International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Literature Survey on Detection of Web Attacks Using Machine Learning

Abhishek Gupta[1], Ankit Jain[1], Samartha Yadav[1], Harsh Taneja [2]

[1]Student, CSE, Bharati Vidyapeeth's College of Engineering, New Delhi, India
[2]Assistant Professor, Bharati Vidyapeeth's College of Engineering, New Delhi, India

ABSTRACT

With the increase in reliability on web applications for day to day activities There has been an immense growth in number of web applications that are being created and used world-wide. But this elevation of web applications has led to the increase in the exploitation of vulnerabilities in web apps that has further lead to web attacks. The industry has suffered due to these rising web attacks. Yet the evolution of information technology and the advent of machine learning has eased web attacks' detection. The detection of these web attacks relies upon the patterns obtained via Machine Learning algorithms which further aids in deciding whether the web attack has been caused or not. This paper comprises techniques that are Classification, Support Vector Machine and Clustering with respect to web attacks and their detection.

Keywords: Machine Learning, Web Attacks, Classification, Support Vector Machines, Clustering

I. INTRODUCTION

In the modern era of the internet, the rapid development of web applications has created many security problems related to intrusions not just on the computer, network systems, but also on web applications themselves. As the users have grown and the security has become stronger so have the web attacks. Security of web applications has become very important as the information processed by those web applications can be of immense value. These web attacks harm to users significantly and might result in the exploitation of their personal information. Some of the web-based attacks that are used commonly in recent times are Buffer overflow attack, cross-site scripting(XSS) attack, Cross-site request forgery attack, Path Traversal attack, SQL injection and iFrame injection attack.

Machine Learning has proven to be a robust tool for detecting such attacks. We use different processes to identify different types of intrusions. In this paper, we have presented the idea and the processes involved as to how machine learning is efficient enough to detect the increasing web attacks. Some of the Machine learning processes involved are Classification, Support Vector Machine (SVM) and Clustering which help us to identify whether there is an attack on our web application or not.

The paper has been segmented as: Segment 1 presents the brief introduction about the paper. In Section 2, brief introduction of various types of Web Attacks are discussed. Segment 3 presents attack detection using Classification, Support Vector

Machine and Clustering based approach. Segment 4 gives the conclusion derived from this article.

II. WEB ATTACKS

Now-a-days, mostly every individual in his day to day life and industries for most of their technical work rely on web-based applications. But, with the growth in the number of web-based applications, there is a risk that these applications become vulnerable towards web attacks. Most of the websites, including the business websites are imbued with web attacks which is undesirable. So basically, a web attack can be defined as an intrusion that is unwanted to the website resource and also can harm the personal reputation of a person or an entire company. A web attack is proved more dangerous to business websites since it deals with the financial data. Web attacks can be further classified as passive and active attacks. In a passive web attack an attacker can access the private data. It does not intend to damage or manipulate the data. An active web attack can be termed as an attack in which the intruder wants to damage or manipulate the private data instead of just monitoring it. It can also be differentiated on the basis of where and when the attack is taking place into the following two categories: Static web attacks and Dynamic web attacks.

Difference between them briefly explained in Table 1

TABLE I

DIFFERENCE BETWEEN STATIC AND DYNAMIC WEB ATTACKS

Static Web Attacks	Dynamic Web attacks
These attacks look for the security vulnerability in web servers, application servers, database servers etc.	These attacks tend to requests legal pages from the server but they modify the parameters that the server expects and hence manipulate the content and extract the main content in the process.
Static attacks are not as severe as dynamic attacks and do not cause much harm.	Dynamic attacks are more severe than static attacks since it involves disclosure of information about web server, command execution etc.

Some of the most common and severe web attacks are:

- Cross-site Scripting
- SQL injection
- Cross-site request forgery
- Buffer Overflow Attack.

I. SQL Injection: In this technique, vulnerabilities are exploited, and an injection of falsified code in SQL query is injected via web page input. This technique might destroy the entire database of the website.

II. Cross-site Scripting (XSS): In XSS, an attacker injects the web -based application with malicious code in the form of browser side scripts through invalid inputs. This is only possible because of errors made at the time of development of the website and can easily occur while output is generated for a particular input without validating for encoding it.

III. Cross-site request forgery (CSRF): In CSRF the end user is tricked to execute some unwanted actions which they are not aware of on the web page. These unwanted actions can make requests like transferring funds, changing their email address,etc without them even knowing. This attack is among the four most common web attacks present today.

IV. Buffer Overflow Attack: This happens when more than allocated data is stored in a buffer, and that data leaks out into the nearby buffers which makes the system corrupt or overwrite whatever data they were holding.

III. MACHINE LEARNING IN ATTACK DETECTION

Machine learning can be defined as a type of Artificial learning in which a machine tends to learn things, adapt itself to any change in data without being externally programmed again and again. It can be further classified as of two types: supervised and unsupervised learning. In case of supervised learning, output datasets are provided as a base model for the machine to learn and adapt whereas in unsupervised learning, there is no system of providing datasets, rather the output datasets are clustered. Supervised learning further includes Classification and Support Vector Machines(SVM) whereas Clustering is a part of unsupervised learning.

Machine learning is widely used for the detection of attacks on we-based application. Classification technique includes Naïve Bayes classifier which can tell the probability of a malicious and non-malicious code. SVM maximizes the margin of training data which results in more datasets for further algorithms to be used. Clustering, as the name suggests, is the assignments of similar sets into a cluster. In machine learning, using many certain models, a code execution, and server execution can be classified as malicious, intrusion based or not.

A. Classification

The goal of classification is to select hypothesis from a set of unlabeled data that best fits a set labeled data. The algorithms use training data to learn which classifier classifies new texts.

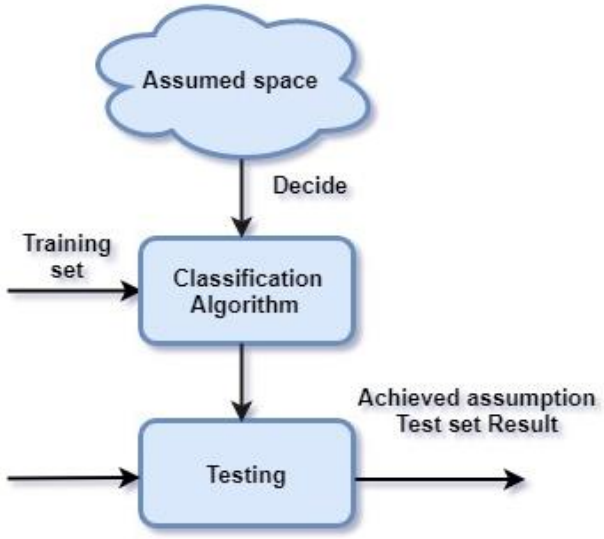

Figure 1. Block diagram of classification algorithm

There are three most popular algorithms used for classification in machine learning.

a) **K-Nearest Neighbor Classifier**: It is a very popular pattern recognition algorithm. It works on an assumption that nature of members of same class will be similar. It is simple and effective method.

b) **Naïve Bayes Method**: It makes independent assumption based on Bayes theorem. It works on a small set of training data to execute algorithm. In this algorithm it is assured of high accuracy along with great speed.

c) **Decision Trees:** This categorization functions on the rule-based inference. Generally, Rules are in the form of 'If..then', where 'If' portion includes conditions and 'then' portion includes conclusion.

Table 2 shows various classification methods used for detection of web attacks. These methods are based on variety of models on classification.

TABLE III
VARIOUS METHODS OF CLASSIFICATION USED TO DETECT WEB ATTACKS

Method	DESCRIPTION	REFERENCE
EDADT (Efficient Data Adaptive Decision Tree) algorithm	Proposes a way that utilizes internal query tree for effective performance of framework from database log.	B. D. Priyaa and M. I. Devi[1]
k-NN Text categorization	Idea of shared nearest neighbours is deployed.	Yun-lei Cai, Duo Ji , Dong-feng Cai[2]
ML-kNN (Multi label lazy learning)	A method for every unseen instance of kNN which is multi label, nearest k neighbours in the training set are identified. MAP principle implemented for determination of unseen instance via statistical information obtained from label sets of neighbouring instances.	Min-Ling Zhang, Zhi-Hua Zhou[3]
SBA algorithm	Novel classification algorithm is acquired by employing dissimilarities for learning decision tree from data having low time and complexity.	Neha Patel, Divakar Singh[4]
a) Averaging	a) Naïve Bayes' model and kernel density estimation is reprocessed by substituting each pdf with expected value and transforming unexpected to deterministic point valued data.	Jiangtao Ren, Sau Dan Lee, Xianlu Chen, Ben Kao, Reynold Cheng and David Cheung[5]
b) Distribution-based	b) Evaluation of class conditional density of uncertain data is done here.	
Classifier model and transforming model	This model transforms each entry into vector and vector.	S. Zhang, B. Li, J. Li, M. Zhang and Y. Chen[6]

B. Support Vector Machine (SVM)

Support vector machines are associated with learning algorithms which label every vector by its corresponding class and plot the training vectors in high-dimensional feature space. Data is categorization of data by SVM, analysing mathematical functions, kernels for constructing in multi-dimensional space through which cases of different class label are separated.

Although it is a rapid algorithm yet it's implementation is complicated. SVM focuses at finding optimal differentiating generalized plane that escalates the training data margins. The problem is solved by differentiation of positive and negative members of the class. Structural Risk Minimization principle is its basis.

To achieve this goal, four different kernel functions are used:

a) Linear: $K(xi, xj) = xi^T xj$

b) Polynomial: The polynomial kernel of the form having degree d is

$K(xi, xj) = (xixj)$

c) RBF: The Gaussian kernel, known also as the radial basis function, is of the form

$K(Xi, Xj) = \exp(-||xi, xj||) / 2\sigma^2$

d) Sigmoid: The sigmoid kernel is of the form

$$K(xi, xj) = \tanh(k(xixj) + r)$$

Mapping of the sample by RBF kernel is done into higher dimensional space, non -linearly for handling case of non-linear relation between class labels and attributes.

Two types of approaches are followed: First involves combining several binary classifiers and second, considers all training data into the formula. The best suited separating hyperplane between classes by concentrating mainly at the edge of class descriptor is found by SVM.

High accuracy in even small sets of data is assured. It has high generalization ability and organizes large spaces of characteristics. Support vector machines used for detection of web attacks has been symbolized by Table 3. For the detection of web attacks, various techniques are amalgamated with SVM.

TABLE IIIII

SVM USED FOR DETECTION OF WEB ATTACKS

METHOD	DESCRIPTION	REFERNCE
SQL injection attack Detection using SVM	Here, the incoming SQL query is broken into tokens which are then feeded to the SVM classifier to predict a labeled output and replace malicious query with original query.	Romil Rawat, Shailendra Kumar Shrivastav[8]
Intrusion Detection with Support Vector Machines and Neural Networks	In this model, SVMs and Neural networks have been compared for evaluating intrusion.	Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung[9]
Cyber Attack Detection System based on iSVM	This modifies the Gaussian kernel in a such that distinguishable between classes elevates.	Shailendra Singh, Sanjay Silakari[10]
DDoS Detection Model using multiple SVMs and TRA	Here, the authors proposed a model that uses multiple SVMs for higher detection of accuracy and low negatives.	Jungtaek Seo, Cheolho Lee, Taeshik Shon, KyuHyung Cho, and, Jongsub Moon[11]
OCSVM for Detecting Anomalous Windows Registry Accesses	The author presents a new ID that supervises accesses to window Registry using RAD.	Katherine A. Heller, Krysta M. Svore, Angelos D. Keromytis, Salvatore J. Stolfo.[12]
Support Vector Machines (Hierarchical)	H-SVM are of two kinds that are based on the separability measure in feature space, k-tree SVM and binary tree SVM, the decision trees of these two are constructed with two agglomerative bottom-up clustering algorithms respectively.	Liu Zhigang, Shi Wenzhong, Qin Qianqing, Li Xiaowen, Xie Donghui[13]
On the Performance of SVM based Jamming Attacks Detection Algorithm in base station	The author bestows an algorithm for detection of jamming attacks based on SVM at the base station in wireless cellular networks . It should not require excessive hardware requirements for external	Javad Afshar Jahanshahi and Mohammad Eslami[14]

	information.	

C. Clustering

It aims at splitting a finite unlabeled data into two different clusters. These clusters in terms of web-based attacks can be termed as malicious and non-malicious statements, comments etc. There are many methods and models proposed by many researchers to detect various web attacks.

Table 4 shows various clustering methods used for detection of web attacks. These methods are based on variety of models on clustering. Different models are combined with various clustering algorithms for web-based attacks detection. Y. Chen, X. Chen, H. Tian, T. Wang and Y. Cai in [15] have recommended a blind detection model for eliciting the real source of DDoS attack that make use of k-harmonic means clustering on a cluster of similar packets.

In [18], the authors have suggested that tracing the single real source is difficult, so a cluster of similar packets are used for clustering. The accuracy using this model is approximately 92.54% that is recorded. Another model was suggested by S. Nath, N. Marchang and A. Taggu[17], Mitigating SSDF attack using medoids clustering. This collaborative method is preferred over single sensing method since it achieves more accurate sensing decision. For establishing the presence of attackers, the stocking of sensing report is mined at the fusion center.
A composite model for detection of phishing-sites [16], proposed by R. Patil, B. Dasharath Dhamdhere, K. S. Dhonde, R. G. Chinchwade and S. B. Mehetre. This model is a hybrid of two approaches. K-means clustering clusters the database on initial URL features and predicts the of validity by implementing Naïve Bayes Classifier prediction.

For anomaly detection [19], a strategy of hardware-based clustering was suggested by Khaled Labib and V. Rao Vemuri, where hardware implementation of k-means algorithm is wielded to cluster network which turn out to be approximately 300 times faster than software-based implementation.

TABLE IVV
VARIOUS CLUSTERING METHODS USED TO DETECT CERTAIN WEB ATTACKS

METHOD	DESCRIPTION	REFERNCE
Technique of blind detection to trace real source of DDoS attack	This technique utilizes k-harmonic means clustering on a cluster containing similar packets for real source of DDoS attacks instead of working on single packet.	Y. Chen, X. Chen, H. Tian, T. Wang and Y. Cai[15]
A composite model for detection of phishing-sites	In this model, k-means clustering is used to cluster database and Naïve Bayes Classifier for determining the validity of website as valid or invalid phish.	R. Patil, B. Dasharath Dhamdhere, K. S. Dhonde, R. G. Chinchwade and S. B. Mehetre[16]
Mitigation of SSDF attack by k-medoids clustering	This method employs k-medoids clustering algorithm in Cognitive Radio Networks in which the sensing report are collected and mined at the fusion center for deducing the presence of attackers. In collaborative mining is preferred over individual sensing	S. Nath, N. Marchang and A. Taggu[17]

	in Cognitive Radio Networks.	
Intrusion Detection (Semi-Supervised Fuzzy C-Means based clustering Algo.)	The authors propound a semi-supervised learning algorithm combined with Fuzzy C-Means algorithm.. Detect ion of attack behaviours by semi-supervised Fuzzy C-means clustering algorithm is more coherent .	F. Guorui, Z. Xinguo and W. Jian[18]
A clustering based approach in process control systems	This is a novel based approach that works upon the Gaussian mixture model to cluster sensor management values and found that this method has outperforms the clustering methods.	I. Kiss, B. Genge and P. Haller [19]
Detection Scheme (Sybil Attack) for detecting a centralized clustering based hierarchical network	A novel detection scheme is being advocated for Sybil attack. Analysis of neighbouring nodes is done by collaborating any two nodes with high energy.	M. A. Jan, P. Nanda, X. He and R. P. Liu [20]

IV. CONCLUSION

Machine Learning is turning out to be an extremely useful platform for detecting any web-based attack. In this paper, we have studied various methods of detecting a web attack using classification, SVM and clustering by many researchers. Each of them has proposed different models to detect an attack more efficiently than previously described method.

From most of the paper it is evident that performance of classification algorithm in text classification is greatly affected by the quality of data set, representation techniques. Hence it was deduced that k-means and bisecting k-means have the best performance in terms of time complexity and cluster quality produced among the unsupervised techniques. Whereas, among the supervised techniques, support vector machines performs the best while naive bayes the worst. This paper is basically targeted for future reference by researchers.

V. REFERENCES

[1] B. D. Priyaa and M. I. Devi, "Hybrid SQL injection detection system," 2016 *3rd International Conference on Advanced Computing and Communication Systems (ICACCS),* Coimbatore, India, 2016

[2] Yun-lei Cai, Duo Ji ,Dong-feng Cai, “A KNN Research Paper Classification MethodBased on Shared Nearest Neighbor”, *Proceedings of NTCIR-8 Workshop Meeting, June 15–18, 2010,* Tokyo, Japan

[3] Ml-knn: “A Lazy Learning Approach to Multi-Label Learning”, Min-Ling Zhang, Zhi-Hua Zhou,*Pattern Recognition, Volume 40, Issue 7, July 2007, Pages 2038-2048*

[4] Neha Patel, Divakar Singh,”An Algorithm to Construct Decision Tree for Machine Learning based on Similarity Factor”,*International Journal of Computer Applications (0975 – 8887) Volume 111 – No 10,* February 2015

[5] J. Ren, S. D. Lee, X. Chen, B. Kao, R. Cheng and D. Cheung, "Naive Bayes Classification of Uncertain Data," 2009 *Ninth IEEE International Conference on Data Mining,* Miami, *FL*, 2009

[6] S. Zhang, B. Li, J. Li, M. Zhang and Y. Chen, "A Novel Anomaly Detection Approach for Mitigating Web-Based Attacks Against Clouds," *Cyber Security*

sand Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference, New York, NY, 2015

[7] J. Yan, X. Yun, P. Zhang, J. Tan and L. Guo, "A New Weighted Ensemble Model for Detecting DoS Attack Streams," *Intelligence and Intelligent Agent Technology (WI-IAT), 2010 IEEE/WIC/ACM International Conference on,* Toronto, ON, 2010

[8] Romil Rawat,Shailendra Kumar Shrivastav, "SQL injection attack Detection using SVM*", International Journal of Computer Applications (0975 – 8887)Volume 42– No.13*, March 2012

[9] S. Mukkamala, G. Janoski and A. Sung, "Intrusion detection using neural networks and support vector machines," *Neural Networks, 2002. IJCNN '02. Proceedings of the 2002 International Joint Conference on*, Honolulu, HI, 2002

[10] Shailendra Singh and Sanjay Silakari , "Cyber Attack Detection System based on Improved SupportVector Machine", *International Journal of Security and Its ApplicationsVol.9, No.9 (2015), pp.371-386*

[11] Ungtaek Seo , Cheolho Lee , Taeshik Shon , KyuHyung Cho ,and Jongsub MoonA, "New DDoS Detection Model Using Multiple SVMs and TRA", *T. Enokido et al. (Eds.): EUC Workshops 2005, LNCS 3823, pp. 976 – 985, 2005. © IFIP International Federation for Information Processing 2005*

[12] Katherine A. Heller,Krysta M. Svore, Angelos D. Keromytis,Salvatore J. Stolfo. , "One Class Support Vector Machines for Detecting Anomalous Windows Registry Accesses", *Proc. of the workshop on Data Mining for Computer Security. Vol. 9. 2003.*

[13] Liu Zhigang, Shi Wenzhong, Qin Qianqing, Li Xiaowen and Xie Donghui, "Hierarchical support vector machines," *Proceedings. 2005 IEEE International Geoscience and Remote Sensing Symposium, 2005. IGARSS '05., 2005, pp. 4 pp*.

[14] J. A. Jahanshahi and M. Eslami, "On the performance of SVM based jamming attacks detection algorithm in base station," *Communication Technologies Workshop (Swe - CTW), 2011 IEEE Swedish*, Stockholm, 2011, pp. 109- 113.

[15] Y. Chen, X. Chen, H. Tian, T. Wang and Y. Cai, "A blind detection method for tracing the real source of DDo S attack packets by cluster matching," *2016 8th IEEE International Conference on Communication Software and Networks(ICCSN)*, Beijing, China, 2016, pp. 551-555.

[16] R. Patil, B. Dasharath Dhamdhere, K. S. Dhonde, R. G. Chinchwade and S. B. Mehetre, "A hybrid model to detect phishing-sites using clustering and Bayesian approach," *Convergence of Technology (I2CT), 2014 International Conference*, Pune, 2014, pp. 1-5

[17] S. Nath, N. Marchang and A. Taggu, "Mitigating SSDF attack using k-medoids clustering in Cognitive Radio Networks," *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference* , Abu Dhabi, 2015, pp. 275-282.

[18] F. Guorui, Z. Xinguo and W. Jian, "Intrusion detection based on the semi-supervised Fuzzy C-Means clustering algorithm," *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on – ,* Yichang, 2012, pp. 2667- 2670.

[19] I. Kiss, B. Genge and P. Haller, "A clustering-based approach to detect cyber-attacks in process control systems," *2015 IEEE 13th International Conference on Industrial Informatics (INDIN),* Cambridge, 2015, pp. 142-148.

[20] M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-Based Hierarchical Network," *Trustcom/BigDataSE/ISPA, 2015 IEEE, Helsinki, 2015, pp. 318-325.*

[21] Z. Zhang and S. R. Kulkarni, "Detection of shilling attacks in recommender systems via spectral clustering," *Information Fusion (FUSION), 2014 17th International Conference on – , Salamanca, 2014, pp. 1-8.*

[22] X. Qin, T. Xu and C. Wang, "DDoS Attack Detection Using Flow Entropy and Clustering Technique," *201511th International Conference on Computational Intelligence and Security (CIS),* Shenzhen, 2015, *pp. 412-415.*

[23] M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized ClusteringBased Hierarchical Network," *Trustcom/BigDataSE/ISPA, 2015 IEEE*, Helsinki, 2015, pp. 318-325.

[24] R. C. Patil and D. R. Patil, "Web spam detection using SVM classifier," *Intelligent Systems and*

Control (ISCO), 2015 IEEE 9th International Conference on – , Coimbatore, 2015

[25] P. J. Koyande and K. P. Shirsat, "T - vigilant: To unmask radical attacks and halt the innocents," *2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, Dehradun, 2015