Chapter - III

3. Design of The System

3.1. Fuzzy Classification Module

The paper’s related work consist of methods like naive Bayesian, K-NNC, SVM, J48, and fuzzy logic filtering methods to detect the emails as spam or ham. The proposed work relies on fuzzy rule based filtering approach which includes fuzzy inference system with fuzzy rules for classifying spam mails. This work focused on classifying the spam words and spam mail addresses by applying fuzzy rule. The spam words and spammer’s email addresses are assigned different values by using fuzzy rules. Collection of spam words list from the paper’s related works, spam words list spammer’s mail addresses are available in the website and spam mails in the inbox. This assigned value helps us to rank the spam features as shown in figure 3.1 and finally fuzzy inference system classifies the input rank values and produces the output.

Figure 3.1: Concept of classification of spam words and addresses

This work used two database files. The first database contains words. This work collected spam words often used in the spam mails by the spammers. This method used 500 spam trigger words collected from many websites. These trigger words which are the words and combination of words that are identified as being commonly used in spam messages. The second database which contains spam email
addresses. These addresses are collected from sender address and reply to addresses fields of the spam mails. Then these words are assigned value accordance to its degree of threat that each word possess. This work used fuzzy rules for ranking the words. These words are ranked as weak, very weak, moderate, strong and very strong words with its value.

The words such as Winner, dollar, award, cash prize, top job opportunities, earn more, beneficiary, good news, claim, high salary are few most triggered words used by the spammers to cheat the users. The internet users get attracted by these words in the mail and contact the sender immediately and gets deceived. So this work considered these words as very strong spam words. The first database contains spam words and rank value fields. The second database contains spammer’s addresses and rank value fields.

This work imports the mail in outlook. It extracts the actual words and actual sender address from the inbox of user. The actual words are extracted from the subject and content of email. The actual words and actual sender mail address are matched against the list of database of spam words and spammer’s mail addresses. If it is matched each other the rank value assigned to the detected spam words and mail address in the list. Fuzzy inference system takes the ranked value as input for classifying the spam mails. Figure 3.2 explains the architecture of spam Classification.
Figure 3.2: Architecture of Spam classification

[Diagram showing the process flow from Email to Output]

Figure 3.3: Fuzzy rule based classification

[Diagram showing the process flow from I/P to O/P through Rules]
In order to classify the spam fuzzy inference system has been designed which take the ranked input value and produce the output.

Figure 3.3 shows the fuzzy rule based classification. The output data are classified in to three linguistic variables i.e. Least dangerous, Moderate dangerous and Most dangerous.

3.2. Spam Filtering Steps

Step1: It is used to read the email from the inbox of user
Step2: The features are extracted from email
Step3: It is used to count the number of spam words
Step4: The features are compared against a list of ranked spam words and spammer’s email addresses in the database.
Step5: The spam words and spam mail address are classified accordance to the rank.
Step6: Input the rank values to the input and produce the result.

3.3. Ranking of Words

If spam word <=0.9 And> =0.7
It is a Very Strong spam word
ElseIf spam word < 0.7 And>=0.5
It is a Strong spam word
ElseIf spam word < 0.5 And>=0.4
It is a Moderate spam word
ElseIf spam word <0.4 And>=0.2
It is a Weak spam word
Else Very Weak spam word

3.4. Classification of Spam Emails

If spam words <=0.9And >=0.5
It is most dangerous spam mail
If spam words <0.5 And >=0.4
It is moderate dangerous spam mail
If spam words < 0.4 And >= 0
It is least dangerous spam mail

X â spam word
0 <= X < 0.2 â Very weak spam word
0.2 <= X < 0.4 â Weak spam word
0.4 <= X < 0.5 â Moderate spam word
0.5 <= X < 0.7 â Strong spam word
0.7 <= X <= 0.9 â Very strong spam word

The mamdani fuzzy inference model is followed in the implementation. This model’s simplicity helps anyone to understand the concept easily. Figure 3.4 shows the process of ranking and classification of spam words and spammer’s email address. Here this work used five linguistic variables for categorization of spam words and sender address and three linguistic variables for classification of spam mails.

**Figure 3.4: Ranking and classification of spam**
This model gives a clear picture of classification process. It explains how the features are classified into very strong or strong, moderate, weak or very weak spam words and spammer’s email addresses. This work gives importance to the fields of an email. This method easily classifies the email as least dangerous or moderate dangerous or most dangerous.