International Journal of Engineering, Science and Mathematics
Vol. 7,Issue 4, April2018,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

ARTIFICIAL INTELLIGENCE: A BOON OR THREAT FOR CYBERSPACE SECURITY

Priti Bali*

Abstract

Nowadays workplace mobility has improved productivity and collaboration but it has also exposed the confidential data of organizations to unknown risks called cyber attacks. In today's connected world, the risk of cyber attacks is on the rise and it is becoming very difficult to ensure cyberspace security. Cyberspace is expanding day-by-day. Usage of smart phones, apps and tablets has expanded the surface of cyberspace for protection as well as attack. Cyber defenders have to protect this expanded surface and cyber attackers target this expanded surface. AI systems can process the huge amount of data generated through this expanded surface in an efficient and quick manner. Evolution of smart devices facilitates professional as well as personal activities. This evolution also leads to increase in cyber crimes. This situation sounds alarmist and should be handled properly because ubiquity and anonymity features of cyberspace make it highly vulnerable to intrusions and cyber attacks. Embedded intelligence is required in all the smart devices and computer networks to combat against evolving cyber attacks. Traditional tools such as sensors, detectors etc. are not sufficient for the protection of cyberspace. Advanced automated tools such as AI systems that are capable of monitoring normal behaviors and detecting abnormal ones must be used to strengthen cyberspace security. Hence, AI is a transformative technology for securing cyberspace. But each revolution has a bright as well as dark side, hence whether AI is a boon or threat in the field of cyberspace security is debatable as AI systems are being used by cyberspace defenders as well as cyberspace attackers.

Keywords:

AI;
Machine Learning;
Deep Learning;
Supervised Learning;
Unsupervised Learning;
Pattern Recognition;
Cyberspace;
Cyber Attacks;
CI;
CII;
GII;
IoT;
DDoS;
BYOD.

Author correspondence:

Priti Bali
Assistant Professor
D.A.V. Institute of Management, Faridabad-Haryana

1. Introduction

AI (Artificial Intelligence) is a transformative technology. AI systems work on underlying algorithms. AI systems can be used to protect the confidential data of organizations from cyber attacks because AI systems are capable of learning from every cyber attack. AI systems are used as a key weapon for managing cyber attacks because these systems are capable of detecting even the most subtle deviations from normal and hence play an important role in cyberspace security where intrusion detection and prevention is the most crucial task. AI systems automatically adapt and improve through experience by analyzing the anomalies in network traffic. Traditional security tools are not capable of detecting these deviations and hence these tools cannot detect the cyber threats at earliest stage. Human beings also are not capable of detecting these threats at initial stages.

AI systems are being used by many organizations for analyzing and predicting behavioral patterns of cyber attackers (or hackers) accurately. But cyber attackers are also using AI systems for their benefit. For example, with the help of AI systems, cyber attackers can improve speed, power and effectiveness of various cyber attacks such as identity theft, Denial-of-Service, password cracking, phishing, sniffing, spoofing, social engineering etc. by analyzing the behavioral patterns of genuine users. AI systems are capable of searching large databases to find out the victim's details such as where they bank, where they study, where they shop, which medical insurance company they have chosen etc. AI systems can pull information from multiple databases to find out the vulnerable target. For example, someone who is travelling or someone who is hospitalized, someone who is out of station may not keep track of transactions in their bank accounts. These people are vulnerable targets. Cyber security experts use AI to fix the vulnerability that had previously allowed unauthorized entry whereas cyber attackers use AI systems to identify new vulnerabilities in the network because AI systems keep on scanning for new ways to enter into the networks without human instructions. Hence, it is very difficult to keep up with tremendous speed of evolving cyber attacks.

AI systems are capable of detecting evolving cyber attacks and make intelligent real-time decisions. Cyber defense systems should evolve with the same pace as cyber attack systems are evolving. Human beings are not capable of detecting and preventing these evolving cyber attacks rather automated systems are required for handling, detecting, evaluating and responding to these attacks. Hence, AI systems have become a requirement for responding timely and accurately to cyber attacks.

Amount of data is increasing exponentially day-by-day. Cyber attackers always find new ways of attacking the network. GII (Global Information Infrastructure) has significantly increased cyberspace security risks because almost all the devices are networked (or connected) and cyber attackers are misusing these networked smart devices for fraudulent activities. That is why people have started referring IoT as "Internet of Threats" instead of "Internet of Things". Hence, there is a need to fully embed intelligent and adaptive cyber security within "IoT (Internet of Things)" because these devices and networks are mostly misused by cyberspace criminals for fraudulent activities.

2. AI: a boon for Cyberspace Security

AI is the smartest tool for cyber defenders. Cyber security firms are using AI systems to protect Critical Infrastructure (CI) and Critical Information Infrastructure (CII) from attackers. Critical Infrastructure is the backbone of a nation. CI includes food and agriculture sector, energy sector, financial sector, health sector, chemical sector, communications sector, manufacturing sector, water sector, telecommunications sector, banking and finance sector, space and research sector, defense sector, law and order sector, Information Technology sector etc. CII is the subset of CI. CII includes communications sector, telecommunications sector, Information Technology sector etc. Intruder detection and prevention is a major application in cyberspace security where AI is expected to have a major impact. With the help of AI vast amount of data can be analyzed and cyber security professionals can identify far more threats that would be impossible to identify if done manually. AI systems can detect even the most subtle deviations from normal and identify a sophisticated external attacker or a trusted insider. Human observers and traditional security tools frequently miss these threats but AI algorithms identify them at the earliest possible stages, before they can do any damage.

AI applications (or methods) such as machine learning, deep learning, supervised learning, pattern recognition etc. provide flexibility and learning capability to software. Among these technologies, machine learning is expected to play a major role in artificial intelligence based cyberspace security. Machine learning is a subset of AI and deep learning is a subset of machine learning. Machine learning seems very promising to combat cyber attacks such as DoS (Denial of Service), DDoS (Distributed Denial of Service) etc. because this technology is based on understanding different patterns in computer networks and adapting to new situations automatically.

What are the primary reasons for your organization's decision to deploy or consider deploying machine learning for security analytics and operations? (Percent of respondents, N=380, three responses accepted)

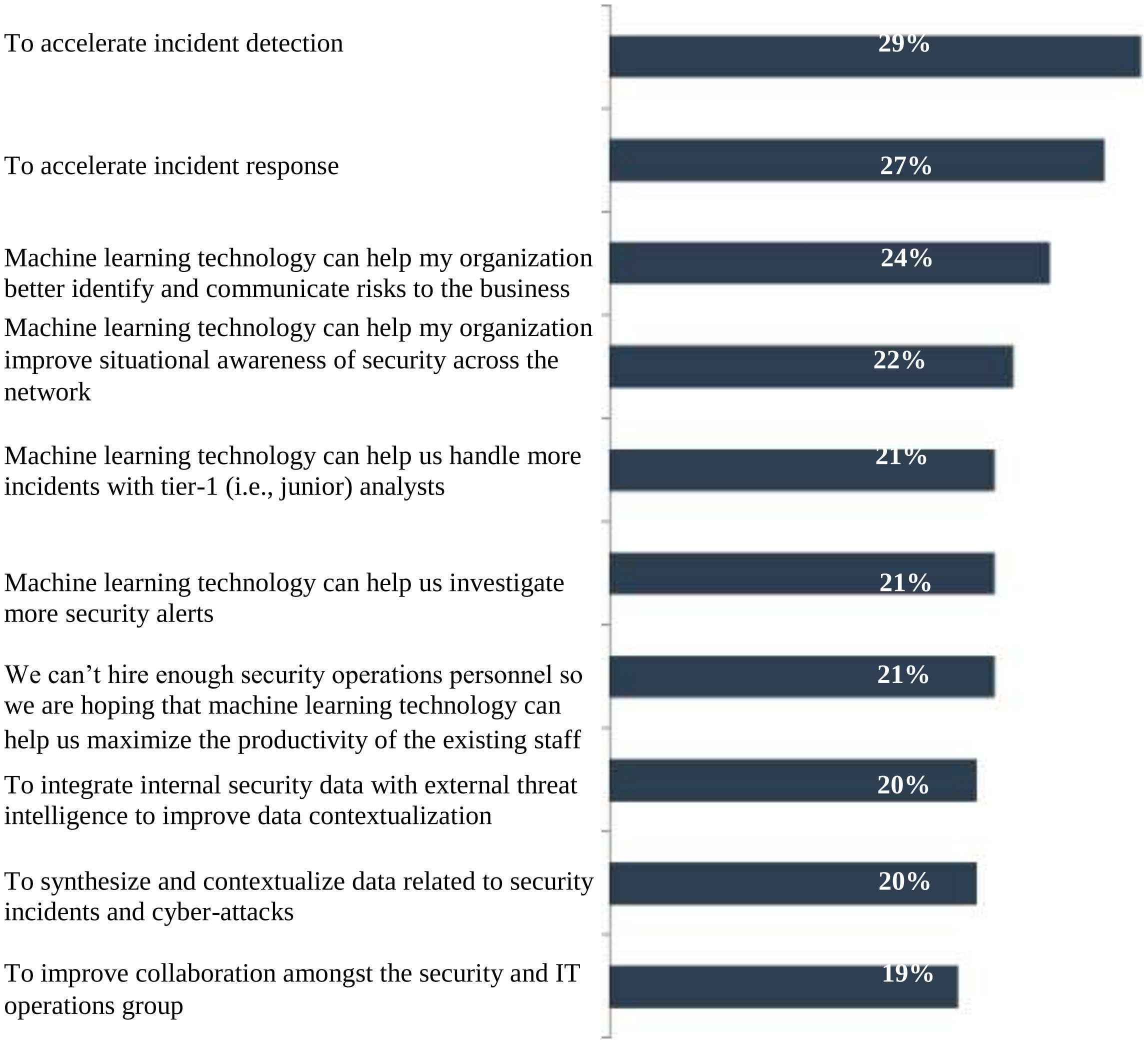

Figure 1. Reasons for Deploying or Considering Deploying Machine Learning for Security Analytics and Operations

Source: Enterprise Strategy Group, 2017 (https://www.mcafee.com/enterprise/en-us/assets/reports/rp-esg-security-ops-and-analytics.pdf)

Machine learning algorithms automatically adapt and improve through experience by analyzing the anomalies in network traffic. Supervised learning and unsupervised learning are the two categories of machine learning that are used to combat cyber attacks. In supervised machine learning, human intervention is applied to help the machines to generate correct set of rules whereas unsupervised machine learning is based on automatic recognition of subtle behavioral deviations in computer networks or other activities without human intervention. In supervised machine learning rules are generated on the basis of current and past knowledge of known attacks whereas in unsupervised machine learning, rules in the underlying algorithms are automatically generated and adjusted according to the observed unknown abnormalities. Hence, unsupervised machine learning is mostly used to combat evolving cyber attacks in real-time because this technology is capable of detecting new types of cyber threats that are being launched every day and distinguishing outliers from normal activity. But, unsupervised machine learning may generate false positives and these false positives should be analyzed by human analysts to combat cyber attacks properly [1].

Supervised machine learning algorithms are less suited for cyberspace security because these algorithms are based on a set of labeled training data (normal network traffic or anomalous network traffic) for predicting future network traffic whereas unsupervised machine learning algorithms are based on unlabeled training data for prediction of all categories [2]. Sometimes, labeling the data becomes very time-consuming and difficult. For example, labeling of the network flow data is very difficult and time-consuming for human analysts. Machines can perform this task of finding patterns in large datasets very easily [3]. Hence, unsupervised machine learning algorithms are most suitable for cyberspace security. Supervised machine learning algorithms learn from the training dataset whereas unsupervised machine learning algorithms devise and present the interesting structure in the data on their own [4]. Therefore, unsupervised machine learning algorithms are well suited for cyberspace security because these algorithms process millions of data every minute, identify anomalous behavior automatically, correlate anomalies across multiple data sources to determine the potential impact of anomalies and detect cyber attacks that have never been seen before [5], [6].

Nowadays, huge amount of data is being produced in cyberspace every day. For handling such data, automation is required. Human beings cannot handle this huge data without automation. Reach of cyberspace is increasing day-by-day and the reach of cyber attacks is also increasing. Investigation of cyber attacks requires flexible algorithms because methods of cyber attacks in networks are dynamically evolving. Cyber attackers make frequent changes in malicious code to avoid detection. Automation in cyber defense tools is must to cope up with evolving cyber attacks. AI systems are capable of making intelligent real-time decisions. AI plays an important and efficient role in detection and prevention of cyber attacks. Cyberspace is highly vulnerable to attacks because of its ubiquity and anonymity features.

AI systems are very promising in critical fields such as data analytics, predictive data analytics, cyber security etc. AI systems can be used for setting up self-configuring networks that could detect vulnerabilities and respond automatically. These self-configuring networks are able to perform self-patch actions for strengthening the cyber security. AI systems are capable of detecting small clues of compromise in networks even if the clues are scattered throughout the network.

AI systems detect whenever a noticeable deviation such as behavioral anomaly occurs and block the cyber threat or issue warning to the main server for necessary actions by the security analysts.

Various AI solutions such as Multifactor Authentication, Data Loss Prevention, Advanced Persistent Threat Protection (APTP) and Intrusion Prevention System (IPS)/Firewall have helped many government agencies and private businesses/instituitions to protect their sensitive data/secret information. Predictive technologies such as AI and machine learning are notably useful in filtering the sensitive data on high priority cyberspace security incidents.

3. AI: a threat for Cyberspace Security

AI is the smartest weapon for cyber attackers. Cyber attackers also focus on the new technologies and if cyber attackers would be ahead of cyber defenders in usage of these technologies then situation will become more critical.

Each and every new technology is misused by cyber attackers. AI can make the attacks launched by cyber attackers more powerful and efficient. Cyber attacks such as identity theft, identity fraud, password cracking, Denial-of-Service, Distributed Denial-of-Service, phishing, spoofing, social engineering, sniffing etc. can be launched at machine's speed with the help of AI. When machines are used for launching cyber attacks, consequences are more catastrophic. For example, if critical infrastructure is being targeted with the help of AI then it can affect millions of people. Cyber attacks launched through AI systems are more dangerous as consequences of these attacks may include power cut in a large area, shut down of hospitals, attack on national defense system etc. This sounds alarmist because launching attacks at machine's speed cause catastrophic consequences. Cyberspace is expanding day-by-day but measures to secure cyberspace are lacking [7].

Cyber attacks such as phishing, spoofing, social engineering, DoS, DDoS, sniffing etc. become more catastrophic if they are launched using AI technologies such as machine learning, deep learning etc. For example, after identifying the message style of victim to and from particular contacts in his address book, AI systems could tailor phishing messages to mimic the message style of victim and convince the victim to click on a malicious attachment.

Hence, AI systems could be used to automate the process of hacking. When machines are launching cyber attacks, these attacks become more dangerous. AI systems can monitor and learn from the patterns and habits of the victim. After monitoring and learning from the patterns and habits, AI technology can even predict the victim's likely answers to security questions. This information can be used to reset the passwords automatically for hacking the email accounts of victims. Hence, AI systems could trick victims to click anything. With the help of AI, more people could be targeted at machine's speed in a very short time [8].

Cyber attackers use AI systems to continuously alter the malicious code to avoid detection. Hence, with the help of AI systems cyber attackers stay one step ahead of cyber defenders. Cyber attackers use AI systems to scan the vulnerabilities as well as exploit the vulnerabilities.

AI systems are capable of detecting, evaluating and patching software vulnerabilities without human intervention and assistance (called as Internet of Things). AI systems are also capable of exploiting these vulnerabilities. Hence, "Cyber defenders can leverage AI for defense and cyber attackers can leverage AI for attack".

Cyber criminals use AI systems to automate their tasks. For example, AI systems can be used for sending phishing e-mails to a large population. Whenever some new technology comes it is used by ethical (or genuine) users as well as misused by cybercriminals for fraudulent activities. For example, nowadays because of tremendous increase in the number of cyber crimes, people have started referring IoT as "Internet of Threats" instead of "Internet of Things".

By writing an intelligent program attacks can be launched very easily at a grand level. Since machines have superior computing skills and can perform harmful acts to damage critical infrastructure at a tremendous speed. Machines can scan millions of ports in seconds to find the backdoors (or trapdoors or security holes).

Cyber attacks are difficult to track and AI will raise more difficulties in attribution. AI based cyber attacks are more dangerous. Attackers can quickly identify the network activities and vulnerabilities (or security holes) in the systems with the help of AI and launch cyber attacks at machine's speed. Cyberspace is expanding day by day and hence reach of cyber attacks is also increasing and technologies like AI are facilitating the job of hackers. AI software is capable of monitoring all the network activities; it can identify the odd patterns and immediately report that such patterns have not occurred before. Hence, suspicious activities can be identified and reported immediately by using AI software. Attackers also use AI to identify the normal patterns of authorized users by writing an intelligent program. Once a malware is written for attack, it will make decisions at a tremendous speed. That is why cyber attackers like AI systems as much as cyber defenders do.

4. Growth drivers for AI based Cyberspace Security

Tremendous increase in the number of cyber crimes is the major growth driver for AI based cyberspace security. Organization's employees are considered as the most likely cause of cyber attacks. Internal penetration is more dangerous than external penetration because internal employees are aware of the various system vulnerabilities and they can easily misuse their privileges of data access. Internal employees have no barriers to cross as they are authorized to access all the resources and it becomes very difficult to track the intrusions performed by internal employees. Hence, constant monitoring of network is required to identify abnormal behaviour. AI systems are capable of identifying subtle deviations in the network traffic. Also, culture of BYOD (Bring Your Own Device) is facilitating cyber attacks. Organizations are adopting BYOD strategy to attain competitive edge and enhance productivity. BYOD strategy poses many benefits but it carries significant risks also. BYOD means employees bring their own devices to access the organization's resources. Employees can work from anywhere, anytime. BYOD strategy reduces the initial set up cost for organizations but it also leads to increased cyber crimes because data is more susceptible to cyber attacks in employee's devices. Various risks are associated with BYOD strategy such as employees may lost their devices, employees may install malicious programs on their laptops unintentionally, dishonest and disgruntled employees can disclose organization's confidential information to outsiders. Traditional tools are not effective against evolving cyber attacks.

In today's hyper-connected world, there are endless opportunities for internal and external penetration. Employees are the weakest link as they are authorized to access all the resources. This increased vulnerability demands for AI systems because only AI systems can go through the vast amount of information to identify the cyber threats in computer networks in real time. Organizations generate voluminous data and use data analytics to improve their product offerings. Human analysts are not capable of analyzing this huge amount of data. AI systems can analyze voluminous data quickly [9]. Response time reduction and growing need of protecting this voluminous data also act as growth drivers for AI based cyberspace security. Other growth drivers such as understaffed IT security teams, obsolete means to combat cyber attacks etc. also contribute to enhance AI's presence in cyberspace security market. Also, expanded IP address space for "IoT" sets new cyberspace security challenges and drives the growth of AI in cyberspace security.

According to a report, "[10] Growing popularity of enterprise Bring-Your-Own-Device (BYOD) strategies are likely to grow AI's presence in the cyberspace security market going forward. In 2016, global AI was worth $1.2 billion. This amount is expected to increase at a compound annual growth rate (CAGR) of 36 percent between 2017 and 2023 [10]". AI based cyberspace security systems are capable of blocking the attacks as well as automatically healing the vulnerabilities. AI technologies such as machine learning and deep learning are capable of identifying compromised database credentials, identifying records, pinpointing network traffic to/from restricted segments, assessing database structures, identifying tables, identifying subtle deviations and detecting database attacks [11].

All the above factors will drive the growth of AI in cyberspace security in the years to come. Hence, there is a strong future of AI in cyberspace security as evolving automated cyber attacks can be detected, prevented and stopped using AI systems. Importance of AI in cyberspace security is beyond doubt.

5. Barriers for AI based Cyberspace Security

There are many barriers that stop AI's entry in cyberspace security market. First barrier is cost; significant cost is involved in deploying AI based cyberspace security. Maintenance cost incurred is also a barrier for usage of AI systems in cyberspace security because continuous scaling of AI systems is required to cope up with the evolving cyber attacks. Also, extensive data is required to train machine learning algorithms. Machine learning algorithms require comprehensive training about basic details of each and every cyber threat to understand the launch and effect of each and every cyber attack. Performance of an AI system totally depends upon the data fed into it. Richness and complexity of data improves the efficiency of AI solutions. AI systems require data of years to perform better. Lack of experienced engineers also act as a barrier for AI based cyberspace security because limited engineers are available for developing effective AI software solutions [12].

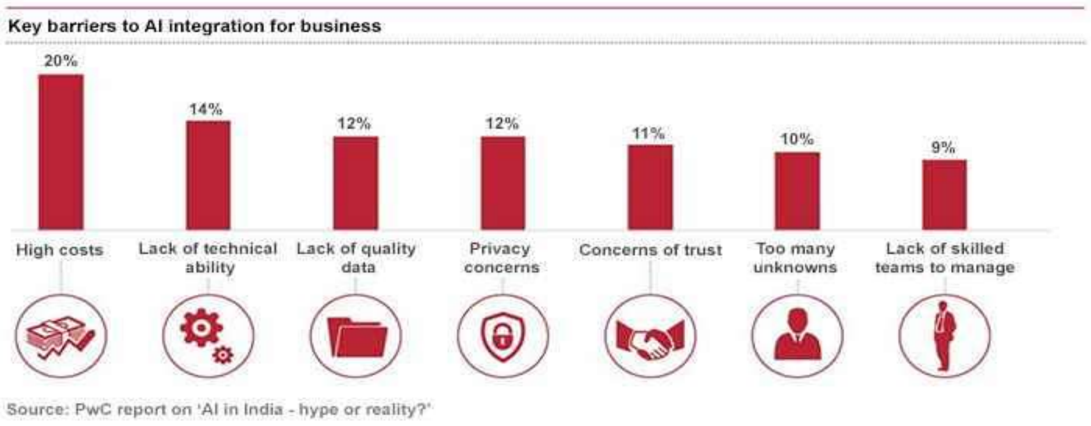

Figure 2. Key barriers to AI integration for business

Source: https://www.pwc.in/press-releases/2018/advance-artificial-intelligence-for-growth-leveraging-ai-and-robotics-for-indias-economic-transformation.html

6. Current and future status of Artificial Intelligence based Cyberspace Security

Most of the organizations are currently using or planning to use AI based cyberspace security in future. According to various surveys and reports, current and future status of artificial intelligence based cyberspace security is as follows:

"[13] California-based Cylance® is the first company to leverage AI and machine learning to cyber security for understanding the root cause of attacks and their prevention. Cylance is revolutionizing cybersecurity with products and services that proactively prevent, rather than reactively detect the execution of advanced persistent threats and malware. Cylance is the first company to apply artificial intelligence, machine learning and algorithmic science to cybersecurity to improve the way companies, governments, and endusers proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance's award-winning product, CylancePROTECT, quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated artificial intelligence and machine learning with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be predictive and preventive against advanced threats [13]".

"[14] The Cisco 2018 Annual Cybersecurity Report shows that 50 percent of organisations in India are reliant on automation, 53 per cent are reliant on machine learning and 51 percent are highly reliant on artificial intelligence. Also the survey found that security professionals see value in behavioral analytics tools in locating malicious actors in networks as 67 percent of security professionals said behavior analytics tools work well [14]".

"[15] According to ESG research, 12% of enterprise organizations have already deployed AI-based security analytics extensively and 27% have deployed AI-based security analytics on a limited basis [15]".

"[16] AI takes cyber security to a new level for HDFC Bank. The capabilities of current security technologies coupled with the power of Artificial Intelligence (AI) will take the cyber security preparedness to the next level, says Sameer Ratolikar, CISO, HDFC Bank, highlighting his bank's AI based Cyber Security Operations Center (CSOC). The bank has close to 100,000 employees. The AI solution will help in monitoring insider threats [16]".

"[17] The "Cisco 2018 Annual Cybersecurity Report" showed that more than half of the organisations surveyed in India are reliant on automation, ML and AI [17]".

"[18] The techno-elite companies like Facebook, Amazon, Netflix, Google, Apple and Microsoft (a.k.a. FANGAM) have successfully leveraged machine learning algorithms across their businesses that include security systems to protect their users, applications and the overall infrastructure [18]".

"[19] Tech Mahindra has entered into a strategic partnership with Silicon Valley-based Balbix for launching an artificial intelligence-powered threat assessment platform to check cyber security breaches. The Tech Mahindra and Balbix platform uses deep learning and specialised AI algorithms to predict how attacks can happen and propagate, providing actionable insights to mitigate the risk of breach, the Indian firm said in a statement. With Balbix, Tech Mahindra's intelligent security operations centre (iSOC) offering can now predict and proactively avoid cyber-breaches by continuously monitoring IT inventories for hundreds of breach risk factors and take appropriate mitigating steps [19]".

GLOBAL ARTIFICIAL INTELLIGENCE IN CYBER SECURITY MARKET, BY SERVICE TYPE, $M (2013 – 2023)

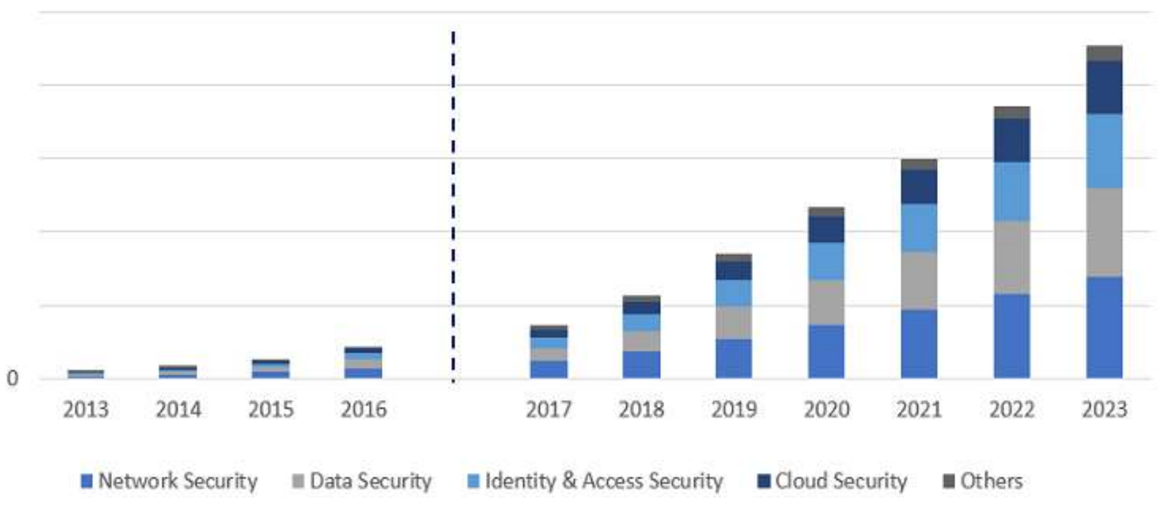

Figure 3. Global Artificial Intelligence in Cyber Security Market by Service Type
Source: https://www.psmarketresearch.com/market-analysis/artificial-intelligence-in-cyber-security-market

"[20] In 2015, the global market for AI was worth 126.24 billion USD and is projected to reach a value of 3,061 billion USD by the end of 2024. The market is anticipated to exhibit an impressive 36.1 percent CAGR between 2016 and 2024 [20]".

"[21] ESG research about driving forces of AI-based cybersecurity technology adoption indicates that 29% want to use AI-based cybersecurity technology to accelerate incident detection, 27% want to use AI-based cybersecurity technology to accelerate incident response, 24% want to use AI-based cybersecurity technology to help their organization better identify and communicate risk to the business and 22% want to use AI-based cybersecurity technology to gain a better understanding of cybersecurity situational awareness [21]".

"[22] The last five years have really seen a rise in AI and ML technologies for enterprises. Most of which can be attributed to advancements in computing power and the evolution of paradigms like distributed computing, big data and cloud computing. Early commercial applications of ML were pioneered by technology titans like Google (in its search engine), Amazon (with its product recommendations) and Facebook (with its news feed). These businesses managed to build a veritable treasure trove of valuable behavioral data from hundreds of millions of users. Organizations are already beginning to use AI to bolster cybersecurity and offer more protections against sophisticated hackers. AI helps by automating complex processes for detecting attacks and reacting to breaches. These applications are becoming more and more sophisticated as AI is deployed for security [22]".

According to CyberVision 2015-2025 (20th to 21st Century Cyberspace Security Trends (Integrated, Adaptive and Intelligent Security):

20th Century (1995 – 2010) security tools	21st Century (2010 – 2025) security tools
Main focus on firewalls and antivirus	Main focus on adaptive and self-organizing cyber tools
Based on physical "spatial" security models such as Castles and Moats	Based on temporal security models such as Artificial Intelligence and Machine Learning
Protection @ "speed of sound"	Protection @ "speed of light"
Based on space	Based on time
IP address space almost fully assigned (IPv 4)	Expanded IP address space for "IoT" sets new cyber security challenges (IPv 6)

Table 1. 20th to 21st Century Cyberspace Security Trends
Adapted from Source: http://www.valentina.net/Rome2016/cybervision-v4.pdf

"[23] Amazon also is adding cyber-security to its AI resume. TechCrunch is reporting that Amazon has acquired AI-based cyber-security company Harvest.ai. According to its website, Harvest.ai uses AI-based algorithms to identify the most important documents and intellectual property of a business, then combines user behavior analytics with data loss prevention techniques to protect them from cyber attacks [23]".

"[24] In 2017, Amazon Web Services (AWS) launched data security service – Macie - with machine learning, to identify, sort and safeguard sensitive data across the cloud service. The idea behind this cloud infrastructure giant using machine learning is to protect and analyze the increasing amount of sensitive data using a picture of historical patterns of positive and negative behaviors, as it grows within an organization [24]".

"[25] The payments giant PayPal keeps fraud losses below industry averages by teaching computers to play detective. Deep learning and other artificial-intelligence approaches have worked to help keep PayPal's fraud rate remarkably low, at 0.32 percent of revenue—a figure far better than the 1.32 percent average that merchants see, according to a study by LexisNexis [25]".

"[26] The online payment platform PayPal uses machine learning algorithms to battle fraud. By leveraging deep learning techniques, PayPal analyzes humongous customer data and assesses risk accordingly. AI is a powerful technology stack that enables enterprises identify and eliminate bottlenecks in their cyber security roadmap to combat ever-increasing cyber attacks in this digital age [26]".

ARTIFICIAL INTELLIGENCE MARKET WILL SURPASS $100B BY 2025:

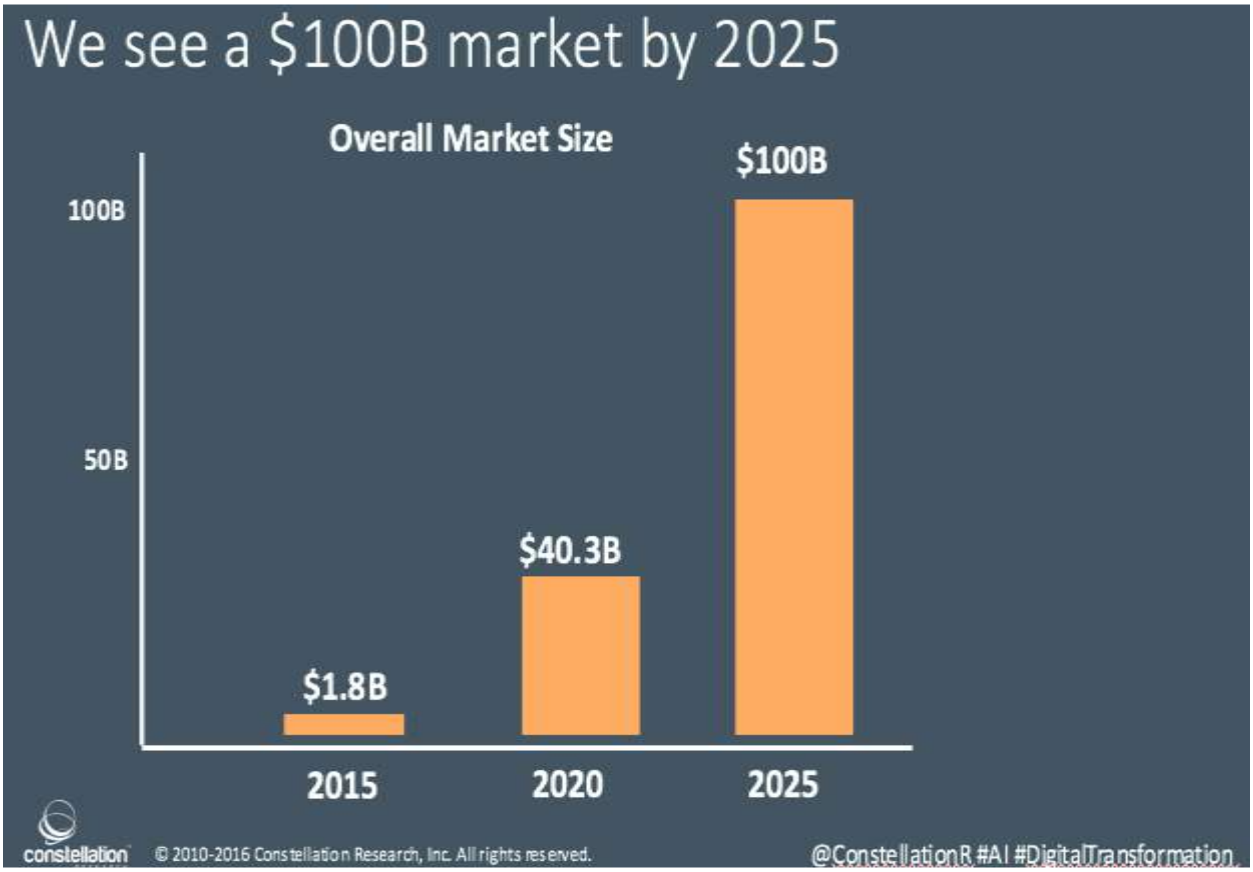

Figure 4. Artificial Intelligence Market by 2025
Source: http://blog.softwareinsider.org/2016/09/18/mondays-musings-understand-spectrum-seven-artificial-intelligence-outcomes/

"[27] According to a report on "AI adoption in India" More than 36% of large financial establishments have already invested in these technologies and around 70% plan to embrace it in the near future [27]".

Hence, most of the organizations are increasingly adopting AI systems to combat cyber attacks.

7. Conclusion

Nowadays, organizations process billions of transactions per day. Cyber attackers are targeting this huge volume of data and it is impossible to check for intrusion manually. Real time and proactive detection of these intrusions is needed to ensure cyberspace security. There should be a mechanism that identifies new patterns in computer networks and modifies its rules according to new patterns automatically. Old tools and technologies are not capable of detecting behavioral abnormalities, odd patterns and unusual behavior. AI systems are capable of differentiating benign and malicious activities in computer networks automatically to identify the cyber attacks. AI systems perform constant monitoring and reporting of an organization's network which makes incident response faster. AI systems are capable of preventing as well as stopping in-progress cyber attacks. That is why artificial intelligence is anticipated to play a significant role to combat cyber-attacks as AI systems are capable of performing deep analysis of network's behavior to understand different patterns and adapt to new situations by thousands of learning iterations to make self-healing networks. Human analysts and traditional security tools are not capable of observing the subtle deviations in computer networks and frequently fail to spot cyber attacks but AI algorithms observe these deviations and identify unknown cyber attacks at the earliest possible stages, before they can do any damage. But AI is not a substitute for human beings as human intervention is required for supervision of AI systems in case if cyber attackers design machine learning algorithms to confuse organization's AI systems. Each and every task will be initiated by human beings and augmented by AI systems because technology cannot work independently. AI systems provide packet validation, pattern recognition, entropy detection, human verification, behavioural analysis, priority traffic shaping, network traffic monitoring, anomaly detection etc. AI systems are best suitable to protect critical infrastructure of a country as AI systems can be quickly scaled to combat evolving cyber attacks.

In upcoming years, fastest growth of artificial intelligence in cyber security market is expected as organizations are witnessing rising incidence of cyber-crimes such as identity theft, identity fraud, phishing, money laundering, cross-site scripting, social engineering, spoofing, packet sniffing, DoS, DDoS, cyberstalking, hacking, cyber terrorism, cybersquatting, DNS (Domain Name System) misdirection, network channel eavesdropping, cybervandalism and malicious attacks on yearly basis.

References

[1] https://www.huffingtonpost.ca/david-masson/cybersecurity_b_11702530.html
[2] https://www.quora.com/How-would-you-approach-cybersecurity-and-machine-learning-through-supervised-unsupervised-or-reinforcement-learning
[3] https://insights.sei.cmu.edu/sei_blog/2017/06/machine-learning-in-cybersecurity.html
[4] https://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/
[5] https://blog.blackducksoftware.com/machine-learning-cyber-security
[6] https://insidebigdata.com/2015/12/11/machine-learning-is-cybersecuritys-answer-to-detecting-advanced-breaches/
[7] https://oem.avira.com/resources/whitepaper_AI_EN_20170717.pdf
[8] https://www.computerweekly.com/news/252435434/AI-a-threat-to-cyber-security-warns-report
[9] https://www.huffingtonpost.ca/david-masson/cybersecurity_b_11702530.html
[10] https://securityintelligence.com/news/what-are-the-prime-growth-drivers-for-artificial-intelligence-in-the-cybersecurity-market/
[11] http://www.marketwired.com/press-release/artificial-intelligence-is-key-to-autonomous-cyber-security-future-2147608.htm
[12] https://oem.avira.com/resources/whitepaper_AI_EN_20180306.pdf
[13] https://www.cylance.com/content/dam/cylance/pdfs/feature-focus/Feature_Focus_PROTECT_Malware_Control.pdf
[14] https://economictimes.indiatimes.com/tech/internet/indian-companies-lost-500000-to-cyber-attacks-in-1-5-years-cisco/articleshow/63019927.cms
[15] https://www.scmagazine.com/how-to-approach-ai-enhanced-cybersecurity/article/761867/
[16] http://computer.expressbpd.com/magazine/ai-takes-cyber-security-to-a-new-level-for-hdfc-bank/23580/

[17] http://www.business-standard.com/article/news-ians/india-to-spend-more-on-ai-based-tools-to-secure-cyberspace-cisco-118022101038_1.html
[18] https://www.venrock.com/how-to-fight-crime-with-machine-learning/
[19] http://www.newindianexpress.com/business/2018/apr/11/tech-mahindra-partners-with-balbix-to-launch-a-cyber-security-platform-1799982.html
[20] http://www.globalopportunitynetwork.org/report-2017/intelligent-cyber-security/
[21] https://www.csoonline.com/article/3250850/security/artificial-intelligence-and-cybersecurity-the-real-deal.html
[22] https://www.forbes.com/sites/quora/2018/02/15/how-will-artificial-intelligence-and-machine-learning-impact-cyber-security/#3bff8eac6147
[23] http://www.newsweek.com/amazon-applies-ai-tools-cyber-security-569372
[24] http://www.ibtimes.com/harvestai-investor-reveals-why-amazon-acquired-cybersecurity-startup-2472688
[25] https://www.technologyreview.com/s/545631/how-paypal-boosts-security-with-artificial-intelligence/
[26] https://cio.economictimes.indiatimes.com/tech-talk/ai-in-security-powerful-hacks-for-dealing-with-security-threats/3006
[27] https://www.pwc.in/press-releases/2018/advance-artificial-intelligence-for-growth-leveraging-ai-and-robotics-for-indias-economic-transformation.html