Survey of AI in Cybersecurity for Information Technology Management

Mainka Saharan

Assistant Professor, Computer Science & Engineering, Sunrise University, Alwar, Rajasthan

Abstract:

Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security.

A. Network security is the practice of securing a computer network from hackers and crackers whether targeted attackers.

B. Application security focuses on keeping software and devices free of threats. A compound application could provide access to the data its designed to protect.

C. C. Information security protects the integrity and privacy of data, both in storage as well as in transit.

D. Operational security includes the processes and decisions for handling and protecting data edge. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared .

The means of cyber is the technology that includes system, networks, programs and data.

The means of security is concerned with the protection of system, networks, applications and information. In such a case we can say that electronic information security or information technology security. In other words cyber security is set of principles and practices designed to protect or computing resources and online information against threats.

Types of cyber security

a. Mobile security

b. Identity management

c. Information or

d. Data security

e. Application security

f. Network security

g. Cloud security etc.

Artificial intelligence: artificial intelligence is a set of technology is that enable computers to perform a variety of advanced functions including the ability to see ,understand and translate spoken and written language, make recommendations and more.

Types of artificial intelligence:

Artificial intelligence can be divided based on capabilities and functionalities.

There are three types of artificial intelligence based on capabilities

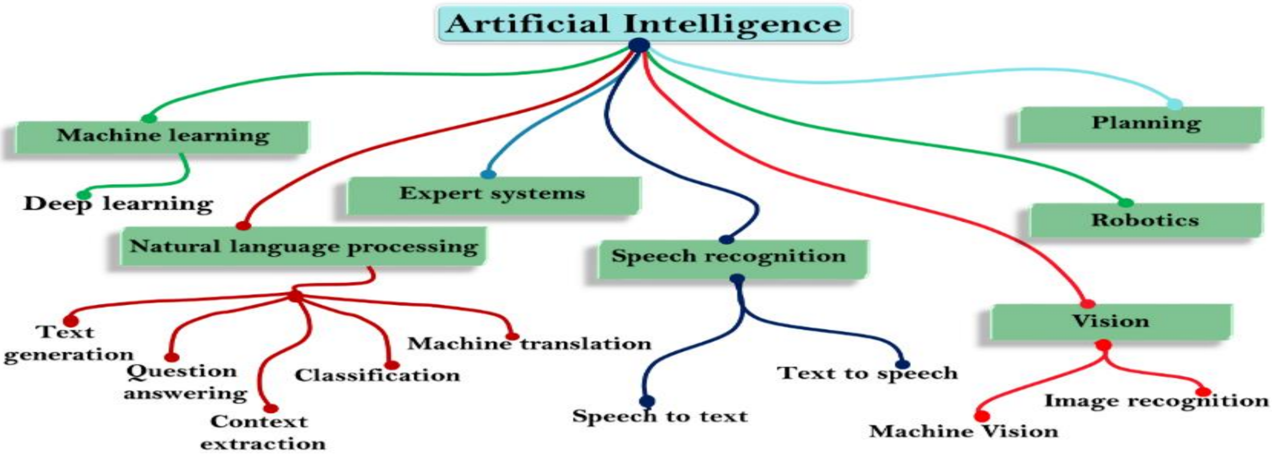
a. Narrow AI

b. General AI

c. Super AI

Under functionalities we have four types of artificial intelligence:

a. Reactive machines
b. Limited theory
c. Theory of mind
d. Self awareness



Keywords: Information Technology Management, Artificial Intelligence, Machine learning, Deep learning, Cybersecurity.

I. Introduction

Importance of cyber security in the digital world can't be understand. To understand why it is important to learn about cyber security you must first know how is solid cyber security system helps and products students, businesses, organisations and the banking sector.

Cyber security is important for students because they often target cyber attacks. In a recent cases, a group of students from a college in the United States targeted by the hackers who gained access to their personal information including their social security numbers and credit card information .The hackers then used the information to frequently charged thousands of dollars to the students credit cards. The students left with massive debt and had to spend months repairing their credit. If students personal information is stolen in a cyber attacks it could be used to commit identify theft.

Real life example of importance of cyber security for the banking sector is the 2014 JP Morgan chess data breach. in this breach hackers gained access to the names, address, phone number, and email address of 76 million households and 7 millions business to the account information including account number send 83 millions JP Morgan Chase customers. This breach highlights importance of cyber security for the banking sector as hackers were able to gain access to large amount of customer data. If this data had fallen into the wrong hands, it could have been used for identity theft or other malicious purposes.

In this paper, we propose to research on the following questions: What is the current status of research in this area? What are the major issues of AI in cybersecurity for business? Currently what kinds of AI techniques are useful in this area? What are the advantage and disadvantage for applying AI techniques in this field?

II. Analysis of Cyber Law in India

The Internet is a global communications infrastructure that provide facilities to the work of governments, corporations, educational institutions, and individuals worldwide. Its rapid expansion has led to an increase in criminal activity such as identity theft, hacking, pornography, credit card fraud, and the forged use of official documents.

To curb this growing problem, society needs a body of cyber law. Cybercrime in India increased by more than 5% from 2019 levels in 2021, as reported by the country's National Crime Records Bureau (NCRB). Cyber law is expanding to include virtually every facet of online wrongdoing. A legal framework for dealing with cybercrime is provided. Cyber law also encompasses any and all issues involving the internet as a subject of law.

The Information Technology Act of 2000 governs cyber law in India. It also establishes the definition of a critical information infrastructure. In 2008, the law was revised. India is among the select group of nations with e-commerce regulations. The government in India has taken measures to improve cyber security and establish India as a global hub for the coordination of efforts to combat cybercrime.

III. Benefits of AI in cybersecurity

A. AI can be a valuable tool

AI can be a valuable tool for strengthening an organization's cyber defence posture. AI's potential benefits in cybersecurity include the following:

Detecting, analysing and responding to security threats faster than traditional security tools.

a. Understanding an organization's networks and systems.
b. Analysing large amounts of data to detect unusual activity.
c. Suggesting options to address discovered vulnerabilities.

Perhaps the top benefit of AI in cybersecurity is levelling the playing field against attackers. Hackers and other bad actors typically have the most cutting-edge tools at their disposal. Organizations should want nothing less if they are to mount a good defence to keep pace with ever-changing threats." Adversaries have been using artificial intelligence tools for some time," said Larry Clinton, president of the cybersecurity trade association Internet Security Alliance. "If you're not doing that, then you are really at great risk of being subjected to sophisticated attacks -- more sophisticated than you may even imagine. "AI-driven security can help an organization move toward a more proactive, forward-looking risk posture, he said. AI tools can quickly and efficiently evaluate potential threats and recommend response options. Machine learning algorithms can also adjust their own behaviour over time, enabling better vulnerability management, more secure authentication and stronger defences against malicious bots."AI may be very helpful in determining how an adversary might attack you and which attempt is most likely to hit you," Clinton said. "So, the AI can certainly help with that kind of data analysis and forecasting. "An underappreciated benefit of AI is its ability to assess vulnerabilities in a hybrid or remote working environment, Vartanian said. Organizations' networks have expanded substantially due to the number of people working from home, which also creates security vulnerabilities. AI can help organizations deal with their growing security needs in response to employees working remotely, he said.

B. Drawbacks of AI in cybersecurity

Among the top drawbacks of investing in AI for cybersecurity is the expense of AI adoption efforts. With LLMs, for example, acquiring applications, integrating them into an organization's IT systems, and then monitoring and maintaining them will be a very expensive process, Vartanian said. Another significant drawback is that, at least for the foreseeable future, AI will be resource intensive. In addition to the underlying infrastructure, AI security models require extensive and diverse training data, as well as personnel who understand how to operate and maintain those models and software programs. "This is something to be watched carefully by CIOs, because we have a lack of enough people who really understand the technology," Vartanian said sufficient data, AI systems can produce incorrect monitoring results and false positives. And these risks can have real consequences for organizations. "Companies are being damaged by AI systems that are formally trained on bad data," Vartanian said. "That can lead to bias in the output, and bias in the output often leads to lawsuits and reputational harm. But most fundamentally, it can just lead to the wrong answer. "Because of these concerns, CIOs must consider AI in light of their organization's cybersecurity strategy, the anticipated costs and the potential rewards before implementation.

C. Current uses of AI in cybersecurity

Many organizations are currently in the experimental stage when it comes to AI, exploring its potential use cases for cybersecurity. One sector that has benefited from investments in AI is banking and financial services, where one promising use case is detecting money laundering, Vartanian said. It's impossible for a human to manually monitor millions of transactions for money laundering every day while simultaneously considering all applicable rules. But with AI models, organizations can identify previously undetectable patterns and monitor for suspicious behaviour at scale. "[Machines] track trends and suspicious activity in ways that human beings cannot begin to do," Vartanian said. Overall, organizations' investments in AI for cybersecurity are largely driven by two opposing impulses, Clinton said. The first is the fear of losing out, which pushes organizations to invest in new technologies so as not to be left behind by their competitors -- regardless of whether the organization is ready to adopt that technology. The second is caution about the potential unanticipated consequences of implementing AI. "Organizations are being pretty cautious about using AI in their cybersecurity because the unknowns are so enormous," Clinton said. "And the people who do cybersecurity tend to be a fairly cautious lot. "Moving forward, Clinton expects to see maturation with respect to the uses of AI tools in cybersecurity, especially LLMs. "ChatGPT, for example -- which is everywhere now -- is not very good for making decisions, but it's really good for generating options," he said. As AI platforms evolve, their decision-making capabilities will need to improve. For now, organizations can start by weighing AI's potential benefits for cybersecurity efforts against its overall business impact.

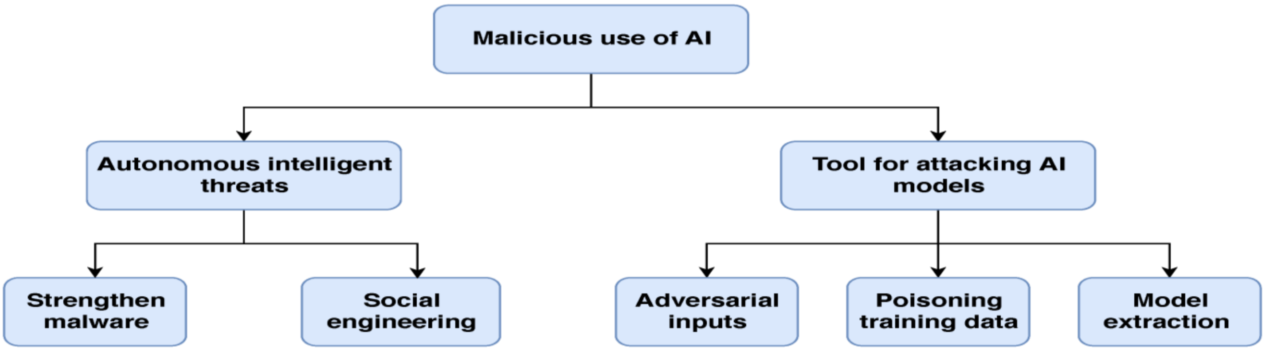
IV. AI Methodology for Cybersecurity

A. AI (Artificial Intelligence) — a broad concept. A *Science* of making things smart or, in other words, human tasks performed by machines (e.g., Visual Recognition, NLP, etc.). The main point is that AI is not exactly machine learning or smart things. It can be a classic program installed in your robot cleaner like edge detection. Roughly speaking, AI is a thing that somehow carry out human tasks.

B. ML (Machine Learning) — an *Approach* (just one of many approaches) to AI that uses a system that is capable of learning from experience. It is intended not only for AI goals (e.g., copying human behaviour) but it can also reduce the efforts and/or time spent for both simple and difficult tasks like stock price prediction. In other words, ML is a system that can recognize patterns by using examples rather than by programming them. If your system learns constantly, makes decisions based on data rather than algorithms, and change its behaviour, it’s Machine Learning.

a. Deep Learning

A set of *Techniques* for implementing machine learning that recognize patterns of patterns -• like image recognition. The systems identify primarily object edges, a structure, an object type, and then an object itself. The point is that Deep Learning is not exactly Deep Neural Networks. There are other algorithms, which were improved to learn patterns of patterns, such as Deep Q Learning in Reinforcement task.



Approaches to Solving ML Tasks

b.1 Supervised learning

Task Driven approach. First of all, you should label data like feeding a model with examples of executable files and saying that this file is malware or not. Based on this labelled data, the model can make decisions about the new data. The disadvantage is the limit of the labelled data.

b.2 Ensemble learning.

This is an extension of supervised learning while mixing different simple models to solve the task. There are different methods of combining simple models.

b.3 Current trends

b.3.1 Unsupervised Learning

Data Driven approach. The approach can be used when there are no labelled data and the model should somehow mark it by itself based on the properties. Usually it is intended to find anomalies in data and considered to be more powerful in general as it's almost impossible to mark all data. Currently it works less precisely than supervised approaches.

b.3.2 Semi-supervised learning

As the name implies, semi-supervised learning tries to combine benefits from both supervised and unsupervised approaches, when there are some labelled data.

VI. Future trends (well, probably)

A. Reinforcement learning. Environment Driven approach can be used when the behaviour should somehow react on the changing environment. It's like a kid who is learning environment by trial and error.
B. Active learning. It's more like a subclass of Reinforcement learning that probably will grow into a separate class. Active learning resembles a teacher who can help correct errors and behaviour in addition

to environment changes.

VII. Machine Learning tasks and Cybersecurity

Let’s see the examples of different methods that can be used to solve machine learning tasks and how they are related to cybersecurity tasks.

A. Regression

Regression (or prediction) is simple. The knowledge about the existing data is utilized to have an idea of the new data. Take an example of house prices prediction. In cybersecurity, it can be applied to fraud detection. The features (e.g., the total amount of suspicious transaction, location, etc.) determine a probability of fraudulent actions. As for technical aspects of regression, all methods can be divided into two large categories: machine learning and deep learning. The same is used for other tasks.

B. Machine learning for regression

Below is a short list of machine learning methods (having their own advantages and disadvantages) that can be used for regression tasks.

a. Liner regression
b. Polynomial regression
c. Ridge regression
d. Decision trees
e. SVR (Support Vector Regression)

VIII. Algorithm

A. Create Public Key

Select two prime no's. Suppose $P = 41$ and $Q = 57$.
Now First part of the Public key : $n = P*Q = 2337$.
We also need a small exponent say e :
But e Must be
An integer.
Not be a factor of $\Phi(n)$.
$1 < e < \Phi(n)$ [$\Phi(n)$ is discussed below],
Let us now consider it to be equal to 2.

B. Create Private Key

We need to calculate $\Phi(n)$:
Such that $\Phi(n) = (P-1)(Q-1)$
so, $\Phi(n) = 2240$
Now calculate Private Key, d :
$d = (k*\Phi(n) + 1) / e$ for some integer k
For $k = 2$, value of d is 2241.
Now we are ready with our – Public Key ($n = 2337$ and $e = 2$) and Private Key($d = 2241$)
Now we will encrypt **“MA”**:
Convert letters to numbers : $M = 13$ and $A = 9$
Thus Encrypted Data $c = (139e)\text{mod } n$
Thus our Encrypted Data comes out to be 252

Now we will decrypt 252
Decrypted Data = (cd)mod n
Thus our Encrypted Data comes out to be 139
13 = M and I = 9 i.e. "MA".

IX. Conclusion

In conclusion, artificial intelligence systems will continue to rise in importance and level of usage. Not only have the business applications been discussed, but personal use as well. These systems are growing and advancing past initial expectations, providing us with the inference that they will soon be more widely applicable and accessible to even the standard consumer. It is already used in our daily lives through the different organizations and entities that we trust our 2019 IEEE Technology & Engineering Management Conference (TEMSCON) information to, but we see this technology becoming more of a ‘household” item regarding personal, unprotected devices we all possess. While artificial intelligence research is currently taking place every single day, these studies will continue to grow in scope and size. The major issues regarding loopholes, innovative hackers, and losing that human element of interpretation will continue to diminish and become less noticeable as these systems become more advanced. Artificial intelligence is the base of today’s best anomaly detection systems and will expand into different sections of cyber-security as they develop. This new automation provides us terrific intrusion detection abilities while identifying false positives and using predictive analysis to keep information more safe online. With a wide range of neural networks, both ANN’s and DNN’s, and expert systems continuing to be released, the future for AI within cyber-security looks bright. This means that the future of the safety of our sensitive information looks bright as well.

Acknowledgement

The work is supported by Dr. S.P. Singh Faculty NIMS University.

References

1 Concanon, K., Williams, R., Feehan, D., Uvin, J., Yudin, M., Foster, D., … Monje, C. (2016). Federal Partnership regarding career pathways [PDF letter]. Retrieved from https://careerpathways.workforcegps.org/~/media/WorkforceGPS/careerpathways/Files/Career%20Pathways%20Joint%20Letter%202016.pdf

2 Conklin, W., Cline, R., & Roosa, T. (2014, March 10). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. Retrieved from http://ieeexplore.ieee.org/document/6758852/ Control-Alt-Hack(R). (n.d.). Retrieved from http://www.controlalthack.com/

3 Costanzo, J. (2017). Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (HRCyber) Mid-Project Report “Bridging the cybersecurity talent gap in Hampton Roads” [PDF]. Retrieved from http://securitybehavior.com/hrcyber/doc/HRCyber%20Mid-Project%20Report.pdf

4 Consortium Enabling Cybersecurity Opportunities and Research. (n.d.). K-20 Cybersecurity - CECOR Project . Retrieved from http://cset.nsu.edu/programs/k20cybersecurityCyberbit Protecting a New Dimension. (2017). Cyberbit Range The First Hyper-Realistic Simulation Platform for Cyber Security Experts [PDF]. Retrieved from https://www.infosecurityeurope.com/__novadocuments/362748?v=636315473978100000

5 Cyberbit Protecting a New Dimension. (n.d.). Retrieved from https://www.cyberbit.com/

6 Cybercops ®: Scholarship for Service. (n.d.). Retrieved from https://www.sfs.opm.gov/

7 Cybersecurity Enhancement Act of 2014, Pub. L. No, 113-274, 128 Stat. 2971. (2014). Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

8 CYBERSECURITY WORKFORCE DEVELOPMENT TOOLKIT How to Build a Strong Cybersecurity Workforce [PDF]. (n.d.). U.S. Department of Homeland Security. Retrieved from https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit

9 Cyber Security Capital We help cyber security professionals succeed. (n.d.). Retrieved from http://cybersecuritycapital.com

B. Cyberseek. (n.d.). Retrieved from http://cyberseek.org/

10 Cyber Competitions. (2017, May 19). Retrieved from https://niccs.us-cert.gov

11 Cyber Discovery | NICERC. (2016). Retrieved from https://nicerc.org/events/cyber-discovery/

12 Cyber Innovation Center. (2016). Retrieved from https://cyberinnovationcenter.org/

13 Cyber IN-security Strengthening the Federal Cybersecurity Workforce [PDF]. (2009, July). Partnership for Public Service and Booz | Allen | Hamilton. Retrieved from https://ourpublicservice.org

14 Cyber IN-security II Closing the Federal Talent Gap [PDF]. (2015, April). Partnership for Public Service and Booz | Allen | Hamilton. Retrieved from https://ourpublicservice.org

15 Cyber Space Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure [PDF]. (n.d.). U.S. Department of Homeland Security. Retrieved from https://www.dhs.gov

16 Dana, J. (2017, April 8). The Utter Uselessness of Job Interviews. The New York Times. Retrieved from https://www.nytimes.com/2017/04/08/opinion/sunday/the-utter-uselessness-of-job interviews.html

17 Security," arXiv [cs.CR], 27-Mar-2018. [30] W. Guo, D. Mu, J. Xu, P. Su, G. Wang, and X. Xing, "LEMNA: Explaining Deep Learning Based Security Applications," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018, pp. 364–379.

18 M. Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," arXiv [cs.AI], 12-Feb-2015.