ARTIFICIAL INTELLIGENCE FOR CYBER SECURITY

Bhargav Ambati[1], Sumanth Pagadala[2], Rohini mote[3]

[1]UG Student, Dept of Electronics & Communication, KG Reddy college of Engineering & Technology and Stanley college of Engineering & Technology for women, Telangana, India
[2,3]UG Student, Dept of Computer Science, KG Reddy college of Engineering & Technology and Stanley college of Engineering & Technology for women, Telangana, India

---***---

Abstract - *In this advanced world, with the upheaval of IoT and connected gadgets, network protection specialists face plenty of experiences. The specialists need all the assistance to forestall assaults and security breaks and react to the assaults. The number of connected working environments leads to weighty traffic, greater security assault vectors, security penetrates, and lots more that the digital territory can't be taken care of by people while not sizeable robotization. It has ended up being obvious that various network safety issues are also settled with progress just systems of computerized reasoning region unit securing used.*

Digital protection processing applications and investigations the perspectives on improving the network safety capacities by proposing artificial intelligence applications and the all around existing techniques.

Key Words: Artificial-intelligence, Cyber security, Cyber Threats, Data mining

1. INTRODUCTION

The day-to-day raising and progressing cyber security threat facing global businesses can be reduced by the integration of Artificial Intelligence into cyber security systems. Machine learning and Artificial Intelligence (AI) are being connected more extensively over industries and applications than at any other time in recent memory as computing power, storage capacities, and data collection increase. This vast measure of information can't be dealt with by people progressively. With machine learning and AI, that peak of data could be carved down in a fraction of time, which helps the enterprise to identify and recover from the security threat.

2. APPLYING AI TO CYBER SECURITY

Data have been generated in today's world is increasing and the information stored or received in any form, whether directly or indirectly, through the Internet. Moreover, the data have to be sent over a network to receive it in a destination due to proper transmission of data plays a vital role in combating cyber-crimes, which is achieved through principles of cyber security. With the growing advancements in Information Technology, criminals are using cyberspace to commit various cyber-crimes, which later creating a considerable disruption in the cyber society. [1]

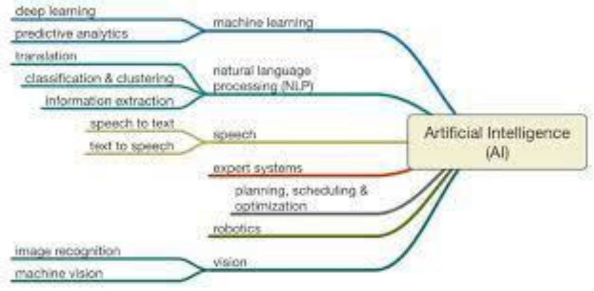

Fig. 1. Areas and Applications of AI

AI and cyber security are broad terms, and we can use it both in organizations to mitigate risks and increase revenue by detecting cyber threats and fraud. However, keeping up with new viruses and malware updates is becoming more difficult, cyber security using artificial intelligence technologies will facilitate the detection and response to threats and malware by using previous cyber-attack data to determine the best course of action.

AI may often be better and more effective than humans in detecting malicious malware. AI is implemented in the organization with multiple security solutions such as Security Information, and Event Management helps security analysts for any threats inside the network of the organization to improve detection. [2]

"The faster the data breach was identified and contained, the lower the costs. This year, the increasing time to resolve a breach was potentially due to the increasing severity of criminal and malicious attacks experienced by a majority of companies. Security automation and intelligent orchestration capabilities that provide visibility across the security operations center can help improve an organization's ability to contain the damage from a breach".

These applications are trained by using a database of previous behaviors and identify each behavior as malware or not. According to IBM, the cost of a data breach worldwide will be reduced if organizations deployed automated security solutions.

"Organizations that had not deployed security automation experienced breach costs that were 95 percent higher than breaches at organizations with fully-deployed automation". [3]

AI in CyberSecurity
Faster Detection
Phishing Detection
Behavioural Analytics
Network Security
Secure Authentication
Preventing Online Frauds

Fig. 2. AI in Cyber security

Many types of AI applications are used in cyber security solutions, as mentioned SIEM, spam filter applications, secure user authentication, and hacking incident forecasting. [4]

2. MACHINE LEARNING APPLICATIONS IN ARTIFICIAL INTELLIGENCE

“Machine learning is a subfield of Artificial Intelligence that allows a computer to learn using sample data without being programmed to anticipate every possible situation”. “The two most common types of machine learning are supervised and unsupervised learning. Supervised learning is used when a dataset of labeled instances is available, and to solve classification problems.

The goal of supervised learning is to train the computer to learn to predict a value or classify an input instance accurately. Unsupervised learning is used when a labeled dataset is not available. Clustering is an unsupervised learning technique that results in similar grouping instances in clusters. Clustering is used to discover patterns in data. In some cases, clustering is performed to classify an unlabeled dataset and using the resulting classified dataset for supervised learning”.[5]

As the threats of cyber security are continually changing and evolving, an automated and immediate response is required. Therefore, machine learning methods, especially deep learning that does not necessarily require previous training or reliance on previous classifications provided by experts, maybe particularly vital as an application of AI approaches to cyber security.

In the following paragraphs, we review an applied case for employing machine learning to enhance cyber security before it is addressed in an independent component of deep learning as a distinct and vital type of machine learning that can contribute effectively to cyber security.

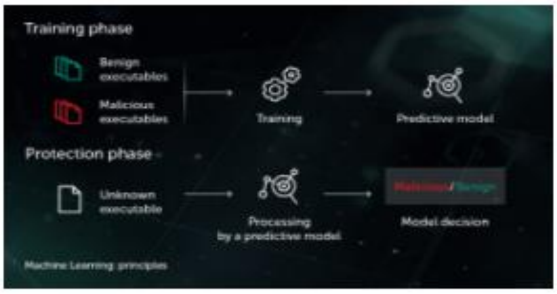

Fig. 3. ML in Cyber security

The study aimed to verify the effectiveness of machine learning methods for cyber security purposes. This study involved applying machine learning methods to identify intrusions, malware, and spam. Emphasis was placed on the effectiveness of machine-based solutions and their major disadvantages that prevent the direct adoption of machine learning methods in cyber security. [6]

3. RECOMMEND SOLUTION

This study was applied to utilize a scientific and graphic exploration approach of writing and past investigations. The outcomes demonstrated the chance of utilizing AI, profound learning, and information digging techniques for network safety purposes in three primary zones: interruption recognition, malware examination, and spam detection.

The results additionally showed that numerous shortcomings limit the viability of utilizing AI strategies for cyber security purposes to such an extent that all passages utilized are liable to counter assaults and require steady re-evaluating and cautiously change boundaries that are trying to computerize.

Additionally, chiefly when similar work is applied to distinguish various dangers, the presentation of the assurance is inadmissibly low, which might be overwhelmed by utilizing distinctive machine-based exercise manuals to recognize explicit dangers.

Additionally, AI is still at a beginning phase, and no end can be reached in regards to its viability for network safety purposes. Significant upgrades might be normal, particularly those that consider contemporary and promising advancement of what is known as ill-disposed learning.

The job of profound learning, particularly unattended, is fundamentally emerging as perhaps the most conspicuous sorts of AI that can add to upgrading cyber security.

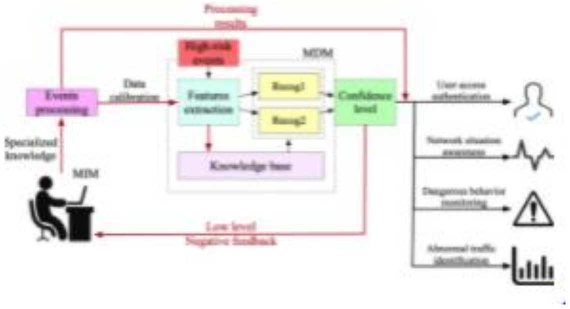

Fig. 4. Processing of Cyber security

There are numerous advantages to online protection frameworks dependent on profound learning calculations, for example, diminishing the measure of manual exertion to distinguish designs in suspicious conduct and the capacity to improve network safety execution better. [7]

Information mining has methodologies and calculations to recognize malware and we need to consider which system will be compelling to distinguish malware from a gigantic arrangement of data that relies upon comparable highlights.

Every one of information mining techniques has various necessities like peculiarity identification, abuse discovery, and crossbreed election. Also, information mining calculations can perform on every procedure except a portion of these calculations has strength and restriction.

Calculations utilized in malware locations are Choice Tree Learning, Innocent Bays Classifier (NB), K-Closest Neighbor, and Backing Vector Machine. A portion of these calculations has a basic restriction referenced underneath [8]:

- Complexity of calculations
- Extensive memory necessities
- High computational exertion

Malware innovations are built up every day and information mining calculations these days can distinguish malware and arrange it. In any case, it is basic to grow new information mining calculations to be quick and adaptable to distinguish and order malware.

3. CONCLUSIONS

From the above, the most relevant results of the present research paper can be drawn as cyber security is a critical and vital topic for protecting data, information, and systems. Moreover, many areas and applications of artificial intelligence can contribute to enhancing cyber security, such as machine learning, deep learning, data mining, and expert systems. The possibility of utilizing data mining algorithms to develop and support cyber security.

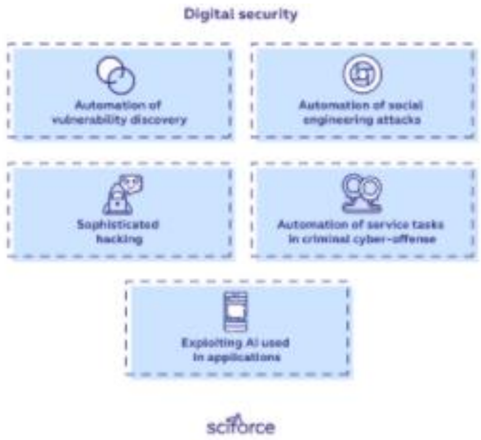
Digital security
Automation of vulnerability discovery
Automation of social engineering attacks
Sophisticated hacking
Automation of service tasks in criminal cyber-offense
Exploiting AI used in applications
sciforce

Fig. 5. Digital Security

REFERENCES

[1] Kamtam, A., Kamar, A., Patkar, U. C. (2016) Artificial Intelligence approaches in Cyber Security. International Journal on Recent and Innovation Trends in Computing and Communication.

[2] IBM Radar Security Intelligence. https://www.ibm.com/security/security-intelligence/qradar

[3] IBM Security (2019) Cost of a Data Breach Report IBM Security. https://databreachcalculator.mybluemix.net/executive-summary

[4] NormShield Cyber Risk Scorecard (2019) Cyber Security with Artificial Intelligence in 10 Question — NormShield Cyber Risk Scorecard. https://www.normshield.com/cyber-security-with-artificial-intelligencein-10-question/

[5] Alpaydın, Ethem. Introduction to machine learning.

[6] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., Marchetti, M.(2018, May). On the effectiveness of machine and deep learning for cyber security.

[7] Atlam, H., Walters, R. and Wills, G. (2018).Intelligence of Things: Opportunities and Challenges. [eBook] University of Southampton, p.4. Available at: https://www.researchgate.net/publication/325295863 Intelligence of Things Opportunities Challenges

[8] Masud, M., Khan, L. and Thuraisingham, B., 2016.Data mining tools for malware detection. Auerbach Publications.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press. K. Elissa, "Title of paper if known," unpublished.

BIOGRAPHIES

Ambati Bhargav
Student
Dept of Electronic & Communications
KGRCET

Sumanth Pagadala
Student
Dept of Computer Science
KGRCET

Rohini mote
Student
Dept of Computer Science
SCETW