

# PREVENTING NETWORK ATTACKS THROUGH SVM AND SDN INTEGRATION

*MINI PROJECT REPORT*

*Submitted by*

**Dinakar Laxmi Viswanath Bodapati (208W1A1201)**

**Sotsava Skandhaa Baji (208W1A1202)**

*Under the Guidance of*

**S. Kranthi**

**Assistant Professor**



**DEPARTMENT OF INFORMATION TECHNOLOGY V R SIDDHARTHA ENGINEERING COLLEGE**

#### (AUTONOMOUS - AFFILIATED TO JNTU-K, KAKINADA)

**Approved by AICTE &Accreted by NBA KANURU, VIJAYAWADA-520007 ACADEMIC YEAR**

#### (2023)

V.R.SIDDHARTHA ENGINEERING COLLEGE

(Affiliated to JNTUK: Kakinada, Approved by AICTE, Autonomous) (An ISO certified and NBA accredited institution)

Kanuru, Vijayawada – 520007



# CERTIFICATE

This is to certify that this project report titled **“Preventing Network Attacks through SVM and SDN Integration”** is a bonafide record of work done by **Bodapati Dinakar Laxmi Viswanath (208W1A1201), Baji Sotsava Skandhaa (208W1A1202)** under my guidance and supervision is submitted in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Information Technology, **V.R. Siddhartha Engineering College** (Autonomous under JNTUK) during the year **2023**.

##### (S. Kranthi) (Dr. M. Suneetha)

**Assistant Professor Professor & Head**

Dept. of Information Technology Dept. of Information Technology

##### EXTERNAL EXAMINER SIGNATURE

Date of examination**:**

**ACKNOWLEDGEMENT**

First and foremost, I sincerely salute our esteemed institution **V.R SIDDHARTHA ENGINEERING COLLEGE** for giving me this opportunity to fulfilling my project. I am grateful to our principal **Dr. A.V. RATNA PRASAD**, for his encouragement and support all through the way of my project.

On the submission of this project report, I would like to extend my honor to **Dr. M. Suneetha**, Head of the Department, of IT for her constant motivation and support throughout my work.

I feel glad to express my deep sense of gratefulness to my project guide **S. Kranthi**, Assistant Professor for his guidance and assistance in completing this project successfully.

I would also like to convey my sincere indebtedness to all faculty members, including supporting staff of the Department, friends, and family members who bestowed their great effort and guidance at appropriate times without which it would have been very difficult on my part to finish the project work.

# DEPARTMENT OF INFORMATION TECHNOLOGY VELAGAPUDI RAMAKRISHNA SIDDHARTHA ENGINEERING COLLEGE

**PROJECT SUMMARY**

|  |  |  |
| --- | --- | --- |
| **S.NO** | **ITEM** | **DESCRIPTION** |
| **1** | **Project Title** | **Preventing Network Attacks through SVM and SDN Integration** |
| **2** | **Student Names& Numbers** | **Bodapati Dinakar Laxmi Viswanath (208W1A1201)**  **Baji Sotsava Skandhaa (208W1A1202)** |
| **3** | **Name of The Guide** | **S. Kranthi** |
|  |  |  |
| **4** | **Research Group** | **Network Security** |
| **5** | **Application Area** | **Cyber Security** |
| **6** | **Aim of the Project** | **The aim is to prevent attacks on network using Machine Learning Model** |
| **7** | **Project Outcomes** | **Ensures security and accurate attack detection on networks** |

##### Student Signatures

1. Bodapati Dinakar Laxmi Viswanath
2. Baji Sotsava Skandhaa

##### Signature of the Guide

S. Kranthi

|  |  |
| --- | --- |
| **TABLE OF CONTENTS** |  |
| [ACKNOWLEDGEMENT](#_bookmark0) | [iii](#_bookmark0) |
| [LIST OF FIGURES](#_bookmark1) | [vi](#_bookmark1) |
| [LIST OF TABLES](#_bookmark2) | [vii](#_bookmark2) |
| [ABSTRACT](#_bookmark3) | [viii](#_bookmark3) |
| [**CHAPTER-1 Introduction**](#_bookmark4) | [1](#_bookmark4) |
| 1.1 [Origin of the Problem](#_bookmark5) | [1](#_bookmark5) |
| 1.2 [Basic definitions and Background](#_bookmark6) | [1](#_bookmark6) |
| 1.3 Problem Statement with Objectives and Outcomes | 2 |
| [**CHAPTER-2 Review of Literature**](#_bookmark7) | [3](#_bookmark7) |
| 2.1 Description of Existing Systems | 3 |
| 2.2 Summary of Literature Study | 4 |
| [**CHAPTER-3 Proposed Method**](#_bookmark8) | [5](#_bookmark8) |
| 3.1 Design Methodology | 5 |
| 3.2 [System Architecture Diagram](#_bookmark9) | [6](#_bookmark9) |
| 3.3 Software Design: Module level | 6 |
| 3.4 Data sets | 6 |
| **CHAPTER-4 Results and Observations** | 10 |
| 4.1 Stepwise description of Results | 10 |
| **CHAPTER-5 Conclusion and Future work** | 15 |
| 5.1 Conclusion | 15 |
| 5.2 Future study | 15 |
| **References** | 16 |

**LIST OF FIGURES**

**Figure Page No**

**Figure-1:** Block Diagram 5

**Figure-2:** Architecture Diagram 6

**Figure-3:** Registration Page 10

**Figure-4:** Login Page 10

**Figure-5:** List of medicines available 11

**Figure-6:** Cart Page 12

### LIST OF TABLES

**Table Page No**

**Table 2.1:** Literature Review 3

### ABSTRACT

The continued growth of connected devices and increasing reliance on digital infrastructure will lead to an increasing number of cyber-attacks on networks. Traditional security solutions such as firewalls and intrusion detection systems will become less effective in defending against these attacks. In this project, we will use a deep learning model-based solution for detecting and preventing network attacks in a software-defined networking (SDN) environment. We will use a popular deep learning framework, to train a deep learning model based on a DDOS attack network security dataset collected from Kaggle. The model we will use is a Linear Support Vector Machine (SVM). The trained model will be integrated into the SDN environment, and using Mininet we build a network and we perform attack generation on the network and the data is tested with the trained model to predict the attack. This will be used to control the behavior of one or more SDN controllers to prevent attacks. The performance of the proposed solution will be evaluated using a simulated network environment and real-world network security datasets. The results will demonstrate that our solution is effective in detecting and preventing network attacks, and has the potential to significantly enhance network security.

Keywords: SDN Environment, DDOS attack, SVM Model, and RYU Controller.

### CHAPTER – 1 INTRODUCTION

This chapter discusses the origin of the problem, objectives and outcomes.

#### Origin of the Problem:

#### 

#### The field of network security is a critical aspect of modern computing systems, with software-defined networking (SDN) offering new opportunities for effective security. The objective of this project is to explore the potential of deep learning algorithms for intrusion detection in SDN environments. The project involves selecting a DDOS attack network security dataset from Kaggle and using deep learning techniques to train a model that can detect and classify different types of attacks. The trained model will be integrated with a software-defined network (SDN) environment, which will use controllers to block the detected attack. This project aims to demonstrate the feasibility and effectiveness of deep learning for intrusion detection in SDN and contribute to the advancement of network security research.

#### 1.2 Basic definitions and Background

The increasing number of cyber-attacks on networks has become a major concern for organizations and individuals. Traditional security solutions, such as firewalls and intrusion detection systems, are becoming less effective in defending against these attacks. This project aims to address this problem by using a deep learning model-based solution for detecting and preventing DDOS network attacks in a software-defined networking (SDN) environment. The solution uses a trained linear Support Vector Machine (SVM) algorithm model to control the behavior of one or more SDN controllers to prevent attacks

#### Problem Statement with Objectives and Outcomes

#### Problem Statement:

The aim of the project is to address the problem of cyber attacks by using a deep learning model-based solution for detecting and preventing DDOS network attacks in a software-defined networking (SDN) environment. The solution uses a trained linear Support Vector Machine (SVM) algorithm model to control the behavior of one or more SDN controllers to prevent attacks.

#### Objectives:

* + - To develop an efficient machine learning model that can classify the given network traffic dataset to various attacks with maximum accuracy.
    - Using SDN controllers to stop traffic from a host based on its Mac address.

#### Outcomes:

* + - A working machine learning-based solution for network security that can detect and prevent network attacks in a software-defined networking environment
    - Improved understanding of the integration of deep learning models into a software-defined networking environment.

### 

### CHAPTER –2 REVIEW OF LITERATURE

This chapter describes the review of literature that we have taken from various papers and considered all the points mentioned in the papers.

##### 2.1 Description of Existing Systems:

**Table 2.1: Literature Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.no** | **Paper Title** | **Authors** | **Publishing**  **year** | **Review** |
| 1. | A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs | Mahmoud Said El Sayed Nhien-An Le-Khac , Marianne A. Azer and Anca D. Jurcut | 2020 | Our approach provides a high detection rate and presents a more efficient better time to build the model. We further tested the trained model on the performance of the SDN controller to evaluate how the used dataset can impact on the performance of the SDN controller. The results showed that the proposed approach does not deteriorate the network performance |
| 2 | Deep Neural Networks for Intrusion Detection in Software-Defined Networking | Wang et al. | 2019 | The authors evaluate the performance of their proposed solution using both simulated and real-world network security datasets and show that deep neural networks can significantly improve the accuracy of intrusion detection in SDN environments. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3  . | End-to-end intrusion detection in software-defined networks using deep reinforcement learning | Qin et al. | 2019 | The proposed solution can effectively detect various types of network attacks in real-time and provide a flexible and scalable solution for SDN security. |
| 4  . | Anomaly-based Intrusion Detection in Software-Defined Networks: A Deep Learning Approach | Zhang et al. | 2019 | The proposed method uses an autoencoder to learn the normal behavior of the network and identify anomalies, which are then classified as either benign or malicious using a deep neural network. |

##### 2.1 Summary of literature:

The aim of this work is to reduce the redundant or irrelevant features without any significant impact on the classification accuracy. We have selected 10 features out of available 48 features using two common feature selection methods IG and RF. The approach provides a high detection rate and presents a more efficient better time to build the model. We further tested the trained model on the performance of the SDN controller to evaluate how the used dataset can impact on the performance of the SDN controller. The results showed that the proposed approach does not deteriorate the network performance.

### CHAPTER-3 PROPOSED METHOD

* 1. **Design Methodology:** As the number of cyber-attacks on networks continues to increase, organizations and individuals are becoming increasingly concerned about their security. Traditional security solutions such as firewalls and intrusion detection systems are becoming less effective in defending against these attacks. To address this problem, this project proposes using a machine learning model-based solution for detecting and preventing DDOS network attacks in a software-defined networking (SDN) environment. The solution involves using a trained linear Support Vector Machine (SVM) algorithm model to control the behavior of one or more SDN controllers to prevent attacks. The design methodology for this solution involves first analyzing the network traffic and identifying the features that are indicative of a DDOS attack. These features are then used to train the SVM model to accurately detect such attacks. Once the model is trained, it is deployed to one or more SDN controllers to monitor network traffic and take action to prevent attacks.

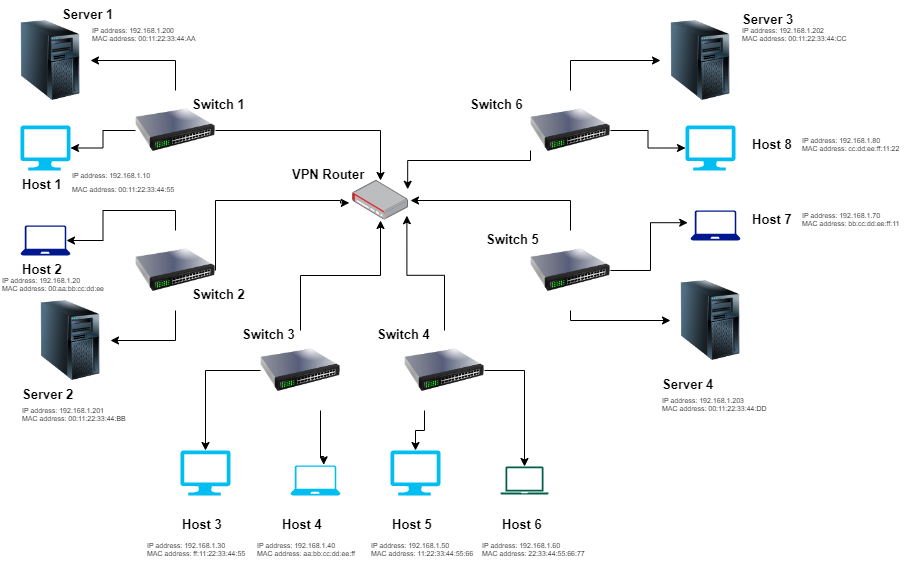


Figure-1: Block Diagram

##### System Architecture Diagram

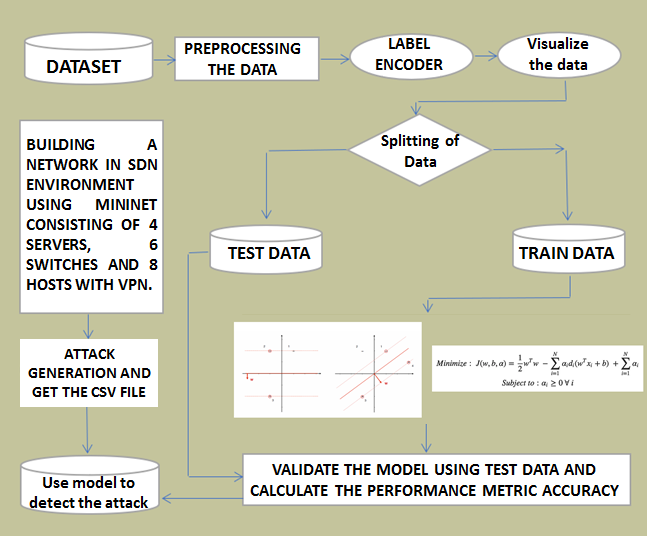


Figure-2: Architecture Diagram

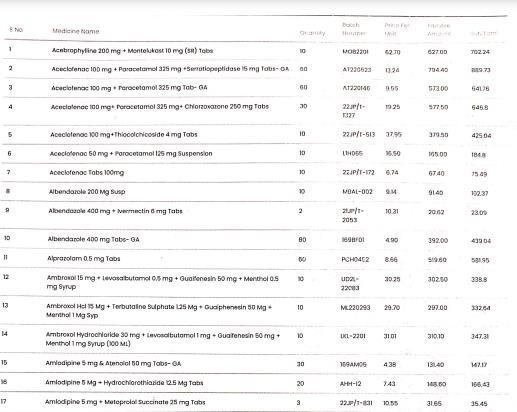
The design methodology also includes testing the effectiveness of the solution on a test network and refining the model as needed. Overall, this solution offers a more effective approach to detecting and preventing DDOS attacks in an increasingly complex and challenging cybersecurity environment.

##### Software Design: Module level

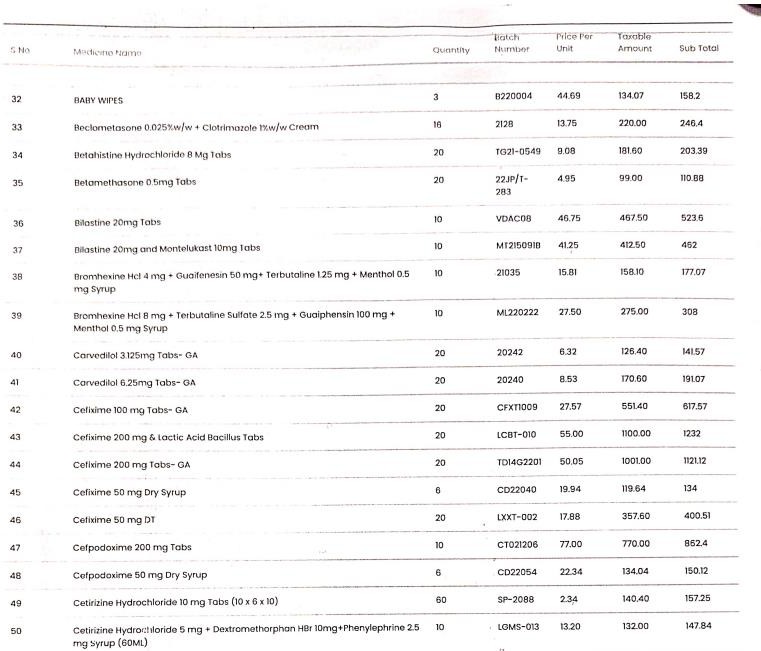
In the above architecture diagram, the illustration goes as follows: The information dataset is collected in csv format from internet. Now we preprocess the data in R Environment convert the categorial data to our required input and we visualize the data. Split the data into training and testing and train the SVM model and calculate the accuracy. Now we build a network in SDN environment with and validate and firstly the user will visit username and password. For new customer the provider needs to give proper name and email address to register After registration is complete the user can purchase any item form the website. There is a search machine form which one can search for specific medicine. After selecting the desired item user can add them to cart and order the item. Then, deliver system will take place. The delivery boy will take the order to nearby store and deliver the item within a short time. The above figure of the flowchart illustrates the methodology in which our system conducts the processes.

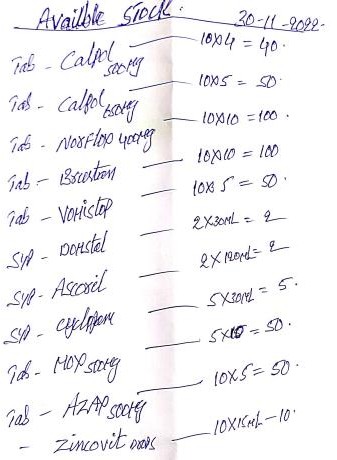
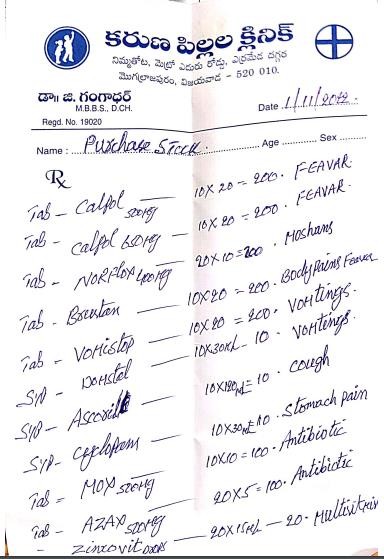
##### Datasets:

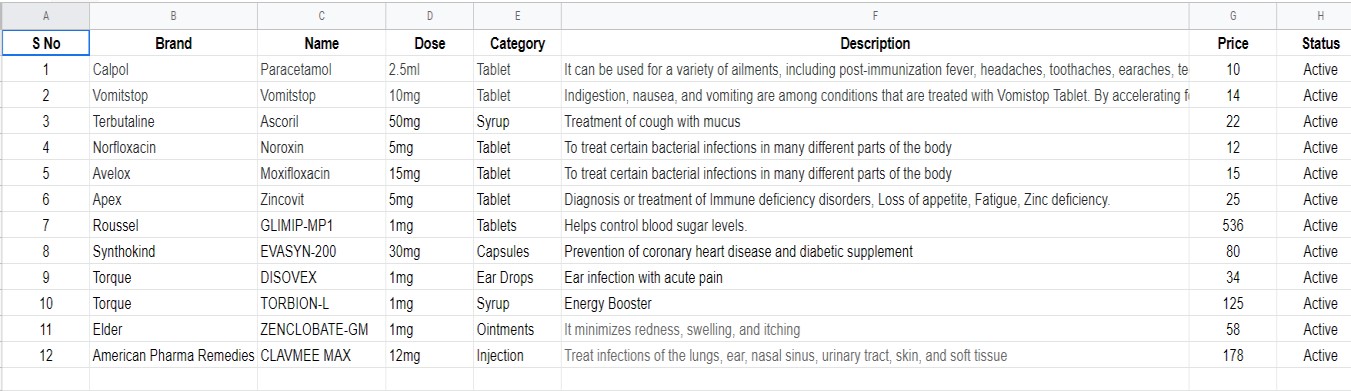
The drug stores we visited provided the Datasets. We had gathered information about the medication stock that was on hand in their store

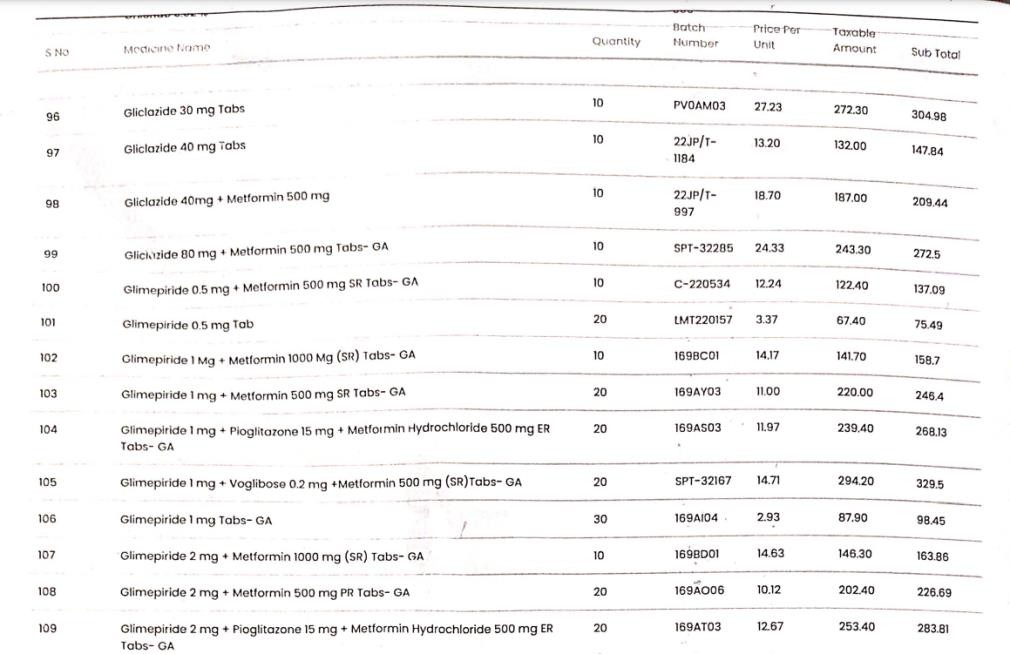












**CHAPTER 4**

##### Results & Observations

**4.1 Stepwise description of Results:** 1.Collecting the dataset for pre-processing 2.Analyzing the datasets we collected 3.The website is as follows:

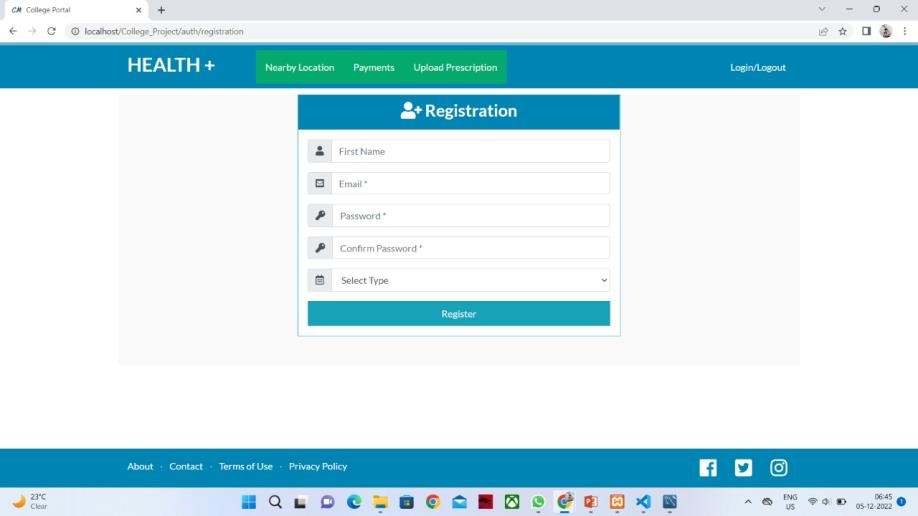


Figure-3: Registration page

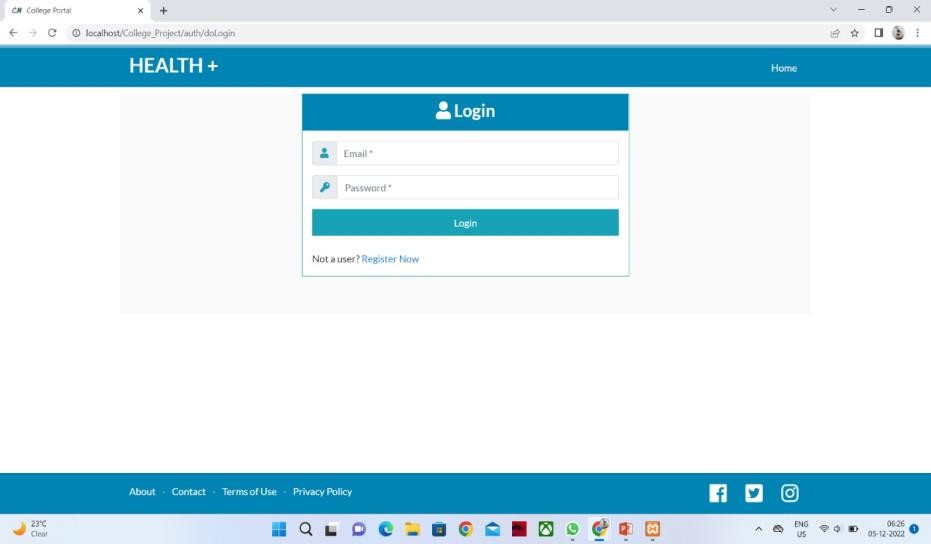


Figure-4: Login Page

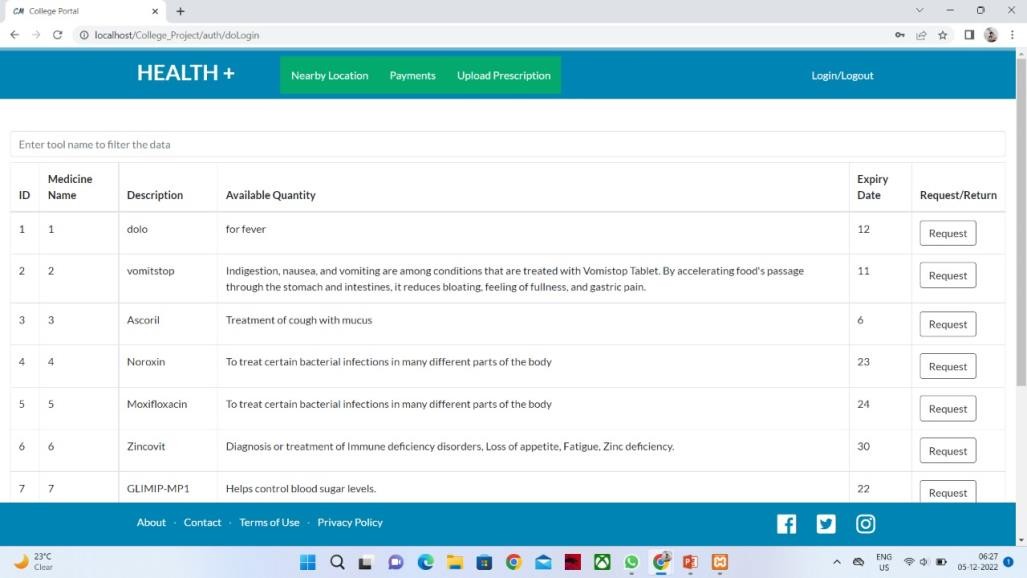


Figure-5: List of medicines available

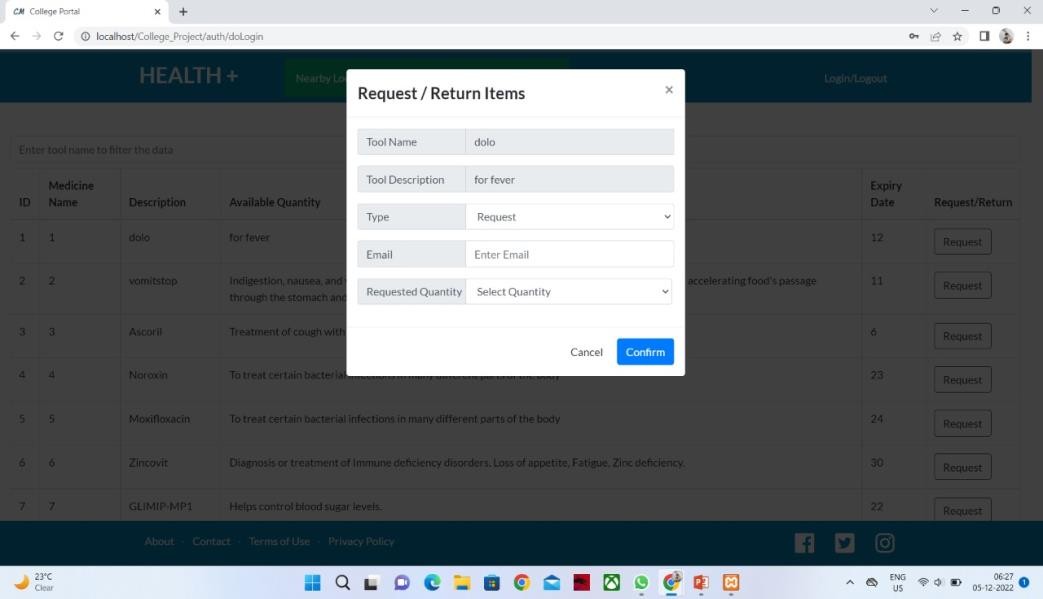


Figure-6: Request/Return items

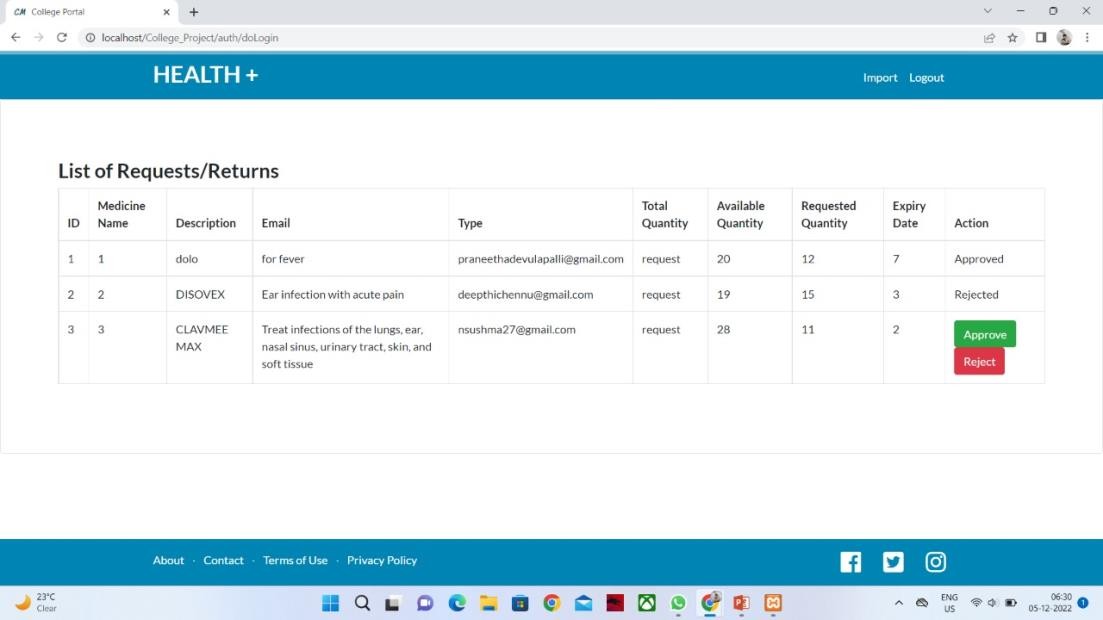


Figure-7: Cart page

## CHAPTER-5

**Conclusion and Future work**

##### Conclusion:

In this paper, we address the development of a web-based medical delivery system. We entered the data and stored it using PHP, HTML, and MySQL with the help of database creation. The speedy door-to-door delivery made possible by this application has an impact on society. The distribution of prescriptions will be facilitated and accelerated by technology, saving both time and money. The availability of a wider range of pharmaceuticals has given the elderly and the disabled more alternatives and made their lives simpler. Customers who use an online drug delivery service are prevented from forgetting to refill their prescriptions or running out of medication by the scheduled reminders. This application affects society by making speedy door-to-door delivery possible for them.

* 1. **Future Study:** Future research for the project will include the expansion of the statistical representation of the currently available stock as well as the history of product purchases on a particular day and over time. The initiative also updates the store's maps and geolocations, making it simpler for customers to locate nearby locations and get prompt delivery.

##### References:

1. Desai, K., Chewning, B., & Mott, D. (2015). Health care use amongst online buyers of medications and vitamins. Research in Social and Administrative Pharmacy.
2. Kotha, S., Rajgopal, S., &Venkatachalam, M.. (2004). The Role of Online Buying Experience as a Competitive Advantage: Evidence from Third-Party Ratings for ECommerce Firms. The Journal of Business, 77(2), S109– S133. Retrieved from [http://www.jstor.org/stable/3663735.](http://www.jstor.org/stable/3663735)
3. Riedl, C., Leimeister, J. M., &Krcmar, H.. (2011). Why eService Development is Different: A Literature Review. Eservice Journal, 8(1), 2–22. [http://doi.org/10.2979/eservicej.8.1.2.](http://doi.org/10.2979/eservicej.8.1.2)
4. Kettle, K. L., &Häubl, G.. (2011). The Signature Effect: Signing Influences Consumption- Related Behavior by Priming Self-Identity. Journal of Consumer Research, 38(3), 474–489. [http://doi.org/10.1086/659753.](http://doi.org/10.1086/659753)
5. Mamoun N. AkroushMutaz M. Al-Debei , (2015),"An integrated model of factors affecting consumer attitudes towards online shopping", Business Process Management Journal, Vol. 21 Iss 6 pp. 1353 – 1376.
6. Grace T.R. Lin Chia-Chi Sun, (2009),"Factors influencing satisfaction and loyalty in online shopping: an integrated model", Online Information Review, Vol. 33 Iss 3 pp. 458 – 475.
7. Dhama, K., Khan, S., Tiwari, R., Sircar, S., Bhat, S., Malik, Y.S., Singh, K.P., Chai-cumpa, W., Bonilla-Aldana, D.K. and Rodriguez-Morales, A.J. (2020) Coronavirus Disease 2019— COVID-19. Clinical Microbiology Reviews, 33, e00028-20. <https://journals.asm.org/doi/10.1128/CMR.00028-20>
8. Awojide, Simon, I. M. Omogbhemhe, O. S. Awe, and T. S. Babatope, “Towards the digitalization of Restaurant Business Process for Food Ordering in Nigeria Private University: The Design Perspective. A Study of Samuel Adegboyega University Edo State Nigeria,” Int. J. Sci. Res. Publ., vol. 8, no. 5, pp. 46–54, 2018.
9. O. I. Mike and A. Simon, “Towards the Digitalization of Hotel Business in Nigeria: The Design Perspective,” vol. 8, no. 2, pp. 1175–1178, 2017.
10. Adithya. R., A. Singh, S. Pathan, and V. Kanade, “Online Food Ordering System,” Int. J. Comput. Appl., vol. 180, no. 6, pp. 22–24, 2017.
11. Varsha Chavan, Priya Jadhav, Snehal Korade, Priyanka Teli, ”Implementing Customizable Online Food Ordering System Using Web Based Application”, International Journal of Innovative Science, Engineering Technology(IJISET) 2015.
12. Patel, Mayurkumar, "Online Food Order System for Restaurants" (2015). Technical Library. Paper 219.