for artificial intelligence with cyber security is 0.000 which is highly significant. Following this is, expert system, intelligence agents and neural agent's significance values that are 0.492, 0.000 and 0.017 respectively. Out of all these values only, expert system does not have a relationship with artificial intelligence whereas, remaining have.

Hypothesis Assessment

The hypothesis assessment is the next important stage of analysis that needs to be undertaken. After carrying out all necessary tests for determining the relationship between variables and their reliability and internal consistency, now the researcher examines whether the hypothesis were achieved or not.

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

Table 5: Hypothesis Assessment

Based on the results shown in the table 5 above, it is evident that apart from expert system, all other hypothesis was accepted. The first hypothesis was artificial intelligence has significant and positive impact on cyber security where it was found that since the P-value was 0.000 therefore, there exists a significant impact. Next was, expert system has significant and positive impact on artificial intelligence where it was found that since the P-value was 0.492 therefore, there exists no significant impact because the P value should be less than 0.05. Next was, intelligent agents have significant and positive impact on artificial intelligence and since the P-value was 0.000 therefore, a significant and positive impact was found.

Furthermore, neural nets have significant and positive impact on artificial intelligence and since the P-value obtained was 0.017 and less than 0.05 therefore, there is a significant relationship. Next was expert system which has impact over artificial intelligence and cyber security and it obtained P-value of 0.493 which is greater than 0.05 hence, there is no relationship between these variables. The next variable was intelligence agents with artificial intelligence and cyber security which obtained P value of 0.000. Similarly, the relationship between neural nets, artificial intelligence and cyber security had 0.018 therefore, a strong and positive impact was observed.

Discussion

The overall results of the study indicated that artificial intelligence has become one of the primary assets for firms to improve their performance in terms of cyber security. The prevailing situation has revealed that cyber security is one of the important aspects for every organisation to ensure because there are chances of large data and confidential information to be attacked by online hackers. With the advancement of technology and rapid globalisation, the personal and financial information of firms are stored on cloud and due to the increased dependence on digital technology, cyber-attacks have become common. The findings of the study revealed that all independent variables had significant and positive relation apart from expert system. Though many other researchers believe that expert system is also essential but since the majority opinion does not support in this study hence, significant results are not obtained.

Limitation and Future Implication

There are many limitations faced by the researcher while conducting this study. One of the primary issue was accessibility and sample size of respondents. Due to current COVID situation, the researcher was not able to directly approach the respondents but meetings were arranged and in small groups, the questionnaires were filled. Secondly, the number of respondents were limited and in future, it is suggested that results can further be improved if more data is collected from large number of people. Moreover, the researcher only focused on I.T industry of Saudi Arabia and hence, the study was geographically limited therefore, for future, the studies can be improved if more comparison with other Middle East countries are done or more variables are included in this study for assessing the impact.

Conclusion

Conclusively, it can be stated that the researcher carried out quantitative based study with primary data collected from employees working in I.T sector of Saudi Arabia. The hypothesis testing was done and it was found that there is significant impact of intelligence agents and neural nets on artificial intelligence. The advancement of technology has led towards increased data storage which requires more data security.

References

1. Komar M, Kochan V, Dubchak L, Sachenko A, Golovko V, et al. (2017) 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), IEEE 2: 853-858.
2. White J (2016) Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. Global Security Studies 7: 23-33.
3. Huang K, Zhou C, Tian YC, Yang S, Qin Y (2018) Assessing the physical impact of cyberattacks on industrial cyber-physical systems. IEEE Transactions on Industrial Electronics 65: 8153-8162.
4. Tariq N (2018) Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce 23: 1-11.
5. Bada M, Nurse JR (2020) The social and psychological impact of cyberattacks. In Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press 2020: 73-92.
6. Taddeo M (2019) Three ethical challenges of applications of artificial intelligence in cybersecurity. Minds and Machines 29: 187-191.
7. Bhatele KR, Shrivastava H, Kumari N (2019) The Role of Artificial Intelligence in Cyber Security. In Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems, IGI Global 2019: 170-192.
8. Conti M, Dargahi T, Dehghantanha A (2018) Cyber threat intelligence: challenges and opportunities. In Cyber Threat Intelligence, Springer, Cham 2018: 1-6.
9. Alqurashi RK, AlZain MA, Soh B, Masud M, Al Amri J (2020) Cyber Attacks and Impacts: A Case Study in Saudi Arabia. International Journal, 9: 217-224.
10. Alshathry S (2016) Cyber-attack on saudi aramco. International Journal of Management.
11. Al Amro S (2017) Cybercrime in Saudi Arabia: fact or fiction? International Journal of Computer Science Issues (IJCSI) 14: 36.
12. Alshammari TS, Singh HP (2018) Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. Archives of Business Research, 6: 131-146.
13. Ahmed SM (2019) Artificial intelligence in Saudi Arabia: Leveraging entrepreneurship in the arab markets. In 2019 Amity International Conference on Artificial Intelligence (AICAI), IEEE 2019: 394-398.
14. Elhajji M, Alsayyari AS, Alblawi A (2020) Towards an artificial intelligence strategy for higher education in Saudi Arabia. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), IEEE 2020: 1-7.

15. Zeadally S, Adi E, Baig Z, Khan IA (2020) Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access 8: 23817-23837.

16. Madhok E, Gupta A, Grover N (2016) Artificial Intelligence Impact on Cyber Security. IITM Journal of Management and IT 7: 100-107.

17. Szychter A, Ameur H, Kung A, Daussin, H (2018) The Impact of Artificial Intelligence on Security: A Dual Perspective

18. Anwar A, Hassan SI (2017) Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. International Journal of Computational Intelligence Research 13: 883-889.

19. Panimalar A, Pai G, Khan S (2018) Artificial intelligence techniques for cyber security. International Research Journal of Engineering and Technology, 5: 122-124.

20. Magcale A, Kekai D, Nautilus Data Technologies Inc (2018) Artificial intelligence with cyber security. U.S. Patent 10: 158-653.

21. Blaikie N (2018) Confounding issues related to determining sample size in qualitative research. International Journal of Social Research Methodology 21: 635-641.

22. Ab Hamid MR, Sami W, Sidek MM (2017) September. Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. In Journal of Physics: Conference Series, IOP Publishing 890: 012163.