International Journal of Research in Engineering, Science and Management
Volume-1, Issue-9, September-2018
www.ijresm.com | ISSN (Online): 2581-5782

Applying Artificial Intelligence Techniques to Prevent Cyber Assaults

Prabodhan Pradhan[1], Gorgi Pawar[2], Alpesh Pawar[3]
[1,2,3]*Student, Department of Computer Engineering, MGMCET, Mumbai, India*

***Abstract*—Cyber security ostensibly is the discipline that could profit most from the introduction of Artificial Intelligence (AI). It is tough to make software for defending against the powerfully developing assaults in systems. It can be cured by applying techniques of artificial intelligence. Where conventional security systems may be slow and deficient, artificial intelligence techniques can enhance their overall security execution and give better security from an expanding number of complex cyber threats. Beside the great opportunities attributed to AI inside cyber security, its utilization has legitimized risks and concerns. To promote increment the development of cyber security, a holistic perspective of associations cyber environment is required in which AI is consolidated with human knowledge, since neither individuals nor AI alone has proven overall success in this sphere. In this manner, socially mindful utilization of AI techniques will be needed to further mitigate related risks and concerns.**

***Index Terms*—Cyber security, Artificial Intelligence, Security intelligence, Cyber defense, Denial of Service, Self-Organizing Maps**

I. Introduction

To execute versatile and persistent protection, security system need to continually conform to changing environment, threats and actors involved in the digital play. Cyber reality, be that as it may, shows up to some degree distinctive. Security methodologies are routinely custom fitted to known assaults, and because of the absence of flexibility and robustness, security framework ordinarily can't adjust consequently to change in their encompassing. Indeed, even with human interaction, adaption processes are likely to be slow and insufficient. Due to their flexible and adaptable system behavior artificial intelligence techniques can help defeat different deficiencies of today's cyber security tools. Although AI has already significantly enhanced cyber security, there are likewise genuine concern. Some see AI as a developing existential hazard for mankind. Likewise, scientist and legal expert have expressed caution at the expanding role that self-governing AI substances are playing in the cyberspace and have raised worries about their moral reasonability. AI is proficient by concentrate how human brain thinks, and how people learn, choose, and work while attempting to tackle an issue, and after that utilizing the results of this review as a premise of creating intelligent software and systems. The motivation behind this work is to highlight the deficiencies of conventional security measures and additionally the advance that has been made so far by applying AI techniques to cyber security. Furthermore this works compresses the dangers and concern connected to this advancement, by investigating AI's existing conditions, tending to present concerns, sketching out heading for what's to come.

II. Application of Agent

A. *Software Agent*

An artificial agent which operates in a software environment. Software environments include operating systems, computer applications, databases, networks, and virtual domains.

Delegacy for software agents centers on persistence. "Fire-and-forget" software agents stay resident, or persistent, as background processes after being launched. By making decisions and acting on their environment independently, software agents reduce human workload by generally only interacting with their end-clients when it is time to deliver results. Additionally, autonomous automation can lead to super-human performance in terms of volume and speed.

Competency within a software environment requires knowledge of the specific communication protocols of the domain. Protocols such as SQL for databases, HTTP for the WWW, and API calls for operating systems must be preprogrammed into the software agents, limiting their useful range.

Amenability for non-intelligent software agents is generally limited to providing control options and the generation of status reports that require human review. Such agents often tend to be brittle in the face of a changing environment, necessitating a modification of their programming to restore performance.

III. Future Work Consideration

One must be aware of the difference between immediate goals and long term viewpoints, when predicting the future work and expansion and application of AI techniques in cyber assault prevention. Many AI techniques are relevant in cyber assault prevention, also there are many current cyber assault problems that need more sophisticated measures. One can observe utilization of totally new standards of knowledge dealing with decision making. These standards in the decision making software incorporate a modular and hierarchical knowledge architecture. To ensure fast circumstance evaluation that provide leaders a decision superiority and decision makers on any C2 level security is only provided by automated knowledge management. Expert systems are as of now being utilized as a part of numerous applications, its presence inside an application is sometimes hidden, same as the software like safety efforts planning software. If in future large knowledge bases will be created, expert systems will get more extensive application. For this purpose knowledge acquisition will require extensive investment, and large modular knowledge bases must be developed. The expert system innovation will require advancement further: in the expert system tools presence of modularity is must and also make use of hierarchical knowledge bases.

IV. Application of Artificial Intelligence

A. *Chatbots*

Artificial intelligence continues to be a hot topic in the technology space as well as increasing its inception into other realms such as healthcare, business, and gaming. AI-powered chatbots in enterprises will also see an influx of people get more comfortable with how AI can actually benefit businesses versus, say, take away their jobs. From an analytical standpoint, AI can be incorporated into interfaces to change how they receive and understand data.

Chatbots, in particular, are always on, delivering smart and flexible analytics through conversations on mobile devices using standard messaging tools and voice-activated interfaces. This dramatically reduces the time to collect data for all business users, thereby accelerating the pace of business and streamlines the way analysts use their time, preparing companies for the growing data needs of the near future.

B. *Artificial Intelligence in E-Commerce*

Artificial Intelligence technology provides a competitive edge to e-commerce businesses and is becoming readily available to companies of any size or budget. Leveraging machine learning, AI software automatically tags, organizes and visually searches content by labeling features of the image or video.

AI is enabling shoppers to discover associated products whether it is size, color, shape, or even brand. The visual capabilities AI is improving every year. By first obtaining visual cues from the uploaded imagery, the software can successfully assist the customer in finding the product they desire. Many e-commerce retailers are already becoming more sophisticated with their AI capabilities, and I only expect this to grow in the future.

C. *AI to Improve Workplace Communication*

Current business communication is overloaded with content, channels, tools, and so-called solutions, depriving individuals (and companies) from hitting targets while also harming work-life balance. Artificial Intelligence will help businesses improve communication internally and externally by enabling individual personalization for each professional, allowing for enhanced focus and increased productivity.

With such AI personalization, each individual will be empowered thanks to an intelligent virtual assistant, helping take care of mundane or repeatable tasks, save time by understanding your needs and goals, as well as recommend next-best-action to take…as to utilize time much more efficiently, without requiring any extra effort. In the short to long run, business processes will improve, innovation will grow as employees will clear their tasks, and stress may decrease

D. *Human Resource Management*

AI and Machine learning are going to drastically and irrevocably change how HR and recruitment work in every company and this is going to be awesome. In fact, HR is likely to be one of the first areas of business that will benefit from AI for two simple reasons. Firstly there are tons of top quality data in HR, and secondly, HR is one part of any company that is both essential and yet feels the pressure of time.

If aspects of the recruiting and HR job can be automated, the HR workers can have the freedom to directly work with people in the business or potential hires, spending the quality human time necessary for a great HR department. It might seem paradoxical but the more Artificial Intelligence a company deploys in HR, the more 'Human' a company it can be.

Artificial Intelligence will essentially take out all of the "worst" elements of every HR professional’s job (mundane screening, time-consuming paperwork, and annoying data entry) as well as deliver powerful tools and insights are a bonus to make their work better. HR's automatic generation of top quality data and the incredible benefits of AI make it one of the first places to experience the 4th industrial revolution.

E. *AI in Healthcare*

In the year ahead, and particularly in the next five to ten years, artificial intelligence is going to have a big impact on the healthcare industry and the ways in which healthcare related companies utilize AI. Here is a short note from Dr. Jeff Dunn, CEO of Redivus Health. Redivus Health is a transformative mobile app used by healthcare providers to prevent medical errors by offering both clinical decision support during critical medical events as well as documenting those events electronically in real time.

AI presents opportunities for our application to take the data we have gathered from patients and be able to clinically innovate to improve patient outcomes to an even greater extent. AI improves reliability, predictability, and consistency with quality and patient safety. For us, AI, as applied to software, is used as a decision augmentation tool, but it should not have free reign without human interaction and guidance. While it can’t replace doctors and nurses, it can make them more effective, efficient and happier on the job as it takes the cognitive burden off our providers – which increases confidence as well as reduces stress and anxiety.

V. Conclusion

Hence, artificial intelligence techniques helps to prevent cyber assaults. Also, it finds application in many fields

References

[1] E. Tyugu. Algorithms and Architectures of Artificial Intelligence. IOS Press. 2007.