Data Analytics and Artificial Intelligence
Vol: 2(5), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/

Applications of Machine Learning in Cyber Security

***Gayathri R, Jayashree P**
MGR College, Hosur, Tamil Nadu, India
*Corresponding author Email: gayathrigaiat16@gmail.com

Abstract. Due to its distinctive qualities, such as adaptability, scalability, and the capability to quickly adapt to new and unknowable obstacles, machine learning techniques have been used in many scientific fields. Due to notable advancements in social networks, cloud and web technologies, online banking, mobile environments, smart grids, etc., cyber security is a rapidly expanding sector that requires a lot of attention. Such a broad range of computer security issues have been successfully addressed by various machine learning techniques. This paper covers and emphasises several machine learning applications in cyber security. The topics covered in this research include phishing detection, network intrusion detection, keystroke dynamics authentication, cryptography, human interaction proofs, spam detection in social networks, smart metre energy consumption profiling, and challenges in security of smart metres

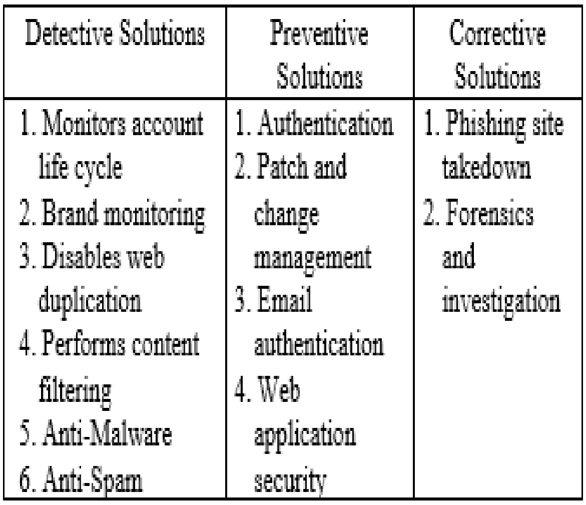
1. Introduction

Attack strategies are advancing quickly to penetrate systems and elude generic signature-based defences, much as online and mobile technologies are doing the same. Due to their ability to quickly adapt to novel and unknowable circumstances, machine learning techniques present prospective answers that can be used to resolve such difficult and complex issues. Wide-ranging issues in computer and information security have been effectively addressed using a variety of machine learning techniques. This paper covers and emphasises several machine learning applications in cyber security. The essay is set up as follows. Applications of machine learning in information security are discussed in Section 2 in terms of phishing detection, network intrusion detection, evaluating the security of protocols, keystroke dynamics authentication, cryptography, human interaction proofs, and spam detection in social networks.

2. Methodology

Phishing Detection: Phishing is intended to steal sensitive personal data. Three main categories of anti-phishing techniques have been identified by researchers [2]: detective (monitoring, content filtering, anti-spam), preventive (authentication, patch and change management), and corrective (site takedown, forensics). Table 1 provides a summary of these categories.[1] is a comparison of phishing detecting methods. Many of the phishing detection methods under consideration were found to have a high rate of missed detection.

TABLE 1. Phishing and Fraud Solutions [1, 2]



Detective Solutions	Preventive Solutions	Corrective Solutions
1. Monitors account life cycle 2. Brand monitoring 3. Disables web duplication 4. Performs content filtering 5. Anti-Malware 6. Anti-Spam	1. Authentication 2. Patch and change management 3. Email authentication 4. Web application security	1. Phishing site takedown 2. Forensics and investigation

Researchers compared six machine learning classifiers, including Logistic Regression (LR), Classification and Regression Trees (CART), Bayesian Additive Regression Trees (BART), Support Vector Machines (SVM), Random Forests (RF), and Neural Networks (NNets), using 1,171 raw phishing emails and 1,718 genuine emails. Figure 1 summarises the error rates of all the classifiers stated above.

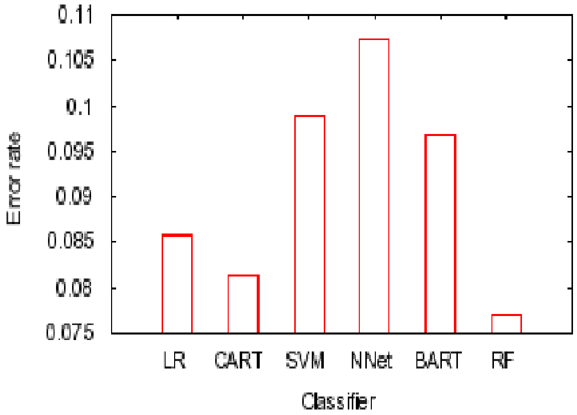


FIGURE 1. The error rates of classifiers [1]

The emails were parsed using text indexing methods as an experiment. The emails' contents' "header information of all emails and html tags" as well as their particular components were extracted, and all attachments were deleted. After that, a stemming algorithm was used to eliminate all the unnecessary terms. All items were then arranged in emails based on their frequency. Because of its low false positive rate, it can be inferred from this work that LR is a more user-friendly alternative (usually, users would not want their legitimate emails to be misclassified as junk). Comparing LR to other classifiers under consideration, it also has the highest precision and relatively high recall. Table provides a comparison of precision, recall, and F-measure.

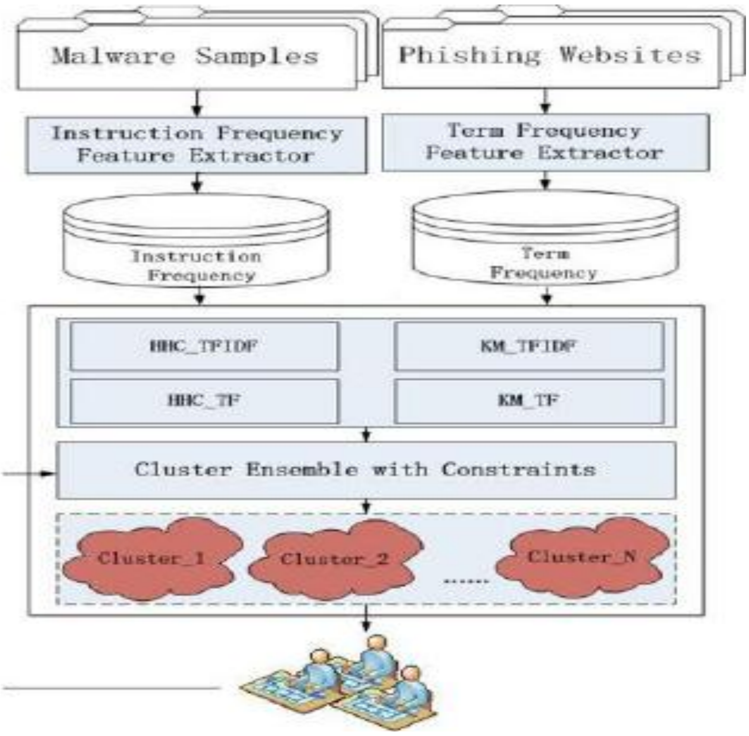


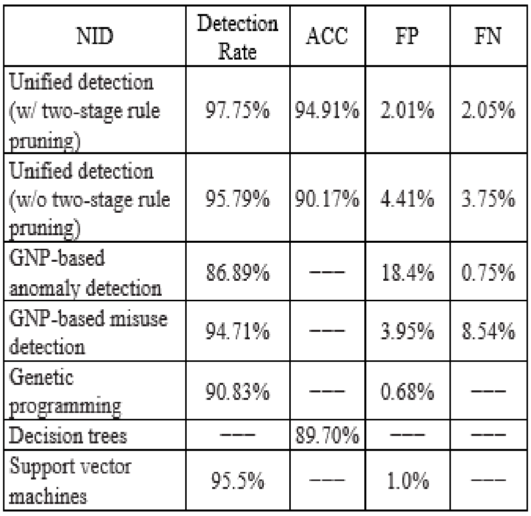
FIGURE 3. The Architecture of ACS [6]

The ACS first parses the malware samples and phishing web addresses. In order to save them to a database, it extracts phrases and particular malware instructions. The information retrieval algorithm is then used by the system to calculate the TF-IDF metrics. The data is then divided into clusters by the ACS using an ensemble of clustering techniques while taking into account constraints that security experts manually created.

Network Intrusion Detection: Network Intrusion Detection (NID) systems are used to identify malicious network activity leading to confidentiality, integrity, or availability violation of the systems in a network. Many intrusion detection systems are specifically based on machine learning techniques due to their adaptability to new and unknown attacks. Lu et al. [8] proposed a unified effective solution for improving Genetic Network Programming (GNP) for misuse and anomaly detection. Matching degree and genetic algorithm were fused so that redundant rules can be pruned and efficient ones can be filtered. The system was tested on KDDcup99 [22] data to demonstrate its efficiency. The proposed pruning algorithm does not require "prior knowledge from experience". The rule is pruned if the average matching degree is less than some threshold. On the training step, 8,068 randomly chosen connections were fed into their system (4,116 were normal, 3,952 –

smurf and neptune attacks). After training the system, the proposed solution was tested on 4,068 normal connections and 4,000 intrusion connections. The accuracy (ACC) is reported to be 94.91%, false positive rate (FP) is 2.01%, and false negative rate (FN) is 2.05%. Table 4 displays the performance comparison of different algorithms including the proposed one. Support vector machines (SVM) and neural networks are used in a classification system to defend against distributed denial of service with the "Snort" programme for intrusion (DDoS) assaults. A virtual environment was utilised to simulate a real DDoS attack, together detection and "packit" for creating and transmitting network packets to the target system.

TABLE 4. The performance comparison of NID systems [8]

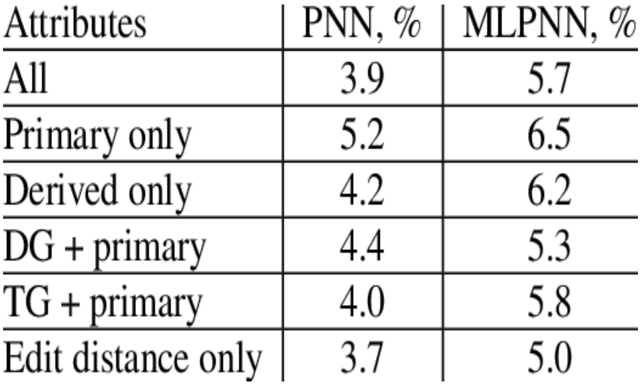


NID	Detection Rate	ACC	FP	FN
Unified detection (w/ two-stage rule pruning)	97.75%	94.91%	2.01%	2.05%
Unified detection (w/o two-stage rule pruning)	95.79%	90.17%	4.41%	3.75%
GNP-based anomaly detection	86.89%	---	18.4%	0.75%
GNP-based misuse detection	94.71%	---	3.95%	8.54%
Genetic programming	90.83%	---	0.68%	---
Decision trees	---	89.70%	---	---
Support vector machines	95.5%	---	1.0%	---

The warnings produced by the Snort intrusion detection programme were recorded and put into support vector machines and a back-propagation neural network for classification as true-positives or false-positives. According to the researchers, this procedure cut the overall number of notifications to be processed by 95%. While support vector machines' accuracy is 99%, neural networks' average accuracy for alert classification is only 83%. NN and SVM comparison using the Threshold Based Method (TBM).

Authentication with Keystroke Dynamics: For keystroke dynamics, Revett et al. [12] suggested using a Probabilistic Neural Network (PNN). Keystroke dynamics, in general, is "a kind of behavioural biometrics that captures the user's typing style." The system was tested using a dataset of 50 users' login and password keystrokes. 30 of them were requested by Revett et al. to repeatedly log in as imposters rather than authentic users. Throughout enrollment and authentication attempts, eight distinct characteristics were tracked. Digraphs (DG, two-letter combinations), trigraphs (TG, three-letter combinations), total username and password entry time, scan code, speed, and edit distance were among these characteristics. The data was then tested after being fed into the PNN system. 90% of the time, the classification of real from imposter was accurate. PNN and a multi-layer perceptron neural network were also contrasted.

TABLE 7. FAR + FRR of PNN and MLPNN [12]



Attributes	PNN, %	MLPNN, %
All	3.9	5.7
Primary only	5.2	6.5
Derived only	4.2	6.2
DG + primary	4.4	5.3
TG + primary	4.0	5.8
Edit distance only	3.7	5.0

Testing Security of Protocol Implementation: Using machine learning to "test the implementation security of protocols." In order to add a message to the original one, the researchers primarily concentrated on "Message Confidentiality (secrecy) under Dolev-Yao model of attackers" [14]. In general, there is no complete method for assessing the security of a protocol's implementation. Experiments can, however, be completed for an issue with a fixed amount of messages. Their paper's main objective is to identify security flaws in a protocol black-box implementation that uses the L* learning algorithm [15]. The researchers developed a teacher in this algorithm who carries out the following three main tasks: 1) Producing an output query from a sequence of inputs; 2) Producing a counterexample that a system outputs . as an incorrect result when analyzing it; 3) Augmenting the alphabet, appending new input symbols in addition to the existing ones. They showed the effectiveness of their proposed technique on testing three real protocols: Needham-Schroeder-Lowe (N-S-L) mutual authentication protocol, TMN key exchange protocol, and SSL 3.0 handshake protocol. As a result, their system identified the introduced flaws in N-S-L and TMN. Also, it confirmed that SSL is secured

Breaking Human Interaction Proofs (CAPTCHAs): Chellapilla and Simard [16] talk about how machine learning can be used to circumvent Human Interaction Proofs (or CAPTCHAs). Seven different HIPs were used in experiments, and the researchers discovered their common advantages and disadvantages. The suggested method aims to identify the characters (segmentation stage) and locate them using neural network [17]. Six tests using EZ-Gimpy/Yahoo, Yahoo v2, mailblocks, registration, ticketmaster, and Google HIPswere carried out. Each experiment was divided into two sections: segmentation and recognition (1,600 HIPs were used for training, 200 for validation, and 200 for testing) (500 HIPs for testing segmentation). Different computer vision approaches used during the recognition stage include grayscale conversio, thres holding to black and white, dilation and erosion, and choosing huge CCs with sizes that are similar to HIP char sizes.

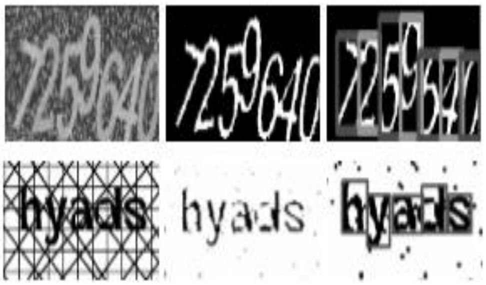


FIGURE 5. Examples of segmentation [16]

Cryptography: A quick and effective cryptography system based on delayed chaotic Hopfield neural networks was created by Yu and Cao [18]. The proposed approach, according to the researchers, is secure because of "the challenging synchronisation of chaotic neural networks with time variable delay. " Two synchronised neural networks can be used for a secret key exchange over a public channel, as demonstrated by Kinzel and Kanter [20]. Basically, two neural networks get an arbitrary, identical input sequence per cycle during the training stage and begin with random weight vectors. Only when the neural networks' outputs are identical do the weights alter. Additionally, the corresponding weight vectors of both neural networks eventually become equal. It has been shown by the researchers that it is computationally impossible.

Social Network Spam Detection**:** K. Lee et al. [7] noted that spammers use social networks to spread malware, conduct phishing attacks, and advertise affiliate websites. A social honeypot was created to find spammers in **social networks like Twitter and Facebook in** order to defend social systems against those attacks. Support Vector Machine (SVM) is the foundation of the suggested solution, which has a high level of precision and a low rate of false positives. An appropriate bot that collects both genuine and spam user profiles and feeds them to the SVM classifier is represented by a social honeypot by a legitimate user profile. The researchers looked at Twitter and MySpace machine learning method performed. Both social networks saw the creation of several legitimate user profiles, and data was gathered over a period of time networks to assess how well the suggested.

Smart Meter Data Profiling: In our most recent work, we used fuzzy c-means clustering for profiling smart metre data [24]. Our research shows that one can utilise a disaggregation technique to determine customer energy consumption profiles by having access to the energy consumption traces recorded by smart metres, which can breach consumers' privacy and have the potential to be exploited in unwanted ways. The window of time between the customer's departure and return home presents chances for house invasion, telephone marketing, or even child behaviour profiling. For instance, our examination of a smart meter's three-day data sequence (Figure 6) reveals a certain pattern of energy consumption behaviour. Here, axis X denotes the measurement's date and time, and axis Y denotes the amount of energy consumed each hour in kW. These observations indicate that Given that the energy usage is constantly at its highest between 8:30 A.M. and 10:00 P.M., it can be assumed that the consumer is a service-providing business (such as a store or restaurant) rather than a household (Figure 7). Additionally, it may be deduced that it uses specific appliances that use 0.55 kW/h every half an hour at night. These gadgets are probably security and/or fire alarm detectors, which have intermittent low and persistent energy consumption. Another pattern was noticed for a single client who was randomly selected from the dataset, as shown in Figure 8.

It demonstrates that during the hours of 1 A.M. and 8 A.M., the amount of energy consumed ranges from 0 to 0.1 kW/h. As a result, it can be assumed that throughout this time, The client rarely makes use of any appliances. This might be the case for two reasons: 1) if it's a residential residence, the resident is probably sleeping at that time; and 2) if it's a business, it's probably not open at that time. We may infer that the client is a typical working home as they typically use between 0.358 and 0.548 kW/h between the hours of 8 p.m. and 12 a.m. (where people sleep at night, go to work all day and come back to have dinner, watch TV and then go to bed again).

Additionally, one can infer information about appliance usage by having access to detailed energy consumption data, and spammers can use this information to their own advantage. Utility companies, on the other hand, can use this information to spot sudden changes in consumer usage patterns, which can be used to spot energy fraud, a critical problem in the smart grid.

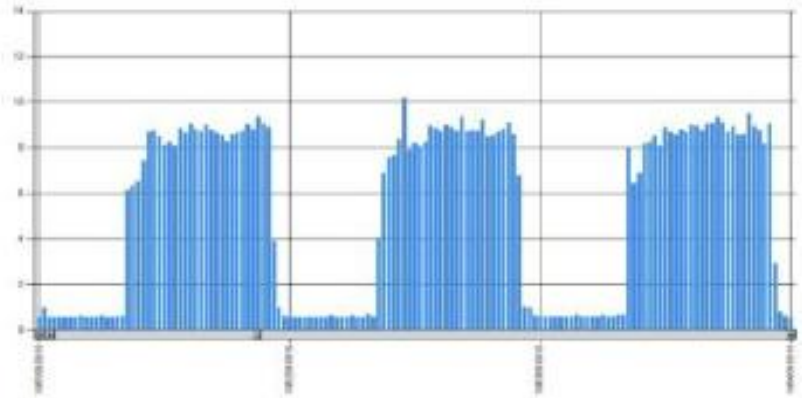


FIGURE 6. Energy Consumption Profile for One Smart Meter for Three Consecutive days [24]

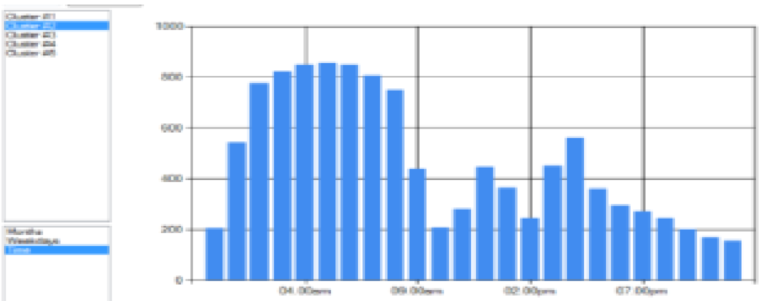


FIGURE 8. Energy Consumption Profile for Single Customer [24]

Security of Machine Learning: M. Bareno et al. [21] go over a variety of methods that a machine learning system can be compromised. The researchers offer a thorough taxonomy of several assaults designed to take advantage of machine learning systems: Attacks that change the training process are classified as (a) causal attacks; (b) attacks on integrity and availability that cause false positives as a system breach; (c) exploratory attacks that take advantage of known vulnerabilities; (d) targeted attacks that are directed at a specific input; and (e) indiscriminate attacks in which all inputs fail. The Reject On Negative Impact (RONI) defence was suggested by the researchers. All training data points that significantly reduce the classification accuracy are disregarded by RONI. They mainly spoke about two different defences. The first sort of defence is against exploratory attacks, where an attacker can produce an assessment. The defence can restrict access to the training process and data to counter this attack, making it more difficult for an attacker to do reverse engineering. Additionally, it becomes more difficult for an attacker to infer the taught hypothesis as a hypothesis space becomes more complex. In order to make it more difficult for an attacker to hack the system, a defender might also restrict the feedback (or send the dishonest one) sent to them. The second kind of protection is one against causal assaults, in which the attacker can alter both the distributions of the training and evaluation data. The RONI defence, which uses a system with two classifiers, can be used by the defender in this situation. A classifier is learned using a basis training set, while a different classifier is trained using both the candidate instance and the base set. The candidate instance is considered malicious if the mistakes of those two classifiers considerably differ from one another. The researchers demonstrated how to use the defensive RONI algorithm by simulating an assault on the SpamBayes spam detection system [23] and demonstrating how well the system defends against indiscriminate causal availability attacks.

3. Conclusion

Machine learning is a powerful technique that may be used in many information security applications. There are some effective network intrusion detection systems and anti-phishing algorithms. Machine learning can be used effectively for creating authentication systems, reviewing protocol implementation, determining how secure human interaction proofs are, profiling data from smart metres, etc. Machine learning supports modern cyber security solutions in a number of different ways. Individually, each one is valuable, and together they are game-changing for maintaining a strong security posture in a dynamic threat landscape. With new devices getting connected to enterprise networks all the time, it's not easy for an IT organization to be aware of them all. With more devices and threats coming online every day, and human security resources in scarce supply, only machine learning can sort complicated situations and scenarios at scale to enable organizations to meet the challenge of cybersecurity now and in the years to come.

Reference

[1]. Jordan, Michael I., and Tom M. Mitchell. "Machine learning: Trends, perspectives, and prospects." Science 349, no. 6245 (2015): 255-260.

[2]. Mahesh, Batta. "Machine learning algorithms-a review." International Journal of Science and Research (IJSR).[Internet] 9 (2020): 381-386.

[3]. Bi, Qifang, Katherine E. Goodman, Joshua Kaminsky, and Justin Lessler. "What is machine learning? A primer for the epidemiologist." American journal of epidemiology 188, no. 12 (2019): 2222-2239.

[4]. Provost, Foster, and Ron Kohavi. "On applied research in machine learning." MACHINE LEARNING-BOSTON-30 (1998): 127-132.

[5]. Burkov, Andriy. The hundred-page machine learning book. Vol. 1. Quebec City, QC, Canada: Andriy Burkov, 2019.

[6]. Athey, Susan. "The impact of machine learning on economics." In The economics of artificial intelligence: An agenda, pp. 507-547. University of Chicago Press, 2018.

[7]. Carleo, Giuseppe, Ignacio Cirac, Kyle Cranmer, Laurent Daudet, Maria Schuld, Naftali Tishby, Leslie Vogt-Maranto, and Lenka Zdeborová. "Machine learning and the physical sciences." Reviews of Modern Physics 91, no. 4 (2019): 045002.

[8]. Zhou, Zhi-Hua. "Learnware: on the future of machine learning." Frontiers Comput. Sci. 10, no. 4 (2016): 589-590.