Crossing Point of Artificial Intelligence in Cybersecurity

Praveen Kumar Donepudi

Principal Architect, IT Infrastructure Services, Cognizant Technology Solutions, **United States**

Source of Support: Nil **No Conflict of Interest:** Declared

ABSTRACT

There is a wide scope of interdisciplinary crossing points between Artificial Intelligence (AI) and Cybersecurity. On one hand, AI advancements, for example, deep learning, can be introduced into cybersecurity to develop smart models for executing malware classification and intrusion detection and threatening intelligent detecting. Then again, AI models will confront different cyber threats, which will affect their sample, learning, and decision making. Along these lines, AI models need specific cybersecurity defense and assurance advances to battle ill-disposed machine learning, preserve protection in AI, secure united learning, and so forth. Because of the above two angles, we audit the crossing point of AI and Cybersecurity. To begin with, we sum up existing research methodologies regarding fighting cyber threats utilizing artificial intelligence, including receiving customary AI techniques and existing deep learning solutions. At that point, we analyze the counterattacks from which AI itself may endure, divide their qualities, and characterize the relating protection techniques. And finally, from the aspects of developing encrypted neural networks and understanding safe deep learning, we expand the current analysis on the most proficient method to develop a secure AI framework. This paper centers mainly around a central question: "By what means can artificial intelligence applications be utilized to upgrade cybersecurity?" From this question rises the accompanying set of sub-questions: What is the idea of artificial intelligence and what are its fields? What are the main areas of artificial intelligence that can uphold cybersecurity? What is the idea of data mining and how might it be utilized to upgrade cybersecurity? Hence, this paper is planned to reveal insight into the idea of artificial intelligence and its fields, and how it can profit by applications of AI brainpower to upgrade and improve cybersecurity. Using an analytical distinct approach of past writing on the matter, the significance of the need to utilize AI strategies to improve cybersecurity was featured and the main fields of application of artificial intelligence that upgrade cybersecurity, for example, machine learning, data mining, deep learning, and expert systems.

Keywords: Artificial intelligence, cybersecurity, data mining

INTRODUCTION

Although numerous individuals have intelligence, huge numbers of them do not have the abilities of approaches to comprehend the issue and discover answers for it. Notwithstanding, with regards to reducing mistakes in operational tasks and discovering inconsistencies, artificial intelligence is in front of human capacity and skill. Artificial intelligence is instrumental in evaluating mistakes that people are helpless against making. Artificial intelligence as an answer for cybersecurity can help shield organizations from Internet threats, distinguish sorts of malware, guarantee handy security norms, and help make better anticipation and recuperation systems. Hence, through this exploration, we will reveal insight into how AI innovations and applications can add to cybersecurity.

Today, Cyberspace security has forced enormous effects on different basic frameworks. Customary security depends on the static control of security gadgets sent on exceptional edges or hubs, for example, firewalls, Intrusion Detection Systems (IDSs), and Intrusion Prevention Systems (IPSs), for network security observing as per the pre-indicated rules.

The everyday raising and advancing cybersecurity danger confronting worldwide organizations can be reduced by the combination of Artificial Intelligence into cybersecurity frameworks. Machine learning and Artificial Intelligence (AI) are being associated more

widely over businesses and applications than some other time in late memory as registering power, storage limits, and information data collection increment. This immense proportion of data can't be managed by individuals logically. With machine learning and AI, that pinnacle of information could be cut down in a portion of time, which causes the tasks to recognize and recoup from the security danger.

It is reasonable that security against insightful cyber bats will be accomplished simply by astute code, and functions of the latest years have demonstrated rapidly expanding intelligence of malware and cyber-weapons. The use of organization focal fighting makes cyber episodes especially risky, and changes in cybersecurity are required. The new security ways like powerful arrangement of secured perimeters, extensive situation awareness, the very machine-driven response on assaults in organizations would require widespread use of AI ways and knowledge-based tools and technologies. Why has the part of astute code in cyber tasks gathered consequently quickly?

Needing closer to the cyber house, one will see the resulting answer. Artificial intelligence is required for a practical response to things on the internet. One ought to have the option to deal with the extraordinary arrangement of information in a matter of seconds to clarify and separate functions that occur in the cybersecurity environment and to time-based decisions. The speed of cycles and the amount of data to be utilized can't be taken care of by people while not significant automation is in the process. However, it is inconvenient to create code with standard mounted algorithms for viably protective against the assaults in cybersecurity, because of new threats appearing unendingly.

Research Methodology

This paper plans to reveal insight into the idea of artificial intelligence, recognize the main areas of artificial intelligence that can be utilized in cybersecurity, and explain the role that these areas can play (particularly machine learning, data mining, deep learning, and expert systems) in supporting cybersecurity in Organizations. Steady with the target behind the current paper, its application depends on a descriptive scientific methodology dependent on extrapolation of past writing in a basic hypothetical and diagnostic way to extract the solution to the fundamental questions of the paper.

Research Background

The idea of Artificial Intelligence was presented following the presentation of the idea of the computerized processing machine. It came because of questions, Alan asked in 1950 that "Can the machine think?" it was trailed by a discussion during the fifties and sixties of the only remaining century on whether the machine can carry out all the work that people can do in their day by day lives. The machine had the option to perform certain capacities for critical thinking and problem solving, however it couldn't play out the full human intellectual capacities, which was referred to as the term Weak AI. To understand the full scope of human intellectual capacities, the idea of Strong AI has gone to the front, which includes the tasks that people have generally performed, the use of a wide scope of foundation information, and the presence of some level of mindfulness (Bibel, 2014).

Artificial Intelligence is an immense and giant study of software engineering, and it is to make frameworks that can work cleverly and freely, like the individual cerebrum's choice tools. With AI, a machine to gain as a matter of fact by handling a lot of information and perceiving the example in them. For instance, Apple Siri, face recognition, and self-driving vehicle these depend on Machine Learning and natural language processing (NLP) which are a subset of AI.

Artificial intelligence has these areas and technologies so it tends to be utilized in numerous industries, for example, financial organizations, education, and wellbeing. Also, it is utilized in numerous applications identified with cybersecurity that are referenced in the next section.

Artificial Intelligence in Cybersecurity

In the early days, Cyber Security and AI were not associated with one another. Artificial Intelligence experts were keen on creating projects to reduce human work, while security experts attempting to fix the outpouring of data. However, the two fields have developed nearer throughout the time, when the cyber-attacks have focused to recreate the authentic exhibition, at the human level as well as at lower framework levels. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is an awesome case of association of artificial intelligence and cybersecurity. This requires the end-user to embed the letters of some unreasonable picture, on certain events with the expansion of a masked sequence of letters or digits that shows up on the screen.

Enhancements in automated character recognition programming, which can be viewed as a sensible development in AI innovation, could propel the field towards more refined example recognition. So in the act of attempting to make sure about properties, for example, online ticket reservations, the productive security market is in a way stimulating advances in artificial intelligence.

Artificial Intelligence encourages us to rapidly distinguishing and examining new exploits and shortcomings to assist ease with promoting attacks and is a fundamental piece of our answers. Artificial Intelligence rehearses are the way to Interference discovery and make it conceivable to react even to mysterious threats before spreading itself.

Artificial Intelligence frameworks that are proposed to learn and adjust, and are capable of identifying even the minutes of changes in the settings, can act significantly sooner and dependent on a tremendous store of information than people with regards to analyzing novel sorts of cyber-attacks.

Research Gap Analysis

In this Axis of research, we will clarify how the monstrous capability of Artificial Intelligence advancements can be utilized to upgrade cybersecurity. The information has been created in this day and age is expanding and the data stored or got in any structure, regardless of whether simply or in a complex way, through the Internet. Besides, the information must be sent over to an organization to get it in an objective because the appropriate transmission of information assumes an essential function in fighting cyber-crimes, which is accomplished through standards of cybersecurity. With the developing progressions in Information Technology, intruders are utilizing cyberspace to carry out different cyber-crimes, which later made a significant interruption in the cyber society (Han et al., 2014).

Artificial intelligence and cybersecurity are expansive terms, and we can utilize it both in associations to moderate dangers and increment income by recognizing cyber threats and misrepresentation. Nonetheless, staying aware of new viruses and malware updates is getting more intense, cybersecurity utilizing artificial intelligence advances will encourage the location and reaction to threats and malware by utilizing past cyber-attack information to decide the best strategy. Figure 1 shows the cost of an information breach in the Middle East if organizations not executed automated security arrangements.

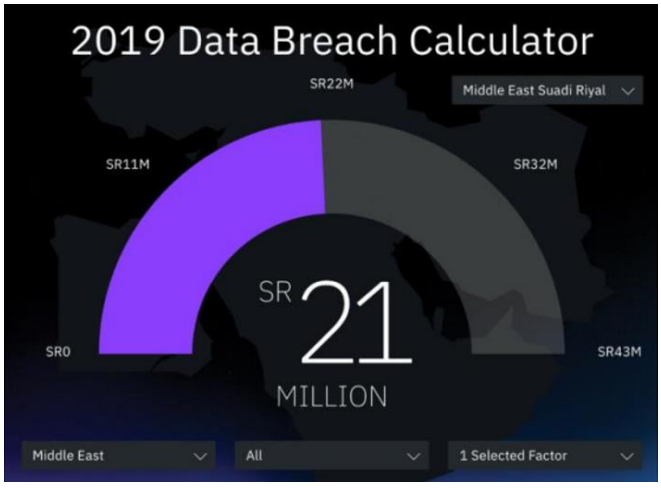

Figure 1: Data Breach Calculation in the Middle East

Artificial intelligence may frequently be preferred and more compelling over people in identifying vindictive malware. Computer-based intelligence is executed in the association with different security solutions, for example, Security Information, and Event Management helps security experts for any threats inside the organization of the association to improve identification (He et al., 2014).

"The quicker the information break was recognized and contained, the lower the expenses. This year, the expanding time to determine a breach was conceivable because of the expanding seriousness of criminal and vindictive attacks experienced by a larger part of organizations. Security automation and wise arrangement capacities that give visibility over the security tasks focus can help improve an organizations' capacity to contain the harm from a breach" (Kremer, 2014).

Artificial Intelligence Approaches for Cybersecurity

Knowledge or Rule-Based Approach

In Knowledge-based AI frameworks, we try to install the information of human experts for their decision-making abilities. Here the thought is to equip the framework with the information needed for a certain task, for instance - clinical diagnosis, and the guidelines to derive bits of knowledge from the information to make a decision. This way all the choices that the KBAI framework takes will be influenced exclusively by the information base made by the human master in the concerned field. Hence, KBAI frameworks are otherwise called Expert Systems.

In this way, the overall design of the KBAI framework comprises of a Knowledgebase and an inference engine. The inference engine largely has IF-ElSE conditions for derivation from the information base. The main information-based framework was MYCIN. It was written for medical diagnosis. The focal idea of information based frameworks was to speak to the information expressly through IF-ElSE conditions. Representation of Knowledge is the central task for building up an AI framework. The rule-based knowledge representation is intensely utilized for the advancement of IBM Watson.

Pattern Recognition Approach

Pattern recognition is another way to deal with Artificial Intelligence. It depends on information, not at all like an information base in rule-based methodology. It attempts to gain proficiency with the information from the data itself. We simply need information and machine learning algorithms to find examples from the information. These examples will determine the choices of the framework in an obscure way. Here is the cutting edge definition of pattern recognition (Bishop): The field of pattern recognition is focused on the automatic discovery of informalities in information using PC algorithms and with the utilization of these consistencies to take actions, for example, arranging the information into various classes. Pattern recognition has been the best way to deal with Artificial Intelligence. Machine Learning is the best way to deal with pattern recognition. In the following area, we will have a deep insight into it.

Machine Learning

In 1959, Arthur Samuel introduced the term "Machine Learning". As per him, "Machine learning is the field of study that enables the computers to learn without being expressly customized". This catches the center thought. Not at all like prior methodologies where we were attempting to characterize a main part of rules to determine knowledge from information, has machine learning produced such frameworks that gain proficiency with those rules themselves from the information. This methodology is nearer to natural learning. For a model, a child figures out how to distinguish an apple after he/she is indicated plenty of instances of apples.

Essentially, we give the machine a ton of information, and the machine without anyone else build up an instinct for the information. In the expressions to Tom Mitchell, "A PC program is said to gain from an experience E concerning some class of tasks T and performance measure by P if its performance at tasks in T, as estimated by P, improves with experience E." Those calculations that allow machines to learn are known as the Machine learning algorithms. However, machine learning algorithms can be characterized into two classifications - Supervised Learning and Unsupervised Learning. There are likewise some different sorts of machine learning like Reinforcement Learning and so on but those are past the extent of this part.

ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBERSECURITY

Expert Systems

An Expert System is a computer framework that duplicates the decision-making capacity of a human. This is the best case of a Knowledge-based framework. These information-based frameworks are made out of two sub-frameworks: the Knowledge Base and the Inference Engine. The information base speaks to the illustrations and assertions in reality. The Inference Engine is a programmed thinking framework. It assesses the current circumstance of the information base and applies the principles relevant to that, at that point affirms new information into it.

This framework shell ought to be supported by a programming framework for adding data inside the psychological object, and it will be reached out with programs for user connections, and with various projects that will be used in hybrid skilled frameworks.

Creating an associate skilled framework implies that, first, determination/transformation of associate skilled framework shell and, second, exploits skilled data and filling the psychological object with the data. The second step is out and away from a great deal of troublesome and time overwhelming than the first one.

CSIA - Cyber Security Artificial Intelligence Expert System has the following segments in the Knowledge base and Inference Engine.

Components of Expert Systems	
Knowledge Base	Malicious IP Address
	Known Malware
	Known Virus
	Approved Applications
	Approved IP Addresses
	End Point Usage Statistics
Inference Engine	IP Address Geographical Location
	Connection Attempts
	Connection Patterns
	Frequency of Program Use
	Document Usage
	Login Timestamps
	Login Attempts
	Port Communication
	File/Folder Access Patterns

Table 1: Components of Expert Systems

The Security expert system keeps a bunch of rules to fight cyber-attacks. It checks the cycle with the information base on the off chance that it is good-known cycles, at that point the security system disregard, in any case, the framework would end the cycle. If there is no such cycle in the information base, then utilizing inference engine calculations (rule sets), the expert system discovers the machine state. The machine state has been formed into three states to be specific safe, moderate, and severe. As indicated by the machine state, the framework alarms the administrator or the user about the status, and afterward, the inference has been fed to the Knowledge base.

Neural Nets

Neural Nets are otherwise called deep learning. It is a serious part of AI. It is inspired by the capacities and working of the human mind. Our cerebrum has a few neurons, which are to a great extent universally useful and space free. It can gain proficiency with information. In 1957 Frank Rosenblatt made an artificial neuron (Perceptron) which was made ready for neural networks. These perceptron can learn and handle interesting issues by joining with different nerves i.e., perceptron. Perceptron learns all alone to distinguish the substance on which they are trained by learning and handling the significant level crude information, as our mind takes on its own from the crude information utilizing our tangible organ's data sources. At the point when we apply this deep learning to cybersecurity, the framework can distinguish whether a record is harmful or genuine without human impedance. This strategy yields a solid outcome in identifying the harmful threats, compared with traditional machine learning systems. The victory of neural nets in cybersecurity is their speed. At the point when they upheld in equipment or graphical processors, it processes quicker. Neural nets can allow the specific

recognition of new malware threats and fill in the harmful gaps that leave organizations wide open to cyber-attacks.

Intelligent Agents

Intelligent Agent (IA) is an independent entity that perceives development through sensors and follows up on an environment utilizing actuators (for example it is an agent) and coordinates its movement towards achieving goals. Intelligent agents may moreover learn or utilize information base to achieve their goals. They may be incredibly straightforward or complex. A reflex machine, for instance, the thermostat is an intelligent agent. It has the conduct like understanding agent interaction language, favorable to animation and reactivity. They can adjust to continuous, learn new things quickly through communication with the environment, and have memory-based standard storage and recovery capacities. An intelligent agent is made in a standoff against Distributed Denial of Service (DDoS) attacks. On the off chance that if there is any lawful or business issue, it ought to be sensible to build up a "Cyber Police". Cyber Police ought to have versatile intelligent agents. For this, we should device the foundation to help the quality and cooperation between the intelligent agents. Multi-agent tools will give a great deal of undeniable usable appearance of the cyber police.

ARTIFICIAL INTELLIGENCE APPLICATIONS FOR CYBERSECURITY

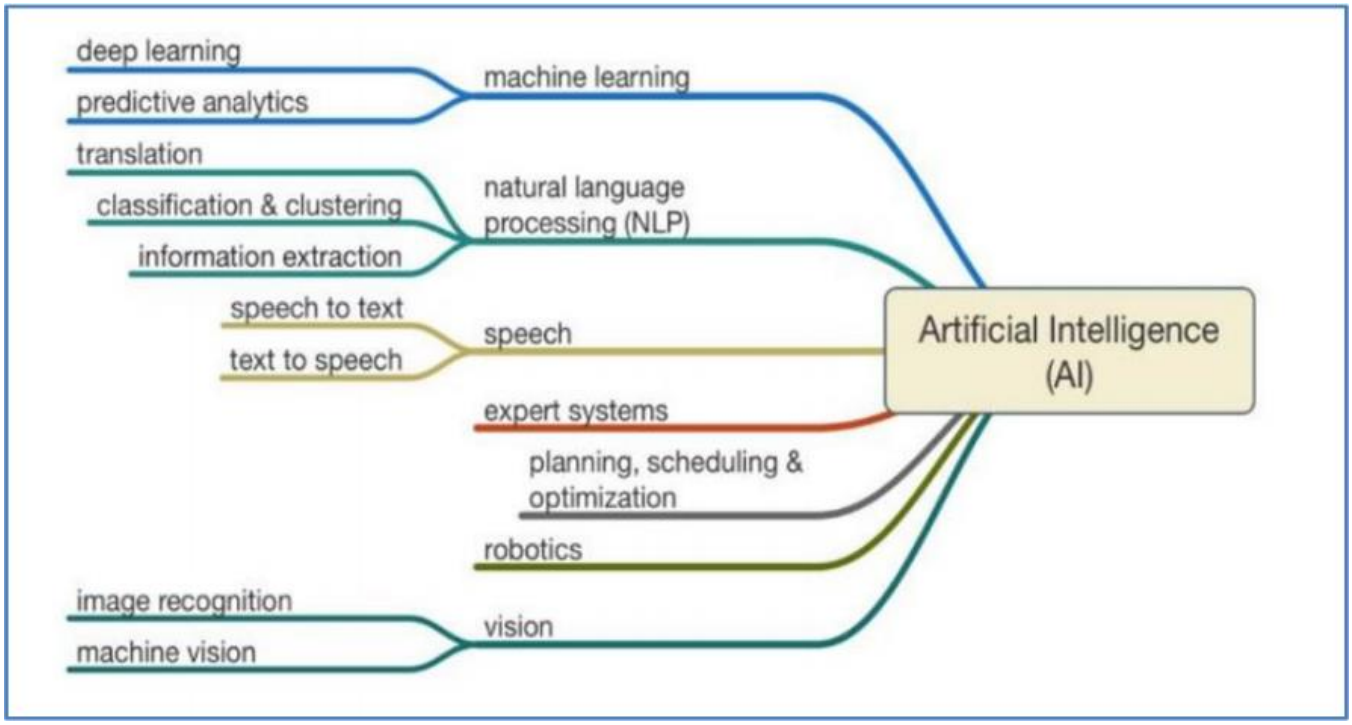

Figure 2: Applications of AI in Cybersecurity

Applications of Expert Systems in Cybersecurity

Expert Systems are one of the most noticeable tools of Artificial Intelligence and are software packages that help in concluding requests that either a client gives or that another product package gives. These frameworks incorporate information content in which expert data is kept in a particular field of utilization. These frameworks likewise remember an inference engine to get to answers in light of the data are given and other extra data with respect to the surrounding conditions (Kremer, 2014).

Applications of Deep Learning in Cybersecurity

The absence of disaggregated information is a typical test in cybersecurity research. Even though its return to privacy factors frequently clarifies this shortage, experience shows that even in secret of huge partnerships with the critical interior ability that security data with respect to threats can be changed into an ordered arrangement of information proper for machine learning. The explanation for this is the presence of an enormous measure of huge and unequal informational indexes, the shortage of time needed to perform manual classification, and fields' unique attributes, for example, an arrangement of semantics that increases the gap between specialized skills and statistical modeling. To this end, there is a push to accommodate these logical inconsistencies and to contend that ongoing analysis on the shortcoming of controlled learning - in which numerous exact techniques are utilized as opposed to exploring and checking genuine data - is a fertile system that can be based upon in cybersecurity research; with

conventional choices for supervised, semi-subject, and non-supervised learning (Nourani et al., 2014).

Applications of Data Mining in Cybersecurity

Data mining is the research for critical examples and patterns in an enormous information base (O'Leary, 2013). The data mining technique expects to acquire significant data and find hidden examples from a huge number of data sets, which measurable methodologies can't find. It is a region of huge orders for research that includes machine learning, information bases, measurements, expert systems, visualization, high-performance computing, neural networks, and knowledge representation. Data mining is supported by a host that catches information in different manners (e.g., clustering, classification, link analysis, regression models, and sequence analysis (Straub & Huber, 2013).

A few instances of employing data mining to recognize breaches of cybersecurity: eliminating typical exercises from warning information to allow examinations to focus on realistic attacks; distinguishing bogus alarm generators, and finding uncommon exercises that uncover a genuine attack; Specifying long and continuous examples of unusual activities (using diverse IP addresses to lead a similar action); summarizing data identified with cybersecurity with the help of insights; and visual representation of information related with cybersecurity. Figure 3 shows the main functional process of data mining.

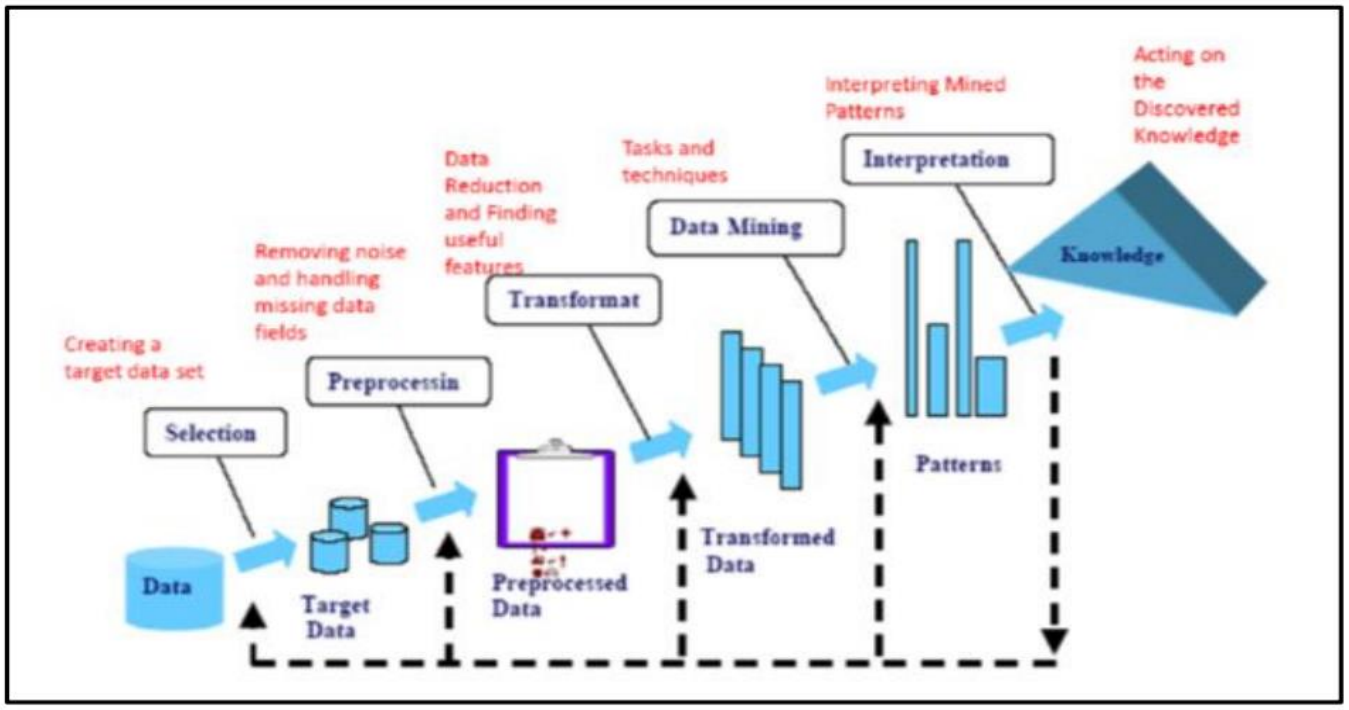

Figure 3: Phases of Data Mining Process

PROPOSED SOLUTION

This study was applied using a systematic and descriptive analysis technique of writing and past investigations. The outcomes demonstrated the chance of utilizing machine learning, deep learning, and data mining techniques for cybersecurity purposes in three primary domains: intrusion detection, malware analysis, and spam discovery.

The part of deep learning, particularly unattended, is fundamentally rising as one of the most noticeable kinds of machine learning that can add to improving cybersecurity. There are numerous advantages to cybersecurity frameworks dependent on deep learning algorithms, for example, reducing the measure of manual exertion to distinguish designs in doubtful behavior and the capacity to improve cybersecurity performance better (Zeng & Mao, 2014). Data mining has techniques and algorithms to identify malware and we need to consider which system will be powerful to recognize malware from a huge set of data that rely upon similar features. Each one of the data mining methodologies has various prerequisites, for example, anomaly detection, misuse location, and hybrid identification. Besides, data mining calculations can perform on every technique except a portion of these calculations has quality and constraint. Algorithms utilized in malware locations are Decision Tree Learning, Naive Bayes Classifier (NB), K-Nearest Neighbor, and Support Vector Machine (SVM).

Malware technologies are built up every day and data mining algorithms these days can recognize malware and characterize them. Nonetheless, it is basic to develop new

data mining algorithms to be quick and versatile to recognize and characterize malware.

Conclusion

From the above mentioned, the most important aftereffects of the current paper can be drawn as cybersecurity is a basic and imperative theme for ensuring information, data, and systems. Also, numerous areas and uses of artificial intelligence can add to upgrading cybersecurity, for example, machine learning, deep learning, data mining, and expert systems. The chance of using data mining algorithms to create and uphold cybersecurity is increasing as the data is progressing each passing day.

References

Bibel, W. (2014). Artificial intelligence in a historical perspective. *AI Communications, 27*(1), 87-102. https://search.proquest.com/docview/1531922017?accountid=35493

Han, K., Kang, B., & Im, E. G. (2014). Malware analysis using visualized image matrices. *The Scientific World Journal, 2014.* https://dx.doi.org/10.1155/2014/132713

He, D., Chan, S., Zhang, Y., Wu, C., & Wang, B. (2014). How effective are the prevailing attack-defense models for cybersecurity anyway? *IEEE Intelligent Systems, 29*(5), 14-21. https://dx.doi.org/10.1109/MIS.2013.105

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & Communications Technology Law, 23*(3), 220. https://dx.doi.org/10.1080/13600834.2014.970432

Lee, R. M., U.S.A.F. (2013). The interim years of cyberspace. *Air & Space Power Journal, 27*(1), 58-79. https://search.proquest.com/docview/1318929537?accountid=35493

Nourani, V., Hosseini Baghanam, A., Adamowski, J., & Kisi, O. (2014). Applications of hybrid wavelet-artificial intelligence models in hydrology: A review. *Journal of Hydrology (Amsterdam), 514*, 358-377. https://dx.doi.org/10.1016/j.jhydrol.2014.03.057

O'Leary, D.,E. (2013). Artificial intelligence and big data. *IEEE Intelligent Systems, 28*(2), 96-99. https://dx.doi.org/10.1109/MIS.2013.39

Straub, J., & Huber, J. (2013). A characterization of the utility of using artificial intelligence to test two artificial intelligence systems. *Computers, 2*(2), 67-87. https://dx.doi.org/10.3390/computers2020067

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197-208. https://dx.doi.org/10.24908/ss.v12i2.4776

Zeng, D., & Mao, W. (2014). Supporting global collective intelligence via artificial intelligence. *IEEE Intelligent Systems, 29*(2), 2-4. https://dx.doi.org/10.1109/MIS.2014.30

--0--