WJAETS

World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Detection of cyber-attacks and network attacks using Machine Learning

Farane Shradha, Gotane Rutuja, Chandanshive Sakshi, Agrawal Khushi and Khandekar Srushti *

Department of Information Technology, JSPM's Jayawantrao Sawant College of Engineering, Pune, Maharashtra, India.

World Journal of Advanced Engineering Technology and Sciences, 2024, 12(01), 128–132

Publication history: Received on 28 March 2024; revised on 17 May 2024; accepted on 20 May 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.12.1.0184

Abstract

The Internet and computer networks have become an important part of organizations and everyday life. New threats and challenges have emerged to wireless communication systems especially in cyber security and network attacks. The network traffic must be monitored and analysed to detect malicious activities and attacks. Recently, machine learning techniques have been applied toward the detection of network attacks. In cyber security, machine learning approaches have been utilized to handle important concerns such as intrusion detection, malware classification and detection, spam detection, and phishing detection. 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 detection of cyber security and network attacks such as IDS, phishing and XSS, SQL injection, respectively. 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.

Keywords: Cyber-crime; Machine Learning algorithms; Phishing attack; Network Intrusion; Cross-Site Scripting (XSS); SQL Injection

1. Introduction

In this modern era of information and communication technologies, physical objects are now connected with each other through cyber networks are collectively called cyber physical system. Attack detection and prevention, also known as stateful firewall, detects and prevents attacks in network traffic. An exploit can be either an information-gathering probe or an attack to compromise, disable, or harm a network or network resource.

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.

In this system, we offer a review on attack detection methods involving strength of deep learning techniques. Specifically, we firstly summarize fundamental problems of network security and attack detection and introduce several successful related applications using deep learning structure. On the basis of categorization on deep learning methods, we pay special attention to attack detection methods built on different kinds of architectures, such as auto-encoders, generative adversarial network, recurrent neural network, and convolutional neural network. Afterwards, we present some benchmark datasets with descriptions and compare the performance of representing approaches to show the

* Corresponding author: Khandekar Srushti

current working state of attack detection methods with 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. Materials and Methods

2.1. Hardware Requirements

- System Type : 64-bit or 32-bit
- Processor : Intel core i3, 2GHz
- Storage Capacity : 256 GB
- RAM : 4GB (Min)
- I/O Devices : Mouse and Keyboard

2.2. Software Requirements

- Operating system : Windows 8/9/10/11
- IDE : Python 3.8.0 IDE
- Front End : HTML, CSS, JavaScript
- Tool : VS Code
- Browser : Google Chrome

2.3. Algorithm

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

2.4. Methodology

The methodology for "Detection of Cyber Attacks and Network Attacks using Machine Learning Algorithms" involves several key steps:

- **Data Collection:** Collect diverse and accurate dataset for XSS, SQL Injection, Phishing attack and IDS. Ensuring the datasets represent diverse attack scenarios and network traffic patterns.
- **Data Preprocessing:** Clean and preprocess the raw data, which may include networktraffic logs, system logs, or packet captures.
- **Feature Selection and Feature Extraction:** Involves choosing a subset of the most relevant features (variables) from the original dataset. Feature extraction involves transforming the original data into a lower-dimensional space while retaining as muchrelevant information as possible.
- **Algorithm Selection:** Choose suitable machine learning algorithms based on the characteristics of the dataset and the nature of the attacks.
- **Result Prediction:** Goal of result prediction is to accurately determine whether a givendata instance corresponds to a legitimate network behaviour or an attack.

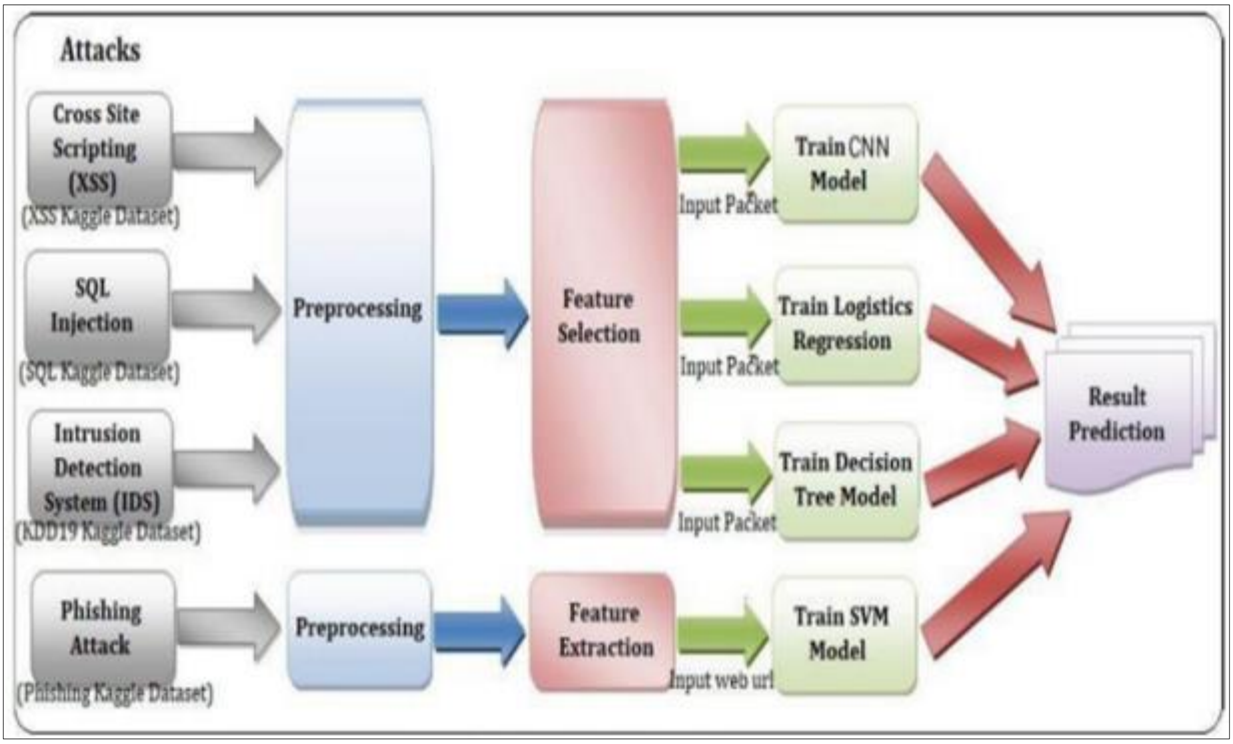
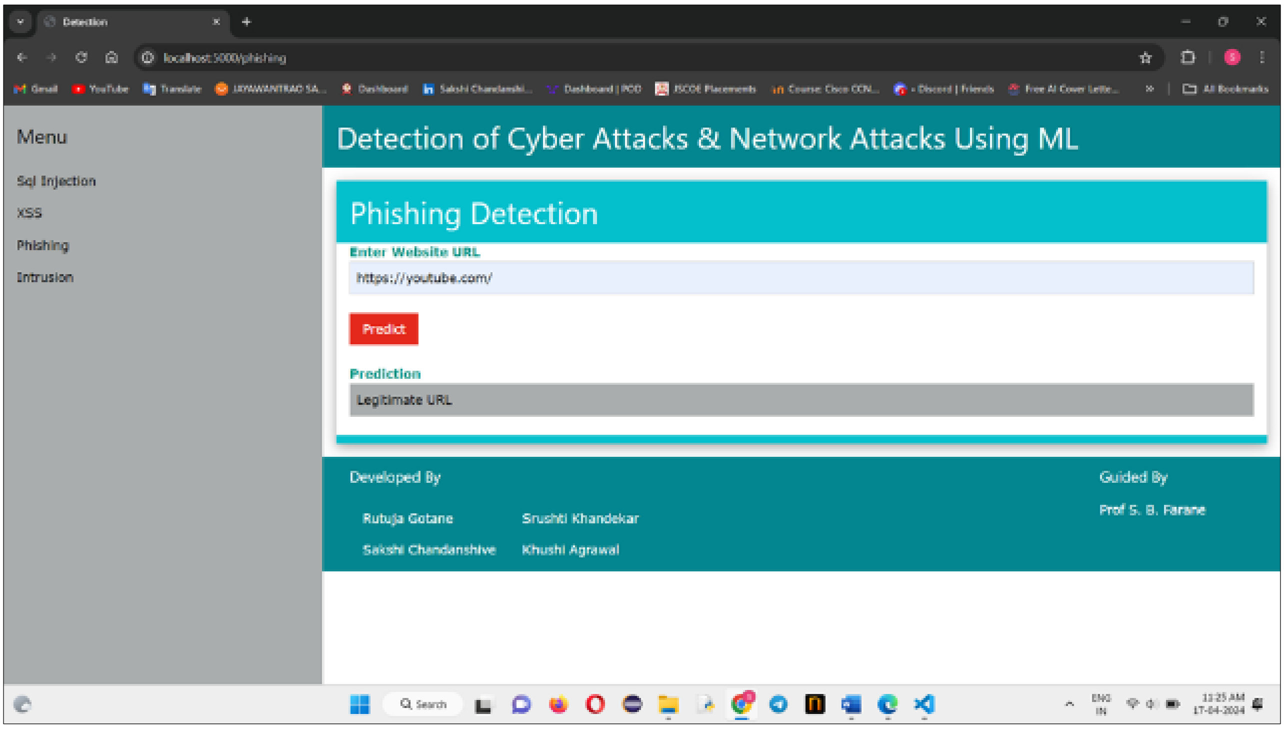


Figure 1 System Architecture

3. Result and discussion



Detection of Cyber Attacks & Network Attacks Using ML

Phishing Detection

Enter Website URL: https://youtube.com/

Prediction: Legitimate URL

Developed By

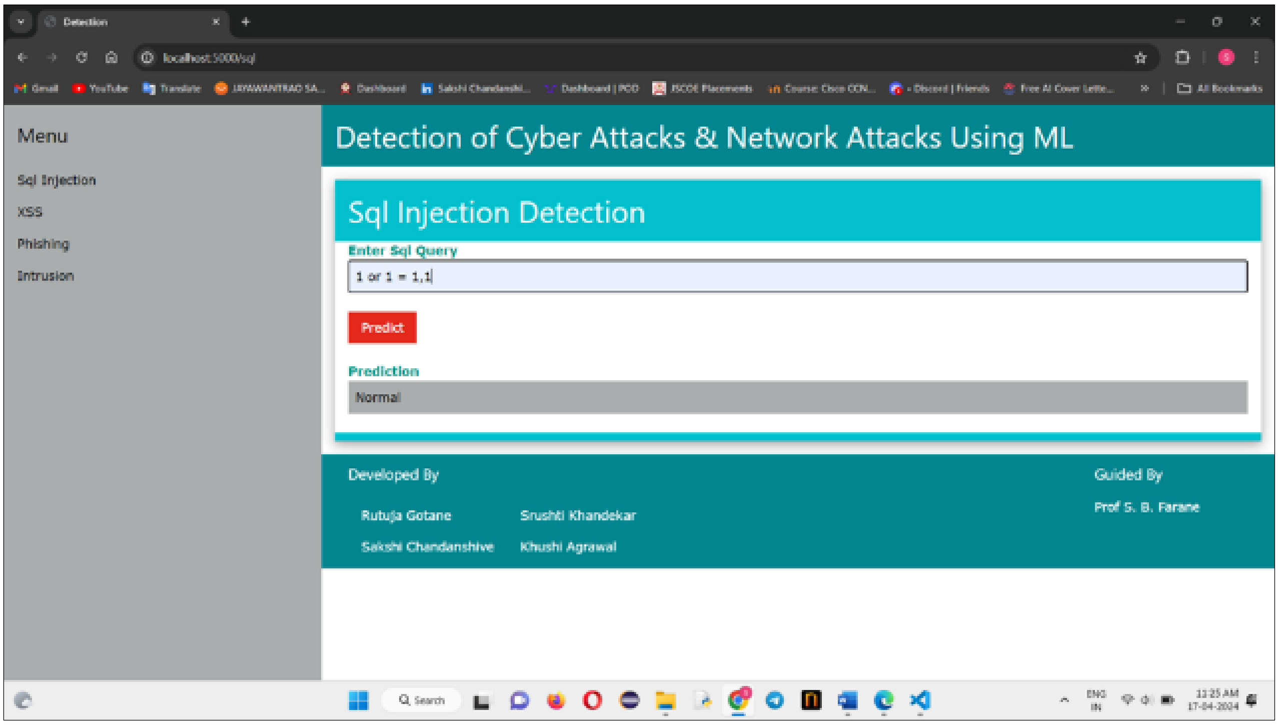
Rutuja Gotane Srushti Khandekar

Sakshi Chandanshive Khushi Agrawal

Guided By

Prof S. B. Farane

Figure 2 Snapshot of Phishing Attack Detection Result



Detection of Cyber Attacks & Network Attacks Using ML

Sql Injection Detection

Enter Sql Query: 1 or 1 = 1,1

Prediction: Normal

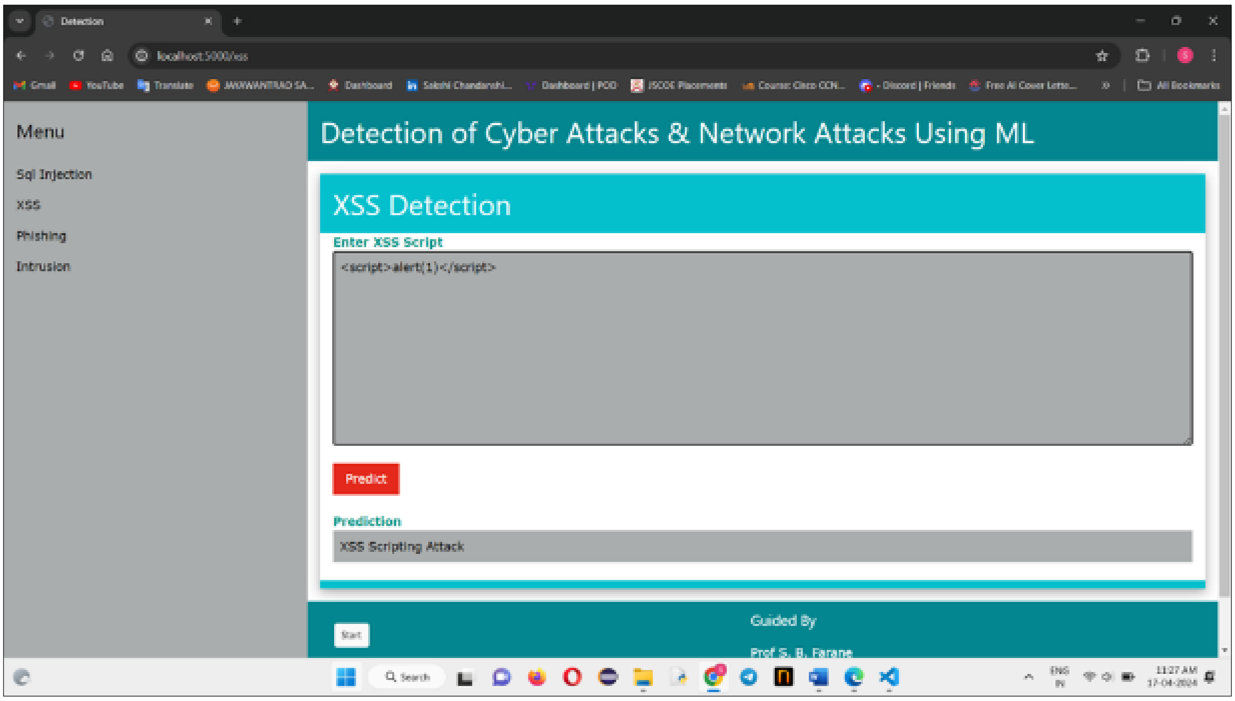
Developed By

Rutuja Gotane Srushti Khandekar
Sakshi Chandanshive Khushi Agrawal

Guided By

Prof S. B. Farane

Figure 3 Snapshot of SQL Injection Attack Detection Result



Detection of Cyber Attacks & Network Attacks Using ML

XSS Detection

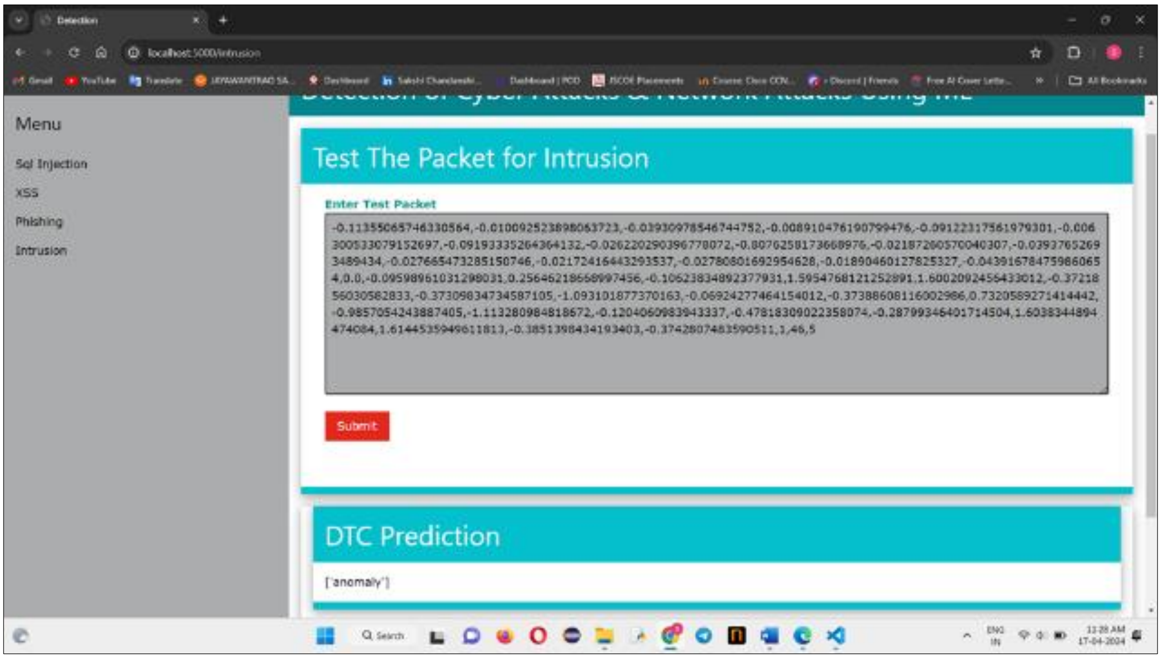
Enter XSS Script: <script>alert(1)</script>

Prediction: XSS Scripting Attack

Guided By

Prof S. B. Farane

Figure 4 Snapshot of XSS Attack Detection Result



Test The Packet for Intrusion

Enter Test Packet

```
-0.11355065746330564,-0.010092523898063723,-0.03930978546744752,-0.008910476190799476,-0.09122317561979301,-0.006
300533079152697,-0.09193335264364132,-0.026220290396778072,-0.8076258173668976,-0.02187260570040307,-0.0393765269
3489434,-0.027665473285150746,-0.02172416443293537,-0.02780801692954628,-0.01890460127825327,-0.04391678475986065
4,0.0,-0.09598961031298031,0.25646218658997456,-0.10623834892377931,1.5954768121252891,1.6002092456433012,-0.37218
56030582833,-0.37309834734587105,-1.093101877370163,-0.06924277464154012,-0.37388608116002986,0.7320589271414442,
-0.9857054243887405,-1.113280984818672,-0.1204060983943337,-0.47818309022358074,-0.28799346401714504,1.6038344894
474084,1.6144535949611813,-0.3851398434193403,-0.3742807483590511,1,46,5
```

Submit

DTC Prediction

['anomaly']

Figure 5 Snapshot of Intrusion Attack Detection Result

4. Conclusion

This project uses Machine Learning algorithms and techniques to detect the network attack andcyber-security attacks. We reviewed several 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.

Hence, efficient adaptive methods like various techniques of machine learning can result in higher detection rates, lower false alarm rates and reasonable computation and communication costs.Characteristics of ML techniques makes it possible to design attacks that have high detection ratesand low false positive rates while the system quickly adapts itself to changing malicious behaviors.One thing is sure, any organization failing to adopt these techniques now or in the immediate futurerisk compromising data or worse servers.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ding Chen, Qiseng Yan, Chunwang Wu and Jun Zhao, SQL Injection Attack Detection andPrevention Techniques Using Deep Learning, Journal of Physics: Conference Series,Volume 1757, International Conference on Computer Big Data and Artificial Intelligence (INDIA 2020) 24-25 October 2020, Changsha, China

[2] Ercan NurcanYılmaz, SerkanGönen, Attack detection/prevention system against cyberattack in industrial control systems, Computers & Security Volume 77, August 2018, Pages94-105

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

[4] 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.

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