IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

MACHINE LEARNING IN CRYPTOGRAPHY

Rajesh kulkarni

H.o.D computer science

HCES BCA college Gadag

ABSTRACT

Cyber security is a critical part of any company. Not only companies but even governments need top-class cyber security to make sure that their data remains private and is not hacked or leaked for all the world to see, And with the increasing popularity of Artificial Intelligence and Machine Learning, these technologies are even becoming key players in the field of cyber security. ML has many applications in Cyber Security including identifying cyber threats, improving available antivirus software, fighting cyber-crime that also uses AI capabilities, and so on. Therefore, Machine Learning based cyber security software is fast becoming a necessity and not only a luxury .This paper review role of machine learning in cryptography

Keywords : ML,cryptography,cybersecurity,technology

Introduction of ML

Machine learning is a branch of artificial intelligence that aims to allow machines to do their jobs skillfully using intelligent software. Statistical learning methods form the backbone of intelligent software used to develop artificial intelligence. Today, the demand for machine learning has increased dramatically with the large number of datasets available. The acquisition of mechanized knowledge from gaining experience using computational methods is machine learning. Domain-specific knowledge is required through expert performance, and some professional AI systems have been created through knowledge engineering. Its regular use has been observed in industry in various fields. Due to the increase in the use and applicability of machine learning, a systematic review of various relevant aspects has been presented in this paper. The paper begins with a brief description of machine learning and the use of machine learning in various applications. It was also featured in the full review. We also looked at

different works done by different researchers in different fields of application. It covers the use of machine learning in healthcare, social media, travel, and robotics. The main focus of its popularity in various applications is its ability to learn once and then work automatically for any type of data or input given to it.

KEYWORDS: ML, automatic, data, cyber security, crypto currency

WHY ML IS IMPORTANT

Machine learning is important part of day today's life. Machine learning is important because it allows companies to understand trends in customer behavior and business operating models, and supports the development of new products. Many leading companies today, such as Facebook, Google, and Uber, use machine learning as a core part of their operations. Machine learning has become an important competitive advantage for many companies.

Machine Learning in cyber security

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data against cyber attacks. It aims to reduce the risk of cyberattacks and protect against unauthorized exploitation of systems, networks and technologies. Cyber security is the safe and responsible use of information and communication technology. It's about keeping information secure but also about taking responsibility for it, respecting others online, and using Internet etiquette.

Machine learning has become an important technology for cyber security. Machine learning pre-empts cyber threats and strengthens security infrastructure through pattern detection, real-time cybercrime mapping, and in-depth penetration testing.

In May 2017, a terrible cyber attack hit more than billion computers in 150 countries. After a successful break-in, a computer scientist encrypted the files on this computer and made them unreadable. To recover trapped hardware, attack targets are told that they must purchase special decryption software. Other forms of cyber intrusion, such as"cryptojacking," are more efficient and less damaging, but still expensive. Crypto jacking is a technique by which cybercriminals distribute malware to multiple computers or servers. This attack takes control of a machine's processing power to mine crypto currency - a process that devours both computing power and electricity - and then sends that crypto currency back to the perpetrator. Even leading companies with robust cyber security protocols are not immune.

Malicious hacks v. machine learning

But in 2018 alone, there were 10.5 billion malware attacks. That's too much volume for humans to handle. Fortunately, machine learning is picking up some slack.

Machine learning uses algorithms from previous data sets and statistical analyzes to make assumptions about computer operations. The computer can then adjust its actions - and even perform functions for which it has not been explicitly programmed. And that's a boon for cybersecurity. With the ability to sort through millions of files and identify potentially dangerous files, machine learning is increasingly being used to spot threats and automatically overwrite them before they can wreak havoc. Microsoft's software is said to have done just that in early 2018. According to the company, the cybercriminals used the Trojan to attempt to "install malicious cryptocurrency miners on hundreds of thousands of computers."In addition to early threat identification, machine learning is used to scan for network vulnerabilities and automate responses.

Cyber Threat Identification

Cybersecurity is a very important component of all businesses. After all, if a hacker gets into their system, they'll toast! The hardest part of cybersecurity is determining if requests to log into the system are legitimate and whether any suspicious activity, such as receiving and sending large amounts of data, is being performed. by experts in certain business fields or cyberthreats. This is difficult to determine for cybersecurity professionals, especially in large organizations where requests always number in the thousands and people are not always accurate. This is where machine learning can be of great help to professionals. The AI and ML-powered Cyber Threat Identification System can be used to monitor all outgoing and incoming calls as well as all system requests to monitor suspicious activity. For example, Versive is an artificial intelligence vendor that offers cybersecurity software combined with AI.

Threat Detection and Classification

Machine learning algorithms are used in applications to detect and respond to attacks. This can be achieved by analyzing large data sets of security events and identifying patterns of malicious activity. ML works in such a way that when similar events are detected, they are automatically handled by the trained ML model. For example, a dataset can be generated to populate a machine learning model using Indices of Compromise (IOC). These can help track, identify, and react to threats in real time. ML classification algorithms can be used using the IOC dataset to classify the behavior of malware. One example of such use is evident in a report by Darktrace, an ML-based corporate immunity solution, which claimed to have prevented attacks during the WannaCry ransomware crisis.

Future of Machine Learning and Cyber security

Machine learning is still a relatively new addition to cybersecurity. However, the above 5 applications of machine learning in cybersecurity are a good start in the field. The only thing to keep in mind is that machine learning algorithms should minimize their false-positive actions, that is, actions they identify as malicious or part of a cyberattack, but not so. Businesses should make sure to consult with their cybersecurity experts who can provide the best solutions to identify and manage new and different types of cyberattacks, even even more precisely through machine learning.

References

 Mitchell, Tom (1997). Machine Learning. New York: McGraw Hill. ISBN 0-07-042807-7. OCLC 36417892.

  The definition "without being explicitly programmed" is often attributed to Arthur Samuel, who coined the term "machine learning" in 1959, but the phrase is not found verbatim in this publication, and may be a paraphrase that appeared later. Confer "Paraphrasing Arthur Samuel (1959), the question is: How can computers learn to solve problems without being explicitly programmed?" in *Koza, John R.; Bennett, Forrest H.; Andre, David; Keane, Martin A. (1996). Automated Design of Both the Topology and Sizing of Analog Electrical Circuits Using Genetic Programming. Artificial Intelligence in Design '96. Springer, Dordrecht. pp. 151–170. doi:10.1007/978-94-009-0279-4_9.*

  Hu, J.; Niu, H.; Carrasco, J.; Lennox, B.; Arvin, F., "Voronoi-Based Multi-Robot Autonomous Exploration in Unknown Environments via Deep Reinforcement Learning" IEEE Transactions on Vehicular Technology, 2020.

  Bishop, C. M. (2006), Pattern Recognition and Machine Learning, Springer, ISBN 978-0-387-31073-2

  Machine learning and pattern recognition "can be viewed as two facets of the same field."[4]: vii

  *Friedman, Jerome H. (1998). "Data Mining and Statistics: What's the connection?". Computing Science and Statistics. **29** (1): 3–9.*

  "What is Machine Learning?". www.ibm.com. Retrieved 2021-08-15.

  Zhou, Victor (2019-12-20). "Machine Learning for Beginners: An Introduction to Neural Networks". Medium. Retrieved 2021-08-15.

  Domingos 2015, Chapter 6, Chapter 7.

  Ethem Alpaydin (2020). Introduction to Machine Learning (Fourth ed.). MIT. pp. xix, 1–3, 13–18. ISBN 978-0262043793.

  *Samuel, Arthur (1959). "Some Studies in Machine Learning Using the Game of Checkers". IBM Journal of Research and Development. **3** (3): 210–229. CiteSeerX 10.1.1.368.2254. doi:10.1147/rd.33.0210.*

R. Kohavi and F. Provost, "Glossary of terms," Machine Learning, vol. 30, no. 2–3, pp. 271–274, 1998.

Gerovitch, Slava (9 April 2015). "How the Computer Got Its Revenge on the Soviet Union". Nautilus. Retrieved 19 September 2021.

*Lindsay, Richard P. (1 September 1964). "The Impact of Automation On Public Administration". Western Political Quarterly. **17** (3): 78–81. doi:10.1177/106591296401700364. ISSN 0043-4078. S2CID 154021253. Retrieved 6 October 2021.*