PalArch's Journal of Archaeology of Egypt / Egyptology

"A COMPARATIVE STUDY ON CYBER SECURITY TECHNIQUES USING MACHINE LEARNING"

Dr. Gayathri Edamadaka[1], Dr. Smitha Chowdary.CH[2], Dr. M. Sobhana[3], M. V. B. T. Santhi[4]
[1]Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur,AP, India
[2]Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India
[3]Senior Assistant Professor.V.R.Siddhartha Engineering College.
[4]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur,AP, India.
gayathri.edamadaka@kluniversity.in[1], smitha@kluniversity.in[2], santhi_ist@kluniversity.in[4]

Dr. Gayathri Edamadaka, Dr. Smitha Chowdary.CH, Dr. M. Sobhana, M. V. B. T. Santhi, A COMPARATIVE STUDY ON CYBER SECURITY TECHNIQUES USING MACHINE LEARNING, -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x

Keywords: Cyber Security; Machine Learning.

ABSTRACT
In several areas of research, the basic characteristics of machine learning technology such as adaptability, scalability and the ability to react quickly to real and unforeseen problems were introduced. Cyber security is a quickly evolving field that demands tremendous effort, as social media, the Internet, web computing, online banking, the world of smartphones, smart grids, etc. have made unbelievable strides. This paper discusses the use of machine learning in computer defense, including cyber-attack statements targeted at machine learning models, as a defensive and offensive contributor. Machine learning systems are particularly addressed in the case of cyber challenges as intelligent botnets, intelligent spear fishing, and prevention of malware. We also illustrated the use of computer safety learning devices to recognize and prevent vulnerability, track and diagnose malware as well as to determine network threats.

1.0 INTRODUCTION
The planet continues to be a top priority for the accelerated numeration of intelligence defense. As network technology improvements such as the Internet, modern technologies and research findings are made available, scholarly articles are

published each day, and the world's biodiversity is becoming more and more accessible. The computer scientists and cyber criminals who are involved in the use of these instruments and information unfortunately have state-of-the-art analyses and developments in technology. In order to identify and counter cyber risks decisively, researching and progressing machine learning resulted in algorithms and technologies. However, because of their unique features such as adaptability, scalability and ability to quickly adapt to new, unknown problems, this enables the application of this knowledge in machine-learning approaches in many disciplines. Cyber security is a growing area that needs a great deal of focus due to phenomenal advances in social networks, cloud and internet infrastructure, online banking, smartphone, smart grid, and so on. Machine Learning is efficiently implemented in order to solve some of the problems AI (see Figure 1)

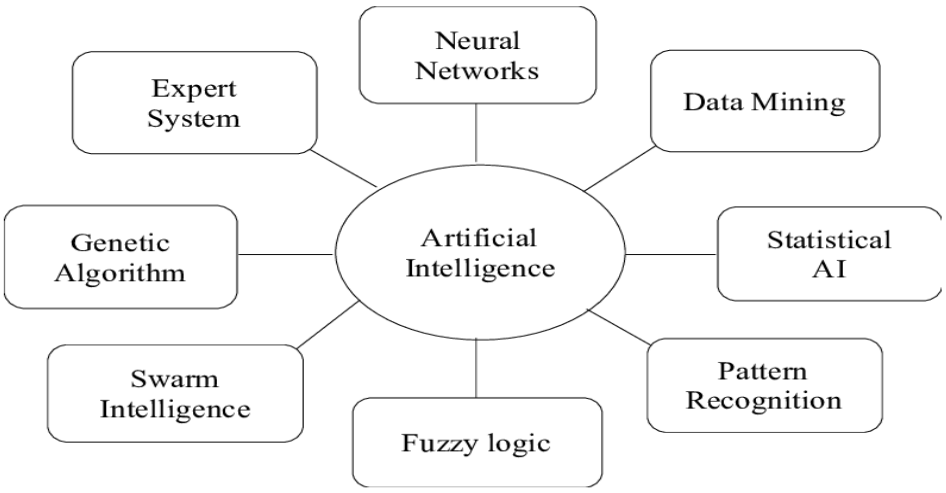

Figure 1: Artificial intelligence branch

Various machine learning approaches have been applied extensively to deal with certain large-scale information security issues.

1.1 Applications of machine learning in cyber security:

Studies are focused on machine learning and its vast range of tools and strategies for the identification, avoidance and reaction to advanced cyber assault. Built on cyber security science, analytical approaches to challenging detection and response can be extended to many fields. It can also improve safety processes by automating recurring tasks and making semi-automatic tasks easier for security analysts to function quickly.

2.0 LITERATURE REVIEW:

L. Zomlot, S. Chandran et al, [1] One special environment for machine learning is the field of cyber crime and security that has numerous implementations such as ransomware and log processing of machine learning. Cyber criminals and technology professionals harness the potential of machine learning. Now we explore how cybercrime and cyber defence use machine learning.

S. Dolev and S. Lodha [2] Machine-learning can be utilised by reviewing historical cyber-attack data sets and evaluating which parts of networks often engaged in those kinds of attacks to simplify this process. It is beneficial to use machine learning, because the results are focused not only on technical knowledge of the networks but, most significant, on data-driven values. G. A. Wang, M. Chau[3] This is the

same technology that moves vehicles and devices that detect and clear obstacles. Machines are able to recognise objects in photographs and can thus be programmed to overcome the captcha scheme that depends on the user to recognise the things in an image before authorisation.

3.0 APPLICATIONS OF MACHINE LEARNING IN CYBER CRIME

Studies have shown that cyber attackers can use tech education to create intelligent ransomware, which can outsmart existing wit security mechanisms. As the machine learning world is fast moving and offers groundbreaking cyber security strategies, cyber criminals also use it to perform more sophisticated operations. All but security specialists and cyber criminals employ modern inventive IA technology actively in addition to their arsenals of electronic weapons. Since cyber security professionals are continuously evaluating the data to better determine an attacker's behaviours, attackers frequently rob user data and analyse them in order to make their attacks more successful. For instance. For starters, illegal e-mails can be looked at and analysed by target users so that their e-mail behaviours are known and used to produce better e-mails. Such popular categories of machine learning based on attacks are:

Unauthorized access: Programming preparation will include unauthorised access to programmes such as captures. A computer vision, which allows a computer to identify objects, is an area greatly affected by machine training. That is the same technology that is used to identify and remove obstacles in cars that use computers. Machines can distinguish images of objects and can also be designed to circumvent a captcha system, which relies on the user to recognise images before acceptance.

Evasive Malware: Malware development generally entails the design of a malicious programme that is often detectable by malware-signature security systems. In some cases, however, malicious code was generated by machine learning which other security systems could not detect, such as machine learning.

Pear Phishing: For instance, machinery learning can be exploited by collecting legit email information from target people and inserting details into a machine learning model that can then learn from the details, derive meaning from the information, and generate emails that are similar and accurate to those learned. This can be augmented in an integrated environment to improve cyber criminals' effectiveness and development as aim phishing attacks are conducted.

Improving Cybersecurity Assurance Model:

Every time a gaggle of auditors are taking part in an IT, data Security or compliance audit, there'll be consistent phases like designing, shaping objectives and scope, elucidating terms of engagements, conducting the audit, corroboratory proof, evaluating risks, news the audit findings and schedule follow up tasks. Designing a cybersecurity audit isn't totally different than any kind of audit. This however will take a great deal of effort thanks to the quality of the many cybersecurity domains. However, most cyber capabilities aren't reviewed by the inner audits' scope. This specific framework includes risk/compliance management, development life cycle, security program, third-party management, information/asset management, access management, threat/vulnerability management, of implementing cybersecurity controls as a part of an overall framework and strategy, the necessity for assurance which will be achieved by management reviews, cyber risk assessments, information management and protection, risk analytics, crisis management and

resiliency, security operation and security awareness and training. Moreover, Deloitte's framework is aligned with trade frameworks just like the National Institute of Standards and Technology (NIST), data Technology Infrastructure Library (ITIL), Committee of Sponsoring Organizations of the Treadway Commission (COSO) and world organization for Standardization (ISO). In addition, there aren't any metrics to live cybersecurity audits and therefore the cybersecurity audit topic is poorly understood because it transforms extremely quickly. Khan considers that to hide a significant scope for designing a cybersecurity audit, the auditors should embrace all relevant areas of any organization; these areas are client operations, finance, human resources, IT systems and applications, legal, purchasing, regulatory affairs, physical security and every one of the applicable third parties that have relationships with the business.

4.0 MACHINE LEARNING IN CYBER SECURITY

Software preparation is a powerful knowledge processing strategy in many ways. Sophisticated intrusion detection technologies and algorithms exist. Authentication processes can be effectively appraised, the protocol 's implementation assessed, the security of human touch facts assessed, and the smart metre data profiled.

Figure: Cyber Security

Machine learning has given the data security sector with a huge opportunity. Thanks to the larger number of computing analyses they can manage, modern machine learning approaches may greatly boost the accuracy of threat detection and maximize network visibility. They also declare a modern age in which a machinery device is wise enough to comprehend how and when to tackle in-progress challenges.

4.1 SECURITY THREADS TO MACHINE LEARNING PRODUCTS

Cyber attackers have already been looking for ways to hack tech vulnerabilities and perform malicious things from the beginning of the digital revolution. Cyber criminals are starting to search for ways to manipulate weaknesses in this area, as artificial intelligence systems explosives. Attacks on machine-learning systems are generally addressed in adverse machine-learning related to security activities such as bio-medical identification, spam philtres, Network Intruders and Malware detection. Attacks to the machine-learning system may also be mentioned.

4.2 Poisoning the training data: Poisoning the training data: Skilled machine learners are well known to focus heavily on data consistency for the success of machine learning programmers. This is commonly known as "waste in waste," which means that the waste model's schooling generates waste effects irrespective of how complicated the model is. A cybercriminal may enter a training framework

for machine learning models, altering data prior to the training without technical knowledge.

Changing a model of machine learning: in this situation, a cyber attacker will reach and modify his / her parameters improperly and influence how the test outcomes are produced. For instance: if the final form of machine learning after training can be represented mathematically as y: x is a parameter of the form input; y is the output of the model; if cyber criminals are able to access the method and change the y equation: 1-2x, it is clear that this would lead, if possible, to misunderstandings and tragic choices.

Evading detection by machine learning models: This entails threats to find inhibitors. In situations where an attacker alters the data used during the measurement process, so that during routine activities the threat is not detected. This can happen. As templates for demonstrating how attacks of this kind could take place, biometric devices were used.

5.0 CONCLUSION

In this section, we learnt how machine learning can be applied from a safeguard and attack point of view in a security framework as well as how future data model issues can be solved. Obviously, machine learning is a powerful way of simplifying nuanced security defense and threats. Therefore, we expect more advanced and major cybercriminal AI-powered attacks now with machine learning. It is therefore necessary for safety specialists and machine learners to continue to be aware of recent developments in machine learning, particularly adverse learning machines, so that they are always on the lookout for new applications relevant to AI 's safety.

Future work:

This paper will be the foundation for more analysis which will concentrate on evaluating current protection technologies and on the varied obstacles in designing and implementing scalable cybersecurity frameworks in production environments.

REFERENCES

1. Morris, T. H., Thornton, Z., & Turnipseed, I. (n.d.). Industrial Control System Simulation and Data Logging for Intrusion Detection System Research.

2. Nguyen, T. T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. Communications Surveys & Tutorials, IEEE, 10(4), 56–76. http://doi.org/10.1109/SURV.2008.080406

3. A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller, "An overview of IP flow-based intrusion detection," IEEE Communications Surveys & Tutorials, 12(3), 2010, pp. 343–356

4. Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. IEEE Communications Surveys and Tutorials,
15(4), 2070–2090. http://doi.org/10.1109/SURV.2013.030713.00020

5. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers
& security 28, no. 1, 2009, pp. 18–28

6. M. Hall, E. Frank, J. Holmes, B. Pfahringer, P. Reutemann, and I. Witten, "The WEKA data mining software: an update," ACM SIGKDD Explorations Newsletter, 11 (1), 2009, pp. 10–18

7. R. Core Team, “R Language Definition,” 2000
8. J. Cano, "Cyberattacks-The Instability of Security and Control Knowledge", ISACA Journal, vol. 5, pp. 1-5, 2016.
9. C. Hollingsworth, "Auditing from FISMA and HIPAA: Lessons Learned Performing an In-House Cybersecurity Audit", ISACA Journal, vol. 5, pp. 1-6, 2016.
10. Li X, Wang J, Zhang X, “Botnet Detection Technology Based on DNS”, J. Future Internet, 2017.
11. Y J Hu, Z H Ling, "DBN-based Spectral Feature Representation for Statistical Parametric Speech Synthesis", IEEE Signal Processing Letters, vol. 23, no. 3, pp. 21-325, 2016.
12. Dinil Mon Divakaran et al., "Evidence gathering for network security and forensics", Digital Investigation, pp. 56-65, 2017.
13. S Fong, R Wong, A V Vasilakos, "Accelerated PSO Swarm Search Feature Selection for Data Stream Mining Big Data", IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 33-45, 2016.
14. M. Khan, "Managing Data Protection and Cybersecurity-Audit's Role", ISACA Journal, vol. 1, pp. 1-3, 2016