NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 8, Aug. -2021

MACHINE LEARNING APPLICATIONS IN THE FIELD OF CYBER SECURITY

Pavan Kantamsetti
Gitam University, Cyber Forensics and Information Security

ABSTRACT
The techniques of machine learning are applied in various areas of science with their unique properties like adaptability, scalability and potential to quickly adjust to new and unknown challenges. Cyber security is also a rapidly growing field with huge demand in all industries and environments due to its progress. Machine learning methods are implemented to tackle the increasing security problems. This paper is about use of machine learning in cyber security field. This paper covers presence of phishing links detection in an organization, monitoring network traffic, security testing of assets and protocols and spam detection and automation of everyday work in cyber field. The methodologies mentioned in this paper gives an overview of understanding about the use of this technology and its utilization at infrastructure level.

Keywords: Cyber Security, machine learning, survey, applications.

INTRODUCTION
In order to understand the best about the importance of machine learning technology in the field of cyber security, we need to understand the requirements present in cyber security and then we need to train the algorithms according to it. Different algorithms are used for different services based on their requirement. The technology is used at a wide range and is trained in such a way that it has a capability to face the complex challenges and upcoming attacks appearing.
The purpose of this research is to bring out the applications of machine learning in the field of infrastructure level. People working at infrastructure level and people looking to shift from machine learning to cyber security, this paper gives a brief idea on the fields this machine learning algorithms are implemented. I gathered the applications and their working from various websites and referring through various research papers proposed by researchers. The main aim of this research paper is to display the importance of machine learning and algorithms designed in the field of cyber security so that a layman can also understand the use of integrating these technologies.
Due to fast evolvement of technologies in web and mobile platforms, the techniques to attack become more sophisticated in penetrating systems and evading generic signature-based approaches. Implementation of machine learning techniques help in offering solutions to complex problems. In this paper, it highlights applications of machine learning in cyber security field.
In this paper, it discusses about use of machine learning in works done in the field of cyber security.

- Presence of phishing links detection.
- Detection of intrusions at network level.
- Security testing of assets and protocols.
- Authentication using keystroke dynamics.
- Cryptography.
- Breaking of human Interaction proofs.
- Detection of spam in social network.
- Issues in security of machine learning product.

METHODOLOGY
Presence of phishing links detection
The main aim of phishing is to steal the sensitive information of a targeted user. There are three principal groups of anti-phishing methods identified by researchers:

- **Detective:** In this method, monitoring, content filtering, anti-spam techniques are carried out.
- **Preventive:** In this method, authentication, patch and change management techniques are carried out.

- **Corrective:** In this method, site takedown, forensics techniques are carried at this phase.

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

It was noted by comparing six machine learning classifiers, using 1,171 raw phishing emails and 1,718 legitimate emails, – The classification techniques used in detection are **"Logistic Regression, Classification and Regression Trees, Bayesian Additive Regression Trees, Support Vector Machines , Random Forests , and Neural Networks"**. The error rates of all the mentioned classifiers are summarized in below Figure.

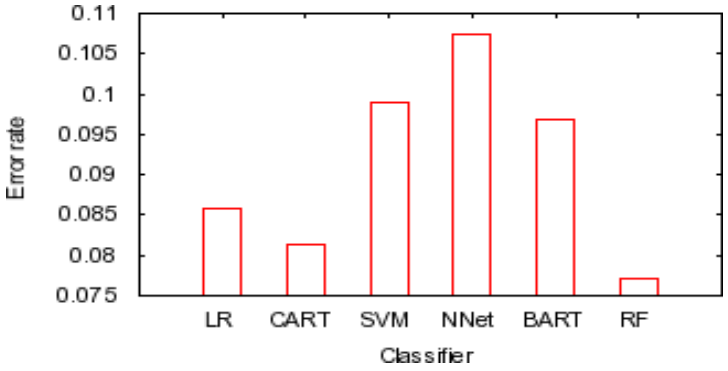

Figure 1: The error rates of classifiers

For parsing of e-mails, text indexing techniques were used. Using this technique, the attachments from all mails were removed. Extracted header information of all emails and html tags from the email bodies as well as their specific elements. To remove irrelevant information, a stemming algorithm is used to meet the requirement. This process is done to sort the items according to their frequency in emails. As a result, linear regression is more preferable for this task as it has low false positive rate. This classification has the highest precision and relatively high recall in comparison with other classifiers under contemplation. The comparison of classifiers is given in below table.

Table 2: Comparison of classifiers

Classifier	Precision	Recall	F1
LR	95.11 %	82.96 %	88.59%
CART	92.32 %	87.07 %	89.59 %
SVM	92.08 %	82.74 %	87.07 %
NNet	94.15 %	78.28 %	85.45 %
BART	94.18 %	81.08 %	87.09 %
RF	91.71 %	88.88 %	90.24 %

Researchers developed an automatic system for detection of phishing. This process is done by applying a cluster ensemble of several clustering solutions. An algorithm based on feature selection for extracting various phishing email traits was used, they are:

Hierarchical Clustering (HC) Algorithm: That uses cosine similarity using the TF-IDF metric. It is used for measuring the similarity between two points,

K-Medoids: It is a clustering approach.

The above clustering methods for phishing website and malware categorization have about 85% performance.

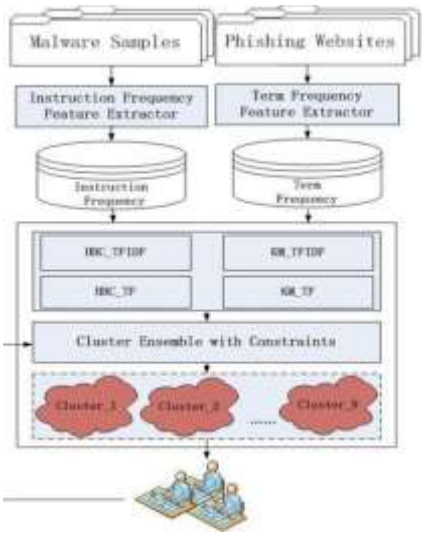

Figure 3: The Architecture of Automatic Categorization System

In the first phase, the ACS architecture is used to parse the malware samples and phished web-sites. It extracts terms and specific malware instructions and saves them in a database. In the second phase, the system applies a retrieval of information algorithm for calculating the metrics. Then, the system uses the ensemble of clustering algorithms and, taking account of constrains manually generated by security experts, and then splits the data into clusters.

Detection of intrusions at network level

These systems are used in identification and detection of intruders entering and malicious network activity which affects in compromising of confidential data, integrity, or availability violation of the systems in a network. Many IDSs work on machine learning algorithms as they adapt to new and unknown attacks.

There is a unified effective solution proposed by researchers for improving Genetic Network Programming (GNP). This helps in misuse and detection of anomalies. The efficient ones can be filtered by matching degree and genetic program and fusing of redundant rules. The rule is eliminated if the average matching degree is less than threshold.

During the training step, some randomly chosen connections of 8,068 were fed into their system in that 4,116 were normal, 3,952 – smurf and neptune attacks. After training, the proposed solution was then tested on connections. In those connections 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%. Below displays the performance comparison of different algorithms including the proposed one.

Table 4: The performance comparison in NID systems

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%	–––

Researchers developed an Alert Classification System using Neural Networks (NNs) and Support Vector Machines (SVM) to prevent against Distributed Denial of Service (DDoS) attacks. For simulation of a real DDoS attack, a virtual environment was kept using "Snort" tool for intrusion detection, and "packit" tool which is used for generating network packets and sending those packets to the target machine. The alerts generated by the snort intrusion detection tool were captured and sent into a back-propagation NN and SVMs for classification of the alerts into true-positives or false-positives. After implementation, this process reduced total number of alerts to process by 95%. The average accuracy obtained through neural network alert classification is 83% whereas through support vector machines, it is 99%. A comparison of classification of accuracies is shown in below table.

Table 5: The Comparison among classification

Type of attack	Classification Accuracy			
	TBM	FIS	NNs	SVM
UDP	75.00 %	84.30 %	85.22 %	99.28 %
TCP SYN	73.00 %	82.34 %	83.56 %	99.45 %
ICMP	73.45 %	81.24 %	83.21 %	99.39 %
ICMP SMURF	70.14 %	77.89 %	81.27 %	98.40 %

Researchers proposed a hybrid solution for detecting intrusions in a Wireless Sensor based Network environment. It is based on clustering technique and implemented for reducing the amount of information to process and the energy to consume. In addition, SVMs are equipped with misuse detection techniques and used in identifying network anomalies. The system has many distributed intrusion detection nodes to communicate each other to identify attacks.

Denial of Service and Probe attacks were considered for testing as they are most common in wireless sensor based network environment. The efficient algorithm for choosing optimal distributed SVMs is:

- Train and test many SVMs according to selected features in a distributed fashion.
- Select the SVMs with the rate of accuracy > 95 %
- Select the SVM with less input features.
- We embed the trained model in the IDS system.

The performance of proposed distributed systems is evaluated and mentioned below.

Table 6: Evaluation based on accuracy of IDS

Number of Features	Accuracy	Detection Rate
9	97.80 %	93.66 %
7	98.47 %	95.61 %
5	96.95 %	91.21 %
4	98.39 %	95.37 %

The proposed approach claims to reduce energy consumption and obtaining higher accuracy with less trained data.

Authentication using Keystroke Dynamics

For this action to be carried out in the field of cybersecurity, there is a proposed technique to handle. For keystroke dynamics, there is a type of approach in neural networks. It is Probabilistic Neural Network (PNN). Generally, keystroke dynamics is defined as "a cluster of biometrics based on their behavior classified into a group that captures the typing style of a user". The system is evaluated by training and testing on a dataset containing login/password keystrokes of 50 people. The researcher Revett et al. gave 30 persons to login as an unauthorized person multiple times instead of authorized users. There are 8 parameters that were considered and monitored during enrollment and authentication attempts. The parameters are:

- Digraphs (DG, two-letter combinations).
- Trigraphs (TG, three-letter combinations).
- Total username time.
- Total password time.
- Total entry time.
- Scan code.
- Speed
- Edit distance.

The data obtained using these parameters is sent into the PNN system and tested. The accuracy obtained by this classification of imposter is 90%. PNN was compared to a multi-layer perceptron neural network (MLPNN) using back-propagation technique and it was found that PNN training time is 4 times less than MLPNN. The summation of False Acceptance and False Rejection Rates of PNN is 1.5 times less than MLPNN.

The comparison of the algorithms can be seen in below mentioned table. The values of this table is obtained by the total of the False Acceptance Rate (FAR) and False Recognition Rate (FRR) of PNN and MLPNN systems.

Table 7: FAR + FRR of PNN and MLPNN

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

Security testing of assets and Protocol Implementation

The main objective of researchers in their research on testing confidentiality of message under Dolev-Yao model of attackers" that injects a message into original one. Generally, there is no solution for testing of a protocol implementation security. However, experiments can be performed with respect to a problem restricted to a finite number of messages. And the main goal is to find some weak spots (that violate security) in a protocol black-box implementation, deploying L* learning algorithm. In this algorithm, the researchers create a teacher that performs three principal actions:

1) Generating an output query given an input sequence.
2) Generating a counter example that a system outputs as an incorrect result when analyzing it.
3) Augmentation of alphabets, appending of new input symbols in addition to the existing ones.
They displayed the effectiveness of their proposed technique by testing them on three 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 and detected flaws in N-S-L and TMN and also, confirming that SSL is secured.

Breaking of Human Interaction Proofs (CAPTCHAs)
In this section, it discuss how the Human Interaction Proofs (or CAPTCHAs) can be broken by implementing machine learning algorithms. The researchers experimented on seven various HIPs and learned their common strengths and weaknesses. The proposed approach is aimed at locating the characters (segmentation step) and employing neural network for character recognition.
6 experiments were conducted with EZ-Gimpy/Yahoo, Yahoo v2, mailblocks, register, ticketmaster, and Google HIPs. Each experiment was split into two parts:
(a) Recognition with 1,600 HIPs for training, 200 for validation, and 200 for testing).
(b) Segmentation with 500 HIPs for testing segmentation.
At the recognition stage, different computer vision(CV) techniques like converting to grayscale, thresholding to black and white, dilating and eroding, and selecting large CCs with sizes close to HIP char sizes were applied.
Segmentation stage is relatively difficult for the following reasons: (a)Computationally expensive.
(b)Complex segmentation function because of an immense non-valid pattern space.
(c)Identifying valid characters face more difficulty.

Table 8: Success Rates

HIP	Success rate for segmentation	Success rate for recognition given correct segmentation	Total
Mailblocks	88.8 %	95.9 %	66.2 %
Register	95.4 %	87.1 %	47.8 %
Yahoo/EZ-Gimpy	56.2 %	90.3 %	34.4 %
Ticketmaster	16.6 %	82.3 %	4.9 %
Yahoo ver. 2	58.4 %	95.2 %	45.7 %
Google/Gmail	10.2 %	89.3 %	4.89 %

Cryptography
Researchers developed a fast and efficient cryptographic system based on delayed chaotic hopfield neural networks. The researchers claim that, the proposed system is secured because “the difficult synchronization of chaotic neural networks with time varying delay”.
Kinzel and Kanter demonstrated how synchronized neural networks can be used for a secret key exchange over a public channel. During the training stage two neural networks start with random weight vectors and receive an arbitrary identical input sequence every cycle. The weights change only if the obtained outputs of neural networks are same. After a short time, the weight vectors of both neural networks become identical.

Detection of spam in Social Networks
There is an observation, that attackers use spamming techniques for social networks to perform phishing attacks, injecting malwares etc. To protect the systems from malicious attacks, the organizations are placing honeypots. These honeypots are developed in such a way that they have a capability of detection of spamming present in social networks of their organization.

The solution for this purpose is based on a machine learning algorithm known as SVM. The false positive rate and high in precision. This technique represents a genuine user profile with a bot helps in gathering spam profiles and feeds them into a classifier based on SVM. The accuracy of the technique is calculated by taking a couple of websites. From those websites, several genuine users were present and their data is retrieved. Profiles such as traps, profiles infiltrating into organization, detection of repeating profiles. The parameters for this technique are: legitimate profiles, deception of spammer profiles, number of spammers and promoters present in social organization.

Security provided to a Machine Learning product

Researchers working on products based on machine learning like cortana, google home and alexa, need to provide counter measures from prevention of compromising the devices.

Researchers need to publish anatomy of the attacks that target systems based on machine learning and artificial intelligence devices:

a) Causative attacks alerting the training process.
b) Attacks on integrity and availability, making false positives as a breach into a system.
c) Exploratory attacks exploiting the existing vulnerabilities.
d) Targeted attacks directed to certain input.
e) Indiscriminate attacks in which inputs fail.

For the above mentioned attacks, the researchers came up with a defensive technique named Reject On Negative Impact named as RONI. This algorithm excludes the training data points leading to negative impact during classification.

There are two types of defenses proposed by them.

One type of defense technique is against exploratory attacks. In this defense technique, attacker creates a distribution of evaluation that the learner predicts. To defend from this attack, there is an option of keeping limitations to training data and making it complex for an attacker to perform reverse engineering attack. Additionally, this defender has a capability to limit the feedback received by an attacker as it becomes complex to enter into the system.

Second type of defense technique is against causative attacks. In this, the attacker has a possibility to manipulate distributions on training and evaluation. At this point, the defender deploys the RONI defense system. In this system, two classifiers are present.

a) One classifier is trained using a base training set.
b) Trained with not only a base set but also with candidate instance.

If the errors of the above mentioned two classifiers differ from each other.

By applying this defensive algorithm, the attackers started attacking the spam detection system [23] and elaborated the strength of the system against available attacks.

CONCLUSION

Machine learning is a growing technology which is implemented in wide areas of information security and also in many other industries. The use of this technology in cyber security is to develop anti-phishing algorithms and network intrusion detection systems in a robust nature. This technology is used for developing authentication systems, evaluation of protocols, security assessment for human interaction proofs etc. The classifiers present in this technology are exposed to vulnerabilities and malicious attacks. Researchers have been constantly working on improvisation of strength of these algorithms and defend them from various attacks. Machine learning in the field of information security is developed in such a way that it has a capacity to address various challenges in this complex domain.

REFERENCES

1) Ford, Vitaly, and Ambareen Siraj. "Applications of machine learning in cyber security." Proceedings of the 27th international conference on computer applications in industry and engineering. Vol. 118. Kota Kinabalu: IEEE Xplore, 2014.
2) Yavanoglu, O. and Aydos, M., 2017, December. A review on cyber security datasets for machine learning algorithms. In 2017 IEEE international conference on big data (big data) (pp. 2186-2193). IEEE.

3) Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
4) Soni, Sumit, and Bharat Bhushan. "Use of Machine Learning algorithms for designing efficient cyber security solutions." 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). Vol. 1. IEEE, 2019.