The internet has undoubtedly become the linking tool for bringing together customers and business people, countries and regions, continents and islands regardless of their economic, political, cultural and social affiliations. Email service providers are going ahead on making email easy to use, allowing a variety of information to be conveniently and reliably sent through the Internet. The popularity of email has also brought with it challenges for Internet users and Internet Service Providers to the extent that if spamming problem is not dealt with urgently, benefits currently enjoyed by stakeholders would be surpassed by spam concerns. Although spam filtering techniques are now available on the market today, no one can deny that these solutions cannot guarantee 100% effectiveness at eliminating the problems of spam because a variety of these filters have weaknesses and strengths. This paper presents an alternative solution using a neural network classifier on a corpus of email messages received by the three researchers who conducted this investigation. The dataset for our system used descriptive attributes of words, symbols and email messages that are commonly used by email users to correctly identify spam received in email inboxes. The results show that our neural network classifier is able to detect and filter spam with success just like the others already on the market today.

Key words: Neural network classifier, spam filter, spam motivation, feature representation, email.

INTRODUCTION

Spam at least for the purpose of this paper is defined as unsolicited, unwanted email that is sent indiscriminately, directly or indirectly, by a sender having no current relationship with the recipient [1,2] or an unsolicited commercial mail usually sent to a large group of recipients at the same time by service providers such as internet service providers (ISPs) to market their products [3] and services, current and new ones. According to the American Heritage Dictionary, spam is defined as "unsolicited email, often of commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroup; junk email [4,5]. Spam exists in different forms such as Usenet spam, sms spam sent by text–messaging services [6] on mobile phones or IM spam sent by instant messaging services and web log spam among others and has become a serious concern to the success of email as a global communication tool. The exponential growth of spamming business led to the development of spam filters to fight against this scourge. This became necessary since users of email are disadvantaged when they want to reach mails in their inboxes. Users lose a lot of bandwidth on cleaning up spam. This problem is really more serious to those who use dial-up Internet facilities. There is no longer quick accessibility to emails because of delays caused by eliminating hostile messages which intrude into our mailboxes. According to reports produced by MacAfee in 2011 the average global spam rate was two trillion a day [7]. This huge production of spam led to the development of spam filters that give user at least relief from the scourge. The available filtering engines are not enough because with time some of them lose their effectiveness or may not be able to cope up with word obfuscation on keywords used by spammers to evade filters. There is no filter on the market today with both 100% effectiveness
Spam and Employee Productivity

Spam continues to be a concern on reduced employee productivity resulting from the need for sorting through a huge number of spam received on a daily basis looking for legitimate business email communications [2,10] and according to report on survey conducted in April 2007, it found that on average users spent an estimated one per cent (1%) of their time dealing with spam each day. There are many spam filters available on the market for use by clients today but even their presence does not erase the fear that a spam filter may block legitimate email which is an unwelcome development for a business, because missing very important and sensitive emails can be extremely destructive to customer relations as reported by Hansel [11] and should be avoided at all cost. A study conducted by Nucleus Research, Inc., reported that spam costs U.S. businesses an estimated $71 billion in lost employee productivity, an amount equivalent to approximately $712 per employee per year [11,12] and these are not simple figures from the business perspectives (Table 1).

Spam and Computer Security

There are security concerns on the ever increasing availability of spam especially for attacks whose purpose is to illegally obtain confidential information from Internet users (phishing) [12,13]. The attacks are suspected of disseminating malicious software such as computer viruses, Trojan horses and Internet worms as discovered by Bratko et al. [14]. Liang [15] found that phishing has significant negative return on the global market value. An economic assessment on the influence and impact of spam on a number of firms whose email advertising was considered spam was also done by Raad et al. [16].

Spam on e-Commerce

Spam is a serious threat in e-commerce since its repercussion on internet users, business offering e-commerce opportunities and their middlemen are not spared. An accurate detection of spam is fundamental on e-commerce because false positives prevent the recipient from receiving legitimate emails while on the other side, false negatives expose the client to spam attacks such as phishing (Table 2). In a related development, a recent report by Smith et al. [17] analysed the effect of cybercrime on advertising activities and shareholder benefit. The results from the report indicate that the cost of cybercrime go beyond physical resources such as stolen assets, business losses and damages on the image of the company. These all have a negative repercussion on the shareholder value. Potential buyers will not have confidence on the security of their payments.

<table>
<thead>
<tr>
<th>Table 1. Showing Statistics of Spam.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Daily Spam emails sent</strong></td>
</tr>
<tr>
<td>Daily spam received per person</td>
</tr>
<tr>
<td>Annual Spam received per person</td>
</tr>
<tr>
<td>Spam cost to all non-corporation Users</td>
</tr>
<tr>
<td>Spam cost to all U.S Corporation in 2002</td>
</tr>
<tr>
<td>Email address changes due to Spam</td>
</tr>
<tr>
<td>Annual Spam in 1000 employee company</td>
</tr>
<tr>
<td>Users who reply to Spam email</td>
</tr>
<tr>
<td>Users who purchased from Spam email</td>
</tr>
<tr>
<td>Corporate email that is considered Spam</td>
</tr>
</tbody>
</table>

Source: Cormack and Lynam [1].

and low percentages of false positives. A filter that achieves 100% spam detection and blocking runs the danger of increasing false positives which is worse off than those with a lower detection rate because the risk of losing one legitimate email must be avoided at all cost.

The remaining sections include a detailed summary of spam problems, current interventions both technical and non-technical are discussed before a survey of related literature. Our spam classifier is described under research methods, followed by results and discussion before finally concluding the paper with a conclusion and future work.

The Impact of Unwanted Messages.

Despite all blame laid against unwanted messages, Chaudry [8] reported about a group of people that voluntarily want to receive these commercial messages regardless of the product or service being marketed. Spammers therefore want to reach this group by sending spam to as many users as possible because the spammers do not know who will respond to their message and who will not. Praed [9] said spammers avoid detection and prosecution by engaging third party skilled people to send spam on their behalf to potential customers. The problems which affect both users and industry are outlined in the next section below:
A technical report by McAfee revealed shocking evidence of the impact spam has on the environment to the extent of incurring huge environmental costs. According to their findings a total of thirty-three billion kilowatt – hours were used by spam, this amount of electricity is equivalent to 2.4 million homes in U.S.A. Further to that cost, spam emailing cause emissions of greenhouse gases at the rate equated to 3.1 million passenger cars using two billion gallons of gasoline, according to Smith et al. [17]. McAfee’s focus in commissioning ICF International to conduct the investigation was meant to examine the overall impact of spam on the global environment and not dealing with a single country. Their findings described both energy consumption and its sources. According to the report the sources included, “(h)arvesting addresses”, “(c)reating spam campaigns”, “(s)ending spam from zombies and mail servers”, “(t)ransmitting spam from sender to receiver via the (i)nternet”, “(p)rocessing of spam by incoming mail servers,” “(s)toring messages,” “(v)iewing and deleting spam and ”(f)iltering spam and searching for false positives.” A notable observation was that the overwhelming majority of spam email emissions come from the process of viewing and deleting or searching for legitimate emails (sic) erroneously trapped in spam filters (false positives). The study further estimates spam recipient expend approximately 104 billion hours reading and deleting spam, at a time spam filters are blocking nearly eighty per cent of spam. According to its key findings, the study showed that though the energy use and emissions associated with spam are staggering, without blocking it would be considerably worse. Fortunately, spam filters and blockers save around 135 kWh of electricity per year, meaning spam blockers have the effect of taking thirteen million cars off the road.

**Table 2. Showing Categories of Spam.**

<table>
<thead>
<tr>
<th>Products</th>
<th>25%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>20%</td>
</tr>
<tr>
<td>Adults</td>
<td>19%</td>
</tr>
<tr>
<td>Scams</td>
<td>9%</td>
</tr>
<tr>
<td>Health</td>
<td>7%</td>
</tr>
<tr>
<td>Internet</td>
<td>7%</td>
</tr>
<tr>
<td>Leisure</td>
<td>6%</td>
</tr>
<tr>
<td>Spirit</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: Azam [18].

Spam and the Environment

When companies continue with exposure to cybercrime, these loopholes reduce faith of customers leaving business in a big loss of future business engagement.

**Current Non Technological Interventions**

These are solutions which do not require application or using technical interventions to address concerns raised by spam but they are meant to scare authors of unwanted hostile messages from flooding the users’ inboxes with spam. The success of these solutions rests on the power of users to fight back on the losses of time and bandwidth spent downloading spam.

**Recipient Revolt**

Azam [18] noted that this intervention is activated as soon as the user receives spam email by revolting against emails in physical world by invoking fear that scares away legitimate companies to keep away from using unwanted messages while at the same time forcing ISPs to change operating policies on issues to do with spam.

**Advantages**

- Forcing ISPs to change policies.
- Legitimate companies will be afraid to send spam emails resulting in removal of email ids from their contacts.
- If proper awareness and devotion is done then the intervention would enjoy quick user feedback.

**Disadvantages**

- This intervention may be a burden on ISPs for handling valid and invalid complaints.
- There is need for authentication of complaints so that complaints are checked so that they are against the right person.
- As spammers hide their identities, it will cause some people to block all mails from unknown persons resulting in hurdles and limited range of communication.

**Customer Revolt**

This intervention suggests that all firms which collect personal data for business purpose should be forced to disclose what they will do with that data. This encourages companies to stick to the agreed purpose. Further to disclosure, Azam [18] noted that there should be proper publishing of policies on web pages, to reveal the reason for data gathering.

**Disadvantages**

- There is a possibility of false complaints
- The problem of separating valid from invalid complaints

**Vigilante Attack**

This solution suggests the need for dealing with spam addresses with anger, treating them with email bombs as well as denial of service attack to as to win the fight.
Table 3. Showing methods for effectiveness and accuracy of ant-spam solution.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Example</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsive</td>
<td>Filters leverage research on actual spam. It is very accurate and legitimate email rarely blocked</td>
<td>Signature based filter</td>
<td>Extensive and well managed spam analysis infrastructure is required for effectiveness</td>
</tr>
<tr>
<td>Method</td>
<td></td>
<td>Attack-driven filter</td>
<td></td>
</tr>
<tr>
<td>Proactive</td>
<td>Filter examines spam looking for a variety of spam attributes</td>
<td>Adaptive/Bayesian filter</td>
<td>Filters require constant training or tuning else the effectiveness drops.</td>
</tr>
<tr>
<td>Method</td>
<td></td>
<td>Heuristic filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Open proxy filtering lists</td>
<td></td>
</tr>
</tbody>
</table>

Source: Zhen et al. [30].

against spammers.

Disadvantages

- An accurate identification of spammer is no mean job
- Results coming from this intervention might be nasty in some cases with the worst case being unethical.

Hide email Address

The use of two email addresses is fundamental for this intervention to bring positive results. The first email address is required to receive all incoming emails where they are scanned by the recipient, after that the valid email addresses are sent to the second email address. Azam [18] pointed out that the second email address is only revealed to known persons and must never be publicised on the Internet.

Disadvantages

- Maintaining a couple of email addresses may not be simple task.
- User should tell all contacts to neither reveal the address to anyone nor have it publicised on the Internet.
- No fundamental work is actually done to stop spamming activities.

Contract–Law and Limiting Trial Accounts

The email service provider organization and the user should enter into agreement before registration is done. This allows more time for studying the identity of the person while the account runs on a temporary basis. If the trial is successful without a report with allegation of spam by user, then the account would be fully registered. In the event of violation at any phase, his account would be abandoned and user punished.

Disadvantage

- Revealing people’s identity without their will to companies which are not trusted by the said users may be an insurmountable task.

Current Technical Interventions

Technical interventions are reactive in nature, meaning once spam is present at the user account then the techniques automatically start dealing with spam. The idea behind is to make life very difficult for spamming community and not stopping them from sending unwanted messages.

The effectiveness and accuracy of existing anti-spam solutions can be categorised into two classes namely responsive and proactive approaches (Table 3) with the former classifying an incoming email message as spam if it meets network expert – set rules that characterise known unsolicited emails while the later relies on corpora of unsolicited and regular email to infer distinguishing attributes to be used for classifying incoming email messages [19]. Each method not only looks at the content of the message, but also at its header information such as list of recipients, source of IP address and subject matter. Stolfo et al. [19] further said that responsive filtering techniques has the advantage of being fast and simple but is not very accurate while proactive approach based on content is more valid but takes more time.

Domain Filtering Systems

A mailers program is configured in such a way that it only accepts trusted mails coming from specific domains recorded in a database. Therefore any email which is not mentioned in the database will be blocked immediately.

Weaknesses

- Spamming community may as well start using legitimate domains.
- The range of communication space is reduced.

Blacklisting Solution

The technique filters out all unknown addresses and
keeps a repository of known violators thereby blocking mails from them. There is need to place servers in a distributed manner which constantly monitors communication of users while at the same time watching spammers and their sites.

**Weaknesses**

- Innocent users might be mistakenly be labelled spammers.
- The cost of maintaining an updated database of spammers.
- Regular updating of databases and retrieval of information coming from distributed databases about spammer is required.
- It is not easy associating email user with an email id because a user who changes his email id may not be recognized; hence the database about spammers becomes outdated.

**White list Filters**

Mailer programs are configured to learn all contacts of a user and allow only email communications from those contacts only. Mails coming from unknown contacts are directed to other folders so that spams are completely prevented from entering user’s inbox.

**Weaknesses**

- Configuring mailer programs to learn about contacts of the user is a special responsibility.
- If contact email id changes, then mailer program will not be informed this, way eliminates that contacts mails from the user inbox.
- There is considerable delay experienced by new parties mails they are not visible to the user because of not being present at the inbox.
- It suffers limited range of communication space.

**Rules Based**

Spam emails are examined by an expert to find features or characteristics on specific words or phrases between email instances and the corresponding class. Experts define rules which are applied by the system to detect spam emails. To enhance the effectiveness of a detection spam solution, certain weights are assigned to rules based on their utility towards class definition. For instance, strange instances may be classified based on the availability or non-availability of predefined rules together with their weights in the email.

**Weaknesses**

- The requirement of a human expert to constantly update the database rules so that it caters for new kinds of spam.
- Rules may be outdated once spamming solution is learnt by spammers.

**Bayesian Filters**

Naïve Bayes classifier is commercial machine learning technique used for filtering spam emails by computing the probability that certain specific words or phrases occur in known unwanted messages and using the probability obtained to classify new messages received. Naïve Bayes is one of the most successful filters at categorizing text documents [20,21].

**Machine Learning Filtering**

This technique is sub specie of Artificial Intelligence which is defined as the design and development of algorithms that are able to learn and adapt to new types email messages displaying similar characteristics to those learned. Machine learning and text classification of note include the famous Bayesian classification, Artificial Neural Networks [22,23] and Artificial Immune System among others.

**Artificial Neural Network**

Artificial Neural Network is a huge volume of algorithms and techniques with capability to classification, regression and density estimation [24,25]. A neural network is made up of a complex collection of functions capable of breaking down into smaller parts that are represented graphically as neurons. The Perceptron and Multilayer perceptron are the main types of neural networks that are used when referring to ANN.

**Literature Review**

Stuart *et al.* [26] in his research used a neural network method on a data set of email messages from a single participant user. Descriptive characteristics of words and messages similar to those required to identify spam messages were used as feature for defining spam messages. Stuart used a total corpus of 1654 emails received by one of the authors over undisclosed number of months. Results of comparisons between his neural network filter and Naïve Bayesian technique indicated that the developed neural network needed fewer features to achieve results produced by Naïve Bayesian approach.

Levent *et al.* [27] developed anti-spam filtering methods for agglutinative languages in general and for Turkish to be specific. He used dynamic methods based on Artificial Neural Networks and Bayesian Networks and his algorithms are user–specific. Further to that the algorithms have the advantage of adjusting themselves with characteristics of incoming email messages.
According to his findings, a total of 750 emails including 410 spams and 340 hams were used in the experiments where a success rate of approximately 90% was achieved.

In a related development James et al. [28] presented a paper on neural network based system for automated email classification. In addition to that he also presented a system which can be defined as a neural network based system used for automatic email categorization problems. His research showed that neural networks can successfully be used for automated email filing into mailboxes and spam mail filtering.

One of the authors who did research based on neural networks is Puniskis et al. [29] who used neural network approach to the classification of spam. The technique employs attributes composed of descriptive features of evasive patterns that spamming community employs rather than using the context or frequency of keywords in the email message. With availability of 2788 ham and 1812 email spam in his possession received during a certain period of months, he noted that artificial neural networks are satisfactory but they are adequate for using alone as a spam filtering tool.

The cited literature is not the only available on the market with a history of tremendous achievement but serves to buttress the fact that artificial neural networks have become one of the new approaches that can be used to reduce concerns caused by authors of email spam. Therefore the use of neural networks for our spam filtering system is supported by clear evidence from quoted literature, so our project would be a success as well.

RESEARCH METHODS

A Neural Network Classifier was designed for Spam detection and classification of spam using attributes based on descriptive characteristics of most evasive patterns which spammers employ adapted from Stuart et al. [26]. A total ham of 1654 emails received and recorded from January 2012 to December 2012 by all the three authors collectively were used for our experiments. All the emails used had no embedded attachments as they were removed just for confidential reasons. Each email communication received was saved as text file and have it parsed so as to identify each header element in order to differentiate them from the body of the message. The researchers made sure that every substring within the subject header and the message body which was delimited by white space was labelled a token. An alphabetic word was defined as a token delimited by white space containing only English letters of the alphabet or apostrophes. In addition to that, the tokens were evaluated to generate a group of seventeen hand-crafted characteristics from each email message (Table 4).

Operation of Neural Network Classifier:

- Every incoming email is treated as a text file, thereafter input layers are searched for any matching tokens. The tokens come in a variety of weight so the system computes a score for each incoming message before classifying as spam or ham.
- System compares computed score with a threshold value, if the score is bigger than the threshold value then the incoming message is labelled spam, else it is considered as a ham.
- When incoming message is spam, the system also adds new token to the adaptive input layers for future training. This allows the system to continue providing useful service on detecting spam.

The architecture of a spam filtering system shown in Figure 1 collects incoming emails considered spam and legitimate email. This spam filtering model consists of initial transformation, user interface, feature extraction and selection, email data classification and an analyser component for effective performance. Machine learning session of required algorithms is applied at the end to train and test the researcher’s model so that the email in question can be classified as spam or legitimate when the decision is finally passed.

The System Training Phase

The training phase requires each incoming message to be treated as a text file, thereafter the message is parsed to identify header information (namely: From, Received, Subject, or To) to differentiate them from the body of the message. The system considers every substring within the subject header and the message delimited by white space as a token. The emails were grouped into 800 legitimate emails and 854 junk emails. We also randomly selected and used half of each group to comprise data set (n = 827) used to train a three layer neural network with the number of hidden nodes from 4 to 14 and the number of epochs ranging from 100 to 500. After this training process, the email messages of the training set were then classified to provide a generalization of accurate results.

RESULTS AND DISCUSSION

The benchmarks for measuring the success of a spam filtering technique are spam recall (SR), spam precision (SP), legitimate precision (LP), and legitimate recall (LR) among the most commonly used performance measures [31,32].

Spam recall is used to measure the proportion of spam mails which were accurately classified as spam while spam precision is defined as the percentages of email messages classified as spam which actually are spam
Table 4. Showing features extracted from each email.

<table>
<thead>
<tr>
<th>Features From the Message Subject Header</th>
<th>Features From the Message Subject Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Number of alphabetic words that did not contain any vowels</td>
<td>2 Number of alphabetic words that contained at least two of the following letters (upper or lower case): J, K, Q, X, Z</td>
</tr>
<tr>
<td>3 Number of alphabetic words that were at least 15 characters long</td>
<td>4 Number of tokens that contained non-English characters, special characters such as punctuation or numeric digits at the beginning or middle of token</td>
</tr>
<tr>
<td>5 <strong>Number of words with all alphabetic characters in upper case</strong></td>
<td>6 Binary feature indicating occurrence of a character (including spaces) that is repeated at least three times in succession: yes = 1, no = 0</td>
</tr>
<tr>
<td>Features from the Priority and Content – Type Headers</td>
<td>Features from the Priority and Content – Type Headers</td>
</tr>
<tr>
<td>7 Binary feature indicating whether a priority header appeared within the message headers (X – Priority and/or X – MSMail – priority) or whether the priority had been set to any level besides normal or medium: yes = 1, no = 0</td>
<td>8 Binary feature indicating whether a content – type header appeared within the message headers or whether the content type of the message has been set to “text/html”: yes = 1, no = 0</td>
</tr>
<tr>
<td>Features From the Message Body</td>
<td>Features From the Message Body</td>
</tr>
<tr>
<td>9 Proportion of alphabetic words with no vowels and with at least seven characters</td>
<td>10 Number of alphabetic words that contained at least two of the following letters (upper or lower case): J, K, Q, X, Z</td>
</tr>
<tr>
<td>11 Number of alphabetic words that were at least 15 characters long</td>
<td>12 Binary feature indicating whether white – space- delimited strings “From:” and “To:” were both present: yes = 1, no = 0</td>
</tr>
<tr>
<td>13 Number of HTML opening comment tags</td>
<td>14 Number of hyperlinks (“href=”)</td>
</tr>
<tr>
<td>15 Number of clickable images represented in the HTML</td>
<td>16 Binary feature indicating whether the colour of any text within the body message was set to white: yes = 1, no = 0</td>
</tr>
<tr>
<td>17 Number of URLs within hyperlinks that contain any numeric digits or any of the three characters (“&amp;”, “%” or “@”) in the domains or subdomain(s) of the link.</td>
<td></td>
</tr>
</tbody>
</table>

Source: Stuart [26].
Table 5. Showing Classification results on the testing set (n = 827).

<table>
<thead>
<tr>
<th>Hidden Nodes</th>
<th>Training Epochs</th>
<th>Spam Precision (%)</th>
<th>Spam Recall (%)</th>
<th>Legitimate Precision (%)</th>
<th>Legitimate Recall (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>91.81</td>
<td>86.65</td>
<td>86.56</td>
<td>91.75</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>400</td>
<td>90.95</td>
<td>89.46</td>
<td>88.94</td>
<td>90.5</td>
</tr>
<tr>
<td>500</td>
<td>93.73</td>
<td>87.59</td>
<td>87.62</td>
<td>93.75</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>300</td>
<td>92.11</td>
<td>90.16</td>
<td>89.73</td>
<td>91.75</td>
</tr>
<tr>
<td></td>
<td>400</td>
<td>91.09</td>
<td>86.18</td>
<td>86.05</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>500</td>
<td>92.48</td>
<td>86.42</td>
<td>86.45</td>
<td>92.5</td>
</tr>
<tr>
<td>12</td>
<td>300</td>
<td>93.52</td>
<td>87.82</td>
<td>87.79</td>
<td>93.5</td>
</tr>
<tr>
<td></td>
<td>400</td>
<td>91.73</td>
<td>88.29</td>
<td>87.98</td>
<td>91.5</td>
</tr>
<tr>
<td></td>
<td>500</td>
<td>92.45</td>
<td>91.8</td>
<td>91.32</td>
<td>92</td>
</tr>
<tr>
<td>14</td>
<td>300</td>
<td>91.58</td>
<td>84.07</td>
<td>84.37</td>
<td>91.75</td>
</tr>
<tr>
<td></td>
<td>400</td>
<td>92.04</td>
<td>86.65</td>
<td>86.59</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>500</td>
<td>91.28</td>
<td>88.29</td>
<td>87.92</td>
<td>91</td>
</tr>
</tbody>
</table>

[33,34].

Legitimate precision is the number of genuine messages classified as genuine that are indeed genuine, whereas legitimate recall refers to the proportion of correctly classified genuine messages to the number of messages originally categorised as genuine. The following counts are defined below:

- $n_{SS}$: Defines the number of spam messages which are accurately classified as spam.
- $n_{SL}$: Represents the number of spam messages that are inaccurately classified as legitimate.
- $n_{LL}$: This is the total number of legitimate messages which are accurately classified as legitimate.
- $n_{LS}$: Represents the number of legitimate messages that the system inaccurately classified as spam.

Below is a list of formulas for each measurement:

 Spam precision (SP) = \( \frac{n_{SS}}{n_{SS} + n_{LS}} \)

 Legitimate precision (LP) = \( \frac{n_{LL}}{n_{LL} + n_{SL}} \)

 Spam recall (SR) = \( \frac{n_{SS}}{n_{SS} + n_{SL}} \)

 Legitimate recall (LR) = \( \frac{n_{SS}}{n_{SS} + n_{LS}} \)

A comprehensive analysis of the results are given on Table 5, showing output on testing set by hidden node count and training epochs. According to the figures presented the trial with 12 hidden nodes and 500 epochs (embolden in Table 5) produced the smallest number of miscalculations, with 35 of the 427 spam messages (8.20%) classified as legitimate ($n_{SL}$) and 32 out of the 400 legitimate messages (8.00%) categorised as spam ($n_{LS}$) for a total of 67 miscalculations.

From a total of 35 misclassified spam messages, 30 of them were short in length with only a few lines which include HTML tags – some were as short as "save up to 27% on fuel" followed by a hyperlink. From the remaining 5 messages; one had many "comments" without comment delimiters resulting in HTML tags which are ignored by some browsers; two were written almost entirely in ASCII escape codes; one had four image files with scrambled English words and sentences and one innovative message used an off-white colour for font typeface to fool the random characters added at the end of email. The observation of the results indicated that 32 legitimate messages were inaccurately classified as spam messages because the messages exhibited characteristics not usually found on personal email. It was noted that twenty-two of these messages were affected by characteristics normally activated by spam; on scrutinising further, 6 came from a known partner who wrote in white typeface on a coloured background because of personal preference, 10 were responses or forwards that quoted html which generated several attributes, 5 were business email from a supplier and lastly one was ranked as low priority from a familiar...
partner. The researcher’s analysis and observation of the remaining 10 email messages were not obvious because; 4 had special characters or vowel-less words in the subject header, 3 included several words with multiple occurrences of strange English features and 3 had a strange number of hyperlinks mainly possibly to links in signature lines.

Conclusion and Future Work

A neural network system is useful and accurate tool for classifying spam messages but to enhance precision performance, supervision is needed. It requires fewer input features to achieve the same results produced by other classifiers such as Naïve Bayesian technique even though we did not carry out comparison in our reporting. We therefore concluded that descriptive qualities of word messages similar to the ones used by human beings can be used accurately to classify spam using a classifier. Further to that, combining keywords and descriptive features may even produce a more accurate classification tool for filtering spam email messages. In future research, we suggest the strategies which combine several techniques in order to yield improved results as the effect of combining strong features from many approaches form a strong defence against spam messages. This is necessary because no single technique can be 100% accurate since spam classifiers have individual strengths and weaknesses. Modification of future could be using a machine learning technique to fine tune input layers and upgrade them to adaptive layers. The researcher’s classifier may not perform better than spam filtering engines from authors whose filters combine at least two classifiers.

REFERENCES

[28] James C, Irena K, Josiah P. A Neural Network Based Approach to Automated Email Classification.


