ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

AI in Cyber Security

[1] B.Arshia, [2] M.Gayathri, [3] P.Manaswini
[1][2][3] Department of Computer Science and Engineering.
G. Narayanamma Institute of Science and Technology (for Women)
Shaikpet, Hyderabad-500104.

"A computer would deserve to be called intelligent if it could deceive a human into believing it was human."

***Abstract* - Today cyber security is something which can't be handled by human security analysts alone. They need some degree of automation and this is where AI (Artificial Intelligence) comes into the picture. Today the world has coupled with the widespread absorption of cloud and mobile technologies having made an infinite platform to cyber security problem. AI-driven cyber security methods are able to learn and get better as they evolve by using the technique like AI2 (AI square), QRadar. By using these methods we show that the system learns to defend against unseen attacks and thus detection rates are reduced fivefold. This in turn helps to keep the systems, networks and sensitive data secure.**

1. EXPLORING AI

Introduction: The creative era has begun! It's time for us to put our thinking caps on and embrace new ideas and change. But who will take care of the routine tasks? A question that has brought our development to a standstill. AI has pushed the boundaries of science and technology in more ways than we could ever imagine. It's become the most trending topic of today's technological communities.

The official idea and definition of AI was first coined by John McCarthy in 1955 at the Dartmouth conference. The original definition or concept of AI goes like this "Every aspect of learning or any other feature of Intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves."

Artificial intelligence is easily one of the most prevalent themes in all of science fiction. The idea that a machine could exhibit the same level of Intelligence and sentience as human being has captivated writers and audiences alike for decades. For example, lets us take the two popular board games chess and go. The best human chess and go players in the world have been defeated by artificial intelligence.

How does a machine learn? Let's use an analogy. Think of a human infant. An infant doesn't really know or comprehend anything. Nevertheless the human brain must be doing something right? Well, for the most part the brain will be searching for patterns. Systematically attempting to identify recurring events in an effort to make sense of the world. Like colorful toys equals fun. Vegetables, not so fun. If mummy and daddy can speak maybe I can speak? A few years of this repetitive learning process and we grow from child to adult to old age. This is essentially what machine learning is all about. You create a simple mathematical model of the human brain and then you feed it with a bunch of information. This artificial neural network will then attempt to make sense of this information by learning from past mistakes and imitation. The result is this, natural evolution that no human could ever manually program. In essence, it could teach itself how to learn new things and in doing so could eliminate the need for a human at the controls.

2. CYBER CRIMES DEMANDING THE NEED FOR CYBER SECURITY

Today Cyber crimes cause huge problems for society personally financially and even in matters of national security. Just in a last few years hundreds of millions of credit card numbers have been stolen, tens of millions of social security numbers and health care records where compromised, even nuclear centrifuges have been hacked, and unmanned aerial drones have been hijacked. This is all done by exploiting vulnerabilities in hardware and software or more often by taking advantage of intentional decisions made by the people using the software. Today the largest countries not only have a Regular Army but also have a well armed Cyber Army. In fact the next World War may not be fought with traditional weapons but with computers used to shutdown National water supplies, energy grids and transportation systems. A virus is an executable program that gets installed usually

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

unintentionally and harms the user and their computer. It's also possible for a virus to spread itself to other computers. Now, how does a virus get on your computer in the first place? There are a couple of ways an attacker can infect someone's computer. They might do a victim into installing a program with deception about the programs purpose, so for example a lot of viruses are disguised as security updates. It's also possible that the software on your computer has vulnerability so attacker can install itself without even needing explicit permission. Once a virus is on your computer it can steal or delete any of your files, control other programs, or even allow someone else to remotely control your computer. Using computer viruses, hackers can take over millions of computers worldwide and then use them as a digital Army, also known as a Botnet, to attack and take down websites. This kind of attack is called a distributed denial of service. A denial of service is when hackers overwhelm a website with too many requests. We call it a distributed denial of service when the attack comes from many computers all at once. Most websites are ready to respond to millions of requests a day, but if you hit them with billions or trillions of requests coming from different places, the computers are overloaded and stop responding. Another trick used by cyber criminals is to send large amount of spam emails in an attempt to trick people into sharing sensitive personal information. This is called a Phishing scam. Phishing scam is when you get what seems like a trustworthy email asking you to login to your account, but clicking the email takes you to a fake website. If you log in any way you have been tricked into giving your password away. Hackers can then use your login credentials to access your real accounts to steal information or maybe even to steal your money. Fortunately there are many companies, laws and government organizations working to make the Internet safer, but these efforts are not enough. With billions trillions of dollars at stake, cyber criminals get smarter each year and we all need to keep up.

3. COMMON METHODS USED FOR SECURITY OF DATA

- Keeping operating systems updated and regularly patched.
- Restricting software and setting up administrative rights so that nothing can be installed on company computers without authorization.
- Use of filtering that controls access to data.
- Blocking access to restricted sites with internet filters to prevent employees and hackers from uploading data to storage clouds.
- Using a firewall plus software that opposes virus, spyware and phishing attacks.
- Keeping browsers updated at all times with the latest version of the software.
- Keeping all system software's updated.
- Encrypting wireless network.
- Removal of USB ports so that malicious data can't be downloaded.
- Implementation of strict password policies.
- Encrypting entire drives, folders and files.
- Use of anti-virus software.

4. LOOPHOLES IN CURRENT SYSTEM

In this current world, people think that our jobs may be replaced by machines and machines may overtake the human race. But is this really true? There are many loopholes in the current system. Let us take a look at a few of these loopholes.

- As the saying goes, "To err is human". Humans are known to make errors and learn from them. But sometimes, these errors come at a price. Could there be a possibility of a zero error situation which would benefit us all? That's what we are bound to find out soon.
- It's possible that antivirus programs may occasionally say a file is a virus when it's actually a completely safe file. This is known as a "false positive." These false positives can damage users' systems – such mistakes generally end up in the news, as when Microsoft Security Essentials identified Google Chrome as a virus, AVG damaged 64-bit versions of Windows 7, or Sophos identified itself as malware.
- Packet filtering by a software firewall can degrade your system's performance, because it's a demanding task to examine every packet of data. A network firewall also can lend users a false sense of security, encouraging them not to maintain security at the machine level. If the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

network firewall fails or is not configured properly, this could prove disastrous.

- Encryption is a very complex technology. Management of encryption keys must be an added administrative task for often overburdened IT staff. One big disadvantage of encryption as it relates to keys is that the security of data becomes the security of the encryption key. Lose that key, and you effectively lose your data.

5. AI TECHNIQUES FOR CYBER SECURITY

AI plays a major role in fighting against this crime.

1. AI² (AI SQUARE):

- To predict attacks, AI² combs through data and detects suspicious activity by clustering the data into meaningful patterns using unsupervised machine-learning. It then presents this activity to human analysts who confirm which events are actual attacks, and incorporates that feedback into its models for the next set of data.

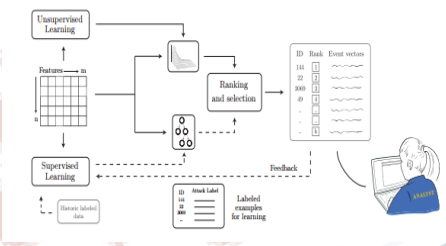

Fig 1: Detection by virtual analyst

- AI system acts as a virtual analyst where in it continuously generates new models that it can refine in as little as a few hours, meaning it can improve its detection rates significantly and rapidly.

- AI2's secret weapon is that it fuses together three different unsupervised-learning methods, and then shows the top events to analysts for them to label. It then builds a supervised model that it can constantly refine through what the team calls a "continuous active learning system".
- Specifically, on day one of its training, AI2 picks the 200 most abnormal events and gives them to the expert. As it improves over time, it identifies more and more of the events as actual attacks, meaning that in a matter of days the analyst may only be looking at 30 or 40 events a day.
- In a nutshell, the basic outline of how the technique AI2 works is, first, using a recurrent neural network and other machine learning techniques, it parses the huge amount of data generated by users, a process called "unsupervised learning." Once it has identified the anomalies it notifies its human analyst and presents its findings. The human confirms or denies each anomaly and then their decisions are relayed back to the AI which turns them into a model to use the next day, in a process called "supervised" learning.

Detection:

AI² is roughly three times better than previous benchmarks, and also reduces the number of false positives by a factor of 5.

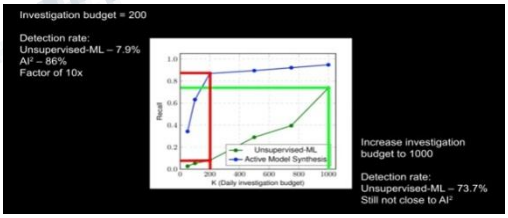

Fig 2: Graph of detection rates by AI2

2. QRADAR SIEM

- This is most popular technique used now a day which helps us in detecting cyber security threads or issues with cognitive intelligence, which helps us in identifying the thread more accurately and resolve them faster than ever before.
- Cognitive technology is being used in cyber security to fend off the hackers in tacking the issues simultaneously.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

- Cognitive security uses intelligent technology like machine learning and natural language processing to mimic the way the human thinks!

Solution:

- QRadar SIEM (security information and event management) with IBM Watson Argument helps to identify and understand sophisticated threads by tapping into unstructured data and correlate with local security Offences.
- This helps to discover the data or malicious file which is seriously and easily missed by the human in their process of viewing the data.
- With this we form informed decisions at unpredictable speed and scale.
- Cognitive Intelligence, embedded with Watson cyber security's (QRadar) uniquely identifies the ability to understand, reason & learn about the computer threads.

Security:

Provides near real-time visibility: For threat detection and prioritization, throughout the entire IT infrastructure.

Reduces priorities alerts: To focus investigations on an actionable list of suspected incidents.

Enables more effective threat management: While producing detailed data access and user activity reports.

- The QRadar Security Intelligence Operating System provides a platform on which users can continue to add new security modules to accommodate new use cases around the intelligent securing and intelligent risk assessment of the enterprise infrastructure.

Features:

- QRadar helps in detecting attacks in real time best practice
- Deploy quickly with minimal intervention from an already overworked
- Maintains and secure clouds services and also compliance with both internal and external regulations.
- High priority incidence detection and fully visibility in cloud networks and users activity.

QRadar Security platform:

- QRadar offers different way in understanding and detecting the problem when compared to others.
- This QRadar Security (fig 3) offers all self contained, within the security intelligence platform, we have the ability to look at all of these different points like vulnerability data, configuration data, packet collection, network analysis, flow data, collects logs and events.

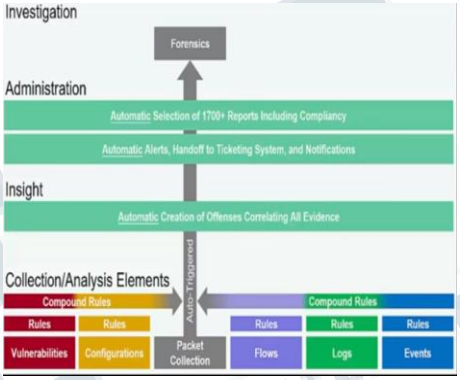

Fig 3: Security platform for QRadar

- The system then uses its own compound rule to correlate the information.
- All the different information together then creates a chain of the data or offences. We then take that data and do notify the every part within that boundary on this QRadar security platform.

Challenges:

- The lack of visibility is one of the biggest cyber security challenges that enterprises face today.
- Security threats are the immediate Cyber security issues that require intelligent solutions that are enforced nowadays.
- Knowledgeable systems are already getting used in several applications, typically hidden within an application, like within the security measures coming up with software system.
- The foremost usually mentioned is perhaps by using the techniques of AI, there are other different technologies that, if they reached an

intensity of sophistication, would change the creation of smarter-than-human intelligence.

- An opportunity that includes smarter-than-human minds is actually different in a manner that goes on the far side of the standard visions of a future stuffed with advanced devices.

6. CONCLUSION:

We hereby present a system that combines analytical intelligence with state-of-the-art machine learning techniques to detect new attacks and reduce the time elapsed between attack detection and successful prevention. It shows that the machine learns to defend against unseen attacks as time progresses. We can reduce the threat in cyber environment by not providing a chance for cyber crimes to develop by these methods which can detect 80 percent of cyber threats.

REFERENCES:

1. Jyothsna S Mohan, Nilina TIJSR Prospects of Artificial Intelligence in Tackling Cyber Crimes. http:// www. ijsr. net / archive/v4i6/SUB155595.pdf

2. Alfredo Cuesta-Infante, Vamsi Korrapatii, Costas Bassias, Ke Li Journal on AI2 : Training a big data machine to defend http: // people .csail .mit .edu /kalian /AI2_Paper .pdf

3. Jatin Borana Applications of Artificial Intelligence & Associated Technologies http: // www .sd technocrats .com / ETEBMS2016/html/papers/ETEBMS-2016_ENG-EE7.pdf