2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT).
India Habitat Centre, Lodhi Road, New Delhi, India. Sep 23-25, 2022

Detection of Cyber Attacks: XSS, SQLI, Phishing Attacks and Detecting Intrusion Using Machine Learning Algorithms

Aashutosh Bhardwaj[1]
Information Technology
International Institute of Information Technology,
Pune, India
aashutosh2899@gmail.com

Saheb Singh Chandok[2]
Information Technology
International Institute of Information Technology,
Pune, India
sahebchandok2001@gmail.com

Aniket Bagnawar[3]
Information Technology
International Institute of Information Technology,
Pune, India
bagnawaraniket66@gmail.com

Shubham Mishra[4]
Information Technology
International Institute of Information Technology,
Pune, India
shubhammishra4579@gmail.com

Dr. Deepak Uplaonkar[5]
Information Technology
International Institute of Information Technology,
Pune, India
uplaonkar@gmail.com

2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT) | 978-1-6654-9365-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/GLOBCONPT57482.2022.9938367

Abstract— **Cyber-crime is spreading throughout the world, exploiting any type of vulnerability in the cloud computing platform. Ethical hackers are primarily concerned in identifying flaws and recommending mitigation measures. In the cyber security world, there is a pressing need for the development of effective techniques. The majority of IDS techniques used today are incapable of dealing with the dynamic and complex nature of cyber-attacks on computer networks. In cyber security, machine learning approaches have been utilized to handle important concerns such as intrusion detection, XSS, SQLI, and phishing detection. Machine learning approaches have been employed in order to detect the issues such as XSS, SQLI, Phishing attacks etc. In this study XSS attack is detected using CNN approach, SQLI attack is detected using Logistic Regression approach, phishing is detected using SVM approach. In addition to the above specified attacks: DTC, BNB, KNN approaches are employed to detect the intrusion in the system. As a result, CNN approach yields 98.59% accuracy for detecting XSS attacks, Logistic Regression approach yields 92.85% accuracy for SQLI, SVM approach yields 85.62% accuracy for phishing attacks. Approaches like DTC, BNB, KNN yields an accuracy of 99.47%, 90.67% and 99.16% respectively for detecting intrusions.**

Keywords—SQL Injection (SQLI), Cross-Site Scripting (XSS), Phishing Attacks, and Intrusion Detection Attack (IDS), Convolutional Neural Network (CNN), K Nearest Neighbor (KNN), Bernoulli Naïve Bayes (BNB), Support Vector Machine (SVM), Machine Learning (ML), Decision Tree Classifier (DTC) etc.

I. INTRODUCTION

Physical things are now connected to cyber networks in the current era of information and communication technology, and these connections are referred to as "cyber-physical systems". Stateful firewalls, also known as attack detection and prevention, identify and block attacks on network traffic. Exploits can be data acquisition probes or attacks aimed at compromise, invalidation, or damage to a network or network resource. The border between the two exploit targets may be blurred. For example, a TCP SYN segment flood can be an IP address sweep that triggers a response from an active host, or it can be a SYN flood attack that aims to overwhelm the network and cause it to malfunction. Intelligence gathering efforts can be seen as a precursor to an imminent attack, as attackers usually precede the attack by scouting the target. That is, it forms the first phase of the attack. Therefore, the term exploit includes both reconnaissance and offensive activities, and the difference between the two is not always clear. Computer networks and the Internet have taken on significant importance in both our daily lives and our organizations. Malicious activity is becoming more and more common as we become more dependent on computers and communication networks. Network attacks are a major problem in today's communications environment. To ensure the reliable functionality of your network and the security of your user information, you need to monitor and analyze network traffic to detect malicious activity and attacks. Network threats have recently been detected using machine learning techniques. Network traffic can be analyzed to find patterns and similarities using machine learning algorithms. There is no requirement for manual analysis to derive attack patterns, unlike signature-based approaches. You may automatically create predictive models to find network assaults by using machine learning algorithms. Particularly as a result of the development of fifth-generation networks and artificial intelligence technologies in cybersecurity, new dangers and challenges to wireless communication systems have emerged. This system offers a summary of attack detection strategies that make use of deep learning methods. It introduces different applications that use deep learning structures and explains the fundamental network security and attack detection challenges. The focus is on attack detection systems based on different types of architectures, including: B. Auto encoders, hostile generation networks, recurrent neural networks, convolutional neural networks based on the classification of deep learning methods. It then provides several benchmark datasets and descriptions, compares the performance of different representational approaches, and presents the current state of attack detection methods using deep learning structures. Finally, we provide a summary of this assignment and go over some suggestions for enhancing attack detection performance through the use of deep learning structures. The main purposes of the above system are: To overcome these shortcomings, typical intrusion detection data must be collected to develop and analyze computer network attack detection mechanisms. In addition to typical normal data, different types of attacks should also be included. Detection of network attacks using machine learning techniques 4. Reduce uptime 5. To improve accuracy and reliability 6. To improve operational efficiency. 7. To provide data security.

II. LITERATURE SURVEY

Nutjahan et al. (2016) [1]. proposes Cyber Physical System cyber-attack detection and prevention. The Chi square detector and Fuzzy logic-based attack classifier (FLAC) were used to identify distributed denial of service and fake data injection attacks. OpNET Simulator has been used to build an example situation. According to simulation results, Chi-square detector and FLAC can accurately identify the aforementioned cyber-physical threats. The above model provided higher accuracy rates for Dos attacks and false data injection attacks when compared to previous models.

Yong Fang et al. (2019) [2]. In this study, the XSS detection model was optimized using RLXSS, a reinforcement learning-based technique. Experimental results show that the proposed RLXSS model successfully mines adversarial samples that avoid black-box and white-box detection while maintaining aggressive features. Additionally, the detection model's escape rate is steadily decreased when the confronting assault model is alternately trained, suggesting that the model can improve the detection model's defense against attacks. As a result the accuracy for the above approach was 99.5% for the above system.

Rishikesh Mahajan et al. (2018) [3]. The goal of phishers is to obtain sensitive information. Experts are looking for dependable solutions for websites that can be attacked by phishing. To detect phishing websites, the Decision Tree, Random Forest, and SVM algorithms are used. In this study researcher detect phishing URLs as well as to narrow down the best machine learning method by analyzing each algorithm's accuracy rate, false positive and false negative rate. As a result, Decision tree algorithm yields 96.80% of accuracy Random Forest approach yields 96.84% of accuracy and SVM approach yields 96.40% of accuracy for the above system.

Vishnu. B. et al. (2018) [4]. XSS can occur when attacker adds malicious code into an application, that can be executed on user's browser. Detecting malicious scripts is an important aspect of an online application's defense. This study uses SVM, KNN and Random Forest algorithms to detect and limit an attack. They have used an intriguing feature that combines syntax and behavioral data to get excellent accuracy on real datasets.

Zohre Nasiri Zarandi et al. (2020) [5]. The CPS model is used in this study. Here one agent acts like a leader and the other agents have to follow the leader. Deep neural network is used for detection. After detection phase, the control system uses reputation algorithm to eliminate the misbehaving agent. Experiments have revealed that deep neural network work much better than the traditional algorithms.

Fawaz A. Mereani et al. (2018) [6]. This study looks into creating classifiers for JavaScript code using SVM, k-NN, and Random Forests to detect and restrict certain attacks, whether they are known or not. It showed that classifiers may produce excellent accuracy and precision on huge real-world data sets without focusing exclusively on obfuscation when an interesting feature set mixing language syntax and behavioral information is used. 94.74% accuracy was achieved by using SVM algorithm. By using KNN, 97.12% accuracy was achieved.

Shinelle Hutchinson et al. (2018) [7]. Phishing's one and only goal is to collect sensitive data from its victims. In this study, we use Random Forest to assess web-based phishing detection. The study identifies some significant URL features and demonstrates how feature selection improves detection performance. In this study, 30 features are extracted. This study achieves an accuracy of 96.3%.

Ines Jemal et al. (2020) [8]. Numerous studies have been done to find ways to nullify SQLI attack, such as either stopping it in its tracks or identifying it as it happens. In this study, author give a summary of the SQL injection attack and categorize the most recent detection and avoidance suggestions. Decision tree and Naive Bayes Algorithm are used in this study. The accuracy achieved is 83.7% and 93.3% respectively.

III. ATTACKS AND ALGORITHM USED

A. SQL Injection:

SQL injection, sometimes referred to as SQLI, is a popular attack method that use malicious SQL code to access information that shouldn't be displayed by manipulating back-end databases. Any number of things, including private customer data, user lists, and sensitive organizational data, can be included in this information. Example of SQL Injection 1. Obtain secret information that can alter SQL queries and produce extra details. Breaks the application logic in clause 2. The application logic might be broken by changing the query. 3. A UNION attack that can access information from several database tables. 4. Look through the database. The database version and structure can be gleaned from this page. Blind SQL insertion. The application response does not contain the outcome of the query you control. To fix this attack, we will train a machine learning platform using a logistic regression model. Logistic regression approach formula:

$$p = \frac{e^{(\beta_0+\beta_1 q)}}{1+e^{(\beta_0+\beta_1 q)}}$$

q is the input value, p is the predicted output, b0 is the bias or intercept term, and b1 is the coefficient for the single input value (x)

B. Cross Site Scripting:

XSS attacks, commonly referred to as cross-site scripting attacks, It is one type of cyber-attack in which malicious code is inserted into the website. An otherwise secure website. An attacker takes advantage of a weakness in a targeted web application to send the user malicious code, most frequently client-side JavaScript. XSS (cross-site scripting) attacks typically target users of the application directly, rather than targeting the application's host itself. When accessing content from users or untrusted sources without the required policies, masking and validation, Businesses and organizations running web applications take risk by opening their door to XSS attack. Increase. When a web application is tricked/bypassed into transmitting data in a format that the user's browser can handle, XSS takes place. The most frequent delivery method is an attacker's mix of HTML with XSS, however XSS can also be used to spread malicious files, plugins, or media assets. To resolve this attack, we will train a machine learning model called Convolutional Neural Network (CNN).

C. Phishing Attack:

Phishing attacks involve sending phone messages that seem to be from reliable sources. Email is typically used for this. The intent is to steal personal information like credit card numbers and login credentials or to infect the victim's computer with malware**.** The message seems to have come from a trusted sender. If it is fooling the victim, they are fooled into revealing sensitive information. Malware can also be downloaded to the target computer. Phishing is a frequent form of social engineering attack designed to acquire user information like login credentials and credit card numbers. This occurs when a perpetrator poses as a reliable source and convinces the target to open an email, instant message, or text message. After that, the recipient is duped into clicking the infected link. This may result in the installation of malware, the freezing of the machine as part of a ransomware assault, or the release of private data’s fix this attack, we will use the SVM model to train a machine learning platform. SVM approach formula

$$F(p) = W^T(p) + c$$

w is the weight vector you wish to minimize, p is the data you're trying to classify, and c is the linear coefficient estimated from the training data in this equation. The SVM's decision boundary is defined by this equation.

D. Intrusion Detection System:

An Intrusion Detection System (IDS) is a hardware or software program that scans your network for malicious activities or rules that have been broken. Using security information and incident management systems, malicious behavior or breaches are often reported or gathered centrally. The purpose of intrusion detection systems is to detect suspicious or malicious activities in network traffic and to ascertain whether an intrusion detection system (IDS) network is being attacked. In order to catch hackers before they really cause network damage, intrusion detection systems are employed to spot irregularities. Either network-based or host-based describe them. Systems for detecting intrusions search for indications of known attacks or deviations from routine behavior. To resolve this attack, we use a decision tree model for training because other algorithms such as BNB and KNN are less accurate than DTC.

IV. PROPOSED SYSTEM

Cybercrime is pervasive around the world and takes advantage of various computing environment weaknesses. The main goals of ethical hackers are to identify vulnerabilities and offer solutions for their mitigation. The cybersecurity community has a pressing need for the creation of efficient methods. The vast majority of IDS solutions in use today are unable to handle the dynamic and intricate nature of cyberattacks on computer networks. Machine learning in cybersecurity has lately grown to be a key concern due to its effectiveness in addressing cybersecurity challenges. Key cybersecurity issues like: B. Intrusion detection, malware classification and detection, spam detection, and phishing detection are addressed using the ML approach. The security analysts can be confident that machine learning can identify cybersecurity risks more effectively than other software-centric approaches, even though it cannot fully automate cybersecurity systems. Effective adaptive approaches can therefore lead to higher detection rates, lower false alarm rates, and lower computational and transmission costs. Examples include machine learning techniques. Our main objective is to demonstrate how fundamentally different the intrusion detection problem is from these other applications, making it far more challenging for the intrusion detection community to utilize machine learning effectively. Machine learning algorithms can be trained and utilized to determine whether a cyberattack occurred. You can notify security users via email when an attack is discovered. To establish whether the attack is a DoS or DDoS attack, you can use any classification technique. An example of a classification algorithm is the support vector machine (SVM), which uses supervised learning to analyze data and spot patterns. Right now, early detection is the best course of action because neither we nor anybody else can predict exactly when, where, or how an attack will take place. This lessens the possibility of such events causing lasting harm. To detect cyberattacks very early and lessen their damage, organizations might employ current solutions or create their own solutions. A system that needs the least amount of human involvement is ideal.

A. Data Preprocessing & Feature Selection

Data manipulation or dropping before it is utilized to ensure or enhance performance is known as data preprocessing, a vital stage in the data mining process. The saying "junk in, rubbish out" is particularly applicable to projects involving data mining and machine learning. The techniques used to collect data are frequently unregulated, which can lead to missing data, out-of-range values (such as Income: 100), and implausible data combinations (such as Sex: Male, Pregnant: Yes). Inaccurate conclusions can be drawn from an analysis of data that hasn't been carefully vetted for these problems. As a result, the quality and representation of the data must come first before any analysis. The most important stage of a machine learning project is typically data preprocessing. For the present system which has 4 different datasets on which each model has been trained requires different methodologies and techniques to preprocess which will eventually help us to gain maximum accuracy for the system.

For Cross Site Scripting Attack (XSS): Some characters have values very big for e.g., 8221 and some are Chinese letters, so we are removing letters having values greater than 8222 and for the rest, we will be considering values greater than 128 and less than 8222 and assign those values so that they can be normalized. Once the data is normalized and processed an image of the matrix is created which will then be fitted into CNN model for training.

For SQL Injection (SQLI): Count Vectorizer is used to convert the strings in the dataset into integer values. The integer values are then concatenated into the main dataset. Then the preprocessed dataset is fitted into Logistic Regression Model for training.

For Intrusion Detection System (IDS): In KDD19 dataset used for IDS we will first remove the outbound i.e., the network traffic going out from our systems will be removed during pre-processing after which we will extract the numerical attribute and then with the help of standard scaler, we will scale it to have zero mean and unit variance. After which with the help of label encoder we converted all the non-numeric attributes to numeric attributes for machine learning model to work effectively. Once the dataset is processed, we will have the top 15 features listed below with the help of Random Forest algorithm. . Fig.1. highlights the various features of intrusion detection system in decreasing order of their importance as listed below:

['src_bytes','dst_bytes','logged_in','count','srv_count','same_srv_rate','diff_srv_rate','dst_host_srv_count','dst_host_same_srv_rate','dst_host_diff_srv_rate','dst_host_same_src_port_rate','dst_host_srv_diff_host_rate','protocol_type','service','flag'].

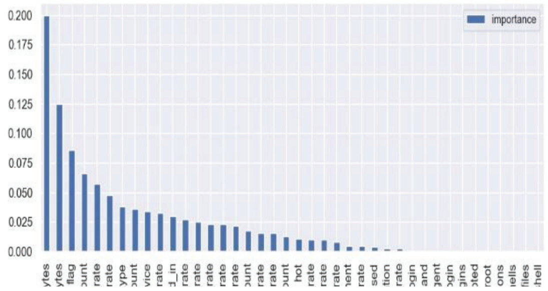

Fig. 1. Importance of Various Features in IDS

For Phishing Attack: We have extracted the following features for pre-processing and detecting live phishing websites like,

Address bar-based features like Using IP address, Long URL to hide suspicious part, URL having @ symbol, Redirecting using // etc.

Abnormal based features like Anchor's URL, Links in <Meta>, and <script> and <link> tags, server form handler (SFH), submitting information to email etc.

HTML and JavaScript based features like website forwarding, status bar customization, disabling right click, using pop up window etc.

Domain features like domain age, DNS_record, website_traffic, PageRank etc. Following are the future scope of this project: The Machine learning is a subfield of computer science that groups and extracts behaviors and entities from data using pattern recognition and artificial intelligence methods. Machine learning algorithms can use previously known patterns and relationships to perform prediction tasks on new data. With today's technology, machine learning algorithms have an impact on our daily lives by being used in a variety of applications. This project has a broad scope because it includes the following features that make it simple to use, understand, and modify: Cyber and network attacks are simple to detect. There is no need to perform additional configuration to handle attacks. Using machine learning techniques to save the environment.

V. RESULT EVALUATION AND PREDICTION

For IDS if the output is anomaly, then it will be considered as an attack, on the other hand if the output is normal then it is a legitimate packet. For SQL Injection, Phishing attack and Cross Site Scripting Attack the output is in the format of 0 and 1, where 0 is not an attack and 1 will be considered as an attack. Once the user login to the portal they will be redirected to the homepage of the web application where the UI directs them to test for various attacks using packets, scripts and SQL queries apart from the above-mentioned attacks user can directly check whether the URL they are visiting is safe or not as the web application automatically warns the user whether it is safe to visit the particular website or not. Following graphs and tables here represents the accuracy of the system and also various metrics to determine how efficient machine learning approach is in detecting the cyber-attacks.

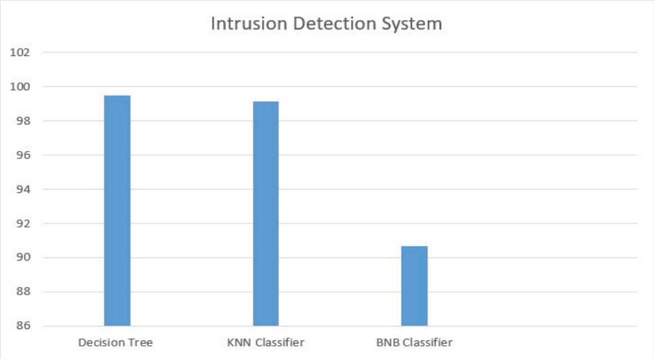

Fig. 2. Accuracy Score of Various Algorithms for IDS

Fig.2. compares the accuracy of Decision Tree, KNN and BNB Classifier. From the obtained result it can be stated that Decision Tree algorithm achieves the maximum accuracy score of 99.47% for the given preprocessed dataset of IDS.

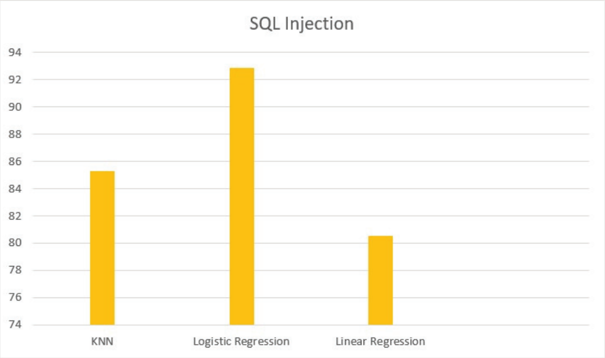

Fig. 3. Accuracy Score of ML Algorithms For SQLI

Fig.3. compares the accuracy of algorithms such as KNN, Logistic Regression and Linear Regression in line with SQLI attacks. Logistic regression achieves the maximum accuracy score of 92.85% on testing dataset.

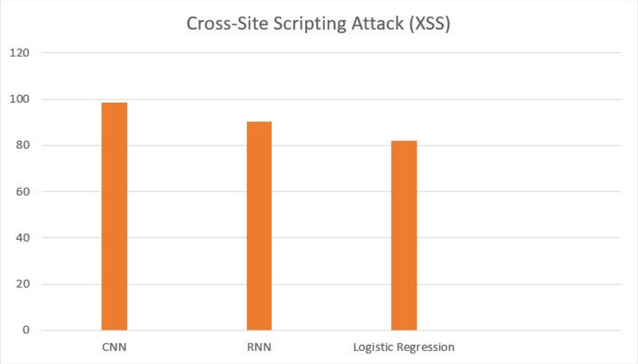

Fig. 4. Accuracy Score of ML Algorithms For XSS

Fig.4 indicates the accuracy score of several machine learning techniques that were used to achieve maximum detection rate and lower false alarm rate according to the results CNN technique gave maximum accuracy score of 98.59%.

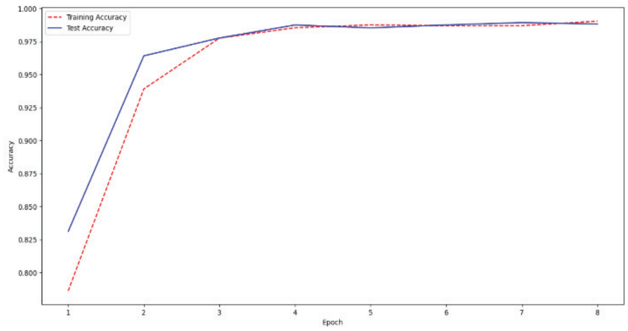

Fig. 5. Epochs Vs Accuracy

Fig.5. plots the increment of accuracy with each epoch in case of CNN model, accuracy increased after every cycle and reached the maximum accuracy of 98.59% after 10 epochs having a batch size of 128.

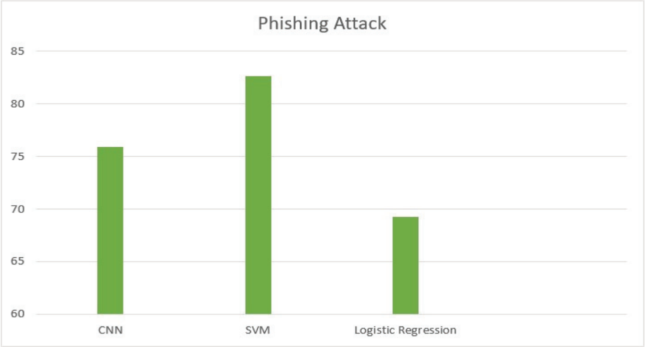

Fig. 6. Accuracy Score of ML Algorithms for Phishing

Fig.6.shows the accuracy score of various algorithms used to train our phishing attack detection model as per the accuracy score obtained the dataset is first trained using SVM algorithm which gave us a maximum accuracy score of 82.63% and later extracted 16 different features from the URL which ultimately helped our system identify whether the given URL is a phishing URL or not.

Table.1. depicts the comparative analysis, which is carried out based on the accuracy score for the various machine learning algorithms.

TABLE I. COMPARATIVE ANALYSIS OF VARIOUS ALGORITHMS BASED ON THEIR ACCURACY

Cyber Attacks	Algorithms Used	Accuracy (%)
IDS	Decision Tree	99.47
	KNN	99.16
	BNB Classifier	90.61
SQLI	KNN	85.27
	Logistic Regression	92.85
	Linear Regression	80.50
XSS	CNN	98.59
	RNN	90.25
	Logistic Regression	82.12
Phishing	CNN	75.89
	SVM	82.63
	Logistic Regression	69.23

VI. CONCLUSION

Applying this control mechanism, it is found that the system could maintain stability, isolate the attacked node, and maintain system performance even in the presence of cyberattacks. A deep layer network with a linear function performs better in a recurrent neural network combined with a deep neural network. As a result, the system might be said to be less complex. The control system decides based on its observations of the system's status as given by the neural network and, if an attack occurs, detects it and isolates it so as not to adversely affect the behavior of other agents.

VII. REFERENCES

[1] Nurjahan, F. Nizam, S. Chaki, S. Al Mamun and M. S. Kaiser, "Attack detection and prevention in the Cyber Physical System," 2016 International Conference on Computer Communication and Informatics (ICCCI), 2016, pp. 1-6, doi: 10.1109/ICCCI.2016.7480022.

[2] Yong Fang, Cheng Huang, Yijia Xu and Yang Li, “RLXSS: Optimizing XSS Detection Model to Defend Against Adversarial Attacks Based on Reinforcement Learning,” Future Internet 2019.

[3] Rishikesh Mahajan, Irfan Siddavatam, “Phishing Website Detection using Machine Learning Algorithms,” International Journal of Computer Applications (0975 – 8887) Volume 181 – No. 23, October 2018

[4] Vishnu. B. A, Ms. Jevitha. K. P., “Prediction of Cross-Site Scripting Attack Using Machine Learning Algorithms”. [2018]

[5] Zohre Nasiri Zarandi, Iman Sharif, “Detection and Identification of Cyber-Attacks in Cyber- Physical Systems Based on Machine Learning Methods”. [2020]

[6] Fawaz A. Mereani, and Jacob M. Howe, “Detecting Cro Cross-Site Scripting Attacks Using Machine Learning,” Springer International Publishing AG, part of Springer Nature 2018.

[7] Shinelle Hutchinson, Zhaohe Zhang, and Qingzhong Liu, “Detecting Phishing Websites with Random Forest,” Third International Conference, MLICOM 2018, Hangzhou, China, July 6-8, 2018, Proceedings

[8] Ines Jemal, Omar Cheikhrouhou, Habib Hamam and Adel Mahfoudhi, “SQL Injection Attack Detection and Prevention Techniques Using Machine Learning,” International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 6 (2020) pp. 569-580

[9] Nutjahan, Farhana Nizam, Shudarshon Chaki, Shamim Al Mamun, M. Shamim, “Attack Detection and Prevention in the Cyber Physical System,” 2016 International Conference on Computer Comrnunication and Informatics (IEEE -2016), Jan. 07 - 09, 2016, Coimbatore, India.

[10] Z. N. Zarandi and I. Sharifi, "Detection and Identification of Cyber-Attacks in Cyber-Physical Systems Based on Machine Learning Methods," 2020 11th International Conference on Information and Knowledge Technology (IKT), 2020, pp. 107-112, doi: 10.1109/IKT51791.2020.9345627.

[11] Ding Chen, Qiseng Yan, Chunwang Wu and Jun Zhao, “SQL Injection Attack Detection and Prevention Techniques Using Deep Learning,” Journal of Physics: Conference Series, Volume 1757, International Conference on Computer Big Data and Artificial Intelligence (ICCBDAI 2020) 24-25 October 2020.

[12] Ercan NurcanYılmaz, SerkanGönen, “Attack detection/prevention system against cyber-attack in industrial control systems,” Computers & Security Volume 77, August 2018, pp 94-105

[13] Arpitha. B, Sharan. R, Brunda. B. M, Indrakumar. D. M, Ramesh. B. E, “Cyber Attack Detection and notifying system using ML Techniques,” International Journal of Engineering Science and Computing (IJESC).

[14] Yirui Wu, Dabao Wei, and Jun Feng, “Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey,” Security Threats to Artificial Intelligence-Driven Wireless Communication Systems, 2020.

[15] Rafał Kozik, Michał Choraś, “Machine Learning Techniques for Cyber Attacks Detection,” Image Processing and Communications Challenges 5, pp 391-398, Springer International Publishing Switzerland 2014.

[16] Pratik Rajendra Chougule, Aniket Sanjay Kumbhar, Vinayak Vasant Pachange, Karan Dinkar Phonde, S. P. Phadtare, “Phishing Websites Detection using Python,” Journal of Web Development and Web Designing, Volume-5, Issue-2 (May-August, 2020)