Journal of Positive School Psychology
2022, Vol. 6, No. 3, 6156–6165 

# Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management

Dr. Geethamanikanta Jakka [1], Nikhitha Yathiraju [2], Dr. Meraj Farheen Ansari [3]

[1,2,3] *University of the Cumberlands, US*
*Email: [1] jmani513518@gmail.com, [2] niki.yathi5@gmail.com,*
*[3] merajfarheenansari25@gmail.com*

**Abstract**

Cyber security is an effective area of "Computer Science and Engineering (CSE)" and this system generates a detailed idea to students of CSE, a hands-on practical experience to mitigate risk related to cybercrimes and system malware. Use of Artificial Intelligence (AI), Machine learning to reduce the risk of cybercrimes is another essential part of CSE. Cyber risk management refers to a subpart of CSE that focuses on network protection, malware attacks, protecting systems and programs from digital hacking process and many other cybercrime related issues. This research article has focused on demonstrating various areas, where AI has taken a crucial role to managing the risk of cyber-attacks within management and CSE field. Number of malwares that are increasing within the business world, rate of cyber-attacks, and importance of cyber security management within CSE and management fields has been discussed in this research article.

Technology investment within cyber security management has been identified in this study by comparing it with investment towards various other fields. Various challenges and opportunities of AI to manage cyber risk and malware attacks have been identified in this research article with the help of various journal articles, secondary sources and primary survey questionnaires based on 50 employees from the IT industry. A mixed method data collection has been considered for this study to get first-hand information from the IT industry and go through a wide range of investigation regarding this topic. The main conclusion from this study is that Cyber security and risk management has accelerated in today's modern world with the help of AI.

**Keywords**— —"AI-based cyber security solutions", "ROS (Robotic Operating System)", "Holistic cyber security risk management", "Microsoft intelligent security graph", "Microsoft 365 Defender", "Webtoos", "Search Azure Resource Graph data", "Java Malware".

## I. INTRODUCTION

Artificial Intelligence (AI) is an effective way of making complex decisions on behalf of humans within this modern competitive world. In today's world, big data makes decisions more complex in terms of any kind of field. AI is essential for every aspect of lives including security and privacy management as well. Cybercrimes are being identified and actions are taken after using AI-based solutions within businesses. AI is essential for augmenting work, which humans regularly do. In terms of cyber risk management, malwares are a common term. AI-based technologies are used intensively to detect malware within systems. Malware detection processes are categorized by several sections such as authentication, security, and confidentiality [1]. All these three aspects are being managed by different AI-based solutions to detect malware and protect computer systems from their vicious attacks. In the modern world, individuals, who directly or indirectly linked to the internet, are highly exposed to Cyber-attacks. Hackers use different types of malwares to attack any computer

© 2022 JPPW. All rights reserved

system and hack it to get essential information. Different types of attacks are there, which is a serious threat for all the internet users.

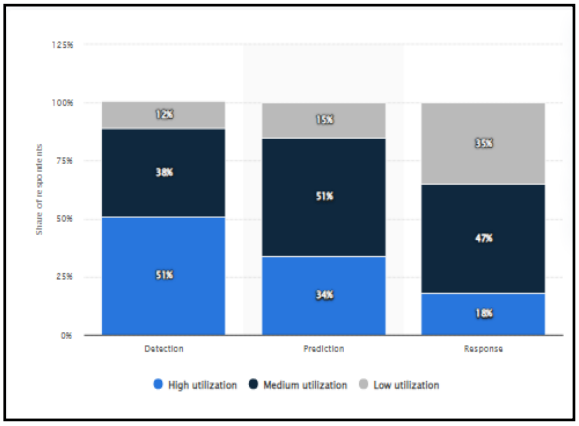


***Figure 1: Utilization of AI as a Cyber security Function in Different Organization of this World (Source: [2])***

As per this above figure, it can be stated that, almost 51% of respondents from different organizations across the world have stated that their organizations have utilized AI-based solutions largely to develop cyber threat detection. On other hand, only 18% of respondents have stated that they have utilized the AI-based solutions within their organizations' responses to cyber threats, not as a detection tool [2]. Use of AI within the Android operating system ranks first in the world, to detect and handle features, that attract cyber criminals [3]. As a result, this research article will investigate different aspects of AI-based solutions to identify the ways under which it manages cyber risks and malware attacks within the managerial as well as IT section of a company. This was a main feature to mitigate the issues within their business by enhancing skills of computer science engineering process. Another objective of this research article was to recommend some effective strategy that companies can take to implement AI-based solutions within their organizational structure for managing cyber security and malware detection processes.

## II. LITERATURE REVIEW

### *A. Concept of artificial intelligence and malware*

AI is the capability of computers or human beings do robots controlled by other computers for doing tasks that, as they need human intelligence. Some common examples of AI are speech recognition, visual perception, and decision-making. AI is about reasoning, learning and problem solving in general and it has four different types such as limited memory, reactive machines, self-awareness, and theory of mind [4]. AI offers transformational potential throughout different industries and sectors ranging from supply chain to medicines to automobiles. It gives opportunities for reinventing business models, changing future works, improving performance, and enhancing human capabilities [5]. In contrast, malware is intrusive software, which is designed for damaging and destroying computer systems and computers. This is a contraction regarding malicious software and some examples of this type of software are spyware, adware, viruses, worms, and ransomware. Detection of malware is important with prevalence of malware because this functions as an initial warning system for computers regarding cyber-attacks and malware [6].

### *B. Concept of Cyber risk management (CRM)*

CRM is the method of analyzing, identifying, addressing, and evaluating cyber-security threats of an organization. This method is completed by taking different steps and the foremost step is cyber risk assessment [7]. It gives a snapshot of threats, which could compromise the cyber security of an organization. Then based on risk appetite CRM program determines the prioritization process to respond effectively to each risk. The process of CRM includes six major steps, the first step identifies risks, then in the second step it analyses severity of every risk through assessing how probable these risks to occur as well as the significant impact of these risks. In the third step, this process evaluates how every risk fit within risk appetite and based on this, organizations priorities the risks. In the next step, organizations set strategies to respond to every risk and lastly, organizations review whether these strategies fit the risks and fulfil the purposes. Organizations use efficient and

© 2022 JPPW. All rights reserved

proactive methods for assessing cyber security risks and it helps organizations about risks that are associated with their organizational works on a regular operation level [8].

*C. Role of AI for spotting malware*

AI is not able to resolve and detect each potential cyber threat or malware; however, when AI combines modelling of good and bad behavior, it could be a powerful and effective weapon as opposed to advanced malware.

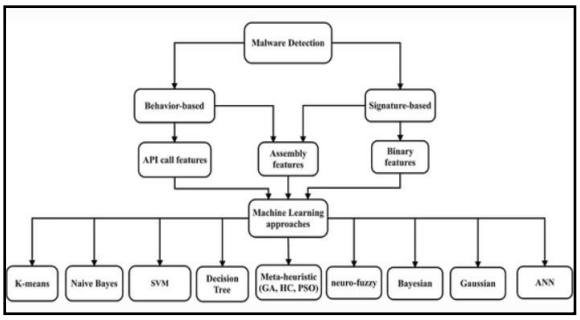


***Figure 2: Approaches of Malware detection (Source: [6])***

In case of detecting malware, there are two types of approaches, which are behavior-based and signature-based. Research has suggested that API calls, binary features and assembly features are the present approaches regarding the method of malware detection [6]. Tools of malware detection must evolve for staying up to date with the ever-changing crimeware. A significant evolution with malware detection is migration through trapping and hunting. In terms of spotting malware, AI has been used significantly, which automates a good-behavior modelling; however, products of malware detection that are based on this model are not easy. Additionally, application of AI towards tasks of development good-behavior model resolves several resources and technical challenges to detect advanced malware [9]. Some Indian companies use AI for cyber security, and these are Infosys, Seconize, and TCS.

*D. Importance of AI for delivering cyber security*

In this digital era cyber security has become a critical thing as it protects data of all categories from damage and threat. It includes sensitive data, PHI (*"protected health information"*), intellectual property, industry, and governmental data, and PII (*"personally identifiable information"*). To make cyber-security stronger AI has been used and it endeavours for simulating human intelligence. AI has a huge potential within cyber-security, and it can be trained for generating alerts regarding threats, identifying new kinds of malware, and protecting sensitive data of any organization [10]. In organizations, AI-based systems help in threat detection as well as response capabilities regarding advanced attacks. Additionally, it helps in responding to data exfiltration, malware, encrypted attacks, and ransomware [11].

*E. Challenges of using AI for enhancing cyber security in organizations*

Although AI has been extensively used regarding cyber-security, it has some challenges to enhance cyber-security within organizations. Some common challenges within AI are as follows.

***Biometric authentication***

Biometric authentication is popular with users, and it is equally dangerous. If biometric data is in the wrong hands, it can be utilised for surveillance of privacy of users [12]. AI technology enables collecting and processing enormous amounts of data, which causes further deterioration of security and digital privacy.

***Cost of implementation***

Another challenge of using AI for cyber-security is implementation cost. Information has suggested that implementation of AI can be expensive because software experts and programmers are required to create the whole system from scratch [12].

***AI-tech is not invincible***

Lastly, AI-technologies are not invincible and a few tasks that are done by artificial intelligence can be exploited if hackers manage for accessing them. For instance, AI-enabled programs can be misled into labelling the malicious software as normal or safe.

© 2022 JPPW. All rights reserved

*F. Benefits of utilizing AI regarding cyber-security*

AI endeavors for stimulating human intelligence and it has huge potential within cyber-security. Security professionals require robust support from AI for working successfully and protecting organizations from any type of cyber-attacks. Some of using AI in terms of cyber-security is as follows.

***AI identifies unknown threats***

Humans could not identify all threats an organization experiences and each year, a significant number of hackers launch enormous numbers of attacks with several motives [9]. These unknown threats may cause huge damages towards a network and to mitigate the issues AI has been considered as one of best technologies for stopping and mapping these threats through ravaging an organization.

***Secure authentication***

Majority of websites have user accounts where an individual's log-in for accessing services and purchasing products. An organization needs an extra layer for running this type of site as it involves sensitive and personal information of users [13]. However, AI secures the authentication anytime users want to login to their accounts. AI uses several tools including CAPTCHA, fingerprint scanner and facial recognition, which help to detect whether long-in attempts are genuine or not.

## III. THEORIES AND MODELS

***Theory of Technological determinism***

Technological determinism (TD) is the reductionist theory, which assumes that technology of society determines development of their cultural values and social culture. Since technological advancement has increased in the past decade, people are now more exposed to technologies, from online shopping to online food ordering they use technologies, and they share their personal information on different sites [14]

*Literature gap*

This literature has discussed relevant topics from the selected research topic. However, while conducting the literature review, some gaps have been identified, which is related to theoretical perspectives. There are a limited number of theories that can be used to analyses the selected topic.

## IV. METHODOLOGY

***Table 1: Overview of methodology***

| | |
|---|---|
| Data collection | Mixed method |
| Data analysis | Thematic and descriptive |
| Research philosophy | Pragmatism |
| Study design | Descriptive |
| Research approach | Inductive |

## V. DATA COLLECTIONS METHOD

Mixed method that incorporates both quantitative and qualitative data has been used in this research paper for expanding and strengthening the paper's conclusions and providing a complete comprehensive vision on this selected research topic [15]. Regarding quantitative data collection, the paper has conducted an online survey on 50 employees from different organizations of the IT industry and three closed-ended questions have been asked to participants.

Additionally, in the case of secondary data, this paper has considered different secondary sources regarding cybersecurity and AI such as company reports, journals, government databases, articles, newspaper articles and magazines to collect topic-related information. It has used Google Scholar to gather relevant journals and articles, which are published within last ten years and in English language. While collecting secondary data, it has considered some keywords, which help to get relevant resources and some examples, are "cyber-security".

© 2022 JPPW. All rights reserved

## VI. DATA ANALYSIS

Since this research has used a mixed method, it has considered two different data analysis methods. Regarding primary quantitative data, Microsoft Excel has been utilised for analyzing data from different charts and graphs. Additionally, for analyzing secondary data, this study has used thematic analysis and with help of thematic analysis the study uses a large amount of data on relevant topics to get broader and appropriate conclusions [16].

## VII. RESEARCH PARADIGM

This research has considered pragmatism philosophy because it used a mixed method to collect data and as per studies, pragmatism philosophy fits appropriately with research that used a mixed method. With help of pragmatism philosophy, this study can identify what secondary information wants to highlight and whether primary data matches with it or not [17]. Next, this paper has chosen descriptive study design for describing, explaining, and validating some hypotheses when it comes to a specific topic, the importance of AI to spot malware and deliver cyber risk management. Lastly, it has considered an inductive approach for exploring phenomena, identifying themes, and creating a clear concept on the role of AI to spot malware and deliver cyber-security risk management.

## VIII. ETHICAL CONSIDERATIONS

In order to complete the research work ethically, it has considered some research ethics and the first one is about taking voluntary consent. Since it has surveyed 50 respondents it took consent from the participants and allowed voluntary participation, where they have the right to withdraw their participation anytime, they want. Additionally, it has ensured privacy of participants so that their personal information would not be disclosed in public. Lastly, it has ensured data security to protect the data from any type of cyber-attacks. It has complied to regulations regarding "Data Protection in India" and followed its legal framework and regulation for protecting digital information and enhancing data security [18].

## IX. RESULT AND COLLECTION

*Primary Data Collection*

*Survey Results*

***Question 1***

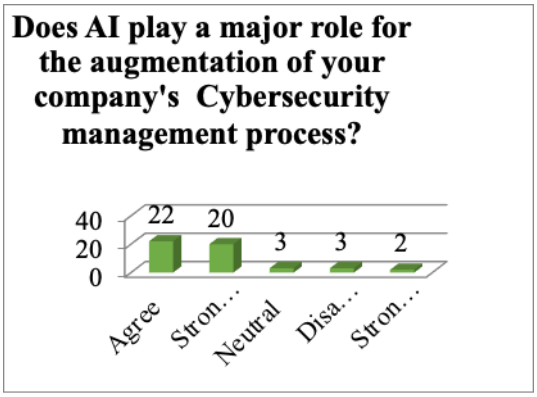


***Figure 3: AI plays a major role within the augmentation process of company's cyber - security management system***

According to the above figure, it can be observed that almost 42 respondents out of total 50 have agreed to the fact that AI-based solutions and its use have a major role within their business in terms of the cyber security management process. The use of AI-based solutions to analyse cyber threats are categorized into two different prices such as dynamic process and hybrid process. Companies use different phases to detect malware within their computer system through machine learning techniques such as android apps, extraction of features, pre-processing, CVS file, and proposed modelling through "GRU (Gated Recurrent Unit)" and others [3].

***Question 2***

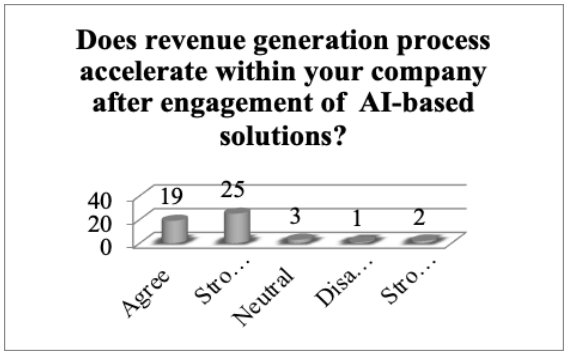


***Figure 4: Revenue Generation Process of Companies have increased due to use of AI-based Cyber Security Risk Management Solutions***

© 2022 JPPW. All rights reserved

According to the above figure, it can be illustrated that most respondents have agreed with the fact that the overall revenue generation process of their company has been increased after their implementation of AI-based malware detection tools. As per reports, it has been found that, companies whether it is from IT industry, or any other industry uses antimalware scanner to maintain the agility and integrity of their recommendation engines that helps to enhance advertising campaigns. Cyber security systems with the help of AI-based solutions are an integral part of business processes that drive additional revenue [19].

***Question 3***

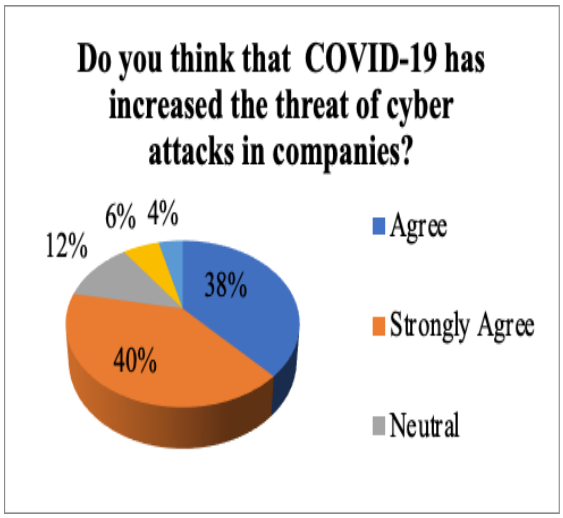


***Figure 5: COVID-19 has increased the risk of cyber-attacks in different domain of the Society***

As illustrated by this above figure, it can be stated that almost 78% of respondents point to a total of 50 employees having agreed that after COVID-19 pandemic, the risk within their organizations related to Cyber security have increased drastically. Due to this pandemic, employees are working remotely, and this has widened the scope for hackers to attack their computer system due to lack of a strong cyber security risk management process at home.

*Secondary Data Collection (Thematic Analysis)*

***Table 2: Overview of Themes***

| ***Themes*** | ***Main Focus*** |
|---|---|
| Theme 1 | Effect of increasing technology investment in AI |
| Theme 2 | AI for "ROS Forensic Investigation Process" |
| Theme 3 | Java Malware detection by Microsoft 365 defender |

*Theme 1: Increase in Technology Investment for AI and ML has accelerated the focus on combating Cyber Risks*

Investment increased on AI-based cyber security, which has accelerated the process of combating cyber risk in various industries all over the world. It has been estimated that global spending on cyber security will exceed $1 trillion from 2017 to 2021. As per various reports, it has been found that almost 82% of firms have implemented "Machine Learning Cyber Security Solution", which is another part of AI Solution, into their Computer Science Engineering process, embedded within their IT section along with their entire management system. Apart from this 82%, almost 53% of remaining companies have a plan to implement AI-based cyber security solutions within their business process.

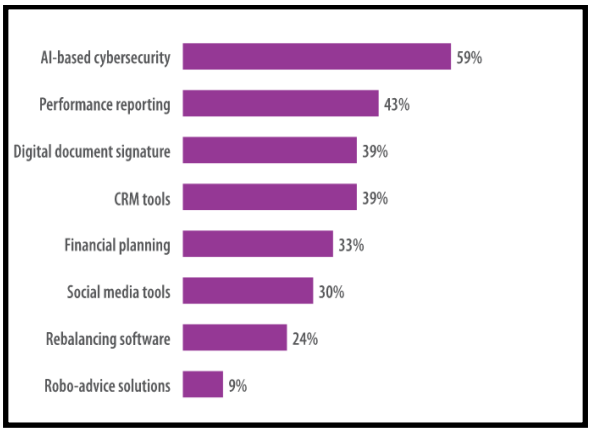


***Figure 6: Investment in AI-based Cyber security Technology all over the World (Source: [20])***

© 2022 JPPW. All rights reserved

According to this above figure, it can be observed that technology investment is highest for AI-based cyber security across the world. Investment in performance reporting and financial planning is lower than the fund allocated for implantation of AI-based cyber security risk management processes. This is effective for mitigating the risk of cybercrimes as much as possible within various industries and companies. Results from the third question of survey have stated COVID-19 as a major aspect of Cyber risk. It has been found that, the current COVID-19 pandemic has increased the level of cyber-attacks; as criminals have taken the advantages of changes in existing workplace [20].

As a result, the traditional cyber security management in most of the cases could not cope up with the new threats. As a result, increase in the technical investment by various countries to implant AI-based cyber security solutions can modern defers to companies within their CSE process [20]. AI-based solutions can provide a holistic cyber security risk management technology to secure several vital infrastructures for a company's IT process, which is essential of CSE. This increasing investment will also be effective for introducing technologies that are essential for assessing cyber risk posture proactively and accurately.

*Theme 2: AI helps in Ensuring Cyber Security to "ROS (Robotic Operating System)" Forensic Investigation Procedure*

COVID-19 outbreaks all over the world have been a major reason to transfer all the business and technology related processes to be done in an online platform. As a result, security differences are essential for this new world. AI-based security strategy has been a major area of concern for businesses all over the world to enhance their security system, which is an essential part of Computer Science Engineering. In various developed countries, it has been found that robots are used within the medical sector to fight against COVID-19 pandemic [21]. Robotic is a major part of computer science engineering, which is used within the NHS to combat with COVID-19 diseases by doing activities that are essential for care homes and hospitals as well. However, issues within the Robot Operating System are an essential part of robotic technology.

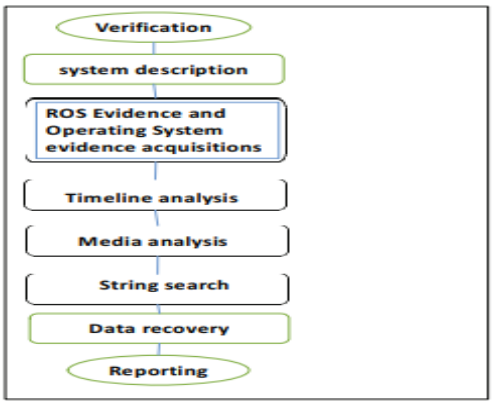


***Figure 7: AI-based Framework for ROS Forensic Investigation (Source: [21])***

As a result, AI-based framework for ROS forensic investigation to resolve these issues is designed with different steps such as verification, system description, Acquisition of evidence from ROS, Timeline and Media analysis along with string research. Apart from these, data recovery and reporting forensic results are also included in this AI-based framework. This forensic investigation process of ROS is slightly different from any other normal investigation process of other digital devices [21]. This differentiation has mainly been incorporated due to distinction of AI-based element characteristic within a robotic system. The security resilience based on the AI build framework for Robotic systems are mainly followed by different guidelines provided from Cyber Law, Network Security Act, and others.

*Theme 3: Combating Java Malware is possible after considering Real-Time Machine Learning by Microsoft.*

Microsoft is a multinational technology corporation that deals with technical goods and services in the market. Some years earlier and still now, the Security research team members of this company have investigated that a surge in emails with malicious java has been found

© 2022 JPPW. All rights reserved

within their company. This malicious java malware uses new technologies for evading antivirus protections within their system. However, their technical team have engaged an automated expert system and real time protection with the help of machine learning technique, which is a major part of AI to avoid this particular risk of malware. It has been found that attackers use "Webtoos malware" to target Linux and Windows systems way before any vulnerability found within the process and Microsoft defender is useful to protect computers from malicious hackers [22].

Microsoft Defender 365 portal has a toolbar that includes a malware view to detect emails that have malware zip in it. Security team of this company works 24*7 to maintain this system portal (Microsoft). Attackers mainly change their methods and tools to attack system software with malware by going through various programming languages. The company has identified that they have changed the process of installation of NSIS for evading AV and delivering ransomware. Researchers of this company's IT field have used "Microsoft intelligent security graph" for monitoring threats generated from a wide range of network sensors [23].

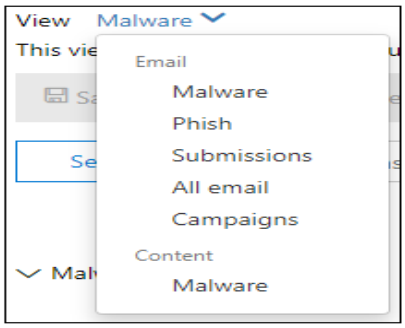


***Figure 8: Microsoft 365 Defender Portal for Combating Malicious Content (Source: [24])***

The above figure shows the way under which Microsoft 365 defender identifies suspicious emails that have Java malware attached with a zip file. Moreover, Search Azure Resource Graph data is essential for those resources that are found to be affected by malware attacks generated from Webtoos. This could query a resource with complex filtering, grouping, and sorting processes [25]. Cloud-based machine learning protections used by this company within their Microsoft defender antivirus can block many new and unknown variants.

## CONCLUSION

AI has become a major part in this digital era and people now extensively use AI-related services and products. Nowadays, people use AI for making intelligent machines for helping needy people. This research has done a robust literature review on the selected topic as it has reviewed the role of AI in case of cyber-security and spotting malware. The findings of this paper have paid attention to several areas that highlighted use of AI by different organizations and their employees to ensure cyber-security and cyber threats. This research has found that if technology investment regarding machine learning and artificial intelligence is increased then businesses or IT companies can effectively reduce the risk of cyber-attacks. Therefore, it can be concluded that in this digital era, when people are connected to internet for 24*7 and share their information, the chances of cyber-attacks and cyber threat is very high. Thus, by investing in technology such as AI and ML, organizations can do cyber security management.

Additionally, study findings showed that AI-based security systems play a crucial role in business concerns for enhancing security systems that are also a critical part of Computer Science and Engineering. AI ensures cyber security towards robotic operations systems and forensic investigation, which means AI, has been successfully implemented in several industries from technological industry to healthcare. Therefore, it can be concluded that implementation of AI systems can help businesses to enhance their security systems like Microsoft who changes their tools and systems to attack malware systems by implementing various useful programming systems.

© 2022 JPPW. All rights reserved

## RECOMMENDATIONS

### *Securing decision-making system of AI*

One of the major security-related risks towards AI system potential regarding adversaries is for compromising integrity of decision-making procedures so that these adversaries do not create any choice in the way that design would desire [10]. Therefore, to accomplish this, businesses can directly control AI systems so that it can decide what output system generates as well as what decision this new AI system makes. With help of this new AI system businesses can ensure cyber risk management, where if attackers try to influence those decisions, it fails their input.

### *Investment on Technology and cyber security management*

Since this research has found that AI has proved that it has a huge positive impact on cyber-security, businesses can focus on technology investment, where they can implement new AI-systems, which will reduce the risk of cyber threat and ensure cyber-security management [12].

## REFERENCES


1. Sharma, S., Khanna, K. and Ahlawat, P, "Survey for Detection and Analysis of Android Malware (s) Through Artificial Intelligence Techniques". In *Cyber Security and Digital Forensics* (321-337). Springer, Singapore. 2022. https://link.springer.com/chapter/10.1007/978-981-16-3961-6_28
2. Statista, Utilization of artificial intelligence (AI) for cybersecurity functions in organizations worldwide as of 2019, by category. (2019), [online] Available: https://www.statista.com/statistics/1028966/worldwide-ai-utilization-cybersecurity/ [Accessed January 4, 2022]
3. Elayan, O.N. and Mustafa, A.M, "Android Malware Detection Using Deep Learning", *Procedia Computer Science*, *184*, 847-852. 2021. https://doi.org/10.1016/j.procs.2021.03.106
4. Kersting, K., "Machine learning and artificial intelligence: two fellow travelers on the quest for intelligent behavior in machines," *Frontiers in big Data*, *1*, pp.6, 2018. https://doi.org/10.3389/fdata.2018.00006
5. Collins. C., Dennehy, D. Conboy, K. and Mikalef, P, "Artificial intelligence in information systems research: A systematic literature review and research agenda," *International Journal of Information Management*, *60*, pp.102383, 2021.https://doi.org/10.1016/j.ijinfomgt.2021.102383
6. Souri, A. and Hosseini, R, "A state-of-the-art survey of malware detection approaches using data mining techniques," *Human-centric Computing and Information Sciences*,*8*(1), pp. 1-22, 2018. https://doi.org/10.1186/s13673-018-0125-x
7. Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H, and Stoddart K, "A review of cyber security risk assessment methods for SCADA systems," *Computers & security*, *56*, pp. 1-27, 2016. https://doi.org/10.1016/j.cose.2015.09.009
8. Keskin OF, Caramancion KM, Tatar I, Raza O, and Tatar U, "Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports," *Electronics*, *10*(10), pp. 1168, 2021.https://doi.org/10.3390/electronics10101168
9. Truong TC, Diep QB, and Zelinka I, "Artificial intelligence in the cyber domain: Offense and defense," *Symmetry*. *12*(3), pp. 410, 2020. https://doi.org/10.3390/sym12030410
10. Rawindaran N, Jayal A, Prakash E. "Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries," *Computers*, *10*(11), pp. 150, 2021.https://doi.org/10.3390/computers10110150
11. Malatji M, Marnewick A, and von Solms S, "The Impact of Artificial Intelligence on the Human Aspects of Information and Cybersecurity," *InHAISA*, pp. 158-169). 2018


© 2022 JPPW. All rights reserved

12. West DM, Allen JR, "How artificial intelligence is transforming the world," *Report. April,24*, pp. 2018, 2018.
13. Qiu X, Du Z, and Sun X, "Artificial intelligence-based security authentication: Applications in wireless multimedia networks," *IEEE Access,7*, pp. 172004-11, 2019.
14. Boyd R, and Holton RJ, "Technology, innovation, employment and power: Does robotics and artificial intelligence really mean social transformation?," *Journal of Sociology*, *54*(3), pp. 331-45, 2018.https://doi.org/10.1177/1440783317726591
15. NayakJK, and Singh P. *Fundamentals of Research Methodology Problems and Prospects*. New Delhi: SSDN Publishers & Distributors, 2021. Available: http://dspace.vnbrims.org:13000/jspui/bitstream/123456789/4653/1/Fundamentals%20of%20Research%20Methodology_Nayak.pdf [Accessed January 4, 2022]
16. Bairagi V, and Munot MV, *Research methodology: A practical and scientific approach*.Florida: CRC Press, 2019. Available: https://books.google.com/books?hl=en&lr=&id=wxaGDwAAQBAJ&oi=fnd&pg=PP1&dq=research+methodology+book&ots=vvSBQ5Xxk4&sig=el2eywLy7K7MILNkTEld01aY41g [Accessed January 4, 2022]
17. Kumar R. *Research methodology: A step-by-step guide for beginners*. California: Sage, 2018. Available: https://books.google.com/books?hl=en&lr=&id=J2J7DwAAQBAJ&oi=fnd&pg=PP1&dq=research+methodology+book&ots=cvphDGMLel&sig=RZlS51T6HA5TH7_iU5RnItiuj-Q [Accessed January 4, 2022]
18. Digital India, DATA PROTECTION IN INDIA, (2018), [online] Available: https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf [Accessed December 22, 2021]
19. McKinsey, Hit or myth? Understanding the true costs and impact of cybersecurity programs. (2020), [online] Available: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx[Accessed January 4, 2022]
20. Infosys,AI and ML in Cybersecurity Risk Management. (2022), [online] Available: https://www.infosys.com/iki/insights/cybersecurity-risk-management.html[Accessed January 4, 2022]
21. Feng, X., Feng, Y. and Dawam, E.S. "Artificial Intelligence Cyber Security Strategy". In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* ( 328-333), 2020, August. IEEE. https://ieeexplore.ieee.org/abstract/document/9251111/
22. Microsoft, Malware-encyclopedia-description, (2022) [online] Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FWebToos.C[Accessed January 4, 2022]
23. Microsoft, Use-windows-defender-application-control-with-intelligent-security-graph, (2022) [online] Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/use-windows-defender-application-control-with-intelligent-security-graph[Accessed January 4, 2022]
24. Microsoft, Malware encyclopedia description, (2022) [online] Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/investigate-malicious-email-that-was-delivered?view=o365-worldwide[Accessed January 4, 2022]
25. Microsoft, Overview. (2022), [online] Available: https://docs.microsoft.com/en-us/azure/governance/resource-graph/overview[Accessed January 4, 2022]

© 2022 JPPW. All rights reserved