Detection of Cyber Attacks and Network Attacks Using Machine Learning Algorithms

Sumeet Babasaheb Suryawanshi[1], Tejas Shital katkar[2], Yash Rajiv Ghute[3], Prof. Nikita Kawase[4], Prof. Deepak K. Sharma[5]

[1,2,3] Students and [1]Asst. Prof. of Department of Artificial Intelligence and Data Science,ISB&M College of Engineering, Savitribai Phule Pune University, Pune.
[4,5]Assistant Professor, ISBM COE, Pune

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 natureof cyber-attacks on computer networks. Because of the effectiveness of machine learning in cyber security issues, machine learning for cyber security has recently become a hot topic. In cyber security, machine learning approaches have been utilised to handle important concerns such as intrusion detection, malware classification and detection, spam detection, and phishing detection. Although ML cannot fully automate a cyber-security system, it can identify cyber security threats more efficiently than other software-oriented approaches, relieving security analysts of their burden. As a result, effective adaptive methods, such as machine learning techniques, can yield higher detection rates, lower false alarm rates, and cheaper computing and transmission costs. Our key goal is that the challenge of detecting attacks is fundamentally different from those of these other applications, making it substantially more difficult for the intrusion detection community to apply machine learning effectively. In this study, the CPS is modelled as a network of agents that move in unison with one another, with one agent acting as a leader and commanding the other agents. The proposed strategy in this study is to employ the structure of deep neural networks for the detection phase, which should tell the system of the attack's existence in the early stages of the attack. The use of robust control algorithms in the network to isolate the misbehaving agent in the leader-follower mechanism has been researched. Following the attack detection phase with a deep neural network, the control system uses the reputation algorithm to isolate the misbehaving agent in the presented control method. Experiment results show that deep learning algorithms can detect attacks more effectively than traditional methods, making cyber security simpler, more proactive, and less expensive and more expensive.

KEYWORDS: Network Protocols, Wireless Network, Cyber-crime, Machine learning techniques, cyber-security system, attacks, SQL Injection, Cross-Site Scripting (XSS), Phishing Attacks, and Intrusion Detection Attack (IDS), etc.

1. INTRODUCTION

The In this modem era of information and communication technologies, physical objects are now connected with each other through cyber networks are collectively called cyber physical system. The stateful firewall, also known as attack detection and prevention, identifies and blocks attacks in network traffic. An exploit can be a data-gathering probe or an attack aimed at compromising, disabling, or harming a network or network resource. The line between the two exploit aims can be hazy in some circumstances. For example, a barrage of TCP SYN segments might be an IP address sweep with the intent of triggering responses from active hosts, or it might be a SYN flood attack with the intent of overwhelming a network so that it can no longer function properly. Furthermore, because an attacker usually precedes an attack by performing reconnaissance on the target, we can consider information-gathering efforts as a precursor to an impending attack—that is, they constitute the first stage of an attack. Thus, the term exploit encompasses both reconnaissance and attack activities, and the distinction between the two is not always clear.

The Internet and computer networks have become an important part of our organizations and everyday life.With the increase in our dependence on computers and communication networks, malicious activities have become increasingly prevalent. Network attacks are an important problem in today's communication environments. The network traffic must be monitored and analysed to detect malicious activities and attacks to ensure reliable functionality of the networks and security of users' information.

Recently, machine learning techniques have been applied toward the detection of network attacks. Machine learning models are able to extract similarities and patterns in the network traffic. Unlike signature based methods, there is no need for manual analyses to extract attack patterns. Applying machine learning algorithms can automatically build predictive models for the detection of network attacks.

New threats and difficulties to wireless communication systems have evolved as a result of the development of fifth-generation networks and artificial intelligence technologies, particularly in cyber security. We provide a review of attack detection approaches utilising the strength of deep learning techniques in this system. Specifically, we firstly summarize fundamental problems of network security and attack detection and introduce several successful related applications using deep learning structure. We focus on attack detection systems built on several sorts of architectures, such as auto-encoders, generative adversarial networks, recurrent neural networks, and convolutional neural networks, based on classificationon deep learning methodologies. Following that, we give some benchmark datasets with descriptions and compare the performance of various representation approaches to demonstrate the current state of attack detection methods using deep learning structures. Finally, we summarize this work and discuss some ways to improve the performance of attack detection under thoughts of utilizing deep learning structures.

2. LITERATURE SURVEY

- Nutjahan, Farhana Nizam, Shudarshon Chaki, Shamim Al Mamun, M. Shamim Kaiser," Attack Detection and Prevention in the Cyber Physical System". [2016] [1] In this paper proposes Cyber Physical System cyber-attack detection and prevention To detect distributed denial of service and false data injection attacks, the Chi square detector and Fuzzy logic based attack classifier (FLAC) were utilised. Activity profiling, average packet rate, change point detection algorithm, cusum algorithm, unexpired user sessions, injected incomplete information, and reuse of session key are some of the fuzzy features used to choose the attacks described. An example scenario has been created using

OpNET Simulator. Simulation results depict that the use of Chi-square detector and FLAC are able to detect the mentioned cyber physical attacks with high accuracy. Compared to existing Fuzzy logic based attack detector, the proposed model outperforms the traditional distributed denial of service and false data detector.

- Yong Fang, Cheng Huang, Yijia Xu and Yang Li, “RLXSS: Optimizing XSS Detection Model to Defend Against Adversarial Attacks Based on Reinforcement Learning”. [2019] [2]. In this research, we introduce RLXSS, a reinforcement learning-based strategy for optimising the XSS detection model to defend against adversarial attacks. First, the adversarial samples of the detection model are mined by the adversarial attack model based on reinforcement learning. Secondly, the detection model and the adversarial model are alternately trained. After each round, the newly-excavated adversarial samples are marked as a malicious sample and are used to retrain the detection model. The proposed RLXSS model successfully mines adversarial samples that avoid black-box and white-box detection while retaining aggressive features, according to experimental data. Furthermore, by alternating training the detection model and the confronting assault model, the detection model's escape rate is continuously reduced, indicating that the model can increase the detection model's ability to defend against attacks.
- Rishikesh Mahajan, Irfan Siddavatam, “Phishing Website Detection using Machine Learning Algorithms”. [2018] [3] Phishing is the most basic method of obtaining sensitive information from unsuspecting consumers. The goal of phishers is to obtain sensitive information such as usernames, passwords, and bank account information. Cyber security professionals are now looking for dependable and consistent detection solutions for phishing websites. The purpose of this work is to discuss machine learning technology for detecting phishing URLs by extractingand analysing various aspects of authentic and phishing URLs. To detect phishing websites, the Decision Tree, Random Forest, and Support Vector Machine algorithms are used. The goal of this study is to detect phishing URLs as well as to narrow down the best machine learning method by analysing each algorithm's accuracy rate, false positive and false negative rate.
- Vishnu. B. A, Ms. Jevitha. K. P., “Prediction of Cross-Site Scripting Attack Using Machine Learning Algorithms”. [2018] [4] Cross-site scripting (XSS) is one of the most frequently occurring types of attacks on web applications, hence is of importance in information security. XSS occurs when an attacker injects malicious code, usually JavaScript, into a web application such that it can be executed in the user's browser. Detecting malicious scripts is an important aspect of an online application's defence. This study studies the use of SVM, k-NN, and Random Forests to detect and limit known and undiscovered assaults on JavaScript code by developing classifiers. It shown that using an interesting feature set that combines language syntax and behavioural information resulted in classifiers that provide excellent accuracy and precision on huge real-world data sets without focusing solely on obfuscation.
- Zohre Nasiri Zarandi, Iman Sharif, “Detection and Identification of Cyber-Attacks in Cyber- Physical Systems Based on Machine Learning Methods”. [2020] [5] The CPS is modelled in this study as a network of agents that move in unison with one another, with one agent acting as a leader and the other agents being ordered by the leader. In this study, the proposed strategy is to employ the structure of deep neural networks for the detection phase, which should tell the system of the existence of the attack in the early stages of the attack. In the leader-follower mechanism, the employment of robust control algorithms in the network to isolate the misbehaving agent has been examined. In the presented control method, after the attack detection phase with the use of a deep neural network, the control system uses

the reputation algorithm to isolate the misbehave agent. Experiments reveal that deep learning algorithms outperform traditional approaches in detecting assaults, making cyber security simpler, more proactive, less expensive, and considerably more successful.

3. OBJECTIVES OF THE PROJECT

The objectives of the system are-

- To overcome these shortcomings, there is a need to collect representative intrusion detectiondata to develop and analyze detection mechanisms for computer network attacks.
- In addition to a representative normal data, it should also contain a proper diversity ofdifferent types of attacks.
- To detect network attacks by applying machine learning methods.
- To reduced operational time.
- To increased accuracy and reliability.
- To increased operational efficiency.
- To provide data security**.**

4. SCOPE OF THE PROJECT

The Machine learning is a subfield of computer science, which uses pattern recognition and artificial intelligence methods to group and extract behaviours and entities from the data. These previously known patterns and relationships trained by machine learning algorithms can be used to do prediction tasks on new data. With today’s technology, machine learning algorithms touch our everyday life by being used in a wide range of applications.

This project has a large scope as it has the following features which help in making it easy to use, understand and modify it:

- Easy to detection of cyber and network attacks.
- No need to do separate configuration to handle attacks.
- To save the environment by using machine learning techniques
- To increase the accuracy and efficiency of the attacks detection procedure.
- Management of Kaggle datasets and its feature selection.

5. PROPOSED SYSTEM

Cybercrime is spreading throughout the world, using any type of weakness in the computing environment. Ethical hackers are primarily concerned with assessing vulnerabilities and offering mitigation methods. The development of effective techniques is a pressing need in the cyber security community. Most techniques used in today’s IDS are not able to deal with the dynamic and complex nature of cyber-attacks on computer networks. Machine learning for cyber security has become an issue of great importance recently due to the effectiveness of machine learning in cyber security issues. ML approaches have been used to address important difficulties in cyber security, such as intrusion detection, malware classification and detection, spam detection, and phishing detection. Although machine learning cannot fully automate a cyber-security system, it can identify cyber security threats more efficiently than other software-oriented approaches, easing the strain on security analysts. As a result, effective adaptive approaches, such as machine learning techniques, can result in higher detection rates, lower false alarm rates, and cheaper computing and transmission costs. Our main goal is to show that the problem of detecting attacks is fundamentally different from these other applications, making it far more difficult for the intrusion detection community to properly use machine learning.

Machine Learning algorithms can be used to train and detect if there has been a cyber-attack. As soon as the attack is detected, an email notification can be sent to the security users. Any classification algorithm can be used to determine whether or not an assault is a DoS/DDoS attack. Support Vector Machine (SVM), a supervised learning approach that analyses data and recognises patterns, is one example of a classificationalgorithm. Since we cannot predict when, when, or how an attack will occur, and absolute prevention cannot be guaranteed, our best bet for the time being is early discovery, which will help lessen the dangerof irreparable damage such occurrences can do. Organizations can use existing solutions or build their own to detect cyber-attacks at a very early stage to minimize the impact. Any system that requires minimal human intervention would be ideal.

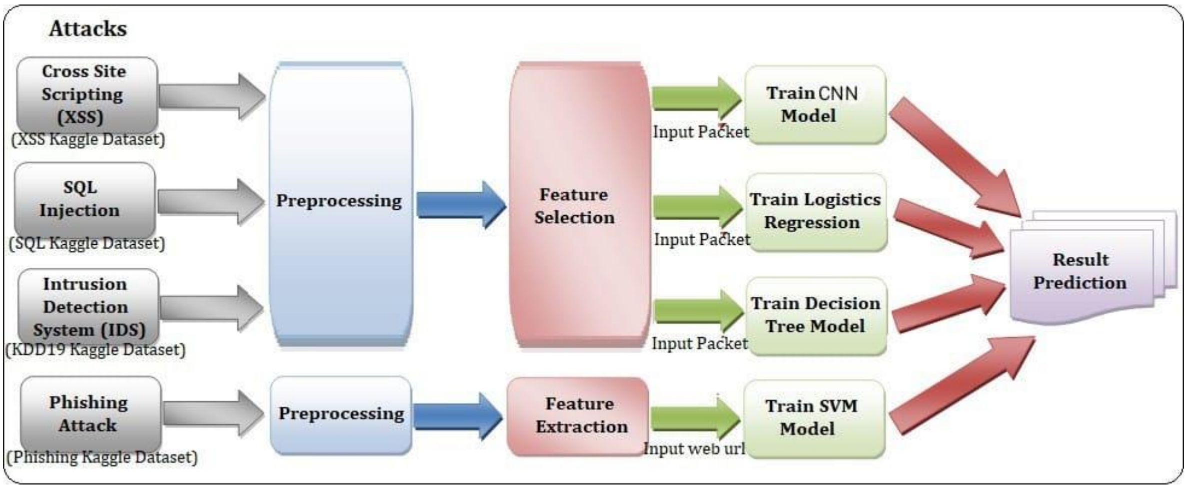


Fig.1: System Architecture

5.1 PREPROCESSING

Data preprocessing is a crucial step in the data mining process that involves manipulating or dropping data before it is used to ensure or improve performance. In data mining and machine learning initiatives, the phrase "garbage in, trash out" is especially apt. Data collection methods are frequently uncontrolled, resulting in out-of-range values (for example, Income: 100), impossible data combinations (for example, Sex: Male, Pregnant: Yes), and missing values, among other things. Analyzing data that hasn't been thoroughly checked for such issues can lead to false conclusions. As a result, before doing any analysis, the representation and quality of data must come first. Data preprocessing is frequently the most crucial stage of a machine learning project.

For example:

In this project for Detection of Cross Site Scripting(XSS) attacks, Some characters have values very big for eg 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.

For Intrusion Detection Attack, we will be extracting numerical attributes and will scale them to have zero mean and unit variance. Further we will turn the result back into dataframe. Then we will extract categorical attributes from both training and test sets, and encode the categorical attributes, and separate the target column from encoded data.

5.2 FEATURE SELECTION AND FEATURE EXTRACTION

In case of Network Intrusion Attack, for extracting important features we have used Random Forest Classifier. Here we have extracted the following 15 attributes from the dataset :
['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']

In case of Phishing attacks we have extracted the following features like,

1) Address bar based features like Using IP address, Long URL to hide suspicious part, URL having @ symbol, Redirecting using // etc
2) Abnormal based features like URL of Anchor, Links in <meta>,<script> and <link> tags, server form handler (SFH), submitting information to email etc
3) HTML and JavaScript based features like website forwarding, status bar customization, disabling right click, using pop up window etc.
4) Domain based features like age of domain, DNS record, website traffic, Pagerank etc.

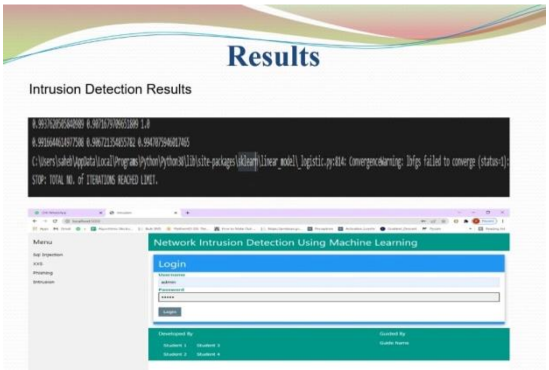
5.3 DIFFERENT TRAINING MODELS

- CNN Model is used to detect Cross Site Scripting (XSS) attacks.
- Logistics Regression Model is used to detect SQL Injection attacks.
- Decision tree model is used to detect Intrusion Detection (IDS) attacks.
- SVM Model is used to detect phishing attacks.

5.4 RESULT 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 malicious.

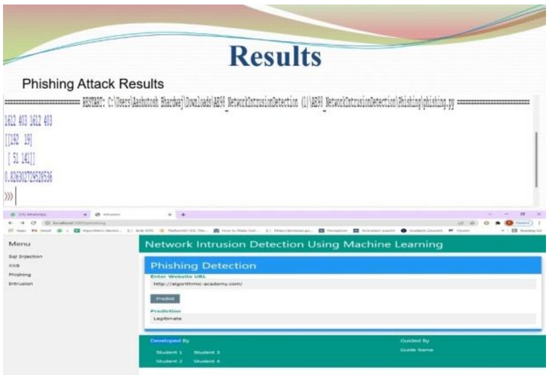


Results

Intrusion Detection Results

```
0.9937628505840989 0.9871679709651889 1.0
0.9916644614977508 0.9867213548557782 0.9947075946017465
C:\Users\saheb\AppData\Local\Programs\Python\Python38\lib\site-packages\sklearn\linear_model\_logistic.py:814: ConvergenceWarning: lbfgs failed to converge (status=1):
STOP: TOTAL NO. of ITERATIONS REACHED LIMIT.
```

Fig.2: ABC



Results

Phishing Attack Results

```
======================== RESTART: C:\Users\Aashutosh Bhardwaj\Downloads\AB98_NetworkIntrusionDetection (1)\AB98_NetworkIntrusionDetection\Phishing\phishing.py ========================
1612 403 1612 403
[[192  19]
 [ 51 141]]
0.8263027295285536
>>>
```

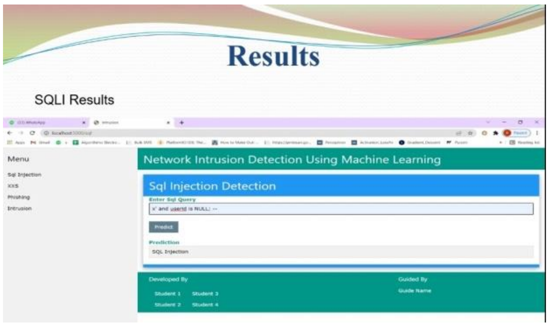
Network Intrusion Detection Using Machine Learning

Phishing Detection

Enter Website URL: http://algorithmic-academy.com/

Prediction: Legitimate

Fig.4: ABC



Results

SQLI Results

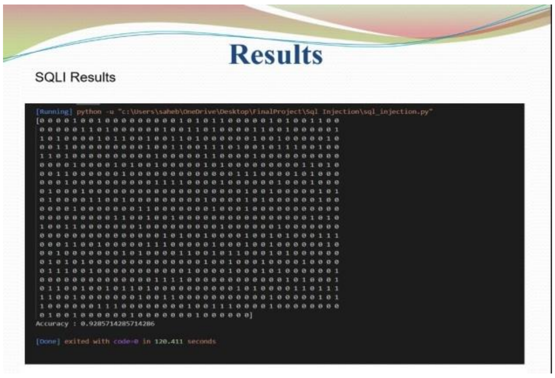
Network Intrusion Detection Using Machine Learning

Sql Injection Detection

Enter Sql Query: x' and userid is NULL; --

Prediction: SQL Injection

Fig.6: ABC



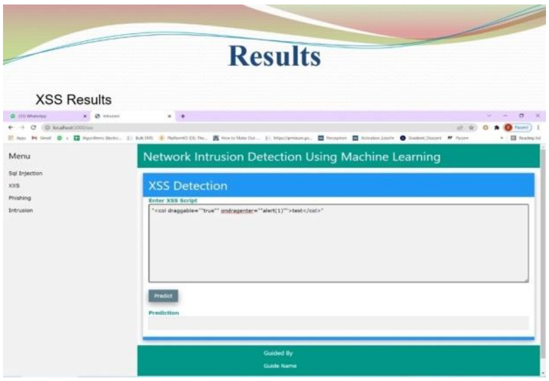
Results

SQLI Results

```
[Running] python -u "c:\Users\saheb\OneDrive\Desktop\FinalProject\Sql Injection\sql_injection.py"
[0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 1 0 1 1 0 0 0 0 0 1 0 1 0 0 1 1 0 0
 0 0 0 0 0 1 1 0 1 0 0 0 0 0 0 0 1 0 0 1 1 0 1 0 0 0 0 1 1 0 0 1 0 0 0 0 0 1
 1 0 1 0 0 0 0 1 0 1 1 0 0 1 0 0 1 1 0 1 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 1 0
 0 0 1 1 0 0 0 0 0 0 0 0 0 1 0 0 1 1 0 0 1 1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 0
 1 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 1 0 0 0 0 1 0 1 0 0 1 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 1 1 0 1 0
 0 0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 1 0 1 0 0 0
 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0
 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 1 0 1
 0 1 0 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 1 0 0
 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0
 1 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 0 0 0 1 1 1
 0 0 0 1 1 0 0 1 0 0 0 0 0 1 1 1 0 0 0 0 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 1 0
 0 0 1 0 0 0 0 0 0 0 1 0 1 0 0 0 0 1 1 0 0 1 0 1 1 0 0 0 1 0 1 0 0 0 0 0 0
 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 0
 0 1 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 0 1
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 1
 0 1 1 0 0 1 0 0 1 0 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 1 1 0 1 1 1
 1 1 0 0 1 0 0 0 0 0 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 1
 1 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 0 1 0 0 1 1 1 0 0 0 0 1 0 0 0 0 0 0 0 0
 0 1 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0]
Accuracy : 0.9285714285714286

[Done] exited with code=0 in 120.411 seconds
```

Fig.3: ABC



Results

XSS Results

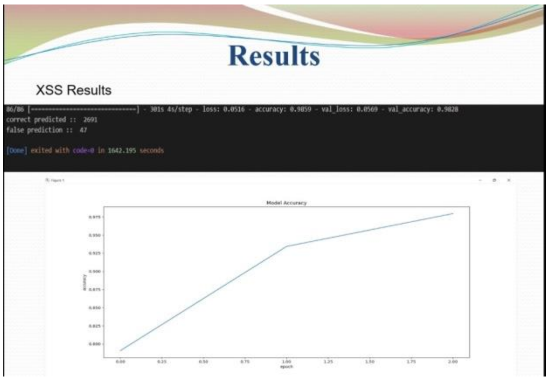
Network Intrusion Detection Using Machine Learning

XSS Detection

Enter XSS Script: "<col draggable=""true"" ondragenter=""alert(1)"">test</col>"

Prediction:

Fig.5: ABC



Results

XSS Results

```
86/86 [==============================] - 301s 4s/step - loss: 0.0516 - accuracy: 0.9859 - val_loss: 0.0569 - val_accuracy: 0.9828
correct predicted ::  2691
false prediction ::  47

[Done] exited with code=0 in 1642.195 seconds
```

Fig.7: ABC

5.5 Math's

A. SQL Injection:

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

Examples of SQL injection:

- Retrieving hidden data, where you can modify an SQL query to return additional results.
- Subverting application logic, where you can change a query to interfere with the application's logic.
- UNION attacks, where you can retrieve data from different database tables.
- Examining the database, where you can extract information about the version and structure of the database.

Blind SQL injection, where the results of a query you control are not returned in the application's responses. To resolve this attack we use Logistic Regression model to train in machine learning platform.

B. Cross Site Scripting:

Cross-site scripting attacks, also called XSS attacks, are a type of injection attack that injects malicious code into otherwise safe websites. An attacker will use a flaw in a target web application to send some kind of malicious code, most commonly client-side JavaScript, to an end user. Rather than targeting the application's host itself, XSS attacks generally target the application's users directly. Organizations and companies running web applications can leave the door open for XSS attacks if they display content from users or untrusted sources without proper escaping or validation.

XSS occurs when an attacker tricks a web application into sending data in a form that a user's browser can execute. Most commonly, this is a combination of HTML and XSS provided by the attacker, but XSS can also be used to deliver malicious downloads, plugins, or media content.

To resolve this attack we use KNN model to train in machine learning platform.

C. Phishing Attack:

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the target’s computer.

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a Ransomware attack or the revealing of sensitive information.

To resolve this attack we use SVM model to train in machine learning platform.

D. Intrusion Detection System:

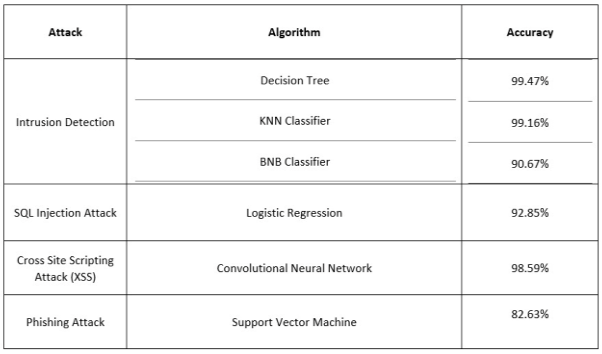
An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system.

Intrusion detection systems are designed to identify suspicious and malicious activity through network traffic, and an intrusion detection system (IDS) enables you to discover whether your network is being attacked.

Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. They can be either network- or host-based. ... Intrusion detection systems work by either looking for signatures of known attacks or deviations from normal activity.

To resolve this attack we use Decision Tree model to train in machine learning platform.

6. RESULTS AND EVALUATION



Attack	Algorithm	Accuracy
Intrusion Detection	Decision Tree	99.47%
	KNN Classifier	99.16%
	BNB Classifier	90.67%
SQL Injection Attack	Logistic Regression	92.85%
Cross Site Scripting Attack (XSS)	Convolutional Neural Network	98.59%
Phishing Attack	Support Vector Machine	82.63%

Table.1: Comparative Analysis

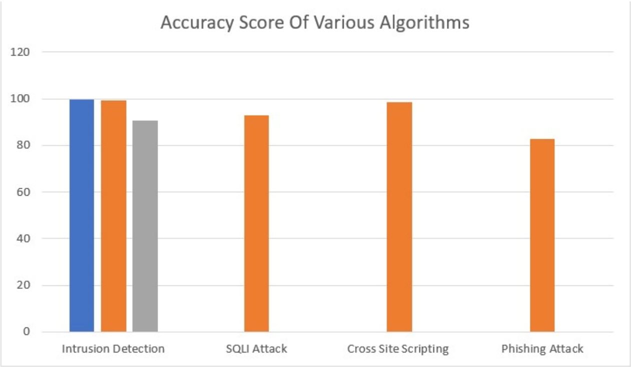


Fig.8: Accuracy Score of various algorithms

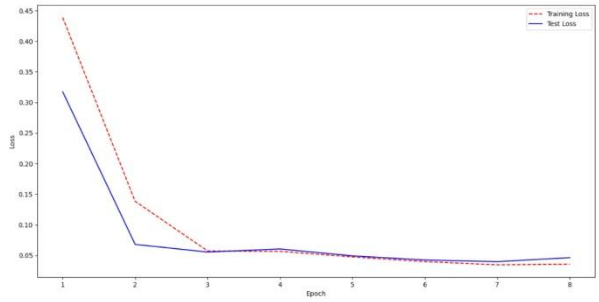


Fig.9: ABC

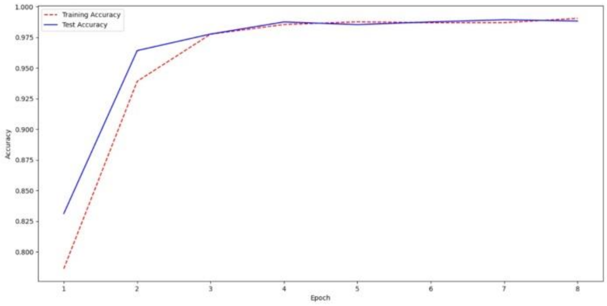


Fig.10: ABC

7. LIMITATIONS

1) No any attack detection software present at all.
2) Time consumed in accessing the attacks of the real time.
3) Manual creation of lists for various activities.
4) The general problem throughout this work is the detection of network attacks.
5) The problem definition gets more specific for any attack type and includes an expanded definition of the attack and its behavior.

8. CONCLUSION

In this study, an attempt was made to use the resilient control consensus method in complex discrete cyber-physical networks with a number of local attacks off. By applying this control method, it was observed that even in the presence of cyber-attacks, the system can remain stable and isolate the attacked node and the performance of the system is not weakened. Using the neural network used in this study, it was observed that with a deep neural network, with 7 hidden layers, the system shows better performance. Also in a recurrent neural network integrated with a deep neural network, a deep layer network with a linear functionperforms better. Therefore, it can be said that the system has less complexity. So With deep learning method, systems can analyse patterns and learn from them to help prevent similar attacks and respond to changing behaviour. To summarise, ML has the potential to make cyber security simpler, more proactive, less expensive, and considerably more successful. After observing the state of the system reported by the neural network, the control system makes decisions based on it and, if there is an attack, detects it and isolates it, so as not to have a detrimental effect on the behavior of other agents. Most techniques used in today's IDS are not able to deal with the dynamic and complex nature of cyber-attacks on computer networks. As a result, effective adaptive approaches, such as machine learning techniques, can result in higher detection rates, lower false alarm rates, and cheaper computing and transmission costs. We reviewedseveral influential algorithms for attack detection based on various ML techniques. Because of the characteristics of ML approaches, it is feasible to construct attacks with high detection rates and low false positive rates, while the system rapidly adapts to changing hostile behaviors. One thing is sure, any organization failing to adopt these techniques now or in the immediate future risk compromising data or worse servers.

ACKNOWLEDGEMENTS

We would prefer to give thanks the researchers likewise publishers for creating their resources available. We are conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

1. 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.
2. Nurjahan, F. Nizam, S. Chaki, S. Al Mamun and M. S. Kaiser, "Attack detection and preventionin the Cyber Physical System," 2016 International Conference on Computer Communication and Informatics (ICCCI), 2016, pp. 1-6, doi: 10.1109/ICCCI.2016.7480022.
3. 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, Changsha, China
4. Ercan NurcanYılmaz, SerkanGönen, “Attack detection/prevention system against cyber-attack in industrial control systems,” Computers & Security Volume 77, August 2018, pp 94-105
5. 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), Volume 11, Issue No.06
6. 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.
7. 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.
8. 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
9. 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.
10. 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)
11. Rishikesh Mahajan, Irfan Siddavatam, “Phishing Website Detection using Machine Learning Algorithms,” International Journal of Computer Applications (0975 – 8887) Volume 181 – No. 23, October 2018
12. Vishnu. B. A, Ms. Jevitha. K. P, “Prediction of Cross-Site Scripting Attack Using Machine Learning

Algorithms," Conference Paper • October 2014.

13. 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
14. 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
15. Fawaz A. Mereani, and Jacob M. Howe, "Detecting Cross-Site Scripting Attacks Using Machine Learning," Springer International Publishing AG, part of Springer Nature 2018