Artificial Intelligence Applications in Cybersecurity

Azzah Kabbas†, Atheer Alharthi††, and Asmaa Munshi†††

University of Jeddah, College of computer science and engineering, Saudi Arabia

Summary
Input here the part of summary. With the development of and the rapid changes in technology, threats related to cybersecurity can increase. And With the focus on the digital transformation of institutions, it became necessary to pay attention to cybersecurity issues and ways to enhance and develop them. The literature has highlighted that the traditional computer algorithms for cybersecurity may sometimes stand helpless in front of the creative and developmental capabilities of hackers and saboteurs, which requires the use of artificial intelligence techniques to enhance cyber security.
Therefore, this research paper aimed to shed light on the concept of artificial intelligence and its fields, and how it can benefit from applications of artificial intelligence to enhance and improve cyber security. Using an analytical descriptive methodology of previous literature on the topic, the importance of the need to employ artificial intelligence techniques to enhance cybersecurity was highlighted and the most important fields of application of artificial intelligence that enhance cybersecurity such as (especially machine learning, data mining, deep learning and expert systems).
Key words:
Cybersecurity, artificial intelligence, data mining, threats.

1. Introduction

Although many people possess intelligence, many of them still lack the capabilities of ways to understand the problem and find solutions to it. However, when it comes to reducing errors in operational tasks and finding anomalies, artificial intelligence is ahead of human ability
and competence. Artificial intelligence is instrumental in assessing errors that humans are vulnerable to making.
Artificial intelligence as a solution to cybersecurity can help protect organizations from Internet threats, identify types of malware, ensure practical security standards, and help create better prevention and recovery strategies. Therefore, through this research, we will shed light on how AI technologies and applications can contribute to cybersecurity.

2. Research objectives and methodology

This research paper aims to shed light on the concept of artificial intelligence, identify the most important areas of artificial intelligence that can be used in cybersecurity, and clarify the role that these areas can play (especially machine learning, data mining, deep learning and expert systems) in supporting cybersecurity in Organizations.
Consistent with the objective behind the present research paper, its application is based on a descriptive analytical approach based on extrapolation of previous literature in a critical theoretical and analytical manner to extract the answer to the main questions of the paper.

3. Research Questions

This research paper focuses mainly on a fundamental question: "How can artificial intelligence applications be used to enhance cyber security?" From this main question emerges the following set of sub-questions:
What is the concept of artificial intelligence and what are its fields?

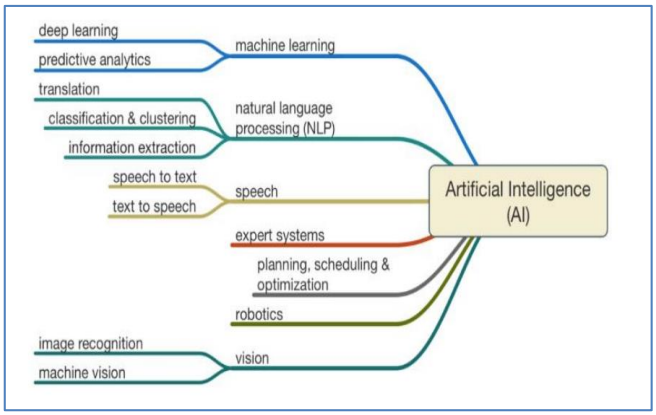

Fig. 1 Areas and Applications of AI

What are the most important areas of artificial intelligence that can support cyber security?
What is the concept of data mining and how can it be used to enhance cyber security?

4. Extensive Background

The concept of Artificial Intelligence was introduced following the introduction of the concept of the digital computing machine. He came in response to a question, "Alan" asked in 1950 that "Can the machine think?" it was followed by a debate during the fifties and sixties of the last

Manuscript received February 5, 2020
Manuscript revised February 20, 2020

century on whether the machine can perform all the work that humans can do in their daily lives. The machine was able to perform some capabilities for problem-solving and reasoning, but it was not able to perform the full human cognitive abilities, which was referred to as the term Weak AI. To realize the full range of human cognitive abilities, the concept of Strong AI has come to the fore, which includes the tasks that humans have traditionally performed, the application of a wide range of background knowledge, and the existence of some degree of self-awareness [1].

Artificial Intelligence is a vast and massive science of computer science, and it is to create systems that can function intelligently and independently, similar to the individual brain's decision mechanism. With AI, a machine to learn from experience by processing large amounts of data and recognizing the pattern in them. For example, Apple Siri, face recognition, and self-driving car these are based on Machine Learning and natural language processing which are a subset of AI.

AI is including many related areas and technologies, as shown in figure1 [2], such as machine learning, deep learning, a neural network, natural language processing, and others.

Below are some research areas in AI explained briefly and with examples in our real-life application that we use every day:

- Machine learning is a multitude of technologies that allow computers to think by mathematical algorithms based on the collected data and specific instructions and rules [3]. "Instead of programming the computer every step of the way, this approach provides computer guidance that enables it to learn from data step by step without instructions from the programmer" [4]. Some examples are virtual personal assistants which are Siri, Alexa, and Google, these assist in finding information and instruct for specific tasks when asked over voice. Also, other examples are video surveillance, which tracks unusual behavior, and social media services to connect with 'people you may know' based on continuous learning according to the usual interest or workplace.
- Deep Learning represents the subsequent development of machine learning, and it is a computer model that performs categorization tasks directly from pictures, text, or sound. This model taught by using a broad set of identified data and neural network architecture that contain many layers. Deep learning achieves recognition accuracy at higher levels. The applications in real life for this model are Tesla automated driving car by detect stop signs, and industrial automation by detect objects are within an unsafe area [5].
- Neural Networks is a pattern recognition system such as face and handwriting recognition that deep learning uses it to implement machine learning. One example of the neural network is RankBrain, which is search engine algorithms that help Google to provide search-relevant results to its users on pages containing the exact words searched for [6].
- Natural Language processing where machines analyze language and speech as it is spoken, such as speech recognition and chatbot for customer support applications, use Machine learning and natural language processing.

AI has areas and technologies so that it can be used in many industries, such as financial institutions, education, and health. Moreover, it is used in many applications related to cybersecurity that are mentioned in the next section.

5. Research Gap

Artificial Intelligence Applications that Contribute to Enhancing Cybersecurity:

In this Axis of research, we will explain how the immense potential of Artificial Intelligence technologies can be used to enhance cybersecurity.

Data has been generated in today's world is increasing and the information stored or received in any form, whether directly or indirectly, through the Internet. Moreover, the data has to be sent over a network to receive it in a destination due to proper transmission of data plays a vital role in combating cyber-crimes, which is achieved through principles of cybersecurity. With the growing advancements in Information Technology, criminals are using cyberspace to commit various cyber-crimes, which later creating a considerable disruption in the cyber society [7].

AI and cybersecurity are broad terms, and we can use it both in organizations to mitigate risks and increase revenue by detecting cyber threats and fraud. However, keeping up with new viruses and malware updates is becoming more difficult, cybersecurity using artificial intelligence technologies will facilitate the detection and response to threats and malware by using previous cyber-attack data to determine the best course of action.

AI may often be better and more effective than humans in detecting malicious malware. AI is implemented in the organization with multiple security solutions such as Security Information, and Event Management helps security analysts for any threats inside the network of the organization to improve detection [8]. "The faster the data breach was identified and contained, the lower the costs. This year, the increasing time to resolve a breach was potentially due to the increasing severity of criminal and malicious attacks experienced by a majority of companies. Security automation and intelligent orchestration capabilities that provide visibility across the security

operations center can help improve an organization's ability to contain the damage from a breach" [9].

Many types of AI applications are used in cybersecurity solutions, as mentioned SIEM, spam filter applications, secure user authentication, and hacking incident forecasting [10]. These applications are trained by using a database of previous behaviors and identify each behavior as malware or not. According to IBM, the cost of a data breach worldwide will be reduced if organizations deployed automated security solutions "Organizations that had not deployed security automation experienced breach costs that were 95 percent higher than breaches at organizations with fully-deployed automation" [9]. In figure 2 shows the cost of a data breach in the Middle East if organizations not implemented automated security solutions.

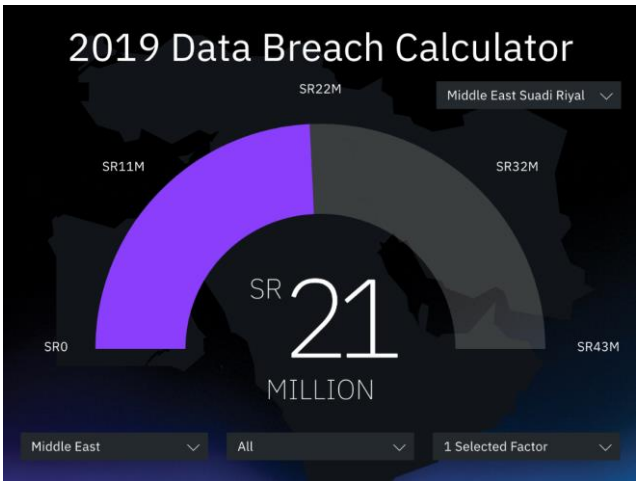

Fig. 2 Data Breach Calculator

Applications of Expert Systems in Cybersecurity

Expert systems are one of the most prominent tools of Artificial Intelligence and are software packages that help in reaching answers to inquiries that either a customer provides or that another software package provides. These systems include knowledge content in which expert knowledge is kept in a specific field of application. These systems also include a reasoning engine to access answers in light of the information provided and other additional information regarding the surrounding conditions [11].

Machine Learning Applications in Artificial Intelligence

"Machine learning is a subfield of Artificial Intelligence that allows a computer to learn using sample data without being programmed to anticipate every possible situation" [12]. "The two most common types of machine learning are supervised and unsupervised learning. Supervised learning is used when a dataset of labeled instances is available, and to solve classification problems. The goal of supervised learning is to train the computer to learn to predict a value or classify an input instance accurately. Unsupervised learning is used when a labeled dataset is not available. Clustering is an unsupervised learning technique that results in similar grouping instances in clusters. Clustering is used to discover patterns in data. In some cases, clustering is performed to classify an unlabeled dataset and using the resulting classified dataset for supervised learning" [12].

As the threats of cybersecurity are continually changing and evolving, an automated and immediate response is required. Therefore, machine learning methods, especially deep learning that does not necessarily require previous training or reliance on previous classifications provided by experts, maybe particularly vital as an application of AI approaches to cybersecurity. In the following paragraphs, we review an applied case for employing machine learning to enhance cybersecurity before it is addressed in an independent component of deep learning as a distinct and vital type of machine learning that can contribute effectively to cybersecurity.

The study [13] aimed to verify the effectiveness of machine learning methods for cybersecurity purposes. This study involved applying machine learning methods to identify intrusions, malware, and spam. Emphasis was placed on the effectiveness of machine-based solutions and their major disadvantages that prevent the direct adoption of machine learning methods in cybersecurity.

Deep Learning Applications in Cybersecurity

The lack of disaggregated data is a common challenge in cybersecurity research. Although its return to confidentiality factors often explains this scarcity, experience indicates that even behind closed doors of large corporations with significant internal expertise that security information regarding threats can be transformed into a categorized set of data appropriate for machine learning. The reason behind this is the presence of a massive amount of large and unbalanced data sets, the scarcity of time required to perform manual categorization, and fields unique characteristics such as categorization of semantics that increase the gap between technical expertise and statistical modeling. To this end, there is an effort to reconcile these contradictions, and to argue that recent research on the weakness of controlled learning - in which multiple empirical methods are employed rather than investigating and verifying actual information - is a fertile framework that can be built upon in cybersecurity research; with traditional options for supervised, semi-subject, and non-supervised learning [14].

Data Mining Applications to Enhance Cybersecurity

"Data mining is the search for significant patterns and trends in large database" [15].

Data mining methodology aims to obtain valuable information and find hidden patterns from a massive number of databases, which statistical approaches cannot discover. It is an area of vast disciplines for research that includes machine learning, databases, statistics, expert systems, visualization, high-performance computing, rough sets, neural networks, and knowledge representation. Data mining is supported by a host that captures data in various ways (e.g., clustering, classification, link analysis, summarization, regression models, and sequence analysis) [16].

Here are a variety of examples of data mining applications for cybersecurity:

- Methods for identifying unusual activities used to identify abnormal patterns and activities.
- Link analysis to track viruses.
- The classification can then be used to group several cyber-attacks using profiles to identify attacks when they occur.
- The prediction to identify possible upcoming attacks based on the information learned [17].
- Furthermore, "Katoua" discussed multiple applications for data mining in cybersecurity, such as:
- Define the characteristics of data flow on networks using the cluster.
- Track viruses using link analysis.
- Identify unusual behaviors and patterns using unusual behavior identification methods.
- Determine future attacks using prediction models.

Nagesh (2013) adds some examples of employing data mining to identify breaches of cybersecurity: removing normal activities from warning data to allow analyses to focus on realistic attacks; identifying false warning generators; and finding unusual activities that reveal a real attack ; Specifying long and continuous patterns of unusual activities (using different IP addresses to conduct the same activity); summarizing data related to cybersecurity using statistics; and visual representation of data related to cybersecurity.

"Figure 3 shows the main functional phases of the knowledge discovery process. This is arranged into a stream of steps:

- understanding the domain in which the discovery will be carried out.
- forming the data set, its cleaning, and warehousing.
- extracting patterns, this is essence of DM.
- post-processing of the discovery knowledge.
- putting the results of knowledge discovery into use" [16].

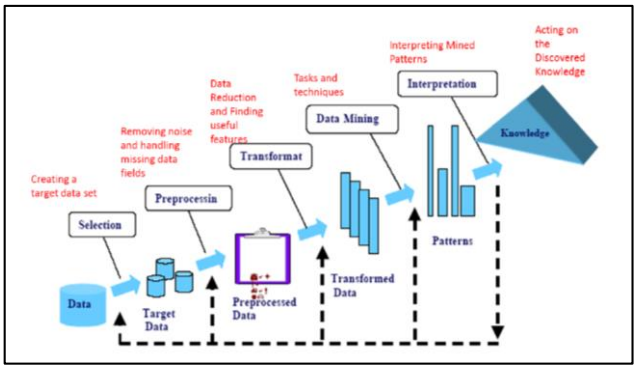

Fig. 3 Phases of Knowledge Discovery Process [16]

6. Recommend Solution

This study was applied using an analytical and descriptive research methodology of literature and previous studies. The results indicated the possibility of using machine learning, deep learning, and data mining methods for cybersecurity purposes in three main areas: intrusion detection, malware analysis, and spam detection.

The results also showed that many weaknesses limit the effectiveness of using machine learning methods for cybersecurity purposes such that all entries used are subject to counter attacks and require constant re-grading and carefully adjust parameters which are challenging to automate. Moreover, mainly when the same work is applied to identify different threats, the performance of the determination is unacceptably low, which may be overcome by using different machine-based workbooks to identify specific threats. Besides, machine learning is still at an early stage, and no conclusion can be reached regarding its efficacy for cybersecurity purposes. Significant improvements may be expected, especially those that take into account contemporary and promising development of what is known as adversarial learning.

The role of deep learning, especially unattended, is vitally emerging as one of the most prominent types of machine learning that can contribute to enhancing cybersecurity. There are many benefits to cybersecurity systems based on deep learning algorithms, such as reducing the amount of manual effort to identify patterns in suspicious behavior and the ability to improve cybersecurity performance better [2]. The data mining has strategies and algorithms to detect malware and we have to consider which strategy that will be effective to detect malware from a huge set of information which depend on similar features.

Each of data mining strategies have different requirements such as anomaly detection, misuse detection, and hybrid

detection. Moreover, data mining algorithms can perform on each strategy but some of these algorithms has strength and limitation. Algorithms used in malware detection are Decision Tree Learning, Naive Bayes Classifier (NB), K-Nearest Neighbour, and Support Vector Machine. Some of these algorithms has a critical limitation mentioned below [18]:

- Complexity of algorithms
- Extensive memory requirements
- High computational effort

Malware technologies are developed each day and data mining algorithms nowadays can detect malware and classify it. However, it is critical to develop new data mining algorithms to be fast and scalable to detect and classify malware.

7. Conclusion

From the above, the most relevant results of the present research paper can be drawn as cybersecurity is a critical and vital topic for protecting data, information, and systems. Moreover, many areas and applications of artificial intelligence can contribute to enhancing cybersecurity, such as machine learning, deep learning, data mining, and expert systems. The possibility of utilizing data mining algorithms to develop and support cyber security.

References

[1] Khandelwal, P. & Sudhir K. (2018). Introduction to Artificial Intelligence and its Applications. On Emerging Trends In Information Technology (NCETIT'2018) with the theme-'The Changing Landscape Of Cyber Security: Challenges: 94.

[2] Atlam, H., Walters, R. and Wills, G. (2018). Intelligence of Things: Opportunities & Challenges. [ebook] University of Southampton, p.4. Available at: https://www.researchgate.net/publication/325295863_Intelligence_of_Things_Opportunities_Challenges [Accessed 6 Dec. 2019].

[3] Big data, artificial intelligence, machine learning and data protection. (2017). 2nd ed. [ebook] Information Commissioner's Office. Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [Accessed 7 Dec. 2019].

[4] Internetsociety.org. (2017). Artificial Intelligence and Machine Learning: Policy Paper. [online] Available at: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AI-Policy-Paper_2017-04-27_0.pdf [Accessed 8 Dec. 2019].

[5] Mathworks.com. (2019). What Is Deep Learning? | How It Works, Techniques & Applications. [online] Available at: https://www.mathworks.com/discovery/deep-learning.html [Accessed 10 Dec. 2019].

[6] Sullivan, D. (2016). FAQ: All about the Google RankBrain algorithm - Search Engine Land. [online] Search Engine Land. Available at: https://searchengineland.com/faq-all-about-the-new-google-rankbrain-algorithm-234440 [Accessed 6 Dec. 2019].

[7] Kamtam, A., Kamar, A., & Patkar, U. C. (2016). Artificial Intelligence approaches in Cyber Security. International Journal on Recent and Innovation Trends in Computing and Communication, 4(4), 05-09.

[8] Intelligence, S. (2019). IBM QRadar Security Intelligence. [online] Ibm.com. Available at: https://www.ibm.com/security/security-intelligence/qradar [Accessed 6 Dec. 2019].

[9] IBMSecurity. (2019). 2019 Cost of a Data Breach Report| IBM Security. [online] Available at: https://databreachcalculator.mybluemix.net/executive-summary [Accessed 6 Dec. 2019].

[10] NormShield Cyber Risk Scorecard. (2019). Cyber Security with Artificial Intelligence in 10 Question | NormShield Cyber Risk Scorecard. [online] Available at: https://www.normshield.com/cyber-security-with-artificial-intelligence-in-10-question/ [Accessed 6 Dec. 2019].

[11] Pandey, M. (2018). Artificial Intelligence in Cyber Security. On Emerging Trends In Information Technology (NCETIT'2018) with the theme-'The Changing Landscape Of Cyber Security: Challenges, 66

[12] Alpaydın, Ethem. Introduction to machine learning. Cambridge, MA: MIT Press, 2014.

[13] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cybersecurity. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 371-390). IEEE.

[14] Anagnostopoulos, C. (2018). Weakly Supervised Learning: How to Engineer Labels for Machine Learning in Cyber-Security. Data Science for Cyber-security, 3, 195.

[15] Ansari, A. Q., Patki, T., Patki, A. B., & Kumar, V. (2007, August). Integrating fuzzy logic and data mining: impact on cybersecurity. In Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on (Vol. 4, pp. 498-502). IEEE.

[16] Katoua, H. S. (2013). Exploiting the Data Mining Methodology for Cyber Security. Egyptian Computer Science Journal, 37(6).

[17] Nagesh, S. (2013). Roll of Data Mining in Cyber Security. Journal of Exclusive Management Science, 2(5), 1-5.

[18] Masud, M., Khan, L. and Thuraisingham, B., 2016. Data mining tools for malware detection. Auerbach Publications.