Asian Journal of Applied Science and Technology
Volume 4, Issue 3, Pages 76-81, July-September 2020

Machine Learning Algorithms Applied to System Security: A Systematic Review

Ibrahim Goni[1], Salisu Bello[2] & Umar T. Maigari[3]

[1]*Department of Computer Science, Adamawa state University Mubi. Email: algonis1414@gmail.com*
[2]*Department of Computer Science, Umaru Musa Yar'adua University Katsina.*
[3]*Federal College of Education Gombe.*

DOI: 10.38177/ajast.2020.4311

Article Received: 19 May 2020 *Article Accepted: 17 July 2020* *Article Published: 19 August 2020*

ABSTRACT

Machine learning are used for numerous functions like image processing, data mining, prediction analysis, online shopping, cybersecurity, digital forensics, network security etc. the aim of this research work is to explore on the research work that implement security system or provide a framework for system security using machine learning algorithms. Furthermore to explore other fields that applied machine learning algorithms to solve their problems. Stipulate the essential use of the technique, once an algorithm was trained on how to manipulate the provided data, the process of implementation remain automatic.

1. Introduction

Artificial intelligence is a collective term for the capabilities shown by learning systems that are perceived by human as representing intelligence. Today, AI capabilities include speech, image and video recognition, autonomous objects, natural language processing, conversational agents, perspective modeling, augmented creativity, smart automation advanced simulation, as well as complex analytics and prediction. Artificial intelligence are practically applied in cyber security to detect, predict and respond to cyber threats in real time using machine learning and deep learning algorithms which spread across Information technology, operational technology, internet of things, control system, security systems, and the cloud in general.

Artificial Intelligence comprised too many fields, machine learning is one of them as described in Fig.1 that permits a designed Computer system to catch up from the environment, through repetitious processes and provide improvement to it as far experiences learned during the training processes.

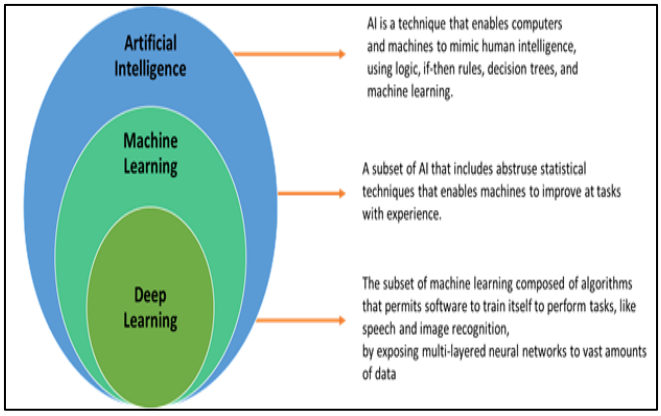

Fig.1: Representation of artificial intelligent and its subfield [2]

Machine learning algorithms arrange the data accordingly, learn from it, gather insights and build predictions supported the data it analyzed while not the requirement for adding explicit programming. Training a model with data and after that using the model to predict another data is the concern of machine learning. Several studies have

been carried out about how to train the machines to learn themselves without human intervention [1]. Machine learning algorithms are popularly categorized as supervised, unsupervised, semi-supervised and reinforcement learning. The main aim of this research work is to explore the researches that applied machine learning algorithm to system security.

2. Machine Learning Categories

Machine learning is popularly categorized under the following:

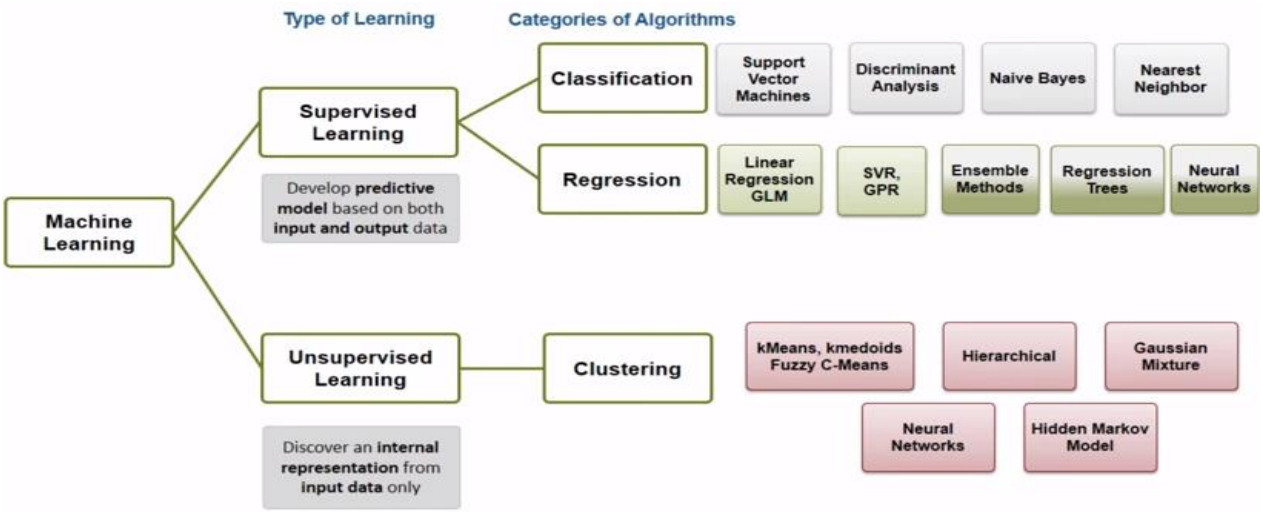

Fig.2: Categories of machine learning [1] [3]

Machine learning is a technique of using algorithm to parse data, learn from the data and make a decision, prediction, detection, classification, pattern recognition, responding and clustering based on the data collected. These algorithms are heavenly depend on the statistical and mathematical optimization. In broader sense machine learning algorithm are used in clustering, regression, (univariate & multivariate) anomaly detection, pattern recognition [27].

Supervised learning

Supervised learning algorithms are machine learning algorithms that require datasets for training and testing the performance. This dataset has to be labeled and consist of features by which events or objects are defined as well as the expected outputs.

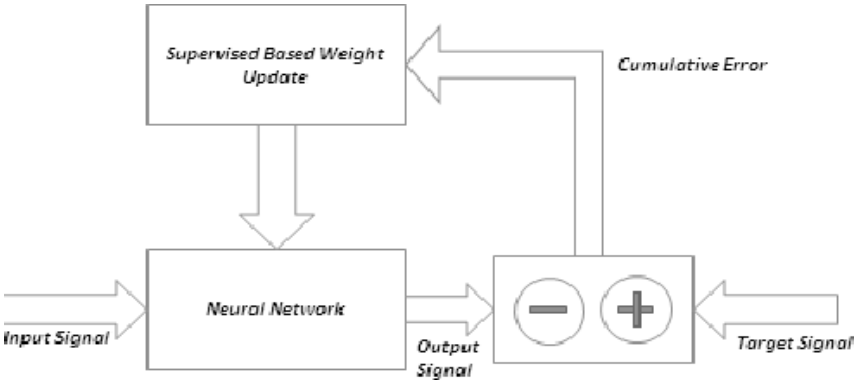

Fig.3: Supervised Neural Network [29]

The most common supervised learning algorithm are decision tree, logistic regression, support vector machine, relevance vector machine, random forest, K-NN, bagging neural networks, linear regression and naïve Bayes [26].

Unsupervised learning

Unsupervised learning algorithm is a machine learning algorithm that required unlabeled datasets for training and testing the system performance the two major techniques used in unsupervised learning are principal component analysis (PCA) and clustering. The most common unsupervised learning algorithms are used especially in security are hierarchical, k-means, mixed model, DBSCAN, OPTIC, self-organizing mapping, Bolzan machine, auto encoder, adversarial network (Matt, 2017)

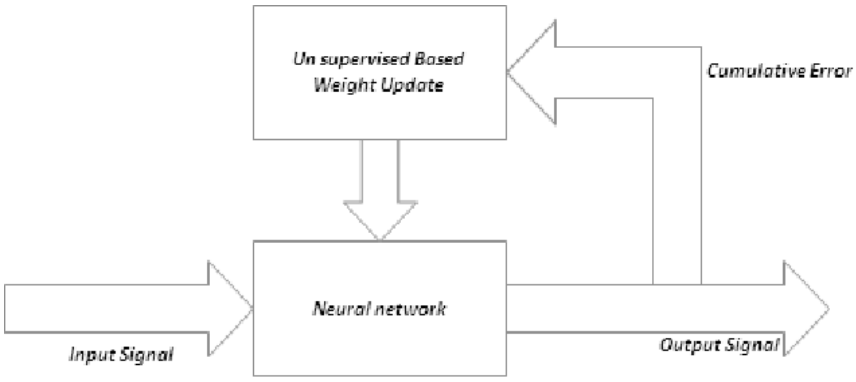

Fig.4: Unsupervised Neural Network [29]

Machine learning algorithms applied to system security

In [7] presented how effectiveness of machine learning and deep learning in the feature of cyber security. Many surveys reviews and systematic reviews are conducted in the application of machine learning, deep learning and artificial intelligence techniques to cyber security, attack, intrusion detection system, network security as in [13], [14], [16], [15], [17]. Machine learning algorithm was also used to study cyber security in [23]. Security Framework was designed by [24] using fuzzy logic. [37] Highlight the role of intelligent system and artificial intelligences in addressing the challenges of cyber security but they didn't illustrate the framework on how to implement the system. In [33] they presented a general review on the malware detection in mobile devices based on parallel and distributed network. [34] They made a comparative analysis between the used of static, dynamic and hybrid technique to malware detection. Forensics analysis was also made on WhatsApp messenger to identify those that are using the application to perpetrate a crime or do illegal business as in the research of [27], [28], [29], [30]. In [35] digital forensics framework was proposed and made a comparative analysis with other framework made with no AI techniques however, there framework has no instant detection and sending signals as compare to our proposed framework.[12] also explore extensively the roles of artificial intelligence, machine learning and deep learning algorithm to cyber space.

Furthermore, machine learning algorithms deep learning algorithms are applied in intrusion detection systems as in the research of [18] presented that machine learning based system can be used to detect intrusion for software defined networks. [19] Presented an extensive survey on anomaly based intrusion detection system. [20] Applied

machine learning algorithm to intrusion detection in mobile cloud in a heterogeneous clients networks. In the work of [21] hybrid intrusion detection system for cloud computing. [22] They used machine learning algorithm to provide a roadmap for industrial network anomaly detection. Anomaly detection system for automobile network was presented by [24]. In addition to [4] has explored the used of clustering algorithms such as K-means hierarchical clustering, k-means kernel, latent drichlet allocation and self-organizing mapping techniques for forensics analysis using text clustering in the large volume of data. [5] Presented a robust forensics analysis method using memetic algorithm. [6] Revealed how artificial intelligence techniques are applied to cyber-attacks security breaches. Machine learning algorithm was used to classified malware in android system in [11]. Machine learning and deep learning algorithm are combined and used for cyber security system in [10]. Machine learning algorithms are also applied to intrusion detection system in [9] and [36]. The researches of [8] systematic survey on the researches that combine machine learning algorithm and data mining to cyber security Deep neural network and fuzzy logic are used to identify abnormality in network traffic [25]. A systematic survey was made by [31] on the techniques that are used for malware detection, while [32] used APIs and machine learning algorithm to detect malware in android.

3. Conclusion and Future Work

This research work reviewed several algorithms of machine learning, Nowadays, machine learning is used by many field of study such as online shopping, updating profiles/photos on social media networks, internet search engines, phone directory inquiry and system security. This research provides a fundamentals to the most of the world used algorithms of machine learning in system security. For future work, the author is intended to comprehensively compare and study the performance of machine learning algorithms and analyze the best among the bests with the used of machine learning in system security.

References

[1] Ayon, D. Machine Learning Algorithms: A Review. Int. J. Comput. Sci. Inf. Technol. 2016, 7, 1174–1179

[2] Data Driven investor.

https://medium.com/datadriveninvestor/unraveling-artificial-intelligence-for-the-non-geeks-the-non-technical-insight-dbae9736bc65

[3] Profile.me. Ukraine, Vinnytsia, https://en.proft.me/2015/12/24/types-machine-learning-algorithms

[4] A. Bandir, (2019) Forensics analysis using text clustering in the age of large volume data: a review. International journal of advanced computer and application. 10(6), 72-76.

[5] Al-Jadir I., Wong K. W., Fing C.C. & Xie H. (2018) Enhancing digital forensics analysis using memetic algorithm feature selection method for document clustering 2018 IEEE international conference on systems, Man and cybernetics 3673-3678.

[6] Suid B. & Preeti B. (2018) Application of artificial intelligence in cyber security. International journal of engineering research in computer science and engineering 5(4), 214-219.

[7] Apruzze G., Colajanni M. F., Ferreti L., & Marchett M. (2018) on the effectiveness of machine learning for cyber security in 2018 IEEE international conference on cyber conflict 371-390 .

[8] Buckza A. L. & Guven E. (2016) A survey of data mining and machine learning methods for cyber security intrusion detection IEEE communication survey and tutorials 18(2), 1153-1176

[9] Biswas S.K. (2018) intrusion detection using machine learning: A comparison study. International Journal of pure and applied mathematics 118(19), 101-114

[10] Y. Xin, Kong L., Liu Z., Chen Y., Zhu H., Gao M., Hou H., & Wang C. Machine learning and deep learning methods for cyber security. IEEE Access 6: 35365-35381 (2018)

[11] N. Miloseivic, Denghantanh A., Choo K.K.R. Machine learning aided android malware classification. Computer and electrical engineering 61: 266-274. (2017).

[12] B. Geluvaraj, Stawik P.M., Kumar T. A. the future of cyber security: the major role of Artificial intelligence, Machine learning and deep learning in cyber space. International conference on computer network and communication technologies Springer Singapore. 739-747. (2019)

[13] H. Mohammed B., Vinaykumar R., Soman K. P. A short review on applications of deep learning for cyber security. (2018).

[14] M. Rege, Mbah R. B. K. Machine learning for cyber defense and attack. in the 7th International conference on data analysis 73-78 (2018).

[15] D. Ding, Hang Q. L., Xing Y., Ge X., and Zhang X. M. A survey on security control and attack detection for industrial cyber physical system. Neuro-computing. 275. 1674-1683. (2018).

[16] D. Berman S., Buczak A.L., Chavis J. S., Corbelt C.L. A survey of deep learning methods for cyber security information 10(4): (2018).

[17] Y. Wang, Ye Z., Wan P., Zhao J. A survey of dynamic spectrum allocation based on reinforcement learning algorithms in cognitive radio network. Artificial intelligence review. 51(3): 413-506 (2019).

[18] A. Abubakar, Paranggono B. Machine learning based intrusion detection system for software defined networks. 7th International conference on Emerging security techniques IEEE. 138-143. (2017).

[19] S.Jose, Malathi D., Reddy B., Jayaseeli D. A survey on anomaly based host intrusion detection system. Journal of physics. Conference series 1000(1): (2018).

[20] S. Dey, Ye Q., Sampalli S. A Machine learning based intrusion detection scheme for data fusion in mobile cloud involving heterogeneous clients network. Information fussion 49: 205-215. (2019).

[21] P. Deshpande, Sharma S.C., Peddoju S.K., Junaid S. HIDS: a host based intrusion detection system for cloud computing environment. International journal of system assuarance engineering and management. 9(3): 567-576. (2018).

[22] M. Nobakht, Sivaraman V., Boreli R. A host-Based Intrusion detection and mitigation framework for smart IoT using open flow in 11th International conference on availability reliability and security IEEE. 147-156. (2016).

[23] R. Devakunchari, Souraba, Prakhar M. A study of cyber security using machine learning techniques. International journal of innovative technology and exploring engineering. 8(7): 183-186. (2019)

[24] E. Alison N. FLUF: fuzzy logic utility framework to support computer network defense decision making IEEE (2016).

[25] A. Taylor, Leblanc S., Japkowicz N. Anomaly detection in auto-mobile control network data with long short term memory network in data science and advance analytics. IEEE international conference. 130-139. (2016).

[26] O. Amosov S., Ivan Y.S., Amosovo S.G. Recognition of abnormal traffic using deep neural networks and fuzzy logic. International Multi-conference on industrial engineering and modern technologies IEEE (2019).

[27] A. Nuril, Supriyanto (2019) Forensic Authentication of WhatsApp Messenger Using the Information Retrieval Approach. International Journal of Cyber Security and Digital Forensics (IJCSDF) 8(3): 206-212. (2019).

[28] A Marfianto, I Riadi. WhatsApp Messenger Forensic Analysis Based on Android Using Text Mining Method. International Journal of Cyber Security and Digital Forensics (IJCSDF) 7(3): 319-327. (2018).

[29] N Anwar, I. Riadi. Forensic Investigative Analysis of WhatsApp Messenger Smartphone Against WhatsApp Web-Based, Journal Information Technology Electromagnetic Computing and Information, 3(1): 1-10. (2017).

[30] S. Ikhsani and C. Hidayanto, Whatsapp and LINE Messenger Forensic Analysis with Strong and Valid Evidence in Indonesia. Tek. ITS, 5(2): 728-736. (2016).

[31] M. Ashawa, S. Morris. Analysis of Android Malware Detection Techniques: A Systematic Review. International Journal of Cyber Security and Digital Forensics (IJCSDF) 8(3): 177-187. (2019).

[32] W. Songyang, Wang, P., Zhang, Y. Effective detection of android malware based on the usage of data flow APIs and machine learning: Information and Software Technology, 75: 17--25 (2016).

[33] Anastasia, S., Gamayunov, D.: Review of the mobile malware detection approaches: Parallel, Distributed and Network-Based Processing (PDP). In: Proc. 2015. IEEE 23rd Euro micro International Conference, pp. 600--603(2015).

[34] D. Anusha, Troia, F. D., Visaggio, C. A., Austin, T. H., Stamp, M.: A comparison of static, dynamic, and hybrid analysis for malware detection. Journal of Computer Virology and Hacking Techniques, 13(1) 1-12 (2017)

[35] H. Parag Rughani. Artificial Intelligence Based Digital Forensics Framework. International Journal of Advanced Research in Computer Science. 8(8): 10-14. (2017)

[36] I. Goni & Ahmed L. Propose Neuro-Fuzzy-Genetic Intrusion Detection System. International Journal of Computer Applications 115(8): 1-5 (2015)

[37] Y. Harel, Irad Ben Gal, and Yuval Elovici. Cyber security and the role of intelligent systems in addressing its challenges. ACM Transaction on Intelligent System Technology 8(4): 1-12 (2017).