International Journal of Ignited Minds (IJIMIINDS)

# Efficient Spam Filtering Based on Artificial Immune System (AIS)

Ms. Athare Sharayu S[a], Prabhudev Irabashetti[b]

[a]*PG Scholar, Computer Engineering, V.A.C.O.E, Ahmednagar, Maharashtra, India.*
[b]*Asst Prof, Computer Engineering , V.A.C.O.E, Ahmednagar, Maharashtra, India.*

**ABSTRACT**

*Spam is an irrelevant or unsolicited messages sent over the internet. The term spam can also be used to describe any "unwanted" email from a company or website. Spam filtering is a service which checks all incoming emails in email accounts using mail filtering rules. These rules include identifying keywords, phrases, specific email addresses or domains which have been blacklisted. The problem of the traditional spam filtering is that it cannot effectively identify the unknown & variation characteristics. Artificial immune system exists diversity, immune memory, adaptive and self learning ability, adopt the idea of mail filtering, and design an improved spam filtering model based on immune mechanism. This paper proposes an efficient spam filtering which is based on artificial immune system.*

***Keywords*** *- Artificial Immune System (AIS), biological immune system (BIS), Self-Organizing Maps (SOM), Danger Theory Ensemble (DTE)*

## 1. INTRODUCTION

Day by Day as the use of internet is rapidly increasing, email has become the most important media for exchange of information. If you are the person using e-mails for communication then you should be familiar with the term spam. Spam is irrelevant or unsolicited messages sent over the internet, typically to large numbers of users, for the purposes of advertising, phishing and spreading malware. Spam is not only offensive & annoying; it causes loss of productivity, decreases bandwidth & costs companies a lot of money. Therefore, every smart company that uses email must take measures in order to block spam from entering their email systems. In order to effectively filter out spam & junk mail, we need to be able to distinguish spam from legitimate messages.

Spam Filtering is an important & typical pattern recognition problem, as spam causes many problems to our daily communication life, we use the classical statistical methods & AIS methods to solve these problems & they focus on studying feature extraction methods & design of classifier. Feature Extraction is used to extract the discriminative information from messages & then further transform these messages into feature vector. The feature extraction method collects & analyzes the numerical characteristics of messages. Numerical Characteristics are term frequencies & relation between terms & email categories. In design of classifiers, the classical pattern recognition methods are used such as Naive Bayes (NB), Support Vector Machine (SVM), Nearest Neighbor (NN) & Artificial Neural Network (ANN) which are based on the statistical theory.

The rest of the paper is organized as follows section 2 gives the literature survey, section 3 explains the related work, section 4 gives the proposed system and Section 5 states the conclusion.

## 2. LITERATURE SURVEY

To fight the spam, there exist many objective measures that can effectively limit the spam email impact on the end users (subjects). Traditional anti-spam techniques include the Bayesian-based filters, rule-based Scoring Systems, DNS MX Record Lookup and Reverse Lookup Systems, DNS Realtime Blackhole List (DNSRBLs) or IP Blacklists. However, these objective measures fail in many situations and they can have a level of accuracy. They suffer from the false positive and the true negative problems. Where a non-spam email can be classified as spam email or the filter can classify a spam email as legitimated email (non-spam) [2].

One of the solution for the spam problem is the "machine learning" method. The ability of a machine to improve its performance based on the previous results is known as machine learning. In machine learning the existing data set training is used to differentiate between the spam & non spam emails. Feature extraction is the major concept used in machine learning. It extracts the feature from the email & then give the result whether it is spam or not & it takes the help of training & learning phase. The data set is divided into the three parts, one is training, second is for testing & third for the cross validation.

M. Basavaraju and Dr. R. Prabhakar published a work on," A Novel Method of Spam Mail Detection using Text Based Clustering Approach". A new spam detection technique using the text clustering based on vector space model is proposed in this research paper. By using this method, one can extract spam/non -spam email and find out the spam email efficiently. Data is represented by using the Vector space model. For data reduction the clustering technique is used. It divides the data into groups based on pattern similarities such that each group is abstracted by one or more representatives.

## 3. RELATED WORK

### 3.1 Artificial Immune System

Artificial Intelligence System (AIS) is a research area which is used to build intelligence models & it takes the inspiration from Biological Immune System (BIS). BIS have several properties which consists of distributed detection, noise tolerance & reinforcement learning. Considering the immune processes related to BIS many AIS models have been developed to solve engineering problems. Examples are negative selection, clonal selection, immune network model & danger theory algorithm & these models are applied on real world problems which are pattern recognition, data mining, spam filtering & computer security. The main function of BIS is to protect the body from molecules which are known as antigens. The feature of BIS is that it has the pattern recognition capability which can be used to differentiate between foreign cells entering in the body (non-self or antigen) & the body cells (self).

### 3.2 Problem Modeling and Design

**INPUT :**

We are going to input Different types of messages.

{msg1, msg2, msg3… msg n}

**OUTPUT:**

As we pass messages as input so as output its will give best classification of the msg.

{Search result 1, search result 2… search result 3}

**PROCESS:**

1. TOK : ( Tokenization )
2. DG : ( Detector Generation)
3. CC : ( Concentration Calculation )
4. TC : ( Training Classifiers)
5. CM : (Classifier model)
6. CDTE : (Classification by DTE)

The input message goes through the two phases i.e. training phase & classification phase. Both the phases are illustrated in the Fig 1. According to the model, concentration based feature vectors are extracted from messages by computing match concentration of detections. Classifiers are then built on the concentration vectors of training corpus. Finally, incoming messages can be classified by using the DTE method. In addition, classifiers are updated at all times based on the drift of messages and classification performance [1].

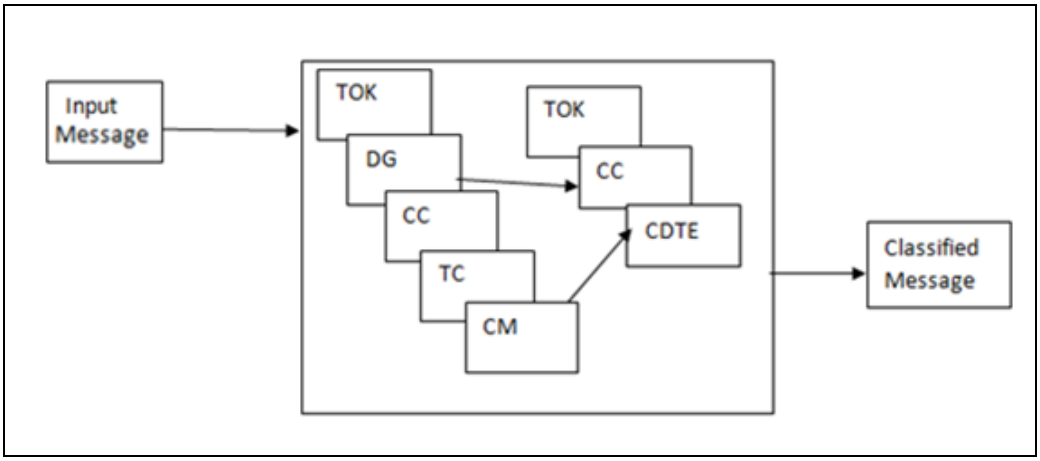


Fig 1: Training & Classification Phase of the immune based model.

In the training classifiers Support Vector Machine (SVM), Naïve Bayesian (NB), & Nearest Neighbor (NN) are utilized as three grounding classifiers. The function of all these three is different. SVM is used for generating match signal, NB for danger signal & NN for self-trigger process.

### 3.3 DTE Steps:

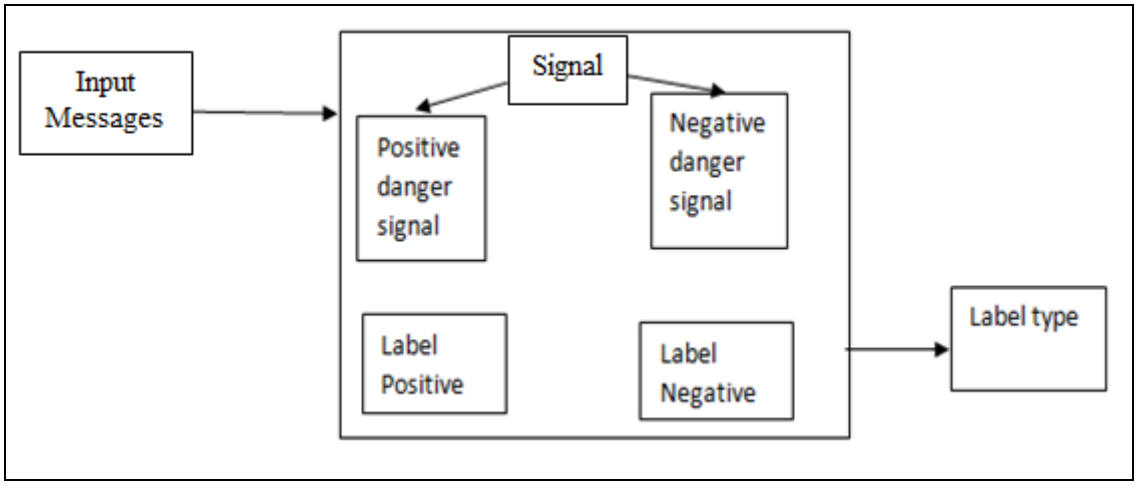


Fig 2: Framework of DTE

Danger theory is the matching in the humoral immune system. It is fundamental that only the 'correct' cells are mathched as otherwise this could lead to a self-destructive autoimmune reaction. Classical immunology stipulates that an immune response triggered when the body encounters something non-self or foreign [11].

The framework of DTE method is illustrated in the Fig 2. A input message is labeled by the two classifiers if both the signals agree with each other i.e. positive danger signal & negative danger signal. In other case, a third classifier i.e. self-trigger process is used to solve the input message & get it classified. The characteristics of the DTE method lie in the interaction among classifiers by using the danger zone and the signals [1].

## 4. PROPOSED SYSTEM

The actual flow of proposed system is shown in the Fig 3. We use the Self Organizing Maps (SOM) algorithm in the proposed work. The existing approaches did not considers the significance of the word sequence in a message and make use of the sequence information for the mail filtering task. The SOM based sequence analysis system is based a new way of document representation, which keeps information regarding the temporal sequences of words, as well as their frequencies. A k-Nearest-Neighbor algorithm with a new cost function is applied on top of SOMs for classification [12].

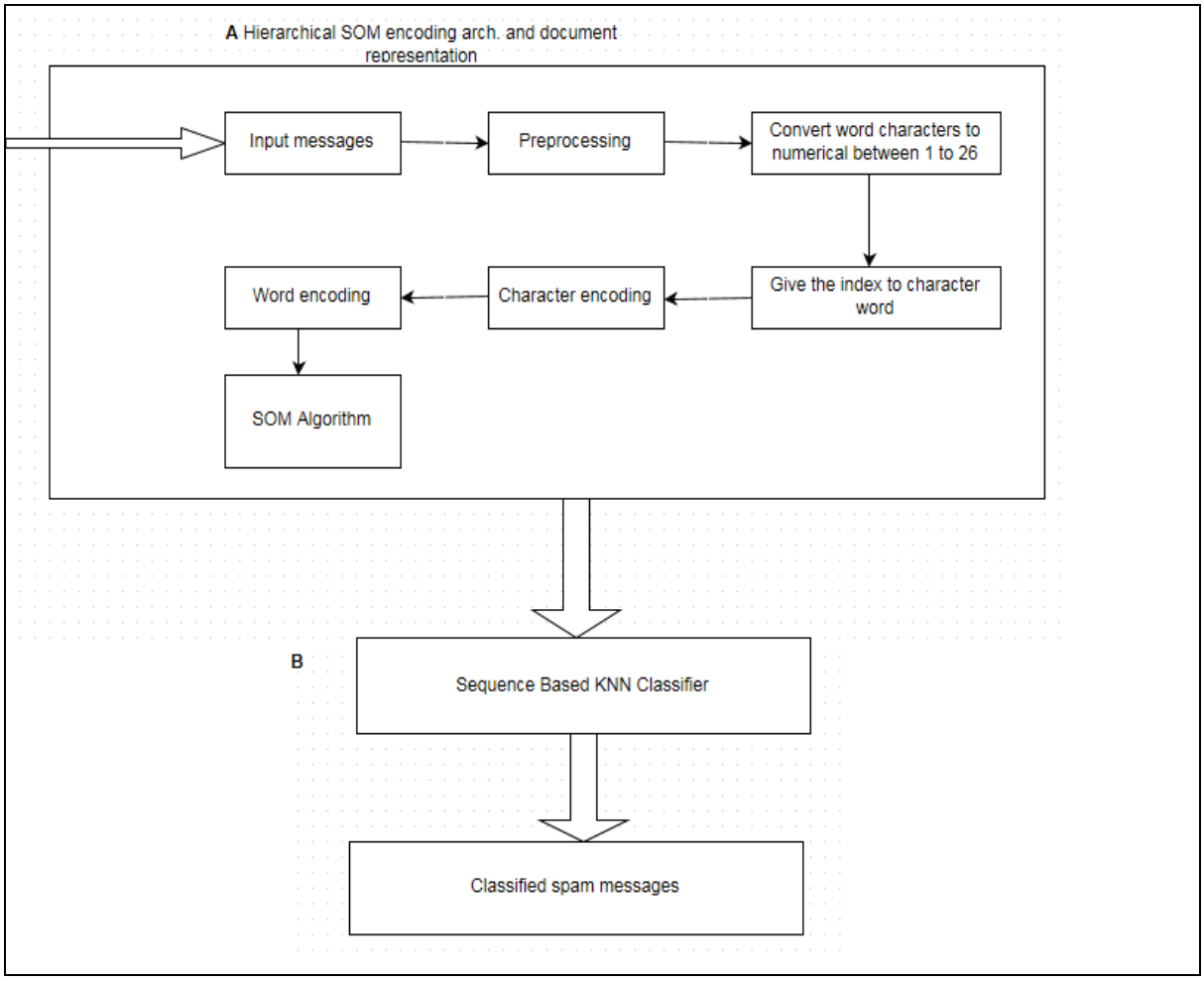


Fig 3: Spam Filtering Using SOM Based Systems.

The input message is pre-processed & the numerical representation is provided to each character between 1to 26. The small case & upper case characters are considered as the same. Then further the index is provided to each character in the word. For e.g. in the word "Filter"- "F" have time index 1, "i" have time index 2, & so on. In the next step the character encoding is done, after that word encoding and finally encoded word sequence is used to represent the document.

## 5. CONCLUSION

In this paper, we briefly introduce our recent advances in immune based spam filtering methods, and put emphasis on combining immune theory with statistical methods. It is shown that combining immune ideas with classical statistical methods can effectively improve the performance of a spam filter. In addition, we present a framework of DTE method & also spam filtering using SOM based systems.

## ACKNOWLEDGEMENTS

We would like to give our sincere thanks to Prof. Kshirsagar M.C, Prof. Natikar sir, Prof. Jaypal P.C. and all the staff of V.A.C.O.E Ahmednagar who helped us directly & indirectly.
Our special thanks to our parents & Mr. Ghorpade S. M for motivating us to publish this work.

## REFERENCES


1. Ying Tan, Guyue Mi, Yuanchun Zhu, and Chao Deng, "*Artificial Immune System Based Methods for Spam Filtering*", IEEE transactions on audio, Speech and Language Processing,Vol.21,No.7, March 2014.
2. Samir A. Elsagheer Mohamed, Efficient Spam Filtering System Based on Smart Cooperative Subjective & Objective Methods, Int. J. Communications, Network & System Sciences, 2013, 6, 88-99.
3. J. Timmis, P. Andrew, N. Owens, and E. Clark, An interdisciplinary perspective on artificial immune systems, *Evol. Intel*, pp. 5–26, 2008.
4. I.R. Cohen, Real and artificial immune systems: computing the state of the body, *Imm. Rev.*, pp. 569–574, 2007.
5. Wikipedia, "Spam". http://en.wikipedia.org/wiki/Spam (electronic)
6. D. Mertz, "Spam Filtering Techniques," 2002. http://www.ibm.com/developerworks/linux/library/l-spamf.html.
7. Ayara M, Timmis J, Castro L. de, and Duncan R, 2002. Negative Selection: How to Generate Detectors. In 1st International Conference on Artificial Immune Systems, pp. 89-98, September.
8. G. Robinson, "*A Statistical Approach to the Spam Problem*", 2003. http://www.linuxjournal.com/article.php?sid=6467 (ac-cessed March 2011).
9. Y. Zhu and Y. Tan, A danger theory inspired learning model and its application to spam detection, In: *Proc. International Conference on Swarm Intelligence*, 2011, pp. 382–389.
10. Y. Yang and J.O. Pedersen, A Comparative Study on Feature Selection in Text Categorization, in: *Proc. Int. Conf. Machine Learning (ICML'97)*, 1997, pp. 412–420.
11. Uwe Aickelin and Steve Cayzer, The Danger Theory and Its Application to Artificial Immune Systems, Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS-2002), pp 141-148, Canterbury, UK, 2002.
12. Xiao Luo & Nur Zincir-Heywood-Comparison of a SOM Based Sequence Analysis System and Naïve Bayesian Classifier for Spam Filtering.