Co-operative Society Management System

by

Examination Roll: 222149

A Project Report submitted to the
Institute of Information Technology
in partial fulfillment of the requirements for the degree of
Professional Masters in Information Technology

Supervisor: Dr. M Shamim Kaiser, Professor

Institute of Information Technology
Jahangirnagar University
Savar, Dhaka-1342

December 2023

DECLARATION

I hereby declare that this thesis is based on the results found by ourselves. Materials of work found by other researcher are mentioned by reference. This thesis, neither in whole nor in part, has been previously submitted for any degree.

Roll:222149

CERTIFICATE

The project titled "Co-operative Society Management System" submitted by Md. Hasibuzzaman, ID: 222149, Session: Summer-2022, has been accepted as satisfactory in partial fulfillment of the requirement for the degree of Professional Masters in Information Technology on the 3rd of January 2023.

Dr. M. Shamim Kaiser
Supervisor

BOARD OF EXAMINERS

Dr. Mohammad Abu Yousuf
Professor, IIT, JU

Coordinator
PMIT Coordination Committee

Dr. M. Shamim Kaiser
Professor, IIT, JU

Member, PMIT Coordination Committee
& Director, IIT

Dr. Shamim Al Mamun
Associate Professor, IIT, JU

Member
PMIT Coordination Committee

Dr. Mohammad Shahidul Islam
Associate Professor, IIT, JU

Member
PMIT Coordination Committee

Dr. Md. Sazzadur Rahman
Associate Professor, IIT, JU

Member
PMIT Coordination Committee

ACKNOWLEDGEMENTS

We feel pleased to have the opportunity of expressing our heartfelt thanks and gratitude to those who all rendered their cooperation in making this report.

This thesis is performed under the supervision of Dr. M. Shamim Kaiser, Associate professor, Institute of Information Technology (IIT), Jahangirnagar University, Savar, Dhaka. During the work, he has supplied us a number of books, journals, and materials related to the present investigation. Without his help, kind support and generous time spans he has given, we could not perform the project work successfully in due time. First and foremost, we wish to acknowledge our profound and sincere gratitude to him for his guidance, valuable suggestions, encouragement and cordial cooperation.

We express our utmost gratitude to Dr. M Mesbahuddin Sarker, Director, IIT, Jahangirnagar University, Savar, Dhaka, for his valuable advice that have encouraged us to complete the work within the time frame. Moreover, we would also like to thank the other faculty members of IIT who have helped us directly or indirectly by providing their valuable support in completing this work.

We express our gratitude to all other sources from where we have found help. We are indebted to those who have helped us directly or indirectly in completing this work.

Last but not least, we would like to thank all the staff of IIT, Jahangirnagar University and our friends who have helped us by giving their encouragement and cooperation throughout the work.

ABSTRACT

The Co-operative Society Management System is a comprehensive software solution created to streamline and automate the functions of Co-operative societies under the Bangladesh Rural Development Co-operative Division authority. This summary offers insights into its main features and advantages.

Co-operative societies are pivotal in sectors like agriculture, finance, and housing, fostering collaboration among members and fostering economic development. Yet, the management of administrative tasks and financial transactions within these societies can be intricate and time-intensive. The Co-operative Society Management System seeks to simplify these processes by providing an efficient and user-friendly platform.

Keywords: Coop, Co-operative Society Management System, Socity Management System, cooperative and loan Management System and Samity Management System.

LIST OF ABBREVIATIONS

IIT	Institute of Information Technology
JU	Jahangirnagar University
IIT	Institute of Information Technology
IIT	Institute of Information Technology
QoS	Quality of Service

LIST OF NOTATIONS

α	Define alpha
max	maximum
$\cos\theta$	maximum
x	maximum

LIST OF FIGURES

Figure

LIST OF TABLES

Table

TABLE OF CONTENTS

CHAPTER I

Introduction

1.1 Overview

The introduction of a Co-operative Society Management System marks a significant leap in the efficient and organized management of Co-operative societies. Co-operative societies play a vital role in various sectors, including agriculture, finance, and housing, by fostering collaboration among members and promoting economic development. However, managing the diverse functions and operations of these societies can be complex and demanding. This introduction provides an overview of the purpose, features, and benefits of such a system.

1.1.1 Purpose

The Co-operative Society Management System is designed to address the unique needs and challenges faced by Co-operative societies. Its primary purpose is to streamline and automate the administrative, financial, and member-related processes within a Cooperative society, ultimately enhancing its efficiency, transparency, and overall performance.

1.2 Background

The concept of Co-operative societies has a deep-rooted history in Bangladesh, dating back to the pre-independence period and gaining significant momentum in the post-independence era. Here's a brief background on Co-operative societies in Bangladesh:

Pre-independence Period: Co-operative societies in what is now Bangladesh can trace their origins to the British colonial period. During this time, Co-operative movements began to take shape, primarily in rural areas. These early Co-operatives aimed

to address the economic challenges faced by farmers and rural communities. However, the concept remained somewhat limited in scope. Post-independence Era: After gaining independence from Pakistan in 1971, Bangladesh faced numerous socio-economic challenges. Co-operatives were seen as a means to empower rural communities, alleviate poverty, and promote economic development. The government of Bangladesh began to actively promote and support Co-operative initiatives as part of its socioeconomic development strategy.

Co-operative societies in Bangladesh have a diverse history and have played a significant role in addressing rural and urban development challenges. With ongoing efforts to overcome challenges and promote transparency, Co-operatives continue to be a valuable instrument for socio-economic development and poverty reduction in the country.

1.3 AIM

The aims of Co-operative societies in Bangladesh are multifaceted and are aligned with socioeconomic development, poverty reduction, and the empowerment of various segments of society. Here are the primary aims of Co-operative societies in Bangladesh:

a. Poverty Alleviation
b. Rural Development
c. Agricultural Advancement
b. Financial Inclusion
c. Empowerment of Women
d. Housing and Urban Development
e. Entrepreneurship Development
f. Social Welfare
g. Community Building
h. Good Governance

Co-operative societies in Bangladesh have a broad spectrum of aims, all of which are geared towards socio-economic development, poverty reduction, and the empowerment of individuals and communities. They play a crucial role in addressing the diverse needs of their members and contribute to the overall development of the country

1.4 Motivation

The motivation behind developing a Co-operative Society Management System stems from the recognition of several pressing needs and challenges within Co-operative societies. Here are the primary motivations:

1. Efficiency Enhancement: Traditional methods of managing Co-operative societies often involve manual paperwork, which can be time-consuming and error-prone. The motivation is to streamline operations and reduce administrative burdens by automating various tasks, ultimately improving efficiency.

2. Transparency and Trust: Co-operative societies rely on the trust and cooperation of their members. By implementing a management system, societies aim to enhance transparency in financial transactions, member interactions, and decision-making processes. This increased transparency fosters trust among members and stakeholders.

3. Compliance and Reporting: Many Co-operative societies are subject to regulatory requirements and reporting standards. A management system simplifies compliance by generating accurate financial reports and statements, making it easier to adhere to legal obligations.

4. Member Empowerment: Co-operative societies exist for the benefit of their members. By providing an online platform for members to access their account statements, apply for loans, and engage in discussions, the system empowers members and improves their overall experience.

5. Data Security: Data security and privacy are paramount. With the rise in cyber threats, a motivation for implementing a management system is to ensure that sensitive member and financial data is securely stored, reducing the risk of data breaches.

6. Scalability: As Co-operative societies grow, the need for efficient management becomes more critical. The system allows for scalability, enabling societies to accommodate a larger membership base and increasing volumes of financial transactions.

7. Cost Reduction: While there may be an initial investment in implementing the system, the long-term motivation is cost reduction. By automating tasks and reducing the need for extensive manual labor, Co-operative societies can save both time and money. The motivation for a Co-operative Society Management System lies in its ability to address the unique challenges faced by Co-operative societies, improve operational efficiency, enhance transparency, ensure accurate financial management, empower members, and ultimately contribute to the long-term sustainability and

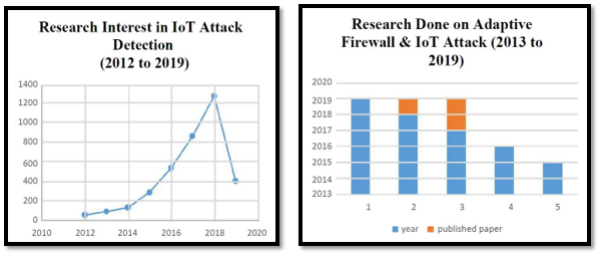

Figure 1.1: Research Interest in Field of IoT

success of these Co-operative organizations.

In figure 1.1 shows the existing research interest in IoT Attack Detection which is increasing day by day for last few years whereas for detecting attack concept of Adaptive Firewall is not so common and used term in this field. This drives us motivated to design adaptive firewall for attack detection and to block illegitimate traffic on IoT Network Model.

1.5 Objective

IoT network model and devices are vulnerable to different kind of attacks. These attacks may vary to different category, so have different approach to detect and block them. The goal of this research is to study and identify potential IoT security attacks, detect and mitigate them by using Adaptive firewall concept. Additionally, machine learning should be considered for classifying attacks and identifying attacks [2]. Specific goals of this thesis that should be mentioned:

- Analyze network traffic to detect the malicious ones that tries to hamper the network.
- Find the characteristics of perception layer's attack to identify specific attacks.
- Extract features from the generated traffic datasets to train machine learning classifiers and apply them to recognize attacks.Propose a centralized attack detection model.
- Design a rule based and ANN based FIS to help SDN controller to evaluate specific attack probability and block the suspicious ones.
- Maintaining the performance of the network.

This proposed model also answers the following questions:

1. What are the major challenges that have guided security in IoT?
2. What is the best attack detection way for IoT network model?
3. Is there any generalized approach for detecting different layer attack?
4. What is the best way to detect a single layer attack?

1.6 Assumptions & Limitations

Though a centralized and efficient model has been proposed to detect attacks on IoT network, it has limitations on which further studies should be done:

- No approach has been mentioned for network and application layer security.
- No real time data has been used for the traffic analysis.
- Here feature Extraction and Selection method has been analyzed but no implementation has been shown.
- No comparison among different IDS model has been analyzed so can't be declared it as the optimal way.
- No performance measure of used Classifier is evaluated here.

1.7 Research Outline

Rest of the report is structured as follows: In **Chapter II** a literature study on related work is given including explanations for the most important terms used in this thesis-basic concept and architecture of IoT Network Model, Attacks on IoT, Concept and architecture of SDN, different model of IDS, Concept of Firewall has been discussed through this chapter. **Chapter III** introduces system model including system architecture, algorithm and flowchart of working procedure of entire system model. **Chapter IV** explains the details of traffic analysis techniques, Feature Extraction and Selection mechanism and tools for this mechanism and reasoning how these mechanisms work for our model. **Chapter V** discusses about the simulation and model performance, to analysis result of the model it describes the basic mechanism of attack detection like Fuzzification, NSL KDD dataset, FIS, Defuzzification,Simulation and confusion matrix. Lastly in **Chapter VI** future work and conclusion is mentioned.

1.8 Limitation

Bla bla bla

CHAPTER II

Literature Review

2.1 Related Work

2.1.1 Soft Engg

Several studies investigated diabetes data and constructed models to predict diabetes. Equation 2.1 give

$$y = \sum_i x_i + C^2 + \frac{1}{\cos\theta} \tag{2.1}$$

Figure 2.1 shows bla bla

Table 2.1: Supervised Machine Learning Classifier

hello	*JU*	Header 2
Shamim	KMA	In this step, we will describe some supervised machine learning classifiers namedLogistic Regression, k-nearest neighbors, Support Vector Machine, Decision Tree,Gaussian Naive Bayes, Random Forest, Gradient Boosting and Linear DiscriminantAnalysis.

2.2 Machine Learning Types

2.3 Supervised Machine Learning Classifiers

In this step, we will describe some supervised machine learning classifiers named Logistic Regression, k-nearest neighbors, Support Vector Machine, Decision Tree,

Gaussian Naive Bayes, Random Forest, Gradient Boosting and Linear Discriminant Analysis.

2.3.1 Logistic Regression (LR)

Logistic Regression (LR) is a supervised machine learning data classification algorithm that mines real-valued features from the input, multiplies each of them by a weight, adds them, and transfers the sum through a sigmoid function to produce a probability. A threshold is used to finalize a decision [3]. A solution for classification of our data set is LR which Instead of fitting a straight line or hyperplane uses the logistic function to squeeze the output of a linear equation between 0 and 1. The logistic function is defined as:

$$Logistic(\eta) = 1/(1 + exp(-\eta))$$

As η goes from $-\infty$ to ∞, logistic (η) goes from 0 to 1, a "squashing function". In our study, we used a maximum 4000 iterations to converge the output.

2.3.2 k-nearest neighbors (KNN)

(KNN) is a non-parametric process we used for diabetic data classification. In KNN a data is classified by a majority vote of its neighbors, with the data being allotted to the class most mutual amongst its K nearest neighbors estimated by a distance function. If K = 1, then the data is simply allotted to the class of its nearest neighbor. KNN algorithm is as below :

Algorithm 1 KNN

1: Let m be the number of training data samples. Let p be an unknown point that needs to be classified
2: Storing the training samples in an array of data points $arr[]$. Each element of this array denotes a tuple (x, y).
3: **for** $i = 0$ to m **do**
4: Calculating distance $d(arr[i], p)$
5: **end for**
6: Making set S of K smallest distances achieved. Each of these distances resembles an already classified data point
7: Returning the majority label among S

2.3.3 Decision Tree (DT)

A DT is a classifier that recursively performs partition of the instance space. The decision tree contains nodes that form a tree, a node called "root" that has no incoming edges is the starting point of the tree. All other nodes have one incoming edge. The leaf nodes are known as decision nodes. The child node is nominated by computing Information Gain (IG).

Information Gain = Entropy(parent) - [weights average] * Entropy(children)

Entropy(Ci) = -P(xi) log P(xi), where P(xi) is the probability of child node i.

Node with the highest IG will be the parent for next level. This process is continued until it gets a leaf node and completed decision tree.

The algorithm for generating a decision tree is as below :

Algorithm 2 DT

1: Create (T)
2: Calculate frequencies (Ci, T)
3: If all instances belong to the same class, returning leaf
4: for every attribute a test is set for splitting criteria. An attribute that satisfies the test is test node K
5: Repeating Create (Ti) on each partition Ti.Adding those nodes as children of node K

2.3.4 Gaussian Naive Bayes (GNB)

The GNB classifier is a probability distribution function having the effect of associating neural activation to the means and variances of activation in various impulse conditions. The production of the classifier is a condition-label. The classifier creates hypothesis that the classes have Gaussian normal distributions.

The z-score distance between the inputted point and each class-mean is estimated for each data point, namely the distance from the class mean divided by the standard deviation of that class.

$$Z_A = \frac{(x - \mu_A)}{\sigma_A}$$

According to the equation for a Gaussian normal distribution, each z-score is then converted into a probability value which is used for observing data point x. The co-variance between dimensions is not modelled by GNB classifier.

2.3.5 Random Forest (RF)

RF is a collective algorithm which was modelled from trees algorithm and Bagging algorithm. It works fine with a data set with a large number of input variables. It is a meta estimator that creates a number of decision tree classifiers on different subsamples of the data set and uses mean value to increase the accuracy of the model and control over-fitting. Suppose training data set is given as: [X1, X2, X3, X4] with labels as [L1, L2, L3, L4] respectively, random forest algorithm may create three decision trees taking input of subset for example, [X1, X3, X4], [X2, X3, X4] and [X1, X2, X4]. Finally, it predicts class based on the majority of votes from each of the decision trees generated. Generally, the more trees in the forest the more robust and reliable the forest is. The random forest classifier works in the same way, the higher the number of trees in the forest gives higher accuracy output .

2.3.6 Gradient boosting (GB)

GB includes three components: a loss function that is to be optimized, a weak learner that makes predictions and an additive model which will add weak learners to minimize the loss function.

2.4 Research Gap

Analyzing related works in this field an be noticed some shortcoming in the security measurements of IoT network. **Firstly**, there is no centralized detection method is mentioned, every layer has specific detection way method but as IoT is becoming a heterogenous network a centralized model should be proposed in controller which will control the traffic of every subpart of network. **Secondly**, by using KDD Dataset most commonly **DDoS, Probe, U2R, R2L** attack has been detected but with advancing technology intruder can attack the network in many other ways. **Thirdly**, no time efficient optimal way is mentioned to detect attack. **Fourthly**, traditional firewall can't detect any encrypted incoming packet which can be removed by using adaptive firewall concept but still much work has not done yet regarding this problem [4, 5, 6].

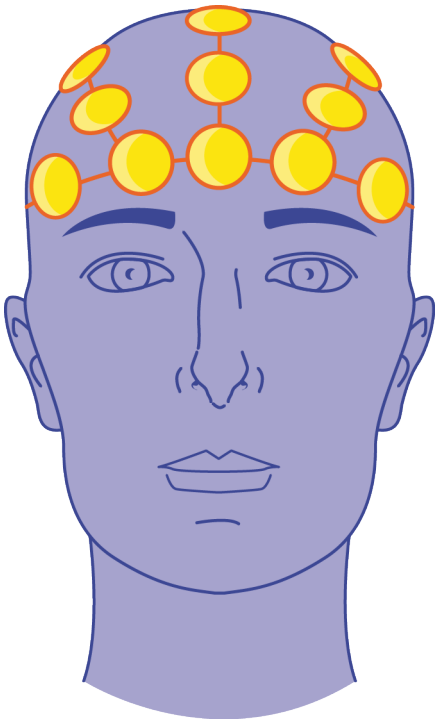

Figure 2.1: EEG probe on brain

CHAPTER III

System Model

3.1 Proposed Architecture

As our main purpose is to secure the network from different types of attacks which are mostly related with the traffic, we have come up an idea to integrate SDN with IoT for better performance, security and access control mechanism.

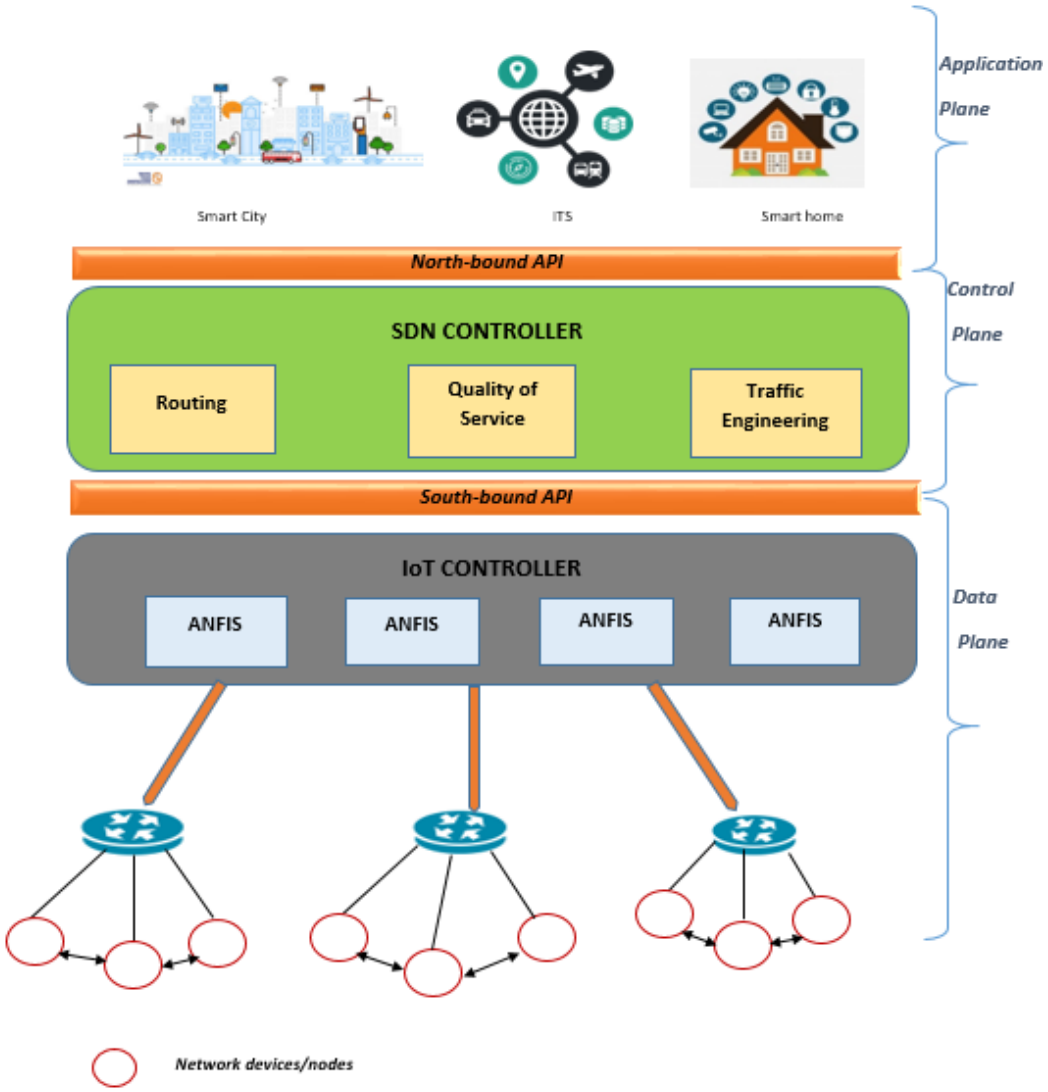

Figure 3.1: System Model

CHAPTER IV

Algorithm Analysis

4.1 Traffic Analysis

A SDN based IoT infrastructure basically provides free-flow of data from sensors and wireless devices and the efficiency of the network depends on the management and security of traffic. Network traffics are dynamic and hence its more prone to malicious attacks such as DDOS, MITM, Replay, Side Channel etc.

4.1.1 Traffic Analysis Technique

There are various classification techniques to classify the network traffic, but among these the following three techniques are mostly used-port based, payload/DPI (Deep Packet Inspection) based and ML (Machine Learning)-technique.

In **Port-based technique**, IP addresses are identified and used to classify the corresponding applications which are registered under Assigned Number Authority (AINA). In the other side, **Payload-based** or **Deep Packet Inspection(DPI)** are basically used to classify dynamic port numbers (peer to peer applications) and packets are analyzed for signatures and authentications of network applications of traffic. **ML (Machine Learning)-technique** uses trained classifiers as input for traffic classification based on the data set.

For our proposed system, to analysis the traffic efficiently we are applying ML-technique, as port-based classification doesn't provide the identification of dynamic ports and payload-based doesn't work for encrypted traffic and requires continuous updating of signature patterns of new applications. ML-technique overcomes these shortcomings of the following classification techniques and works more efficiently to classify data packets [7, 8].

ML (Machine Learning)- Technique

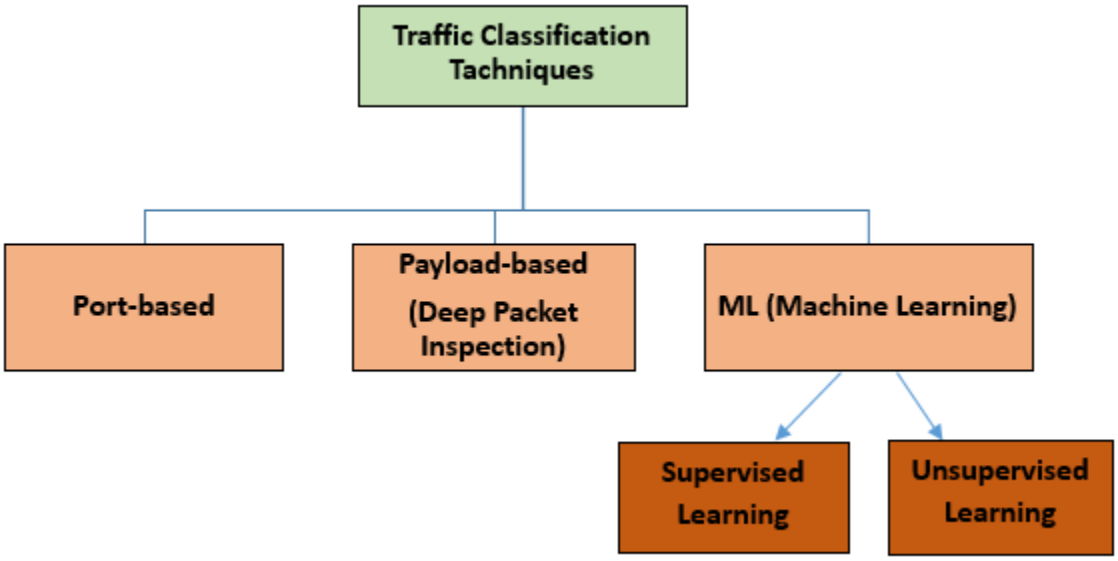

Figure 4.1: Traffic Analysis Technique

Machine learning is used for dynamic analysis for traffic and uses **WEKA** tool for detection method. It has two techniques for classification- supervised and unsupervised. In **Supervised** technique there is a training data set as input to train the system model for the expected output but in **unsupervised** technique there is no training/known data set and it works based on the prior knowledge or the statistical information.

4.2 Feature Extraction

By analyzing the network traffic, we get a data set which is the combination of the malware and benign data packets and this is the first major component for any malware detection system. A feature extractor is used to extract the features from the specified data set and we need to extract a group of features to detect attacks, which is not possible by extracting any specific or single feature.

4.2.1 Feature Extraction Tool

Here we are using the **Wireshark** and **Net Mate tool** for the corresponding live data packet capturing and feature extraction purpose.

1. **Wireshark:** Wireshark is an open source software and an efficient network

packet analyzer. Wireshark captures the network traffic from various wireless devices and displays them with very detailed protocol information and save the captured data packet. It can also export some or all packets in a number of capture file formats and filter them on many criteria. The basic features of Wireshark tools are-

- Capture traffics from live network or read data from already captured file.
- Terminal version, named Tshark or GUI is used to browse captured traffic.
- Display filter is used to refine and edit traffic programmatically.
- For dissecting protocols, Plug-ins is developed.
- Captured traffic can be used to detect VoIP calls when compatible encoding is used for encoding.
- Only selected traffic appears with several timers, settings and filters.

2. **Net Mate Tool:** After capturing data packets, the features are extracted using Net Mate tool as features depict the behavioral description of traffic. Net Mate includes two types of modules:

   - Packet Processing Modules designed to implement different metrics
   - Export Module that implement different output module

   Our concerned flow features are implemented in **Packet Processing Module**. Two different types of rules are used to produce the output: description rules and recognition rules.

4.3 Feature Selection

Feature Selection is an important step after traffic analysis to detect the abnormality occurring in a system. It can be defined as automatic selection of attributes in data samples that are most relevant to the predictive modeling problem. It does the mapping to excludes the irrelevant or redundant attributes and specifically defines most prominent for the better performance of the system.

As in our proposed system we are working on a large amount of a traffic of a network so feature selection should be done for the following requirements:

- To create an accurate predictive model that will give a better accuracy whilst requiring less data.

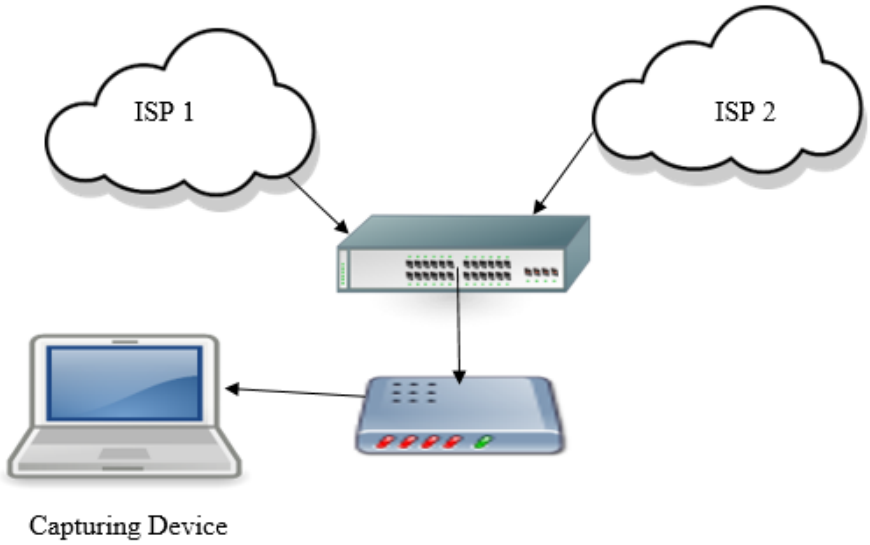

Figure 4.2: Feature Extraction Process

- it reduces the complexity of a model and makes it easier to interpret the required result.
- It enables the model to train faster on data sample as there is no redundant attributes.
- This method also reduces the problem of over fitting by enhancing the generalization in the model.

4.3.1 Selection Method

There are mainly three methods that are used in feature selection:

1. **Filter Method:** Here features are selected on the basis of their scores in various statistical tests for their correlation with the outcome variable which is Machine Language Independent.**Pearson's Correlation, LDA, ANOVA, Chi- Square** are the methods which are used to define correlation among the features.
2. **Wrapper Method:** This method considers the selection of a set of features as a search problem or algorithm to validate the prediction where different combinations are prepared, evaluated and compared to other combinations. After evaluating it assigns a score based on model accuracy. It can always

provide the best subset of features. But this method has a high computational cost.

3. **Embedded Method:** This method tries to combine the efficiency of other two methods and performs the selection of variables in the process of training and is usually specific to given learning machines. It basically learns which features best contribute to the accuracy of the model while the model is being created. Most common algorithms are the **LASSO, Elastic Net, Ridge Regression**used in this method.

For our model **Wrapper Method** is most applicable. As at first we have analyzed network traffic and after that we have implemented a Search process for extracting Unusual features to detect our attacks. From the complete list of Feature set we have further selected the most effective features to make our feature domain more powerful.

4.3.2 Selection Tool

The immediate step after feature extraction of any attack detection procedure is feature selection which is the final input feature set to feed into the system by using any machine learning technique. To select the desired features from the extracted features set, an efficient tool-set, WEKA is used in our attack detection process.

WEKA: WEKA, (Waikato Environment for Knowledge Analysis), named after a flightless New Zealand bird, supports many feature selection techniques, i.e. correlation based, information gain based, learner based etc. Weka is a set of machine learning algorithms for data mining tasks. The algorithms can be used directly on dataset or it can be called from Java code.

Weka contains tools for data pre-processing, classification, regression, clustering, association rules, and visualization. It provides SQL access with assistance of Java Database Connectivity. Weka provides four UI:

- Explorer
- Experimenter
- KnowledgeFlow
- Simple CLI.

Explorer is the main user interface of Weka which have following panels:

1. **Preprocess:** Choosing the data file.

2. **Classify:** Applying and experimenting with different algorithms on preprocessed data files.

3. **Cluster:** Applying different clustering tools, which identify clusters within the data file.

4. **Association:** Applying association rules, which identify the association within the data.

5. **Select attributes:** Seeing the changes on the inclusion and exclusion of attributes from the experiment.

6. **Visualize:** Seeing the possible visualization produced on the data set in a 2D format, in scatter plot and bar graph output.

The user cannot move between the different tabs until the initial preprocessing of the data set has been completed. This procedure can also be done with component based KnowledgeFlow and from Simple CLI. Experimenter provides option to compare predictive performance of machine learning algorithms on data-sets.

4.4 Feature Specification on Proposed Model

From extraction procedure eighteen features are collected which are grouped into nine features for the convenience of our work.And these nine features are taken as input for the further process.The mapping or selection of features are simplified as the below figure 4.3

1. **Server Overload:** It is one of the most common feature that happens in any kind of physical layer attack in the network. Increase of volume of data packets, excessive traffic is the indication of Server Overload. Though it's a common feature but there is possibility of Side Channel Attack, Malicious Code and DDoS attack.

2. **Slow Down:** It's a common feature of DDoS and Malicious Code Attack. In DDoS there creates traffic floods in bandwidth and resources so the performance evaluation becomes very poor. It is definitely a symptom that something is wrong with the system. In malicious code there occurs illegitimate actions which creates load on the system.

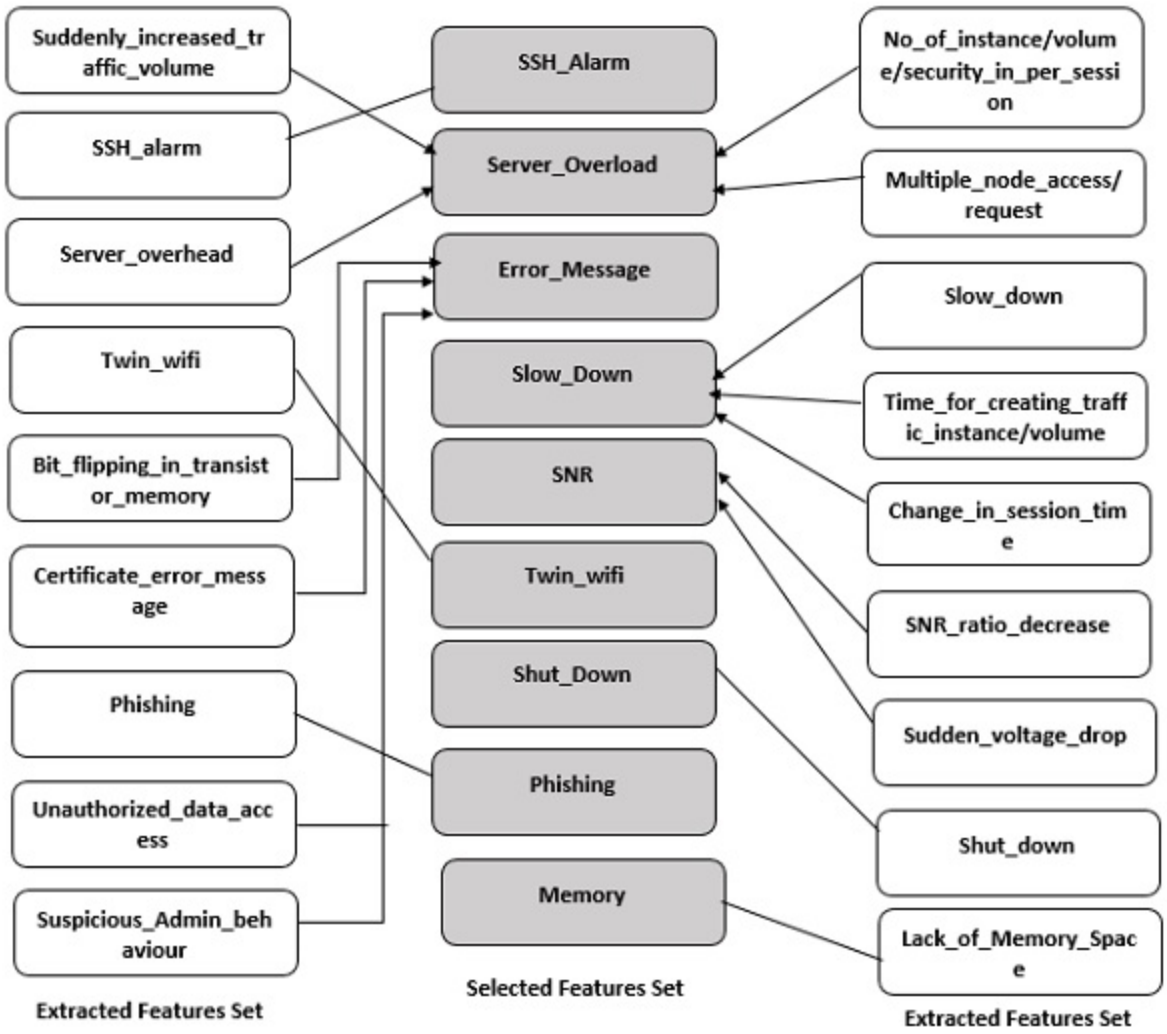

Figure 4.3: Feature Extraction and Selection

3. **Sudden shut Down:** It's the extreme case of DDoS attack in the network. a denial-of-service attack (DDoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its legitimate users by temporarily or indefinitely disrupting services of a host connected to the internet. So when network will not able to manage the overload it will just shut down.

4. **Error Message:** It is the most common characteristics of attacks that frequently occurs in IoT network model. It will generate automatically from the Operating System when it will suspect unusual activities in the network. So it is a great source of predicting that there is a third party in the network who

is trying to do something illegal in the network. Features-Bit flipping in memory cells, Suspicious Admin Behavior, Unauthorized Data Access are redundant which is mapped to exclude after feature selection method. Because all these three activities are unusual and it will result an error message. DDoS, Side Channel Attack, Malicious Code Attack, Man in The Middle(MITM) attack can be suspected by this feature.

5. **SSH Alarm:** SSH is one of the most popular communication protocols on the Internet used by admins, developers. SSH alarm is an email alert, when someone logs server via SSH (Server Secure Shell) can be pretty useful to track who is actually using server. It's a very unique feature to track MITM attack as an intruder might not login at first attempt.

6. **Twin-WiFi:** In MITM the main aim of an intruder is to entry the network and hampers the integrity, confidentiality, authenticity of admin. To get illegal access he can adapts the method of duplicate WiFi SSID or Address that is a very prominent feature to identify that the system is being attacked by the third party.

7. **Phishing:** It's a great threat to the security of users. It is actually a cybercrime in which targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking information, credit card details, and passwords. Intruder who conducts MITM attack mostly does this to earn in an illegal way.

8. **SNR decrease:** When noise of a system increases the SNR decreases that indicates the poor performance of the system. Voltage drops with proportional to SNR, that is not definitely a good symptom for a model. It is the most prominent feature to detect the Side Channel Attack. it is caused by the information gained from the network so the noise increases which should be noticed to detect attack.

9. **Lack of Memory Space:** Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software easily. It describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content. So sometimes it suddenly just occupies the memory space of user device and

gives warning to the user of "Memory is Full". That's definitely occurs a great problem of storing.

Here FIS will primarily work on these **Nine** Selected features where rules will be considered in controller to identify DDoS, MITM, Malicious Code Attack and Side Channel Attack. Rules are defined according to the priority of the features.

CHAPTER V

Performance Analysis

5.1 Fuzzification

5.1.1 Fuzzification Method:

Fuzzy logic is a form of

- Fuzzification Unit
- Knowledge Based Rules
- Decision or Controller Unit
- Defuzzification Unit

$$y = \cos(x) + \sin(x) + \beta \tag{5.1}$$

where y is the output of the system and x is the input of the system.

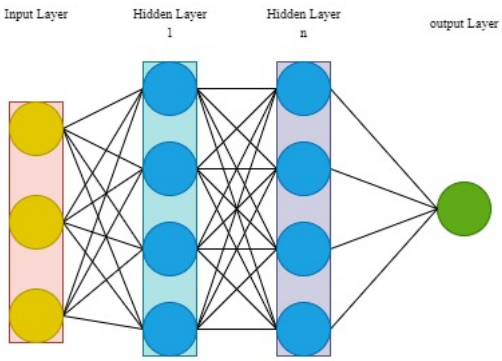

Figure 5.1: CNN architecture

Table 5.1: Deep learning Algorithms [1]

Name of Algorithm	**Description**
CNN	It includes input, hidden and output layers .
RNN	It is useful for time series data. It takes output and fed into input

Figure 5.1 shows a CNN architecture.

Table 5.1 shows deep learning algorithm [9].

CHAPTER VI

Discussion and Conclusion

6.1 Limitations

Co-operative society management systems, like any other systems, have their limitations. Here are some common limitations associated with Co-operative society management systems:

a. Limited Resources

b. Technical Expertise

c. Data Security Concerns

d. Integration Challenges

e. Limited Access to Technology

f. Resistance to Change

g. Maintenance and Upkeep

h. Customization Needs

i. Dependency on Vendors

j. Legal and Regulatory Compliance

Addressing these limitations requires careful planning, adequate resources, and a willingness to adapt to new technologies and processes. Co-operative societies need to assess their unique needs and challenges to select and implement a management system that aligns with their objectives and resources.

6.2 Future Plan

Creating a robust Co-operative society management system requires careful planning and consideration of various aspects. Here's a future-oriented plan to enhance the efficiency and effectiveness of a Co-operative society management system:

a. Digital Transformation

b. Data Security and Privacy

c. Member Engagement:

d. Financial Management:

e. Governance and Compliance

f. Community Building

g. Analytics and Reporting:

h. Continuous Improvement

i Disaster Preparedness

j. Environmental Sustainability

By integrating these strategies, a Co-operative society can not only streamline its operations but also enhance member satisfaction, foster community engagement, and ensure long-term sustainability in an ever-changing future landscape.

6.3 Conclusion

The implementation of a Co-operative Society Management System can have several positive outcomes for both the society and its members.

In conclusion, a Co-operative Society Management System not only modernizes the functioning of the society but also enhances member satisfaction, financial stability, and community development. It is a strategic investment that can pave the way for the sustainable growth of Cooperative societies in the future.

References

[1] M. Mondal, P. Mondal, N. Saha, and P. Chattopadhyay, "Automatic number plate recognition using CNN based self synthesized feature learning," in *2017 IEEE Calcutta Conference (CALCON)*, pp. 378–381, Dec. 2017.

[2] F. Ricci, L. Rokach, and B. Shapira, "Introduction to recommender systems handbook," in *Recommender systems handbook*, pp. 1–35, Springer, 2011.

[3] D. B. Johnson and D. A. Maltz, *Mobile Computing*, ch. Dynamic source routing in ad hoc wireless networks, pp. 153–181. Kluwer Academic Publishers, February 1996.

[4] M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, and A. Hussain, "A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications," *Cognitive Computation*, vol. 10, pp. 864–873, Oct. 2018.

[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[6] "Coronavirus." Access date: 24 June 2020.

[7] B. Noris, M. Barker, J. Nadel, F. Hentsch, F. Ansermet, and A. Billard, "Measuring gaze of children with autism spectrum disorders in naturalistic interactions," in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5356–5359, Aug 2011.

[8] P. Santi and D. M. Blough, "The Critical Transmitting Range for Connectivity in Sparse Wireless Ad Hoc Networks," *tmob*, vol. 2, no. 1, pp. 25–39, 2003.

[9] "Cnn," 1982. `https://en.wikipedia.org/wiki/CNN`. Accessed July 3, 2020.