Use of Artificial Intelligence to Prevent Cyber Attacks

Dr. Sumit Kumar Kapoor[1], Mr. Ajay Kumar Savita[2]
[1]*Associate Professor, Poornima University, Jaipur*
[2]*Associate Professor, Kanpur Institute of Technology, Kanpur*

Abstract: The Artificial Intelligence innovations are being used as the best answer to the cyber-attacks. The experts in the field are using AI, including its subset machine learning, to effectively combat these attacks. At present, security analysts use this technology to detect abnormal activities, thereby redeemable phase and decreasing overall business expenses. In the current digital landscape, with the widespread use of IoT and interconnected devices, cyber security experts face numerous challenges. The prevention of attacks, protection of vulnerabilities, and quick response to threats require holistic instruments. Nevertheless, even though traditional security systems are not up to the challenge or sufficient for the task at hand, AI methodologies can enhance general security strategies considerably and furnish robust protection from the increasing instances of advanced cyber threats. This study, therefore, focuses on exploring the use of artificial intelligence in concert with human reasoning to enhance cyber security. The main aim of the current research is to elucidate the work done so far in applying artificial intelligence techniques for countering cyber threats.

Keywords: Artificial Intelligence (AI), Security intelligence, Cyber defense, Cyber security.

I. INTRODUCTION

Artificial Intelligence (AI) refers to the human faculties of reasoning, understanding, pattern recognition, memory, decision-making, and learning through experience. It aims at replicating the capabilities of the human brain so that computers can perform these operations more effectively. Recent advancements in AI have greatly affected various fields of life, such as politics, journalism, game development, and the public sector. In political terms, use of AI has enabled the saving of resources, energy, and time in all electoral campaigns with the help of better targeting on specific demographics. Cyber-attacks are also the biggest threats for governmental bodies, businesses, and other organizations. These concerns are better reflected by such occurrences as data breaches against the FBI and Department of Homeland Security that have made the details of almost 200 million personal records publicly accessible, with significant leaks among them. In recent times, focus is placed on developing an AI system which understands human behavior and can predict them. Advances in this area, however, have been slow and restricted. The international market for cyber security has expected to spread 170 billion by 2020 according to Forbes. This growth comes along with technology trends and continuous evolution of security requirements. Under this development, AI and cyber security integration has gained acceptance. Cyber security is found to be most effective using AI capabilities for defending and protecting digital information [10][11]. AI is a very powerful ally in combating threats since it can be trained to identify and learn patterns to detect even slight deviations.

Machine learning is one of the crucial components of AI, using data collected to continue improving its functionality and creating prevention strategies for potential attacks. Its capability to know user actions, identify patterns, and anomalies positions AI at the helm to address cyber security challenges. Furthermore, artificial intelligence possesses the capability to formulate its own strategies and functionalities derived from the data it collects. Ultimately, the primary aim of artificial intelligence is to facilitate intelligent operation of computers and machines. Within the context of cyber security, artificial intelligence can serve as an instrument for swiftly and precisely detecting emerging vulnerabilities, thereby reducing the risk of potential attacks. Through the automation of specific tasks, artificial intelligence eases the pressure on human security personnel, who are often faced with extreme pressures and tend to make mistakes. An intelligent automation-driven cyber security framework allows machines to handle most of the laborious activities, and only notifies human agents when necessary. This approach enables security personnel to utilize their time and expertise more efficiently. This research highlights the limitations of conventional security mechanisms and evaluates

the progress made in combating cyber threats through artificial intelligence techniques [6][7].

II. APPLICATIONS OF ARTIFICIAL INTELLIGENCE

The development of artificial intelligence is changing numerous sectors, and experts predict the global market of AI and robotics to be $153 billion in 2020. The benefits of AI are very multifaceted; it not only saves money but also keeps time, increases correctness, and productivity. It has been remarkable in the progress made in AI development, with Google estimating that robots will possess human-level intelligence by 2015, resulting in the replacement of one-third of jobs by robots and other intelligent machines [2].

A. AI in Healthcare Companies

AI in Healthcare Companies are placing their bets on AI to improve patient outcomes and reduce costs in healthcare. Machine learning is used to make diagnoses more rapidly and accurately than is possible for humans. A major health technology company is IBM Watson, which is capable of interpreting regular language and producing responses to queries. The system evaluates patient data and other pertinent information to generate hypotheses, accompanied by a confidence scoring mechanism. Additionally, AI applications in healthcare include chatbots—computer programs designed to assist users and answer queries online. These tools help schedule follow-up appointments and guide patients through the billing process. Virtual health advisors also offer basic medical insights [1].

B. AI in Business Robotic process

Robotic process computerization is increasingly being functional to automate jobs that are highly repetitive in nature but conventionally carried out by human workers. Machine learning algorithms incorporated into analytical frameworks and customer relationship management (CRM) systems enable organizations to derive insightful information regarding the optimization of customer service. Chatbots have made it possible for websites to offer instant customer support. Automation of job roles has generated considerable debate among scholars and information technology analysts.

C. AI in education

AI might take the grading tedium away from the educator's hands, freeing up some time for other activities. It can keep track of the students and adjust to their needs, which ensures proper learning for a student at whatever pace he or she learns. The use of AI tutors helps students stay on track. Future changes in the way students learn might replace teachers with AI.

D. AI in finance

Artificial Intelligence is fundamentally transforming the financial sector via its utilization in personal finance applications, including platforms such as Mint and TurboTax. These tools gather user-specific data to provide tailored financial guidance. Additionally, IBM Watson has been employed to facilitate the home-buying experience. Currently, a considerable share of trading activities on Wall Street is carried out by software.

E. AI in law

The discovery and document sifting in the legal field can be very exhaustive for human beings. The best use of time would thus be to automate these processes using AI technologies. Startups are developing question-answering computer aides capable of analyzing database taxonomy and ontology to respond to predefined queries.

F. AI in manufacturing

Manufacturing has been the leader in introducing robots to workflows. Industrial robots were initially applied for single tasks and kept separate from human workers, but technological advancements have changed this situation.

G. AI in Cyber Security

Artificial Intelligence can be a valuable ally in the fight against cyber security threats. It can be accomplished to continuously identify and study patterns, thus providing a line of defense against hackers [9].

III. ADVANTAGES OF ARTIFICIAL INTELLIGENCE

Many different threats are presented to an organization every day, which makes it unmanageable to try to examine and classify each of them. However, this is not an impossible task when using Machine Learning proficiently. When exploring unsupervised and supervised machine

learning techniques, we can take full advantage of our current understanding of threats and vectors. Our systems will be significantly enhanced in terms of protection against threats when joint with the capacity to identify novel attacks and uncover new susceptibilities, thereby bringing about improved efficiency.

A. Error Reduction
It is commonly used in the form of minimization of risk and increased accuracy by a significant degree of precision in artificial intelligence.

B. Difficult Exploration
The integration of artificial intelligence and robotics in fields such as mining, fuel exploration, and complex oceanic research has surpassed the limitations associated with human capabilities.

C. Daily Application
Artificial intelligence has become increasingly ubiquitous in daily life, with financial and banking institutions widely using it to process and control data. It is also used for the recognition of fraudulent transactions in smart card-based systems [8].

D. Digital Assistants
Advanced organizations employ digital assistants, known as avatars, which interact with users and reduce the need for human staff. Unlike humans, machines are not influenced by emotional conditions or moods, ensuring that decisions are made fairly and with maximum productivity.

E. No breaks
Long-term operating machines do not have the need for frequent breaks or snacks, allowing them to work uninterruptedly without feeling bored [4].

F. Increase Work Efficiency
AI-powered machines perform well in repetitive tasks, where human errors are eliminated and accurate results are achieved.

G. Reduce cost of training and operation
Artificial intelligence uses deep learning and neural network algorithms, allowing machines to learn like humans, without the essential to rewrite program [5].

IV. FUTURE OF CYBER-SECURITY USING AI

Cyber-attacks have become a huge threat to businesses, governments, and institutions in today's world. In 2016, data breaches exposed over 200 million personal records, affecting major entities such as the Department of Homeland Security and the Federal Bureau of Investigation (FBI). It should be noted that 99 percent of these incidents exploited vulnerabilities that had already been identified. Unfortunately, our current reliance on firewalls as a means of protection is insufficient, because determined attackers can bypass them. Currently, only humans, to my knowledge, plan to predict the actions of other humans before those actions come into existence [3].

When discussing Artificial Intelligence, people tend to automatically relate it to movies such as Terminator and SkyNet. My response to the movie Terminator was very melodramatic and I had torn clothes and wore adult diapers for some time because of flashbacks. Therefore, one can imagine the tremendous work involved in traversing my first response after recently learning about Artificial Intelligence (AI) and Machine Learning (ML). The impression of AI and ML has touched every industry, and cyber security is no exception. A number of cyber security companies, ranging from new startups to established companies, have started developing products that leverage AI to enhance data protection for their customers. Regardless of the industry, whether it's AI mobile applications or blockchain technology, cybersecurity is an integral part of both, with AI greatly adding to its effectiveness. [13].

V. CONCLUSION

Artificial intelligence is now finding its place as a tool for the enhancement of security models for organizations and individuals alike. However, at the same time, it has also become much more accessible for the bad actors. Only through the custody of ethical practitioners will Artificial Intelligence be assured to be used only for security purposes by trusted persons. Even though Artificial Intelligence has unmatched speed and cognitive capacity, it still requires humans to function effectively. Therefore, organizations should focus on the need to recruit and develop AI professionals who will effort together with the technology for product security. This will undoubtedly help the cause of fighting cybercrime. In conclusion, Artificial Intelligence is

increasingly playing a very pivotal role in organizational network and data protection. And as these technologies, namely machine learning, AI, and intelligent automation, are developed further, organizations will need to remain abreast in terms of adoption in order to remain one step ahead of cybercriminals.

REFERENCES

[1] Imtiyaz Hassan, Designing a flexible system for automatic detection of categorical student sentiment polarity using machine learning, International Journal of u- and e- Service, Science and Technology, vol. 10, no.3, Mar 2017, pp. 25-32, doi: 10.14257/ijunesst.2017.10.3.03, ISSN: 2005-4246.

[2] Syed Imtiyaz Hassan, NabaSuroor. Identifying the factors of modern day stress using machine learning, International Journal of Engineering Science and Technology, vol. 9, Issue 4, April 2017, pp. 229-234, e-ISSN: 0975–5462, p-ISSN:2278–9510.

[3] Hernándeza, Á.B., (2018). Using machine learning to optimize parallelism in big data applications, Future Generation Computer Systems, 86, 1076- 1092.

[4] J. Beal, P. H. W inston, Guest Editors' Introduction: The New Frontier of Human-Level Artificial Intelligence, Intelligent Systems, IEEE 24.4: 21-23,2009.

[5] Irani, Z. (2017). Critical Analysis of Big Data Challenges and Analytical Methods, Journal of Business Research, 70, 263-286.

[6] S. Russell, P. Norvig. Artificial Intelligence: fashionable Approach,2000.

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

[8] C2-level Security, [Online: Available], https://msdn.microsoft.com/enus/library/windows/desktop/aa376387 (v=vs.85).aspx.

[9] Syed Imtiyaz Hassan, Extracting the sentiment score of customer review from unstructured big data using Map Reduce algorithm, International Journal of Database Theory and Application, vol. 9, issue 12, Dec 2016, pp. 289-298, doi: 10.14257/ijdta.2016.9.12.26, ISSN:2005-4270.

[10] Frivold, Anderson, Valdes, Next- Generation Intrusion Detection Expert System(NIDES).

[11] S. Alghamdi, B. Iftikhar. Application of artificial neural network within the detection of dos attacks, 2009.