The Role of Artificial Intelligence in Cyber Security

Chapter · January 2019

DOI: 10.4018/978-1-5225-8241-0.ch009

3 authors, including:

Kirti Raj Bhatele
Rajiv Gandhi Proudyogiki Vishwavidyalaya
16 PUBLICATIONS **25** CITATIONS
SEE PROFILE

Harsh Shrivastava
National University of Singapore
7 PUBLICATIONS **19** CITATIONS
SEE PROFILE

Chapter 9
The Role of Artificial Intelligence in Cyber Security

Kirti Raj Bhatele
RJIT, India

Harsh Shrivastava
RJIT, India

Neha Kumari
RJIT, India

ABSTRACT

Cyber security has become a major concern in the digital era. Data breaches, ID theft, cracking the captcha, and other such stories abound, affecting millions of individuals as well as organizations. The challenges have always been endless in inventing right controls and procedures and implementing them with acute perfection for tackling with cyber attacks and crimes. The ever-increasing risk of cyber attacks and crimes grew exponentially with recent advancements in artificial intelligence. It has been applied in almost every field of sciences and engineering. From healthcare to robotics, AI has created a revolution. This ball of fire couldn't be kept away from cyber criminals, and thus, the "usual" cyber attacks have now become "intelligent" cyber attacks. In this chapter, the authors discuss specific techniques in artificial intelligence that are promising. They cover the applications of those techniques in cyber security. They end the discussion talking about the future scope of artificial intelligence and cyber security.

DOI: 10.4018/978-1-5225-8241-0.ch009

INTRODUCTION

Is artificial intelligence less than our intelligence. (Jonze, S., 2017)

"Intelligence" is only the property that distinguishes human from anything else on this planet. The idea of having that Intelligence in man-made machines is quite fascinating although the machines can't have that inherited intelligence. Instead of natural human intelligence, the scientific, philosophical and other communities working for understanding human mind started pondering over this "Why can't machines think?" As a result of multidisciplinary efforts in areas of cognitive science, neuroscience and computer science, this idea of creating "Artificial Intelligence" began to attract the attention of researchers around the world. Around the 1960s and 70s, researchers started expecting very high from AI Research, but it was pretty much in vain without any breakthroughs.

We can define Artificial Intelligence as the scientific field that tries to understand and model human intelligence. Many Researchers have their own understanding of AI such as quoting Peter Norvig and Stuart Russel's Artificial Intelligence: A Modern Perspective "Artificial Intelligence is the study of agents that exist in the environment and perceive and act".

There has been an effort for decades to create such systems that can understand, think, learn, and behave like humans. We'll discuss some of the important approaches for AI that has pushed AI research further (Russell, S., J., & Norvig, P., 2000).

Historical Attempts

Warren McCulloch and Walter Pitts in 1943, for the first time, attempted to create an intelligent system. They proposed a model of the Artificial networked neural structure and claimed that if this structure would be defined properly, then it could learn like the human brain.

Recently after some year, Alan Turing published "Computer Machinery and Intelligence "in which he explored the idea of "Artificial Intelligence". In his work, he also proposed "Turing test" as a test to measure the machine's ability to exhibit intelligence. The setup for the test requires a natural language generating a machine, an evaluator (which is human) and a human. The evaluator will converse (interact) with the machine and the human and try to identify the machine based on the conversation. Both the machine and human will try to persuade evaluator that he or she is interacting with a human on the other side. If the evaluator fails to distinguish machine conversation from the human conversation, then the machine will be considered intelligent.

John McCarthy coined the term "Artificial Intelligence" in 1956. Two years later, he invented LISP, a high-level AI programming language for use in AI programs. In the next section we'll discuss one of the most widely adopted AI approaches historically, then we'll discuss the current and the best date approach to AI (Pattern Recognition).

Knowledge or Rule-Based Approach

In Knowledge-based AI systems, we try to embed the knowledge of human experts for their decision-making. Here the idea is to equip the system with the knowledge required for a task, for example - medical diagnosis, and the rules to infer insights from the knowledge to take a decision. This way all the decisions that KBAI system takes will be affected solely by the knowledge base created by the human expert in the concerned field. Therefore, KBAI systems are also known as Expert Systems. So, the general architecture of KBAI system consists of a Knowledgebase and an inference engine. Inference engine generally has IF-ElSE rules for inference from the knowledge base. The first knowledge-based system was MYCIN. It was written for medical diagnosis. The central Idea of knowledge-based systems was to represent knowledge explicitly through IF-ElSE rules (Russell, S., J., & Norvig, P., 2000).

Representation of Knowledge is the core task for developing an AI system. The rule-based knowledge representation is heavily used for the development of IBM Watson.

Pattern Recognition Approach

Pattern recognition is another approach to Artificial Intelligence. It is based on data unlike knowledge base in rule-based approach. It tries to learn the knowledge from data itself. We just need data for and machine learning algorithm (section 2) to discover the patterns from the data. These patterns will derive the decisions of the system in an unknown environment. Here is the modern definition of pattern recognition (Bishop): The field of pattern recognition is concerned with the automatic discovery of regularities in data through the use of computer algorithms and with the use of these regularities to take actions such as classifying the data into different categories. Pattern recognition has been the best approach to Artificial Intelligence. Machine Learning is the best approach to pattern recognition. In the next section we are going to dive in it (Russell, S., J., & Norvig, P., 2000).

MACHINE LEARNING

Machine intelligence is the last invention that humanity will ever need to make (Bostrom, N., 2015)

In 1959, Arthur Samuel coined the name "Machine Learning". According to him, "Machine learning is the field of study that gives the computer the ability to learn without being explicitly programmed". This captures the core idea. Unlike earlier approaches where we were trying to define a bulk of rules to derive insight from knowledge, machine learning develops such systems which learn those rules themselves from the data. This approach is closer to natural learning. For an example, a kid learns to identify an apple after he/she is shown a lot of examples of apples. Similarly, we give the machine a lot of data and the machine by itself develop an intuition for the data. In the words of Tom Mitchell, "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T, as measured by P, improves with experience E." Those algorithms that allow machines to learn are called the Machine learning algorithm. Generally, machine learning algorithms can be classified into two categories - Supervised Learning and unsupervised learning (Russell, S., J., & Norvig, P., 2000). There are also some other kinds of machine learning like Reinforcement learning etc. Those are beyond the scope of this chapter.

Supervised Machine Learning

In supervised learning, the data is labeled. Let's say, we want the system to learn to distinguish cats' images from other images. We will write a program which should take input as an image and should output whether or not it's a cat (i.e. 1 for cat and 0 for non-cat). To accomplish this task, we first need to train the machine. What this means is we'll first show the machine that this is cat image, this is noncat image and so on for a large number of images. Then we'll evaluate its performance on the images It has never seen. If the performance is not up to our expectation then, we'll train it on more data. The data used for training is known as "training set" and the data used for testing the trained system or "Model" is known as "Testing set". The examples of images in data are known as "Sample". For each sample, we have a corresponding true label in the supervised learning setup. The problem we discussed is called "Classification", the classes being only two i.e. Cat and Non-cat. When there are two classes, its known as "Binary Classification" and if there are more than two classes, its known as "Multi-class classification problem".

Unlike Classification problem, in regression we want our system to predict "continuous values". For example, predicting House prices in a locality. What data we need to collect in this setup? We'll try to collect data on the parameters that affect

the house prices such as House size, no of rooms in a house etc. The parameters are known as "Features" in machine learning terminology. Here also, we'll have actual prices of the samples in the training set but not in the test set (obviously it's the data we test our system on). Another regression example could be predicting stock market prices. Another classification example could predict whether the person has cancer or not. You got the idea (Russell, S., J., & Norvig, P., 2000).

Unsupervised Learning

In Unsupervised learning, we don't provide the sample's true label or value. The data is unlabeled. The purpose of the unsupervised learning algorithm is to find the structure in the input data. Its goal is to discover hidden patterns from the data. It tries to cluster the data into characteristically separate groups (Russell, S., J., & Norvig, P., 2000). This task is known as Clustering. Let's try to understand how this is useful. A book selling company wants to improve its sales. It has a huge amount of data about the purchase history of its customers. The company feeds that data to a "Cluster" learning algorithm which outputs 5 segments of customers to the company and the company finds out that some 1st segment likes romantic genre book, 2nd like x genre book and so on. With this insight, the company can personalize its offering according to the market segments. Clustering techniques have used in Astrophysics, Computer science, etc.

General Machine Learning Pipeline

We are going to give a brief overview of the general steps that we go throw when building machine learning based solutions to the problems.

"Understanding the problem" statement is first and the most important step in an ML project. This may seem a trivial but actual problem and how you are going to model it in a way that it could become a machine learning task gets sometimes difficult for some problems. Also, a deep understanding of the problem will help somewhat for sure while taking a decision in designing ml pipeline.

Next step is to "collect enough data" for your problem. If the task is to classify emails into spam and non-spam, then collect lots of emails with their true labels. Collected data should be similar to data that your trained system will see when deployed (Russell, S., J., & Norvig, P., 2000).

As now a good number of samples are collected so it's time to prepare it for machine learning. Yes, raw data can't be directly fed to learning algorithms. Raw data can be too much noisy, biased, incorrect, missing etc. And so, we need to transform it so that it becomes useful for learning. This step is called "Data Preparation". Things like error correction, filling, normalization and more all happen in this step. Then

we randomize the data and split it into training and testing set. Well, assume that the data is prepared, let's move forward.

Next step is to "select the learning model". There are so many machine learning models developed for a particular problem. In this step, we select some models based on the data. In this step, we explore the data and get some intuition about its structure. Then we chose a set of models to try on the data. For example, for classification, there many models like support vector machines, logistic regression etc.

It's time for "training" the model. We have enough data and a learning model. We'll train each learning model we selected for training on the training set. In training, the model tries to learn the best "weights" for each feature for predicting the label with the highest accuracy. Here a weight represents the importance of the feature in predicting the label.

After the model has come up with the best weights, we'll "evaluate" its performance on the unseen data. We'll run the trained models on testing set and note down the accuracy of prediction of each model. Only the best model with the highest accuracy will be selected.

In the next step, we'll tune the best model to increase its performance. There are some parameters in a model for example learning rate (how smooth the model learns) and some others. In this step, the goal is to discover the best combination of different parameters of the model. Those best parameters will then be used for prediction in the real world.

Now we'll deploy the model in the real world. The system will be maintained to keep up the accuracy same as it had at the beginning (Russell, S., J., & Norvig, P., 2000).

CYBER SECURITY

One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks. Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats. Think data, but also business services integrity, awareness, customer experience, compliance, and reputation (Nappo, S., 2017).

Consider a set i.e., (Artificial Intelligence, Machine Learning, Block Chain, Deep Learning, Big Data Analysis, Data Science, Internet of Things etc.). This set consists some of the most thrilling and talked off technologies today. In this era of exponentially increasing expansion of the Internet and heavy workloads in the fields enclosed in the above set, cyber-security becomes a big question?

Cyber term means 'related to the culture of the computer, information technology or/and virtual reality'. This makes clear that we are talking about the security of computers, networks, information etc. Moving on to the clearer definition, cybersecurity refers to the various measures/techniques for the protection of inter-connected networks, software, hardware and data from cyber-attacks (unauthorized access and damage). While looking at the computing context both securities of cyberspace and physical space is equally important. Application security, information security, network security, operational security, etc. are some of the elements of cybersecurity, which harmonize the entire information system. This design is giving an intuition of a multilayer protection system spread all over the system involving various elements of the system and it is one of the successful defense mechanisms available.

Role of Cybersecurity

Nowadays the crowd is more frequently falling prey to cyber-attacks due to the evolutionary nature of risks in the cyberspace. Pathways are constructed through malignant and offensive activities, which give unauthorized access to predators (hackers and crackers) on computer systems or networks. These activities are called cyber threats. Predators work on the bugs and faults in the system or network to establish these pathways. There are numerous cyber threats like ransomware, virus, worms, Trojans, spyware/adware, attack vectors, social engineering, Man in The Middle (MITM) and many more (Panimalar, A., Giri, P.U. & Khan, S., 2018).

Everybody possess some valuable assets and confidential data which are under their authority and when an outsider gets access to those assets and data, they can cause extreme harms. Taking cyberspace into consideration, these accesses without the consent of the owner can be the results of one or more cyber threats. Here cybersecurity comes into play. It ensures the availability, confidentiality, and integrity of your system or network and helps it to work efficiently without compromising with the security.

Principles of Cyber Security (Principles Forming the Base for Cybersecurity)

To ensure the three important goals of cybersecurity, i.e., availability, confidentiality and integrity, some simple but effective principles can be followed.

1. **Focus on Prior Systems:** Stabilizing the degree of availability, confidentiality, and integrity of resources comes under biggest challenges and hence it is

achieved by focusing on the vital systems and providing best protection shield to it whereas other methods are applied for the protection of less-prior systems.

2. **Different Users, Different Level of Accessibility:** What data is accessible by whom should be based on what type of user he is, and no single person should get access to all the data and information. This means minimum privileges to particular responsibility. Hence the change in responsibility is directly proportional to change in privileges.
3. **Provision of Independent Defense (Protocols):** Several authentication protocols for a single job is a far better idea than a single protocol. It highly reduces the risk of successful cyber-attacks and the basic principle is increasing the work of the attacker as he has to perform numerous tasks to break through several protection layers.
4. **Backups:** Failures can occur but planning the consequences after failure can reduce extreme harms to the system, network or individual. This is a highly effective technique and is in practices in various fields.

Keeping records of all breaches: Cybersecurity staffs should keep the records of all the breaches and these should constantly be studies and protection measures should be generated. This process should be a rapid one because hackers are not waiting; they are increasing their skills as well as improving cyber-attack tools (Panimalar, A., Giri, P.U. & Khan, S., 2018).

A Modern Warfare (Warfare in Cyberspace)

The world has experienced wars in the past which has never been a pleasant experience. These inhuman activities never proved to be fruitful for any of the parties, but still, these activities continue and are now taking the benefits of the modern technologies. These days warfare grooms itself in the cyberspace and the term used to describe it is cyber warfare but there is no fixed definition for cyberwarfare; Richard A. Clarke defines it as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".

Threats leading to Cyberwarfare:

1. **Espionage:** The act of spying on bodies for political or military reasons.
2. **Sabotage:** Deliberate disruption of things especially due to political reasons.
3. **Propaganda:** Cyber propaganda refers to the biasing of information in directions which highly influence public interests.

All these things are nowadays performed in the cyber world giving rise to cybercrimes which gradually grows and leads to cyber-terrorism. Dealing with cyber

terrorism is a tough task and can be achieved by either a reduction in cybercrime or introducing highly secured systems. Modern technologies from the above set can be used to design intelligent systems which can secure it.

Modern Challenges in Cybersecurity

Cyber Security is a shared responsibility, and it boils down to this: In Cyber Security the more systems we secure, the more secure we all are (Johnson, J., 2014).

After having the basic idea about how intensely cyber world is impacting every single entity starting from individual level, organizational level to national-international levels, let us dive into the complications fabricated by the technologies mentioned in the set from the previous section, i.e., {Artificial Intelligence, Machine Learning, Block Chain, Deep Learning, Big Data Analysis, Data Science, Internet of Things, etc.}. Are these technologies causing threat to cyber security? If yes, why?

Heavy technical works in the set field are going on to create products and services for mankind; In this long run of economic benefits and work convenience, the two basic necessities, privacy and protection are compromised. All these crafts and developments are leading to highly growing dependence on Internet, complex digital systems and clouds-based computation which are recently bombing technologies and consist of many loop holes that has not only increased the number of cyber-attacks but also the diversity in them.

The reason threats couldn't be countered is the lack of trusted and standard computing platforms and infrastructures. Challenges can be of different forms; their sources can be diverse, and they could be at different levels. Let's us visualize them from few different perspectives.

1. **Technologies:** Technologies is spreading everywhere every single day and predators (cyber criminals) are constantly spying in search of loopholes. The constantly increasing rate of cyber-crimes is generating 3.5 million new jobs in the field of cyber security, which will remain unoccupied. Elevations in new technologies in half a decade have increased the security requirements about three hundred and fifty (350) times, an enormous rise.
2. **User:** Technologies are not only the challenges to cyber security, but user at large scales are also one. The habit of users of doing things without thinking and sometimes unawareness of threats associated with the facilities they use are some common reasons behind the same. We could also not ignore the involvement of some user in malicious activities and irresponsible behavior of few people at higher authorities. Many a times, it is just one click of user, which makes all the disasters.

3. **Financial Expenditure:** While considering the scenario of cyber security, enhancement in the technologies, products and services are just one face of it and many a times we could not see the other one, the expenditure in these enhancements. People and organizations only expend on cyber security when they become victim of cyber-attacks. Investment in cyber security considering future threats is an obsolete practice giving invitations to predators (cyber criminals).

Evolving Computer Networks (Challenges by Complex Computer Networks)

Evolution of computer networks is increasing their complexity and these complexities are challenging cyber security. There are users and organizations those who don't have records of the assets they have directly or indirectly tied to the network and due to lack of information of assets it's hard to ensure security in these complex networks. Security in depth (multilayer protection) is a tedious task in complex computer networks.

Internet of Things (IoT Arising Challenges for Cyber Security)

Starting form homes, markets, institutions to big offices, all of these places are filled with variety of electronic gadgets and Internet of Things keeps all of these gadgets connected. Working of these connections in gadgets is primarily dependent on user's private/confidential data and these connections generate huge amounts of data and process it using internet. The main challenge is the poor mechanism for authentication and improper encryption of these large chunks of data. Analysis of efficiency versus security aspects of IoT implies the inverse dependence of security on efficiency. 70% of the IoT devices are vulnerable to cyber-attacks.

Block Chain (Block Chain Technology and Challenges Associated)

The astonishing development in crypto currency like bit coin and Ethereum has revolutionized the payment systems. It offers irreversible, quick and cheap transactions and good exchange values. Medical record management, decentralized access control and identity managements are some of the future goals associated with block chain technology. And here comes the security aspect, cyber security experts have to raise the level of principles as well as the techniques for ensuring security from cyber-attacks.

Botnets (Modern Threat)

Large collection of devices (IoT devices, servers, personal computers, mobile phones connected to internet) infected by same malware is called Botnet. Cyber predators monitor these infected devices and attacks on these systems are mostly through emails or frauds based on clicks. Botnet word is derived from robot and network. Here it means that devices in the infected network become robot/slave of the attackers.

Lack of Talents (Demand Versus Availability of Cyber Security Experts)

Many studies have revealed that due to lack of talents there is a misbalance in the demand and availability of cyber security experts. With the exponential growth of cyber threats, demand for skilled and experienced cyber security experts has also exponentially increased but their availability is a big question.

According to a survey by Leviathan Security Group it has been found that:

1. 16% of the organizations felt only half of their applicants are qualified
2. 53% of them said finding a qualified applicant can take at least six months, in case they find one.
3. 32% of them find it difficult to fill the positions of cyber experts.
4. Reasons behind this lack of cyber experts can be the under-investments on cyber education, growth in cyber-attacks, demand of experienced experts and less participation of women in cyber security field.

AI COMES TO RESCUE

With the increasingly important role of intelligent machines in all phases of our lives--military, medical, economic and financial, political--it is odd to keep reading articles with titles such as whatever Happened to Artificial Intelligence? This is a phenomenon that Turing had predicted: that machine intelligence would become so pervasive, so comfortable, and so well integrated into our information-based economy that people would fail even to notice it (Kurzweil, R., 2005).

Cyber-attacks have become more pervasive and diverse due to ubiquitous connected computers, cloud and mobile technologies. Volumes of connected devices provide cyber criminals with plenty of access points to attack on. In addition, the access points are security deficient. Rise of IOT has caused a wave of cyber-attacks that has expanded wider than ever. Topics on cyber frauds are not rare in news and media.

Traditional methods for cyber security require tremendous human efforts to identify the threats, extract properties of threats and encode properties of threats into software to detect the threats. Moreover, conventional methods are not as sophisticated as present days cyber-attacks.

In earlier days, AI and cyber security were not related in any way. But over time, the boundaries became blurred. The CAPTCHA ((Completely Automated Public Turing test to tell Computers and Humans Apart) is a very good example of the connection of AI and cyber-security. In this test, user is asked to type the letter in a masked image or with some other deformation. Traditional cyber-security techniques are primarily called as "Signature based techniques". Our focus is to discuss Machine learning based techniques but after a brief overview of signature-based techniques.

Signature Based Techniques

Signature based techniques are those approaches of information security which detects the cyber-attacks or malwares [section 7] by matching certain signature (at least a byte sequence of code) of the instance of malware in question with the database of signatures of malwares stored. The database has known malicious programs and they are called as "blacklists". The signature-based techniques assume that the malicious software can be described using the signatures (also called as malicious patterns). This method fails completely in case of new attacks or malwares, for which known patterns or signatures are not available. Unfortunately, the current scenario is against these techniques of signature detection. Still it can be used on the beginning level. Nonetheless signature-based techniques have once been one of the most common malware detection techniques. This technique has the following disadvantages:

1. **Susceptible to Evasion:** The signature patterns are commonly known since they are used for deriving signatures for malware or attacks. They can be easily duped by the hackers by techniques like inserting no-ops and code reordering (obfuscation).
2. **Zero Day Attacks:** Since the signature-based malware detection systems are built on the basis of known malware, they are not able to detect new and unknown malware, or even the variants of known malware. Thus, without accurate signatures, they cannot effectively identify polymorphic malware. Therefore, signature-based detection does not provide zero-day protection. Moreover, since a signature-based detector uses a separate signature for each malware variant, the database of signatures grows at an exponential rate (Shabtai, A., Menahem, E., & Elovici, Y., 2011).

Machine Learning Based Approach

Signature based approaches have a number of drawbacks. Recently due to availability of high compute power and enormous data, machine learning has been on rise. It has entered into almost every business and industry. There is hardly any area of work machine learning has not been used where human intelligence required. Cyber world is no exception. In almost all the conferences being organized on cyber security, you will find researchers, industrialists, businessmen, security experts, analysts and everyone speaking about the applications of machine learning in cyber security. Some might argue that AI will replace the human analysts. The truth is we are not at that stage yet. AI is for sure and asset for human analysts. Combined efforts of human and machine will surely help us fight with cyber-criminals with more excellence that separates efforts.

Data is enormous whether its firewall logs, user activities logs or network packets, it's difficult for human analysts to analyze it properly. This is where machine intelligence comes into picture. Armed with rapid and trustworthy analysis provided by machine learning can be used to take informed decisions by the organizations.

In general, we are trying to detect anomalies in cyber security. Both supervised and unsupervised machine learning techniques are used in this direction. It should be noted that the former approaches are more promising. For the purpose of understanding application of supervised learning, we can consider the problem of malware identification or classification of malicious files - where we want to detect malware or malicious files. We need to have an enormous amount of data for training. The data should have malware - label pairs. The data is then broken into training and testing data. This problem falls into category of classification in machine learning. Consider another problem of network traffic log, we'll cluster them into two groups "Normal logs" and "infected logs". Clustering will eventually output two clusters. We'll discuss these techniques in detail in coming sections. Machine learning based techniques extract the most important feature for the problem on their own and surprisingly for human it's very hard to extract such features. This is why machine learning based techniques are superior to other methods.

Network Intrusion Detection Using AI

Act of getting access to computer networks without the consent of the owner is known as Network Intrusion. Intrusion can be of two types, physical or logical. Physical intrusion involves the physical presence of intruder trying to access your computer system whereas in logical intrusion the intruder's gains access to the computer system via network. Network Intrusion is a deliberate act, which is

performed to utilize network resources or/and threatening the network or/and data (Chatzigiannakis, V et.al, 2004).

Network intrusion can be divided into five different stages:

1. **Gathering Information of the Target:** In this stage intruders collect information about each and every aspect of the target. They try to comprehend their target and its strong and weak points. This information includes email addresses, open-source details, details of the network, etc. To smoothly contrive attack, they even try to knowledge about the all functionalities of the various devices in the network and spent time in finding the vulnerable points for exploitation.
2. **Inceptive Exploitation:** In this stage begins the intrusion activities. Exploitation of networks is done by infecting the frequently used websites by the victim. Water holing, phishing, SQL injection are some more ways to threaten the network and gain more control over it. Intruders patiently perform exploitations to avoid chances of getting caught.
3. **Establish Persistence:** Intruders continues their malicious activities without getting in ears of the victim. There is a rapid increase in undetected exploitation activities which include peeping into the scripts and discovering run keys.
4. **Malware Installation:** This is the stage of doing the original work by installation of malwares in the network starting with less harmful ones to the powerful ones.
5. **Penetrating Deep Into Network:** Gradually intruders gain access all over the network and now they can exploit whatever they want. They fulfill their intension and leave the network.
6. **Removal of Traces:** Some intruders who are concerned about detection of intrusion ties to remove their traces before leaving the network (Iftikhar, B., Alghamdi, A., S. 2009).

This is how the whole process of network intrusion takes place. What are the different attacks used in network intrusion?

1. **Trojans:** Trojans do not replicate itself rather it appears to useful. It follows the path of Denial of Service (DoS) attack. It erases stored data and constructs pathways for the attackers. Source of Trojans are online file repositories and archives.
2. **Worms:** Unlike Trojans worms replicate itself but without altering the user approved program files. Its abrupt replication ultimately consumes all the network resources (such as bandwidth, CPU cycles) leading to the unavailability of resources for the user approved programs/tasks. Some worms also try to

extract confidential information from important files. Sources of worms can be Internet Relay Chat protocol or attachments send via emails.

3. **Buffer Overflow Attack:** Attacks where some special parts of the network memory is targeted and over-writing in done on it; these overwritten set of code are many a times part of the attack and are executed during the attack. Networks with large buffer size and no checking codes are more prone to this attack (Iftikhar, B., Alghamdi, A., S., 2009).
4. **Traffic Flooding:** It is also a type of Denial of Service attack and its targets are web servers. Attacks know how to control and manage Transmission Control Protocol (TCP) connections and it order to orchestrate attack a lot of TCPs are generated aiming to stop the server and hamper its performance.
5. **Asymmetric Routing:** In asymmetric routing, the packets travel through one route from source to destination and different one from destination to source. Here the attackers plan to packets to bypass some critical sections of the network as well as the intrusion detectors.
6. **Protocol Specific Attack:** Network activities involve some protocols (examples: ARP, IP, TCP, UDP, ICMP, etc.) and some of them unknowingly leaves loop holes for network intrusion. Example, In Address Resolution Protocol (ARP) there is not message authentication process inviting Man in the Middle attack.

Network Intrusion detection systems monitors the network and analyze its traffic to protect system from network-based threats. Generally, A NIDS reads incoming and outgoing packets from access points in a network and tries to recognize the patterns of the threats in disguise of normal packets. When a network threat is discovered it sends notifications to the administrator about the security of the network.

An example of a NIDS would be installing it on the subnet where firewalls are located in order to catch someone who is trying to break into the firewall.

Machine Learning Based Network Intrusion Schemes

There are several methods proposed for Network intrusion detection. Machine Learning based methods have got an edge over all traditional methods for the reason that they are robust, very functional and improved.

Network intrusion detection system tries to find the anomalous activity in the network. The core task is to classify various network data packets or activities into - Normal and abnormal or anomalous. This can be clearly adapted to a classification task in supervised machine learning. Particularly, it's a binary classification task, classes being - Normal and Anomalous. To model it into a machine learning problem, we need to have a dataset of network activities samples. People have already gathered

such datasets such as datasets provided by Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) and other similar organizations. In this dataset, a hybrid of real modern normal activities and attack behaviors were generated. This dataset contains total forty-seven features and also contains over 2 million sample data. Not all the features are important for the task, so feature selection is performed where we select only the features correlated with Target variable (i.e. Label variable). Now that we have prepared data, we'll apply three approaches to this task: Logistic regression, Support vector machine and Decision Trees.

Logistic Regression

Logistic regression is known to be the simplest machine learning technique for classification. Logistic regression tries to come up with a straight line to separate the anomalous activities and normal activities, this is why it can be thought of as learning an equation of line: $y' = mx + c$. Here y' is the predicted output for the sample x, m is the slope of the line and c is the y-intercept. This is also called as score function. It maps input features to output labels. The values of y' can be very large and very small, we won't be able to decide which class does the sample xi belongs to and so for that purpose we'll pass the score to the sigmoid function y' = sigmoid(y'). Sigmoid (y') is equal to 1/1+e^-y'. This function takes the value and scales it in between 0 and 1. Thus if the sigmoid outputs above 0.5, the class is positive (or Normal) and if its below 0.5, the class is negative (anomalous). So, our final equation for logistic regression is: y' = sigmoid (mx + c). Due to sigmoid function used, Logistic regression is also known as sigmoid regression. Now to measure, how good and bad the predication of the learning algorithms is, we'll define cost function as:

$$\text{Cost}(y', y) = -\log(y') \text{ if } y = 1 \quad (1)$$

$$-\log(1-y') \text{ if } y = 0, \text{ here y is the true label.} \quad (2)$$

The cost represents how large the error. The goal is to minimize the cost. We can see that the we have to find the best possible values of m and c that will minimize the cost. To minimize the cost, we'll use optimization algorithms. Gradient descent is generally used and so we'll use it in our problem.

Repeat until convergence

{

$$m = m - \alpha \partial \partial m \text{ Cost } (m) \tag{3}$$

}

At running this algorithm for a hundred of times, we'll see that optimized value of m is found. This m is then used for future prediction.

Support Vector Machines

Here is another classical linear classifier which more robust and power than Logistic regression. We'll try to give a brief overview of this technique. The score function in svm is similar to logistic regression. The cost function is a bit different and more complex, so we will avoid writing here. Basically, it tries to learn as straight-line boundary which is a farthest as possible from the sample points. The margin (distance from the sample) it learns is large and thus it is also known as Large margin classifier. We can use other optimization techniques along with Gradient descent such as Minibatch gradient descent or stochastic gradient descent for SVM. The SVM allows flexibility in learning non-linear decision boundaries by incorporating a nonlinear function as score function, polynomial being the most common choice. After a good number of iterations of optimization, we can find the best parameters with the least error possible by this learning algorithm. Now we'll give a slight look out third technique "Decision Trees".

Decision Trees

As the name suggests, Decision Tree uses a tree-like model of decisions. Although it's a commonly used tool in data mining for deriving a strategy to reach a particular goal, it is widely used in machine learning, which will be the main focus of this section. A decision tree is drawn upside down with its root at its top. Every internal node in a tree is a binary condition. It splits into two branches that meet another node. The branches are yes-no branches. The last nodes that don't split into branches are known as decision nodes. Decision nodes determines which class does the sample belong. There are many advantages of decision tree-based learning like:

1. Easy to understand, interpret and visualize
2. It learns linear as well as non-linear relationships
3. It implicitly performs feature selection and extraction.

Now that we have applied all these three Learning algorithms, we will keep the model which has provided us the best accuracy. We'll then search for improved parameters for that model so that we can get more accurate results. This is called grid search. Now we'll use learned parameters on the unseen data for prediction.

Malware Detection Using AI

Malware is comprised of words 'malicious' and 'software'. Simply malware can be considered a piece of code designed to cause harm to the computers, data/ information and networks. The harms associated with malware can take place only after the installation or implantation of these malicious codes. Objectives behind these malwares are spying and stealing of confidential data, providing system control to intruders and poor performance or mal functioning of the infected systems. Following are some malwares:

1. **Virus:** Its full form is Vital Information Resources Under Seize. This malware replicates itself and this process is done via placing its codes into programs and modifying them. Its activation depends on opening of program by the user. Spreading through the user email, corrupting data, data loss, erasing data from hard-disk are some of the damages caused by virus.
2. **Worms:** Refer the previous section.
3. **Trojans:** Refer the previous section.
4. **Rootkits:** Attackers can gain continuous access to root-level using rootkit without recording its presence. It is the result of direct attack such as exploitation of known vulnerability or password. It conceals itself in the Operating System.
5. **Remote administration tools:** These pieces of software allow attackers to control infected system and give the privileges to perform all the possible tasks on the system. Their detection is difficult as they don't appear on the running programs list and many a times expected to be a benign as they were originated for legitimate use.
6. **Botnets:** Refer section 4.
7. **Spyware:** Malwares that tries to collect data about the usage of the infected device keeps records of key strokes and all activities taking place in the system. Adware, data theft, botnets, key loggers and net-worms are all part of this malware (Panimalar, A., Giri, P.U. & Khan, S., 2018).

Effects of malware on computers system:

1. It can cause slowing down of connections and computer tasks; some can even crash your system.
2. Frequent display of error messages and problem in shutting down or restarting.
3. Hijacking of browsers for redirection to malicious sites.
4. Theft of identity and confidential data.
5. Misuse of email for exchange of spam.
6. Creating path for intruders to have control over the system and resources.

Malware Detection

Malware detection system is used to determine whether a program is malicious or not. Malware comes in several forms as discussed earlier. Earlier detection systems for particular malware like for virus, antivirus systems were developed. Recently the focus has shifted towards general malware detection systems. Though it's harder but it would be universal tools to fight with these threats. Malware detector is used as a tool of defense against the malware. The quality of particular detector depends on the technique employed in its development.

Generally, malware detection techniques fall into three categories:

1. Signature based techniques,
2. Behavior based techniques and
3. Specification based techniques.

We have already discussed Signature based techniques. The Behavior based detection techniques analyze behavior of particular program which is suspicious of containing threats for the system. The specification-based techniques are modifications associated with behavior-based techniques. Suppose a behavior-based technique has a high false alarm rate, then some specification is made in the detection scheme (Yu, W., Zhang, N., Fu, X., &Zhao, W., 2010).

Malware Detection Using Machine Learning

Malware detection is also the task of classification. All the methods discussed earlier (Logistic Regression, Support Vector Machines and Decision Trees) are equally applicable in this case. In this section we'll just give you a brief introduction to another technique for classification which land us into the era of deep learning. In Machine Learning, A human analysts creates features that he thinks will be very

useful for prediction, but in deep learning the model itself extracts the important features from the data. The model here is "Artificial Neural Networks". The idea of ANN is inspired form the biological neuron. Although we don't exactly know how actually our mind works, but Researcher came up with an innovative model of learning inspired from human brain. This mathematical model is now a days a buzz word and it's the best algorithm for supervised machine learning given its data requirement is fulfilled. Yes, Deep learning approach requires millions of millions of data (Zolkipli, M., F., &Jantan, A., 2010).

ANN is built upon the bricks of linear classifier like logistic regression. The classical Neural Network can be imagined as layers stacked together. In each layer, many logistic units are present and the output from each unit of previous layer is connected as input in each unit of present layer. The first layer from the left is known as Feature layer and the last layer is known as output layer. The last layer has only one unit as we want to classify into two classes. The computation flows from left to right and the similar to other approaches; The cost function is calculated and optimized using an optimizer. Check references for digging deeper. Neural Networks are the most powerful machines learning approach we have ever discovered.

FUTURE ASPECTS AND SCOPE

Researchers predict that by 2020, artificial intelligence technologies will be implemented in almost all new software products and services, which will inevitably bring a sea change the way we work, live and do business. Though AI is in its infancy, it has shown to the world its infinite potential in performing task efficiently and accurately in an array of industries from manufacturing, retail, education to healthcare and cyber security.

As always, a coin has two faces. AI is no exception. People have shown their worries for destructive use of AI. A report from The Guardian warns "As AI capabilities become more powerful and widespread, we expect the growing use of AI systems to lead to the expansion of existing threats, the introduction of new threats and a change to the typical character of threats,". Fortunately, the discussion on AI still ends up with bright face of AI.

No doubt, if AI is implemented and trained with proper care, it can improve cyber security in many ways. It can protect against the cyber-attacks in real time with lesser resources. As cyber threats are constantly evolving, data is bursting new patterns that are hard to capture and analyze for human analyst can be crunched down by a machine learning technique in seconds. Equipped with power of deep analysis provided by Machine learning, Human analysts can focus on interpreting

the results and devising novel techniques for fighting with criminals proactively. Therefore, using Deep learning and machine learning in defense systems will surely take cyber security to a new level of intelligence.

REFERENCES

Bai, J., Wu, Y., Wang, G., Yang, S. X., & Qiu, W. (2006). *A very distinctive intrusion detection model based on multilayer self-organizing maps and principal part analysis. In Advances in Neural Networks*. Springer.

Barika, F., Hadjar, K., & El-Kadhi, N. (2009). Artificial neural network for mobile IDS resolution. Security and Management Journal, 271–277.

Bostrom, N. (2015), *TED Talk on Artificial Intelligence*. Retrieved from https://en.tiny.ted.com/talks/nick_bostrom_what_happens_when_our_computers_get_smarter_than_we_are

Chatzigiannakis, V., Androulidakis, G., & Maglaris, B. (2004). A Distributed Intrusion Detection Prototype Using Security Agents. In *Proceedings of Workshop of the HP Open View University Association*. University of Evry.

Iftikhar, B., & Alghamdi, A. S. (2009). Application of artificial neural network within the detection of dos attacks. *Proceedings of the ordinal international conference on Security of knowledge and networks*, 229–234.

Johnson, J. (2014). *Remarks by Secretary of Homeland Security Jeh Johnson at the White House Cybersecurity Framework Event*. Retrieved from https://www.dhs.gov/news/2014/02/12/remarks-secretary-homeland-security-jeh-johnson-white-house-cybersecurity-framework

Jonze, S. (2017). *28 Best Quotes About Artificial Intelligence*. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/07/25/28-best-quotes-about-artificial-intelligence

Kivimaa, J., Ojamaa, A., & Tyugu, E. (2008). Pareto-Optimal state of affairs Analysis for the selection of Security Measures. *Proceedings of Military communications conference, MILCOM 2008*.

Kivimaa, J., Ojamaa, A., & Tyugu, E. (2009). *Graded Security accomplished System. In Lecture Notes in engineering* (Vol. 5508, pp. 279–286). Springer.

Kurzweil, R. (2005). *The Singularity is near*. Penguin Group.

Lunt, T. F., & Jagannathan, R. (1988). An example amount of your time Intrusion-Detection accomplished System. Proceedings of IEEE conference on Security and Privacy.

Nappo, S. (2017). *Goodreads*. Retrieved from https://www.goodreads.com

Panimalar, A., Giri, P.U. & Khan, S. (2018). Artificial Intelligence Techniques in Cyber Security. *International Research Journal of Engineering and Technology, 5*(3).

Preda, M. D., Christodorescu, M., Jha, S., & Debray, S. (2008). A Semantics-Based Approach to Malware Detection. *ACM Transactions on Programming Languages and Systems*, *30*(5), 1–54. doi:10.1145/1387673.1387674

Russell, S. J., & Norvig, P. (2000). *Artificial Intelligence: A Modern Approach*. Prentice Hall.

Salvador, P., Nogueira, A., França, U., & Valadas, R. (2009). Framework for Zombie Detection Using Neural Networks. *Proceedings of The Fourth International Conference on Internet Monitoring and Protection ICIMP*. 10.1109/ICIMP.2009.10

Shabtai, A., Menahem, E., & Elovici, Y. (2011). F-Sign: Automatic, Function-Based Signature Generation for Malware. *IEEE Transactions on Systems, Man and Cybernetics. Part C, Applications and Reviews*, *41*(4), 494–508. doi:10.1109/TSMCC.2010.2068544

Tang, Y., & Chen, S. (2007). An Automated Signature-Based Approach against Polymorphic Internet Worms. *IEEE Transactions on Parallel and Distributed Systems*, *18*(7), 879–892. doi:10.1109/TPDS.2007.1050

Tang, Y., Xiao, B., & Lu, X. (2011). Signature Tree Generation for Polymorphic Worms. *IEEE Transactions on Computers*, *60*(4), 4. doi:10.1109/TC.2010.130

Yu, W., Zhang, N., Fu, X., & Zhao, W. (2010). Self-Disciplinary Worms and Countermeasures: Modeling and Analysis. *IEEE Transactions on Parallel and Distributed Systems*, *21*(10), 1501–1514. doi:10.1109/TPDS.2009.161

Zolkipli, M. F., & Jantan, A. (2010). Malware Behavior Analysis: Learning and Understanding Current Malware Threats. *Second International Conference on Network Applications, Protocols and Service IEEE*, 218-221. 10.1109/NETAPPS.2010.46

KEY TERMS AND DEFINITIONS

Artificial Intelligence: A machine's ability to make decisions and perform tasks that simulate human intelligence and behavior.

Block Chain: A block chain is a perfect place to store value, identities, agreements, property rights, credentials, etc. Once you put something like a Bit coin into it, it will stay there forever. It is decentralized, disinter mediated, cheap, and censorship-resistant.

Botnet: It is an infected computer terminal which can be used a platform to launch various attacks like DDoS attacks, Spamming, mining of bit coins, etc.

DDoS Attack: DDoS stands for distributed denial of service. In this type of an attack, an attacker tends to overwhelm the targeted network in order to make the services unavailable to the intended or legitimate user.

Deep Learning: The ability for machines to autonomously mimic human thought patterns through artificial neural networks composed of cascading layers of information.

Machine Learning: A facet of AI that focuses on algorithms, allowing machines to learn without being programmed and change when exposed to new data.

Malware: Malware stands for malicious software. Malware intended to infiltrate and damage or disable computers.

Supervised Learning: A type of machine learning in which output datasets train the machine to generate the desired algorithms, like a teacher supervising a student.