Chapter 2
Role of AI and Its Impact on the Development of Cyber Security Applications

A. Anandita Iyer and K. S. Umadevi

Introduction

In this era of technological advancements, every sector of the community is heavily and constantly relying on computer networks and different information solutions. With this exponential growth in networks, comes an equally drastic growth in cyberattacks, thus making all the sectors vulnerable to these attacks. A cyberattack can be defined as an attempt to destroy, alter, expose, disable or steal data or gain unauthorized access to any system, organization, or any device. Since the first denial-of-service (DOS) attack, in 1988, there has been an astounding growth in the number of cyberattacks and its impact [1], thus paving a way to the urgent need of cyber security that will help in protecting and practicing safety measures for network devices and safeguard data from unauthorized access and attacks by a nefarious party.

In a traditional cyber security environment, the response to an attack is based on static control, which means that either the attack is responded after the attack has already taken place or the response will be based on certain rules predefined by the system admin based on the signatures of the previously occurred attacks. For example, in a network intrusion attack, the system will monitor incoming traffic based on a set of rules and will notify the admin after the attack has occurred or in certain cases will block those packets of data that are considered malicious. But since this method depends on the following certain rules for identifying an attack, there are many such possible scenarios where the attacks can be morphed into data packets that can pass the detection system unnoticed. Such an incident was reported by Equifax in 2017, where an attacker hacked the systems exposing data of more than 140 million customers [1]. The attackers discovered a flaw in the online portal of the company and uploaded a programming language to their server to gain remote

A. Anandita Iyer · K. S. Umadevi (✉)
Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
e-mail: umadeviks@vit.ac.in

V. Sarveshwaran et al. (eds.), *Artificial Intelligence and Cyber Security in Industry 4.0*, Advanced Technologies and Societal Change,
https://doi.org/10.1007/978-981-99-2115-7_2

access and uncovered database credential of Equifax. Then used it to search for all the user sensitive document and stole the data. Apart from this, threats like advanced persistent threat (APT), zero-day attacks, etc., are attacks where attacker camouflages their activities, and before the admin can even discover the vulnerability in the system, the system is attacked and the sensitive data leveraged. In such an unpredictable environment, a different approach to prevent attacks from occurring is a priority rather than waiting for notifications of attacks that have already taken place.

We live in digital world, where data is vital and its security has become more important than ever. With every passing day, hackers are evolving, getting smarter and finding innovative ways to exploit vulnerable data leading to new attacks, data breaches, data crashes, data poisoning, etc. More and more complex yet sophisticated attacks are being launched every day making cyber security measures a very serious and crucial requirement to be implemented by organizations and individuals as well. Main security objectives have always been confidentiality, availability, non-repudiation, authentication and integrity [2]. These goals can be achieved by the use of artificial intelligence (AI), whose main motive is to mimic the cognitive behavior of humans and carry out tasks that would usually be conducted by a human being. Artificial intelligence is an independent entity that behaves like human, thinks like human and performs tasks like a human being. In today's time, we have been surrounded by AI, in the form of personal assistants, automated transportation, facial recognition, computer gaming experience, aviation, voice recognition, etc. In cyber security, an AI can identify risk, prioritize the security requirements, detect malware in a network, notice intrusion in a network, before it even starts and also prepares a proper incident response plan.

Overview of Artificial Intelligence

Artificial intelligence was officially born in 1956 as a summer research project by John McCarthy at Dartmouth, where his goals were to explore various ways where a machine can simulate few aspects of intelligence, which is still the basic idea behind the continuous development of artificial intelligence. Fast forward to eighteenth century where Thomas Bayes designed a framework for reasoning based on the probability of collective events and continuting to nineteenth century, logical reasoning was discussed by George Boole. Heuristic search was introduced by Newell and Simon, and later, Samuel's self-play, self-improved checkers' playing program laid out the first instance of machine learning (ML) in work. Later on, Rosenblatt's perceptron model based on biological neurons served as the basis for artificial neural network (ANN) [3]. In 2004, NASA created autonomous driving for Mars rover, a self-driving and navigation system based on machine learning. From here on, artificial intelligence has grown and developed to become one of the most indispensable technologies that we know of today.

A precise definition of artificial intelligence, that matches its sophisticated and popular image is quite difficult. In its simplest form, artificial intelligence can be defined as an activity that is committed in making machines intelligent, as intelligence is a feature that is required by an entity to work appropriately and on its own as well as make predictions about its environment. To this day, human intelligence is far superior when compared to artificial or biological world, and this is because human beings have the ability to understand, reason, perceive, achieve goals, generate language, create art, summarize information, etc. [3], thus making human intelligence a default choice to modify and train an AI. With the rapid growth of technology, matching a human ability can be considered as a sufficient condition and not a thumb rule, as there exist many systems which surpass certain levels of human intelligence, for example—speed.

Another way to define artificial intelligence, as described by John McCarthy, is "an approach which employs mathematical logic to formalize basic facts about events and their effects." An artificially intelligent machine can learn, understand and act on the basis of the information obtained from events and their effects [1].

The definitions presented in Table 2.1 concentrate on human behavior and knowledge representations to develop intelligent agents. That is comparing and understanding how the human mind functions, process knowledge, make decisions with respect to the computer program for e.g., using reason to conclude results, using logical approach to achieve goal etc. These agents (something that perceives and acts) grow and exchange knowledge with other agents and repeat the same process until they find an efficient solution to a problem.

This chapter will briefly discuss about artificial intelligence and its impact on cyber security as well as discuss various applications of AI in cyber security in detail. The chapter will be organized as follows: the chapter will start with an abstract, followed by first section: Introduction, which will establish the foundation of the chapter and its contents. Section "Literature Survey" will be a brief survey on the use of artificial intelligence by organization to secure their ecosystem. This section will talk about the existing research based on artificial intelligence and cyber security and how AI has evolved in providing better security to industries. Section "Artificial Intelligence Techniques for Cyber Security" elaborates AI techniques and AI-based use cases in cyber security. In addition, it explores the scenarios where artificial intelligence has proved to be an exceptional tool in terms of cyber security by using real-life examples. Section "Applications of AI in Cyber Security" enlists various applications of AI in security. This section will discuss in depth about various applications of AI

Table 2.1 Definition of AI [1]

	Humanly	Rationally
Thinking	A machine should think and solve problems like a human would	A machine must use proper logic and arguments and facts to find a correct solution
Acting	Machine must act like human. It should have the ability of natural language processing, reasoning and knowledge representation	Machine should proceed based on rational factors. It must act in order to produce a more efficient outcome based on the given scenario

in cyber security and how these applications are deployed. Section "Limitations of AI in Security" will discuss about limitations of using AI for cyber security. Using examples, the section will talk about how AI can be manipulated to nullify security measures. To conclude the chapter, section "Conclusion": Conclusion will be at the end, summarizing the whole chapter leading to the last section which will cite the references.

Literature Survey

AI in cyber security is targeting issues like malware detection, network intrusion, spam and phishing detection. Ongoing researches show different combinations of existing AI algorithms or different AI techniques combined together to solve various security problems. These combinations have generated great results, some better than the other. Reference [1] mentions that as AI has proved to be a boon for mitigating threats, AI will also prove to be a curse with the cases of AI-based attacks and threats increasing.

The combinations to develop a new security model are decided based on the data properties in a system. The learning algorithms must be first trained accurately using the security data and target information acquired from the system, before it can start intelligent decision-making. Reference [4] has reviewed various deep learning and some standard neural network approaches that can be used to build a security model, including supervised learning, semi-supervised learning, unsupervised and reinforcement learning. They included convolutional neural network (CNN), self-organizing maps (SOM), recurrent neural network (RNN) and many more. They concluded that deep neural network models and their hybrid combinations can intelligently resolve many existing security issues and also will help in predicting unknown attacks. Similarly, [5] discusses application-level security by integrating AI and cyber security models. The paper talks about how to identify and avoid network intrusion attacks and detect suspicious activities in network by using artificial intelligent models and malicious activities in server which is monitored by cyber security methodology, hence reducing the load on network. Cyber security is a vast sea, which holds many different security models for various threats that exist. Discussing one such model, Identity and Access Management (IAM) and its relationship with artificial intelligence. The study conducted in [6] explains that even though organizations are applying AI tools for security measures, they have still not matured enough in their approach to information and access management. If artificial intelligence is applied to IAM along with an appropriate monitoring and reporting tools, visualization of network connectivity and data access will become possible, thus reducing network breaches.

Various studies have been performed to compute the effectiveness of AI in cyber security ecosystem. One such work conducted in [7] presents an extensive review to compare different machine learning algorithms in cyber security applications: malware analysis, intrusion detection, spam and phishing detection. Commercial products were not included in the study as there is a high possibility that the vendor will not reveal their original algorithm and there may be some cases where they might overlook certain limitations in their systems. The study included analysis of botnet and Domain Generation Algorithm (DGA) for intrusion detection via ML. For malware analysis, the paper includes polymorphic and metamorphic features of the malware and how ML algorithms can help to mitigate them. Lastly, they suggest ML algorithms from the family of supervised and unsupervised learning algorithms that can be useful in addressing various attacks discussed. Another study focused in Iraq talks about effectiveness of AI models against cyber threats [8]. Research data was collected from 468 employees from IT industry, and basic analysis of model, discriminant validity, confirmatory factor analysis were carried out. First, an expert system analysis of data was carried out by the team without including any AI or cyber security techniques. Later for the same test cases, a smart PLS (variance-based structural equation modeling using the partial least squares (PLS) path method) was applied. It was seen that there was a huge impact on the results when AI was used.

Technology is slowly depending on artificial intelligence day by day as it can be seen in different sectors like education, health, transport and economic sectors. Most seen applications of AI are personal assistant, precise health consultation and treatment and cyber security. Reference [9] performs a rigorous survey on impact of AI in today's digital society and concludes that AI has shown tremendous success in the area of security by detecting and preventing serious threats and AI will emerge to be a very useful tool in future for cyber security. AI will come into aid for manufacturing and e-commerce by making the plants self-reliant. Research in neural networks proves that in future, AI can match human- like thinking. Machine learning methods are used in most sector nowadays, and social media is being one of it. An article on application of machine learning on social media discusses how ML algorithms have become a very convenient tool to measure sentiment of the user, and based on it sorting news and other digital data for the user to view [10]. Apart from this, the article speaks about how ML can be used to identify fake news and malicious content on social media. Moving further, it discussed the integration of cyber security with AI and the need for same in battling adversarial machine learning and privacy problems.

Federated machine learning has taken over the buzz now, as it provides a way for participants to learn a shared machine learning model, without exposing their local data. But, studies show that an intruder can still exploit shared parameters and compromise user's local data, for example medical smart watch, self-driving cars, etc., which can be very dangerous. Reference [11] proposes a privacy-enhanced federated learning model (PEFL) scheme for industrial artificial intelligence. The proposed method is meant to safeguard the local information of the user by considering them as local gradients and using deep learning algorithms along with their proposed model, thus providing postquantum security (next-generation security). On one hand, cyber security industry has successfully incorporated some AI techniques, that are used to mitigate threats, forensic analysis, intrusion detection, prevent sensitive data leak, predicting unknown attacks, critical infrastructure protection, malware detection, etc. On the other hand, rise of adversarial AI is evident, whose key idea is to break down artificially intelligent tools and systems for profit and even for fun [12]. With the use of AI to provide security, new AI vulnerabilities are coming into light, like system manipulation and data poisoning. Reference [13] says, adversaries are using these vulnerabilities to attack AI and alter the system behavior. Reference [14] concludes that every technology comes with its own drawbacks and issues, and after exploring the balance between AI-based security and AI-based threats, it is safe to say that AI security is better than no security as well as AI will provide better strategic plannings to mitigate new attacks.

Artificial Intelligence Techniques for Cyber Security

Information technology is a hotspot today and therefore an easy target to commit crimes and also being used as a medium for committing crimes as well. Readily available devices and high-end products have made it even easier to execute attacks from any location and be untraceable. Digital crime or Computer crimes or Network crimes come under Cybercrime, where the intent of the criminal is to steal sensitive data like hack bank servers for monetary gains, steal personal data and so on. Cybercrimes encompass offenses like online extortion, misuse of intellectual property rights, international money laundering, economic espionage [15]. As these crimes have become common, they have also grown to become more threatening. Traditional security methods fail to prevent and at times even identify these attacks until it has already happened and then it is too late, as the sensitive data is either out in the open or they are misused.

Hence, the introduction of artificial intelligence in cyber security has proved to be a game changer. As presented above in the survey section, there are organizations and researchers working tediously to develop new and innovative ways to incorporate AI with security, and this has proven to be very useful in many organizations which will be mentioned further in this section. As already discussed, AI is a tool that finds ways to push machines to be more intelligent and replicate human-like behaviors like learning, planning, thinking, reasoning, etc. To counter this issue of trying to be more intelligent, a simplified approach was stated that will divide the main goal, i.e., making the machine intelligent into smaller sub-goals, thus breaking down the roles into different characteristics that should be mimicked by the system [15].

The different characteristics are as follows: Deduction, reasoning and problem solving—agents; neural networks, statistical approaches to AI; Knowledge representation—ontologies; Planning—multi-agent planning and cooperation; Learning—machine learning; Natural language processing—information retrieval, text mining; Motion and manipulation—mapping, navigation, localization; Perception—facial recognition, speech recognition; Social intelligence—empathy simulation; Creativity—artificial imagination; General intelligence—strong AI.

Now that it is discussed how AI strives to become more and more intelligent, and let us take a look at how AI works. AI works in three ways [1]:

1. Assisted intelligence: this helps people to improve what they have already been doing.
2. Augmented intelligence: provides help with things that cannot be easily done by people.
3. Autonomous intelligence: machine learning features that are a separate entity and that act on its own.

Keeping this outline in mind, it can be said that AI focuses on solving tasks which can simply be a support to the existing system to dealing with some most difficult issues on its own, like cyber security since cyberattacks have proved to potentially catastrophic.

Various Artificial Intelligence Tools and Techniques Are Mentioned Below

Expert system (ES):

An expert system is built to solve complex problems and provide human-like decision ability. Based on the user query, an expert system extracts knowledge from knowledge base and uses inference rules to make sound reasoning and returns the result [16]. Expert system aids in decision-making by combining both heuristics and facts just like a human expert. To solve any complex issue, this system extracts knowledge from its knowledge base and uses available facts to come to a certain conclusion. The name expert systems came to life because it stores expert knowledge about a specific domain and helps to solve complex issues in that particular domain. The accuracy and performance of expert system come from the knowledge it stores in this knowledge base. More knowledge saved in the knowledge base, the better the system improves its performance. Figure 2.1 represents how the expert system functions.

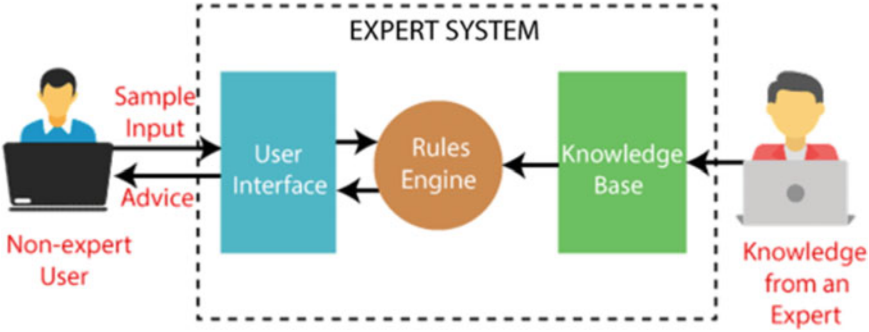

Fig. 2.1 Working of expert system in AI [16]

Expert systems have following characteristics: high performance—expert system solves complex issues with high performance, accuracy and efficiency; understandable—takes input from the user in human understandable language and returns output in same, and thus, it is easily comprehended by the user; reliable—can easily rely on this system for accurate results; highly responsive—complex queries can be solved within a very small-time frame.

ES can be bifurcated into two important components: knowledge and inference engine [1]. Knowledge is the heart of *knowledge-based* systems and stores all the information gathered by the machine as experiences which will be used to train the system. Knowledge base can be understood as a database where all the expert information (data received from the experts of a domain) regarding the domain is stored. Every data is stored with its corresponding attributes or feature, thus making it more efficient. Again, knowledge base contains two types of knowledge: factual knowledge—based on facts and accepted by the experts, and heuristic knowledge—based on experience, practice and its ability to learn.

Reasoning of these stored knowledge is done by *inference engine.* Inference engine can otherwise be referred to as the brain of the expert system. Inference rules are applied by the inference engine to the knowledge base in order to generate error-free solution to a posted query or to find new information based on the query, which is stored back to knowledge base for future reference. Rules are generated on the basis of two types of inference engine: deterministic inference engine—deductions are totally depended on facts and rules and are always assumed to be true, and probabilistic inference engine—contains uncertainty as the conclusions are based on probability.

These expert systems help in solving two scenarios, case-based reasoning and rule-based reasoning [1].

Case-based reasoning—These reasoning techniques pull out problem cases similar to the current problem scenario and assume that the solutions derived to solve the past cases can be applied to the current scenario to obtain a suitable solution. And, this solution is evaluated and revised until needed and then added to knowledge base.

Rule-based reasoning—Experts define rule to solve the problem. Rules are composed of two parts: condition and action. The problem is evaluated based on the condition, and then, necessary actions will be taken for the same. This technique cannot modify its existing rules or learn new rules.

Expert systems are considered as one of the best tools for making decisions as it has no memory limitations, has high performance, accuracy and efficiency, is an expert in a domain, takes into consideration all the facts, experiences and regular knowledge update which make it even more accurate and efficient. However, it also can give wrong results if the knowledge is wrong, cost of development and maintenance is too high, and these systems cannot self-learn.

Machine learning:

Machine learning is a part of artificial intelligence which enables a system (or machine) to learn from data, enhance its performance by inferring from its experience

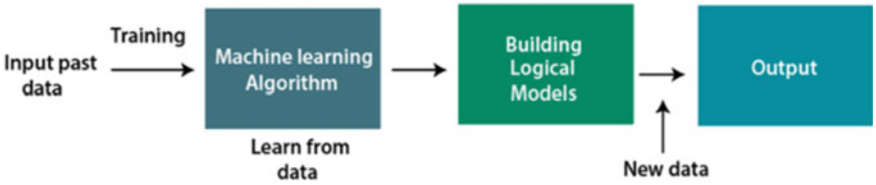

Fig. 2.2 Typical machine learning algorithm working [17]

and predict new outcomes. The goal of machine learning is to develop mathematical models and make predictions based on historical information. First, the machine is trained with the help of historical or pre-existing or in other words training data. Using this, the machine builds a decision-making or prediction model which as name suggests is used for taking a decision and/or predicting new outcomes. From here, whenever the machine receives a new input, it refers to the model it built and generates the result. Figure 2.2 depicts the work flow in a machine learning algorithm.

Machine learning helps system to understand the underlying connection between data and how to learn from data itself and past experiences without the need to be explicitly programmed. Machine learning uses statistical methods to discover new patterns, extract information from raw data and deduce connections even when dealing with huge amount of data. Machine learning algorithms are discussed further in the chapter. Commonly used algorithms in machine learning are: Support Vector Machine, Decision Tree, K-means clustering, Random Forest, K-nearest neighbors, etc.

Deep learning:

As it is pre-established that machine learning is a subset of AI, similarly deep learning is a subset of machine learning. Deep learning has the same goals as machine learning, and only difference is that deep learning is heavily influenced by human brain. Deep learning hopes to achieve the similar way of thinking and deductions, as is done by the human brain, and in order to achieve this, deep learning uses neural networks. A neural network is inspired by the biological neural system in human body. It can be taught to neural network to identify as well as classify patterns and information in the same way as the human brain would. Each layer of neural network can be understood as a filter that sorts the data to achieve an accurate result. A neural network contains different layers as depicted in Fig. 2.3, which contains input layer, three hidden layer and an output layer, where x is input data and y is the outcome of the neural network.

Artificial neural network (ANN) has the needed properties that equip deep learning models with capabilities to solve complex problems, that would be impossible by a machine learning algorithm to solve. The main factor that distinguishes deep learning algorithm from machine learning algorithm is feature extraction method. Machine learning performs feature extraction to draw the needed attribute from a dataset. Feature extraction is a complex process that requires in-depth knowledge about the domain, whereas deep learning does not require feature extraction as that is supported

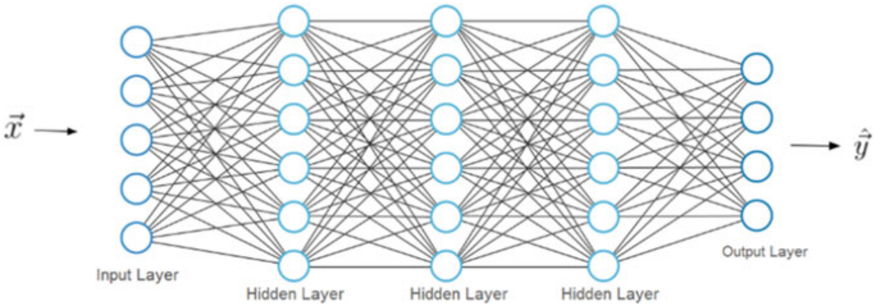

Fig. 2.3 Typical neural network [18]

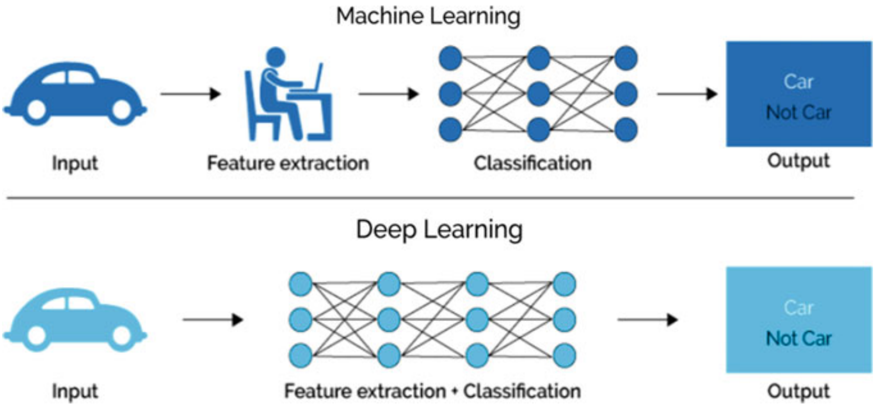

Fig. 2.4 Machine learning versus deep learning [18]

by ANN itself, thus making deep learning superior. This difference can be seen in Fig. 2.4.

Deep learning helps the computers to learn from their experiences in the same manner a human being learns new things from experience. Deep learning enables system to learn tasks that can be done by a human being, without any human intervention. It mimics human brains and nervous system by generating new patterns for the machine to use decision-making techniques. It keeps creating extensive neural networks and trains these networks with huge datasets, thus increasing the performance of neural networks.

Artificial immune systems (AISs) are models for computational analysis that are able to learn continuously and dynamically from its environment and easily adapt to ever-changing surrounding. This concept is based on the biological immune system, which detects and discards intruders (bacteria or virus) in a living organism; similarly, AISs imitate this biological system when applied for network security and act as a constantly evolving intrusion detection system [15].

Another AI technique inspired by biological system is *Genetic Algorithm*, which is a learning methodology that follows the process of natural selection. Genetic algorithm helps in solving complex mathematical problems that has a large set of input variables and possible outcomes. These algorithms are used for generating classification rules for attack patterns and can even generate pattern-specific rules as well. The basis of this algorithm is natural selection process that means poor solutions will be replaced by offspring of best possible solutions from the mix until a precise outcome is guaranteed [15].

Machine Learning Algorithm Used to Train a Machine

When AI or ML is used for security, one of the usual problems that still stand is to identify attack patterns efficiently, understand it, classify and take necessary actions. As attack signatures keep getting modified by the attacker to surpass the security of the system, it is an utmost important job to find every deviation of the attack pattern. A negative detection of the network traffic is as problematic as numerous false-positive detections. To train the machine, three learning algorithms are used, as mentioned in detail below:

Supervised learning

Supervised training is a form of learning algorithm, that trains a machine by utilizing *labeled data,* and using this data, possible outputs are predicted. A labeled data is nothing but predefined outputs tagged to their respective inputs. It can be understood in this way, that the labeled training data used to train the machine is a supervisor, guiding the machine to accurately predict an output. The machine is provided with input along with its correct output and the machine should be able to map the new input with an output correctly, hence being the goal of the supervised learning algorithm, i.e., to being able to map input variable (x) with output variable (y) $\{f(x) \rightarrow f(y)\}$.

Supervised learning functions as follows: it uses two types of datasets, training data and testing data. Training data is the labeled data, which helps the machine to learn patterns within the dataset, and based on this, the model is tested using the testing data and the machine predicts the output.

Figure 2.5 shows how the machine is trained with labeled dataset (shapes and their names), and after the training, it is tested with test dataset and the machine has to predict the names of the shapes. In this form of learning, the machine understands how to map any input data to its corresponding output based on given sample data. The machine is trained till it becomes so accurate that it can precisely calculate outputs from the new inputs.

This learning algorithm is classified into two main groups: classification problems and regression problems [19, 20].

Classification algorithm is used for categorical output data, which means that when the output of a training set is binary: Yes/No, True/False, Male/Female, etc.

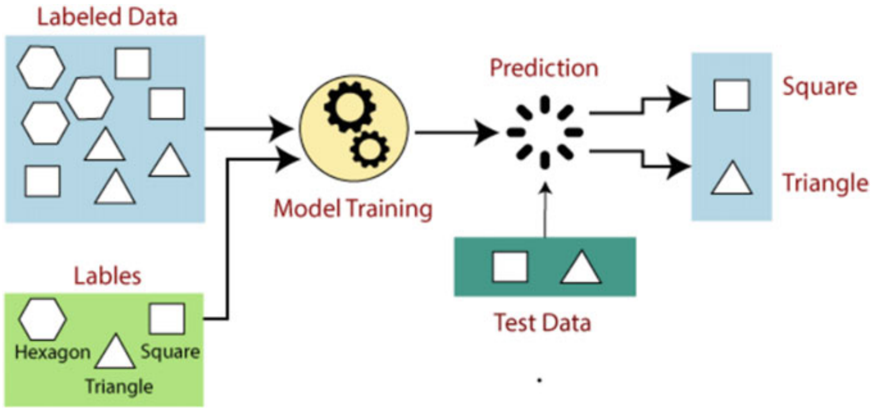

Fig. 2.5 Working of supervised learning [19]

Classification algorithm returns discreet outputs, e.g., classification of a book based on color black or green. Here are few of the classification algorithms—Random Forest, Decision Tree, Logistic Regression, Support Vector Machines.

Regression algorithms are sought when there exists a relationship or dependency in between the input and the output variables. This algorithm returns prediction values such as cost, weight, and it can be a continuous variables like market trends and weather forecasting, etc. Some of the regression algorithms are Linear regression, Nonlinear regression, Regression Trees, Bayesian Linear regression and Polynomial Regression.

There are enough datasets containing malware files, thus allowing easier training to these algorithms, which lead to improved detection of attacks and less numbers or false positive and false negative. These algorithms have contributed in smarter and more advanced approach in detecting cyberattacks than traditional string-matching techniques or address blacklisting techniques. Supervised learning can predict outcomes based on experience, and in real-world issues, it has proved quite useful in spam filtering, fraud detection, etc. However, this algorithm is not good for complex tasks and requires huge computational time.

Unsupervised learning

As opposed to the supervised learning where the machine is trained with labeled dataset, in unsupervised learning, the machine is trained with no sample labeled data. As the name suggests, the machine is not supervised using labeled training data, rather the machine tried to identify hidden patterns and knowledge from the provided dataset.

The aim of machine learning is to understand the structure of the given dataset and find similarities among the data, divide it into similar group and present the outcome. For example, if the machine is given a dataset that contains the images of fishes and birds but no label to it, the machine will have no clue about the features of the dataset.

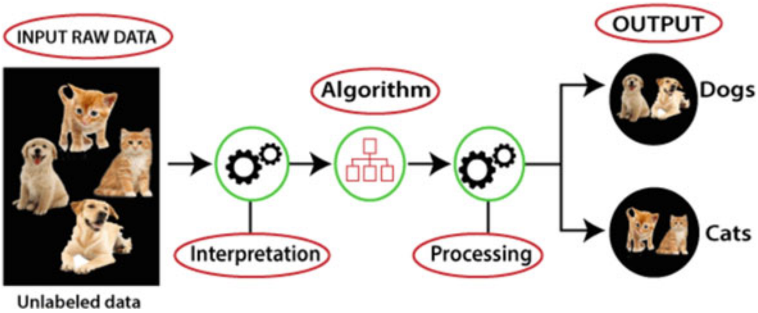

Fig. 2.6 Unsupervised learning algorithm [21]

Now, the goal of the machine is to learn on its own and differentiate the features and categorize them into groups (clusters) based on the similarities between the features. Unsupervised learning aids in identifying important insights from a given dataset, as it works very similar to how human being thinks and understands based on their own experience thus making this a real AI. The machine is expected to understand the data and learn from data alone regarding the underlying patterns and deduce the correct output for the new inputs, as can be seen in Fig. 2.6 with an example of dogs and cats. Unsupervised learning can be categorized into three types, namely: clustering, association and dimensionality reduction.

Clustering: A method in unsupervised learning model which divides data into different groups based on the similarities in the features and sorts the features with less to no similarity in another group.

Cluster analysis finds common items/features between data objects and categorizes them accordingly. When used for security, the algorithm identifies and groups similar type of network traffic data into relevant clusters and in the process isolating abnormal network traffic like shown in Fig. 2.7, for e.g., failed login events, data accessed by a user which is usually not accessed by him, connections from unusual locations, etc.

Association: These unsupervised methods categorized inputs based on association rules, which are based on finding relationship between the input variables in a large dataset. Association rule learning methods attempt to establish rules and relationship between large databases. It discovers set of items that usually occur simultaneously or are dependent on each other. For example, let us say a person who goes to buy candles, also can buy matches. These rules majorly benefit marketing strategies.

Dimensionality reduction: Dimensionality reduction methods serve very well in real-time intrusion analysis. Dimensionality reduction works by reducing the number of features (an attribute of various elements that exist in a dataset) of data which will help in solving the problem easily [20]. Suppose a network traffic has n number of features like source IP, destination IP, port number, protocol, routing information, MAC address, etc., analyzing each and every feature is cost ineffective and takes huge time to process, thus rendering real-time applications useless. However, if we

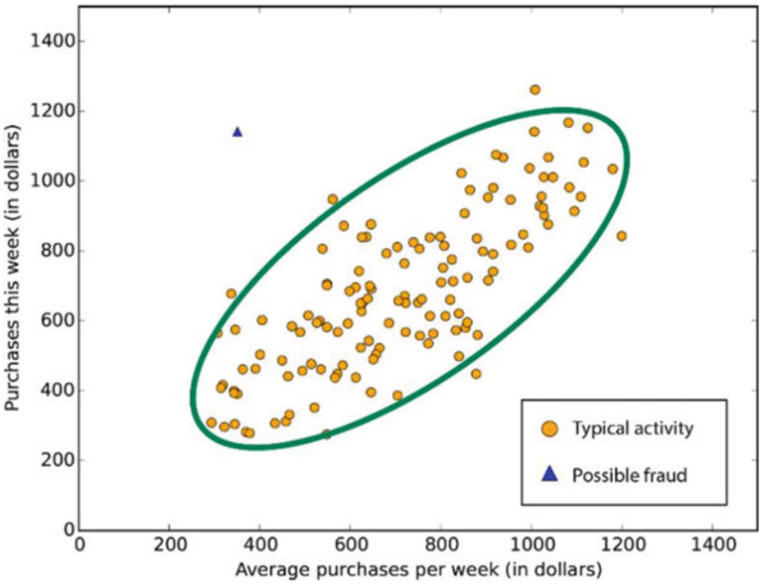

Fig. 2.7 Detection of online fraud using clustering (Microsoft 2017) [20]

are able to reduce the number of features to more relevant ones and divide them into manageable sets, the problem will be easier and quicker to solve.

Some of the algorithms of unsupervised learning are: K-means clustering, K-nearest neighbor (KNN), Apriori algorithm, hierarchal clustering, anomaly detection, etc. Unsupervised learning algorithm is used to perform more complex tasks and is more preferred as it uses unlabeled training data, which are much easier to acquire. However, the result of this learning algorithm can be less accurate and is intrinsically difficult.

Reinforcement learning:

A feedback-based learning algorithm where the agents (something that perceives and acts) learn how to behave in a given environment by the feedback they receive based on their actions. Positive feedback is given for a good or correct action and negative feedback is given for a wrong action as shown in Fig. 2.8. This algorithm also trains with no labeled data, and its actions and learning are purely based on experience. The agent associates with the environment and explores the same on its own. An agent under reinforcement learning aims to enhance the performance by receiving maximum positive rewards. Reinforcement learning can be described as a hit and trial method of learning, where every hit is rewarded (positive feedback) and every miss is punished (negative feedback). It is a combination of both supervised and unsupervised learnings which learns the next moves based on rewards or punishment. This learning algorithm is used when there is very little to no data provided.

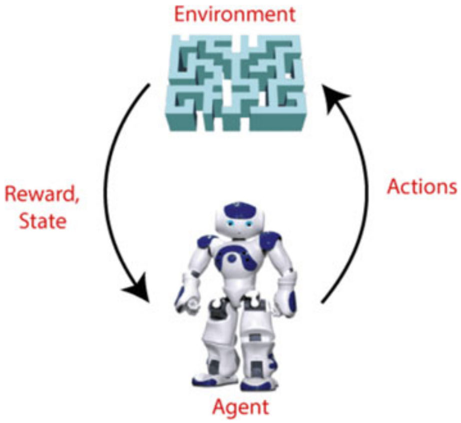

Fig. 2.8 Machine learning via reinforcement learning algorithm [22]

Why AI is Preferred Over Current Anomaly Detection and Prevention Systems?

The current system of anomaly prevention and detection system offers ways to detect unknown attacks, but there are certain limitations that entail them. One of the major issues faced by these traditional methods is difficulty in establishing a proper model that can encase list of acceptable behaviors and rules for attack patterns, as they generate a high number of false positives, which is in reality caused by a normal network traffic but might have some deviations with respect to the defined rules. It is very common for behaviors to change and modify depending on the environment, what is difficult here is that the detection and prevention system has to be updated regularly for the same so that it enables machine to recognize normal traffic from malicious ones [15]. Other limitations of these systems are:

- Any legitimate activity that gets marked as malicious one by the detection/prevention system (known as false positives) results in defective communication or exchange of data, as the prevention system will attempt to stop or change the activity it identified as malicious.
- Attackers can easily shutdown the intrusion detection systems, if they can learn how the system functions.
- Integrating data from heterogeneous environments proves to be an issue.
- Any intrusion detection and prevention system should adhere to certain legal regulations and/or service level agreements.

Artificial intelligence on the other hand is ever-learning and ever-growing technology that will keep updating its knowledge base, depending upon the new inputs and its environment [23]. The rules are updated and modified as and when required with minimum involvement of the system admin, thus paving a path toward robust and secure systems.

Use Cases of Artificial Intelligence in Cyber Security

Everyone is connected via internet today. This means, there are numerous personal and public data available on internet that can lead to many cyber security issues. Manual analysis of this data is impossible given its sheer volume, and for the same reason, cost to prevent attacks on such large volume of data is also too high. Designing and implementing new algorithms for every new threat that uncovers itself require lot of effort, money and time. AI comes to the rescue here, by examining huge data accurately and more efficiently within a short period of time. Even with ever-changing threat patterns, AI can predict similar type of attacks that can happen in future and avoid it by using the threat history. The main reason that AI is a perfect fit for cyber security is because: it can handle huge data volume, it can predict and discover new possible attacks and it learns continuously from its environment to respond better to future threats. Artificial intelligence can single handily reduce the response time and improve the network security when an attack or any malicious activity is detected.

Use cases [24]:

(i) Network Threat Identification:

Protecting the network infrastructure of any organization is very vital, and this requires understanding every aspect related to the network topology and building necessary cyber security processes that will be tailored according to the network's needs. Keeping track of all the information coming in and going out of the network is difficult for human professional to address, and it will also require considerable amount of time. To add on to this, figuring out which system is under attack or device is malicious is a challenging task for any professional. And when it comes to large-scale organizations, it requires huge amount of time to identify malicious apps or activities in the network and human professionals do not always provide accurate services. Thus, an AI security system for the organization's network traffic will help with monitoring all incoming and outgoing traffic and detect suspicious patterns in it. The data that is combed by an AI is usually a large volume of dataset that is difficult for a network professional to go through and find threat patterns [25].

Example: Versive is an AI vendor that provides cyber security based on artificial intelligence, which identifies threats based on dissonant detection. Dissonant detection means any sound that is so annoying or disruptive that it puts any listener on edge (alarm going off, scream of a person, etc.). This organization provides its services to banks and other financial institutions to identify any security threats. Cyber security offered by Versive takes DNS, Proxy and NetFlow as inputs for their security engine. Anomaly detection is used to monitor network to find discrepancies in the data.

(ii) User Behavior Modeling:

There exist certain security attacks that steal the private login credential of a client in a company without their knowledge and use these credentials to access company's network. Since it is a user's login credentials, it does not raise any red flags, and thus, these attacks are very difficult to detect and stop. AI-based risk management systems play an important role in this area. These systems analyze any changes in password pattern of a customer in the organization. Any inconsistency is being notified to security team to take necessary action.

Example: An AI vendor called “Darktrace” provides a security software which is used as a machine learning algorithm to inspect the information on network traffic and understand the user behavior in a company. This software alerts the company as soon as it detects any suspicious behavior that is contrary to normal user behavior.

(iii) Fighting AI threats:

As researchers and system admins are using AI to establish better cyber security, hackers are utilizing this technology to detect entry points within an organization’s network. Thus, in future, one of the biggest security defenses against AI-adopted attacks will be AI-based software. NotPetya and WannaCry are the firms that suffered badly against cyberattacks and ransomware in past few years. These attacks are only going to grow here after, and these attackers can make a bigger impact on the technological sector by using AI to launch attacks.

Example: A security software called, Falcon Platform developed by CrowdStrike, a cyber security technology company, uses artificial intelligence to protect against ransomware attacks. The software uses anomaly detection for endpoint security.

Applications of AI in Cyber Security

As mentioned above, AI was introduced to learn human behavior and mimic them and to understand real-world issues from a human point of view. AI was required to make machines more intelligent and learn from its experiences. AI has made it possible as well as convenient to store and process large volume of data intelligently. AI has been using such processing capabilities to provide applications in different sectors like space exploration and defense [26].

Applications of AI can also be seen in healthcare sector where it is helping physicians to make a proper diagnosis, generate treatment plans based on patient’s medical history and even help perform surgical treatments. Another most crucial application of AI can be seen in cyber security. Cyber security encompasses technologies, practices and process to protect devices, programs, network and data from unauthorized access or in case of attacks.

Various frameworks exist in cyber security such as ISO 27001/27002/27017, NIST, CCM, HIPAA, NERC [26]. These security standards control different security domains. Some of the crucial areas of study in cyber security are—Application security, Network security, Infrastructure security, Web security, Threat intelligence, IoT security, Identity and access management, Mobile security, Cloud security, Incident response plan, Human security.

Cyber security measures focus on managing risk and vulnerabilities to increase system's durability at the time of attack. Attacks are inevitable. An individual and especially an organization must always be prepared to bear and mitigate attacks. The key to effectively do this is to monitor network behaviors, anomalies and latest malwares. Cyber security is based on threat analysis, i.e., preparations to mitigate threats should be in place and enough protection should be provided for the system to endure the threat and come out of it with minimum to no loss. The major challenge for any cyber security methodology is to be able to function even when the system is under attack, rapidly end the attack and restore all the functionalities to the point (normal state) before the incident (attack) took place. An organization's security strategy is built on estimated risk and threat analysis.

Threat, risk and vulnerability are interconnected in cyber world. The system or a network is a valuable asset to the organization and has to be protected at all cost. Any organization will try to protect its system from malicious attacks/threat, mitigate risks and keep updating the system security to avoid vulnerability. Threat can be defined as any harmful activity, like an attack that puts a system at harm's way. Vulnerability points to weakness in the system, which might lead to an attack or increase the chances of an attack to occur, whereas risk is expected damage that can occur in the system [1].

Cyber security is interdisciplinary area including computer science, system and criminology. There are many factors that come into play while dealing with it, like people (user, admin, employee, etc.), network and application process and integration with other technologies, and therefore, problem can arise at any point in any factor associated with security, as shown in Fig. 2.9.

Lately, cyberattack numbers have increased exponentially along with the sophistication of the attacks. Cyber-criminals keep learning how to deploy latest tools and techniques to hack, attack and steal information from a user and/or a system, and traditional security measures have proven to be inadequate to prevent breaches resulting from such attacks. Therefore, artificial intelligence was introduced to build smart models to defend the networks from attacks. As AI can evolve rather quickly to understand complex situations, it has become an elementary tool in cyber security. AI techniques help in rapid identification of network intrusions, malware attacks, data breaches, phishing attacks, etc., as well as alert the necessary party when the attack occurs [1].

Use of AI can teach us how to enable expert security measures to monitor and analyze abnormalities in the system. Organizations apply AI in these four areas to enhance cyber security measures [2]:

Automated defense: Cyber security systems are divided into two types—Analyst-driven system and Automated systems. Analyst-driven systems are people dependent, and they are developed and operated by people. On the other hand automated systems make use of AI tools. These intelligent tools are self-learning systems. Humans alone cannot defend cyber space, and thus, a need of automation is very much necessary. With the unprecedented growth of data and network complexity, AI is a blessing for organizations to monitor secure their systems. These automation tools can easily be integrated with some of the existing security measures. Some of the functions are:

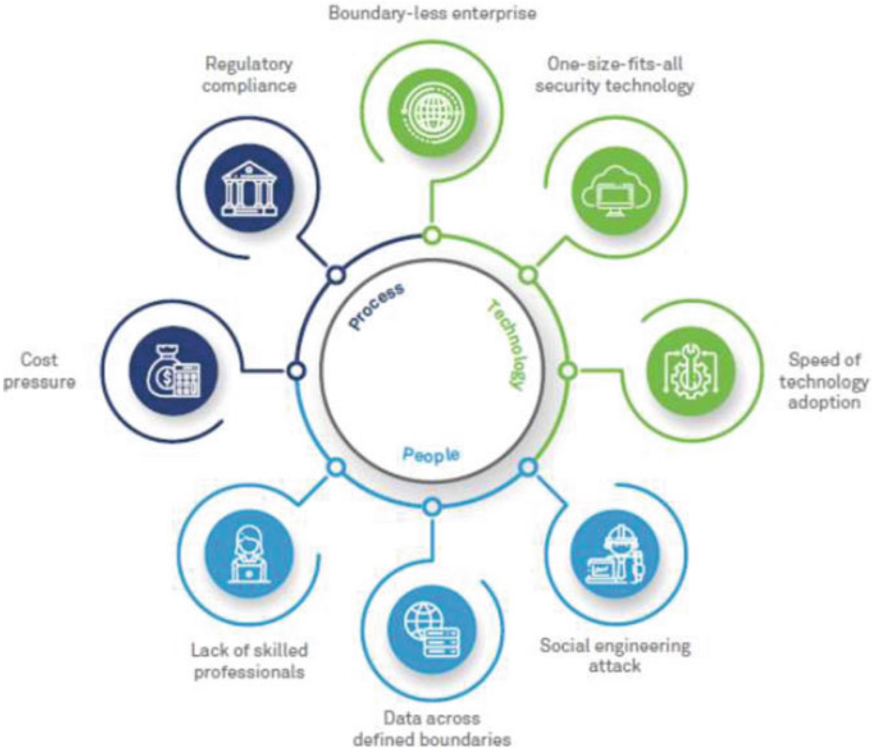
Boundary-less enterprise
Regulatory compliance
One-size-fits-all security technology
Process
Technology
People
Cost pressure
Speed of technology adoption
Lack of skilled professionals
Social engineering attack
Data across defined boundaries

Fig. 2.9 Security issues associated with people, process and technology [2]

- Detecting threats and malicious activities using predictive analytics.
- Securing conditional authentication and access.
- Enhancing learning and analysis through natural language processing.
- Improving human analysis—from malicious attack detection to endpoint protection.
- Using automation in mundane security tasks.

Cognitive Security: This approach combines human intelligence as well as AI. It is an advanced form of AI that uses different forms of AI. Cognitive security is related to AI in a way that both push the boundaries of machine intelligence. The only difference between the two is in the way they react with humans. AI can be described as a technology that strives to return a most accurate result or action based on algorithms while requiring human intervention, whereas cognitive security aims at overcoming the boundaries of programming and unite with humans to help them make better decisions.

Adversarial training: An adversarial learning is associated with using artificial intelligence for malicious reasons. Using this learning, AI can be taught to misbehave and spill sensitive data. But, training AI with adversarial attack models can help detection of vulnerabilities that can be fixed in early stages and help to make the model more robust.

Parallel and dynamic monitoring: When a system is targeted with new learning abilities, it needs to be monitored constantly. This is done so that any deviation between the actual and expected outputs can be noted and addressed.

AI Solutions for Cyber Security [26]

- AI2: An artificial intelligent platform—AI2 was developed by MIT and PatternEx to predict cyberattacks. This platform resulted in 86% accuracy while detecting and predicting cyberattacks which was regarded as three times better than any previous prediction model. AI2 uses clustering algorithm from unsupervised learning technique and isolates suspicious activities, which are then passed to system analyst who decides whether the incident was an attack or not. Every outcome from the platform is added to a dataset by the analyst to enable future learning based on existing data (supervised learning). New models are also generated by this platform for better detection of future attacks.
- Darktrace: Darktrace is a security solution that helps in identifying and recognizing new cyber threats, that a traditional security model would normally miss. It detects anomalies in an organization's network by using Enterprise Immune System (EIS) technology and machine learning algorithms. EIS works with mathematical principles, which means that it does not employ rules or signatures and therefore can detect and respond to new and/or unknown security attacks which the system has not experienced before. Using machine learning and mathematical principles, Darktrace adapts and learns user behaviors, device and network behavior so that it can distinguish between genuine behaviors and behaviors that may indicate attack. Self-learning technology of Darktrace allows organization to view a detailed network analysis and proactively respond to threats to mitigate risks.
- CylanceProtect: Launched in 2018, CylanceProtect is an integration of artificial intelligence with information security tools that helps in threat prevention. Script-based attacks, memory-targeted attacks and attacks on external devices are protected by the use of information security and artificial intelligence which helps in identifying known and unknown malicious software. CylanceProtect helps in preventing unknown as well as known zero-day attacks. It also protects the device without causing any inconvenience to the end user.
- Deep Instinct: This software was developed to protect firm's mobile devices and services in real time against malicious attacks. Using artificial intelligence, Deep Instinct detects hostile activities on devices, office workstations and services. It then employs deep learning techniques to predict unrecognized cyberattacks. The aim behind this is to help the software learn different types of combinations of requests that occur when dealing with malicious systems. The aim of using deep

learning here is to slice the software code into smaller code snippets for future survey.

- Human security: Organizations prepare its network, system and devices to evade or tolerate external attacks, but they should also protect their resources from threats that may originate within the firm. Such threats can be originated from an employee that works in the company or an intruder who has assumed the role of an employee and cause damage from within, making the assets of the company weak. They can escalate their privileges to access more sensitive data from the company or they can steal customer information. Applying artificial intelligence to monitor the user behavior is must here. Any slight modification that might indicate potential attacks must be red flagged and notified to the admin immediately.

Limitations of AI in Security

As seen above, artificial intelligence methods are an indispensable tool to fight cyber-crimes, but it comes with its own fair share of consequences. There are certain limitations associated with AI such as intensive training, high resources and cost. If adequate resources are used for training and testing any machine learning model, it is a quite convenient process, but with limited resources, AI systems may take huge processing time since the volume of data required to train a system is equally huge. One of the big drawbacks is that hacker can also pursue AI methodologies to develop malware and train it to become unnoticeable from AI detection tools like inserting adversarial data into the mix, model stealing, data poisoning. Though AI provides extensive support in the field of cyber security, if the same is used against security, it can make the future of attacks more dangerous and unpredictable [2].

Ethical Issues Related to AI [27]

Data ethics plays an important role in determining the boundaries to ethical access of data. It is clearly established that AI requires data to train its models and therefore requires data collection and data processing. This means that the AI and data are completely intertwined. In cases like these, setting an ethical boundary for data and its use or access has become a very complex problem. Some concerns that come up are:

- Is the data safe?
- How AI manages sensitive data?
- What happens if a piece of data is modified?

According to researchers, in about 50 years there is a huge possibility that AI may become a serious threat to humanity. By year 2040 there is said to be a 50% similarity in the thinking and understanding process of a human and a machine which could jump to 95% by the year 2075, where one would not be able to distinguish between a human and a machine based on their thinking processes.

Ethical issues related to artificial intelligence can be divided into two types:

1. Data collected, its processing and data analysis.
2. AI making decisions that are based on generalized data.

The primary ethical problem arises with the collection and analysis of user data, which include social data, digital data, personal data. Companies need this data to train machines for better data mapping and generating self-resilient security models. Ethical issue that rises here is that all these data are stored in one dataset to train the machine, and any malicious activity with it and billions of user sensitive data is compromised, but imposing over the top restrictions on data access will generate poor security models and slow down development of AI in cyber security [27, 28].

Another issue is the making decisions based on generalized data. Let us take an example, AI used in the development of military needs like smart missile, etc., and these use geographical location as data input and make decision based on it. These intelligent weapons can help to save thousands of lives when deployed correctly; if there is even a slight tweak in the data, it may even target the creators. Seeing this network security point of view, an AI security model designed to prevent attack for an organization is modified by a hacker and all the hacker did was add some adversarial inputs in the dataset mix, then there is a huge possibility that the model developed to provide security may be a security threat to the system.

AI-Based Threat to Cyber Security [27]

After analyzing the trends in creation and use of artificial intelligence, two criminological risks come to the surface:

1. Direct risk: When the risk of using AI will have a direct effect on the user. These risks are; certain wrong data in a self-learning AI can lead to decisions taken by AI that may constitute crime; intentional actions taken by AI that can harm its user for example, AI personal assistant misusing the customer data; and AI which was created by hackers with the main aim of committing crimes.
2. Indirect risk: Unintended AI hazards that affect the user. These risks can be explained as AI system or software error, error made by AI during its operations, etc. These risks make system vulnerable and create a backdoor for the hackers to attack or gain access to the system.

IT experts classify threats that can be created by AI in three ways:

- Malware attacks.
- Attacks using social engineering techniques.
- Physical attack: defines attack on physical AI objects, like attack on drones.

Using AI for cyber security is a blessing but also a curse, although better has been done compared to misuse of AI. As easily as AI can provide strong security models, cyber criminals can use the same features of AI to launch threating attacks as well. Therefore, the above-mentioned challenges are the reason why AI is not completely used as a cyber security solution.

Conclusion

AI is an ever learning and ever developing as well as fast emerging technology. It has become a must have standard in the industry to defend cyberattacks. With the ever-growing data volume, it has become a difficult task for humans alone to factor and secure enterprise-level attack surface. Artificial intelligence comes to a much-needed rescue here by providing in-depth data analysis and threat identification, which will help security professionals to reduce security breaches in the organization and enhance the security of an organization. In cyber security ecosystem, AI has achieved successful discovery of attacks, prioritizing risks in a system, direct incident response plan, malware detection, prevention and analysis and identification and prevention of unknown attacks before they even occur.

Artificial intelligence is growing tremendously fast in every sector, especially in cyber security, as can be seen by various organizations launching a new intelligent tool to handle different types of cyber threats, both known and unknown. Despite of all the outstanding achievements made by AI in the field of security, one must still stay very cautious regarding the extensive dependency on AI when it comes to network security.

References

1. Morovat, K., Panda, B.: A Survey of Artificial Intelligence in Cybersecurity. Paper presented at the International Conference on Computational Science and Computational Intelligence 109–115 IEEE December (2020)
2. Das, R., Sandhane, R.: Artificial intelligence in cyber security. Int. J. Phys **1964**(4), 042072 (2021)
3. Stone, P., Brooks, R., Brynjolfsson, E., et al.: Artificial intelligence and life in 2030: the one hundred year study on artificial intelligence (2022). arXiv:2211.06318
4. Ghillani, D.: Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. Authorea Preprints (2022)
5. Anitha, A., Paul, G., Kumari, S.: A cyber defence using artificial intelligence. Int. J. Pharm. Technol. **8**(4), 25325–25357 (2016)
6. Azhar, I.: The interaction between artificial intelligence and identity & access management: An empirical study. Int. J. Creat. Res. Thoughts 2320–2882 (2015)
7. Lubin, A.: Cyber law and espionage law as communicating vessels. Paper presented at the In 2018 10th International Conference on Cyber Conflict 203–226 (2018)
8. Alhayani, B., Mohammed, H.J., Chaloob, I.Z. et al.: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Proc. Mater. Today (2021)

9. Raimundo, R., Rosário, A.: The impact of artificial intelligence on Data System Security: A literature review. Proc. Sens. **21**(21), 7029 (2021)
10. Thuraisingham, B.: The role of artificial intelligence and cyber security for social media. Paper presented at the IEEE International Parallel and Distributed Processing Symposium Workshops 1–3 May (2020)
11. Hao, M., Li, H., Luo, X., et al.: Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Trans. Ind. Inform. **16**(10), 6532–6542 (2019)
12. Bertino, E., Kantarcioglu, M., Akcora, et al.: AI for security and security for AI. In: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy 333–334 (2021)
13. Feng, X., Feng, Y., Dawam, E.S.: Artificial Intelligence Cyber Security Strategy. Paper presented in the In 2020 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress 328–333 IEEE (2020)
14. Sahu, A., Harshvardhan, G.M., Gourisaria, M.K.: A dual approach for credit card fraud detection using neural network and data mining techniques. Paper presented in the In 2020 IEEE 17th India Council International Conference 1–7 IEEE (2020)
15. Dilek, S., Çakır, H., Aydın, M.: Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review (2015). arXiv:1502.03552
16. Javapoint What is expert system? Javapoint Available via https://www.javatpoint.com/expert-systems-in-artificial-intelligence
17. Javapoint Machine Learning Available via https://www.javatpoint.com/machine-learning
18. Artem Oppermann What is Deep Learning and How does it work? Towards Data Science. Available via https://towardsdatascience.com/what-is-deep-learning-and-how-does-it-work-2ce44bb692ac. Accessed 13 November 2019
19. Javapoint Supervised Machine Learning Available via https://www.javatpoint.com/supervised-machine-learning
20. Veiga, A.P.: Applications of artificial intelligence to network security (2018). arXiv preprint arXiv:1803.09992
21. Javapoint Unsupervised Machine Learning Available via https://www.javatpoint.com/unsupervised-machine-learning
22. Javapoint Reinforcement Learning Available via https://www.javatpoint.com/reinforcement-learning
23. Chan, L., Morgan, I., Simon, H., Alshabanat, et al.: Survey of AI in cybersecurity for information technology management. Paper presented in the In 2019 IEEE technology & engineering management conference 1–8 (2019)
24. USM (2020) AI & ML in Cybersecurity: Top 5 Use Cases & Examples. USM system. https://usmsystems.com/ai-ml-in-cybersecurity-use-cases-examples/. Accessed 05 June 2020
25. Gaurav Belani The Use of Artificial Intelligence in Cybersecurity: A Review. IEEE Computer Socitey. https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity
26. Vähäkainu, P., Lehto, M.: Artificial intelligence in the cyber security environment. In: Proceedings of the ICCWS 2019 14th International Conference on Cyber WarfarSe and Security: ICCWS, Stellenbosch, South Africa 431 (2019)
27. Khisamova, Z.I., Begishev, I.R., Sidorenko, E.L.: Artificial intelligence and problems of ensuring cyber security. Int. J. Cyber Criminol. **13**(2), 564–577 (2019)
28. Atiku, S.B., Aaron, A.U., Job, G.K., et al.: Survey On the applications of artificial intelligence in cyber security. Int. J. Sci. Technol. Res. **9**(10), 165–170 (2020)