IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Review Paper on Spam Detection Antiphishing Techniques

Namrata[1*], Suman[2]

[1,2] Dept. of Computer science, DCRUST, Murthal, Sonipat, India

**Corresponding Author: dahiya.namrata@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 09/May/2018, Published: 31/May/2018

Abstract: Internet nowadays is very important share of our day to day life solving many problems on a daily basis. It turns out to be a helping hand to human in so many ways. Among the many advantages of internet, one is sharing of knowledge. Email is that application which is used by all to fulfill the purpose of sharing information. Our email inbox contains some mails which are not required or are unwanted or whose sender is not an authorized person. These types of mails are called the Spam. To detect the spam among the required mails is one kind of hectic task. So many methods have been implemented for this. A spam could be in the form of picture or text which is very harmful for the computer. Thus, Spam has been categorized into the category of problems which occurs frequently and should be handled by the internet user with the help of some better technique. A number of methods have been designed to overcome the issue of spam messages and mail. Already implemented techniques for spam detection have been described in this paper.

Keywords: Email, Heuristics, Phishing, Supervised and unsupervised learning, Spam Filter

1. INTRODUCTION

E-mails are fastest and cheapest technology of information sharing application now a day. People generally read their e-mails on regular basis. Email that contains bogus details tends to annoyed users and consume a lot of space in the mailbox as well. These kinds of mails are known as spam. Spam mails are critical issue that must be handled carefully. E-mail or text messages spam tends to send contrasting, false and impulsive information to large number of internet users [1]. The motive of these spam mails is advertisement of certain products, upgrading and spreading backdoors or malicious programs. People waste a lot of time in reading and then deleting of those spam emails. A spam mail not only irritates the user but it is harmful too. A user can lead to phishing site or malwared site if he follows all the links present in the mail itself [2]. As per the reports of Symantec, 75.9% of email messages all over the internet are spam and harmful [3].

An important issue in finding spam arises from active hostile endeavors to use classification. A person who is sending spam uses a number of techniques that rely on the working model of used antispam algorithm, so that they can escape detection. Handling of spam emails can direct companies to incur high money on spam detection filters [4]. The basic approach used in a spam filter is depicted in the following image [5]:

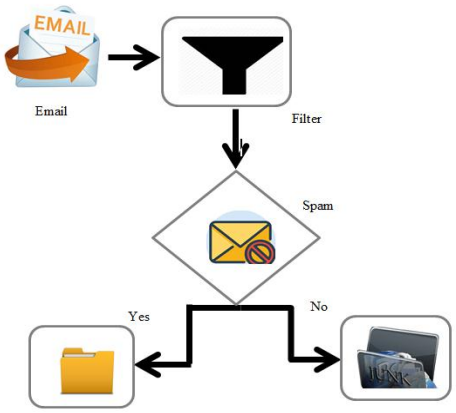

Fig.1 Basic approach used to detect spam

Spam emails are distinguished by following three main features:

- Obscurity [2]: The details of the person who is sending spam is kept secret.
- Bulk mailing [2]: The email is then delivered to a big group of users.
- Unrequested: The email is not asked or demanded by the users.

Spam hasn't constrained itself only to emails but prevails in short message service (SMS), newsgroups, social media sites. Spams are find out and handled through many algorithms, which comes under the category of machine and non-machine learning techniques. In this review paper, we tried to highlight some important mechanisms that were proposed to tackle spams and phishing.

Phishing is the try to gain confidential information such as login Ids, passwords, and trade secrets, often for destructive reasons, by impersonating as a truthful existence on Internet. Phishing is an example of social engineering techniques which are used to cheat users, and exploits shortcomings in current web security. Instead of discovering so many anti-spam techniques, researchers are still not able to diminish the threats of spam completely. Many phishing and forge sites are created and destroyed on daily basis. As per the survey of Anti-Phishing Working Group, a phishing website remains in existence for average of 4 days. It is expired after a certain period of time. While on the other side, security attackers are designing new and efficient methods so that they can overcome the effects of anti-spamming and anti-phishing applications.

Phishing is an upcoming danger which targets to a large number of users. For example, mobile phishing generally attacks the user who is using the services of online banking or who is shopping online or who is socially active on websites. Now a day's phishing is implemented through mobile due to many reasons. It becomes easy for the attackers to fool the users on mobile. Top reasons could be small screen on mobiles, the hardware restrictions, difficulty in switching in certain applications, priorities of the mobile user etc. There are so many phishing detection methods which are mainly categorized into two sections: heuristics-based schemes and blacklist-based schemes [23]. Blacklist methods have a limited work area. They detect the phishing sites only when their names are present in the blacklist and they cannot perform on the sites which exist only for some hours. It could be the case that these small duration sites can gain the personal details of the users before they are being added into the blacklist. Whereas Heuristics-based methods basically rely on the current characteristics which are collected from the URL or the html code of the websites. These phishing detection schemes work online and trust the current online information. However sometimes it happens that the gathered information from the features online is not true and they can easily filter through the heuristics based antiphishing schemes [6].

II. RELATED WORK

Guang Gang Geng et al [7] suggested a approach which is based on the half supervised learning technique. It just combines one extra factor and that is link. It works on labeled data and a large amount of unlabeled data to enhance the performance of the classifier. This algorithm exploits the benefits of two approaches. One is self-training where machine learns from the existed heuristics and another is link learning where machine learns through visiting links present on the sites. Initially, in order to train the classifier, it is feed with small amount of labeled data which already exists in the database. And this unlabeled data is sorted by using trained classifier. Then the classifier presents a rough estimate of the spamicity value. Spamicity value is updated for the unlabeled data through the nearest neighbor's approach. This is done with the help of link learning technique.

$$Ps(x) = p_{spam}(x) / p_{spam}(x) + p_{normal}(x) \quad (1)$$

$$Ls(h) = \Sigma_{v \in Nh} (ps(v)) \times weight(h,v)) / \Sigma_{v \in N(h)} \times weight(h,v) \quad (2)$$

Where v, h are the hosts, weight (h ,v) is the weight of host h ,v ,weight (h,v) € {1,n, log(n)}, where n is number of hyperlinks between h and v. N(h)€ in link (h) or outlink (h). Inlink (h) represent the link set of h, and outlink (h) is the outline set of h.

Algorithm1. Algorithm to detect spam using classifier

1. Weight initialization
2. While i < number of iterations
3. Train labeled training set
4. Detect unlabeled set and compute their spam values.
5. Annotate host level graph with ps values.
6. Compute link learning process.
7. Select largest spam samples in each iteration according to Ls value.
8. End while
9. Train the classifier on labeled train set.
10. Test the samples with trained classifier.

Faraz Ahmed et al [3] proposed a Markov cluster-based algorithm detecting spam data on open system networks. This is an unsupervised machine learning approach which is very fast and reliable. A true Facebook dataset is considered for work which contains both authentic and spam profiles. A defined set of features are taken to describe the interaction among profiles. A weighted graph is drawn to explain the process which helps in a better understanding of same profiles. Profile data is extracted from the Facebook pictures, posts sharing and tags. This is real data. Then the next step is characteristics recognition. This is done through the weightage given to Facebook wall posts, photos sharing and tags. Weighted graph comes in picture here.

R. Malarvizhi et al. in [5] contains discussion on assessment and comparison among a number of spam filtering approaches Technologies such as Ad Boost classifier, MCL, Fisher Robinson algorithm have been explained in detail in this paper. Bayesian technique is discussed in detail and used in implementing spam filter [24]. Freund and Robert Schapiro proposed a classifier named Ada Boost which is a machine learning approach. This algorithm exploits features of confidence-based learning which combines with the concept of active machine learning. Confidence based learning or CBL is the measurement of one's confidence of the correct knowledge. Classifier is then feed with the features that are extracted from the CBL and active learning process and predicts a score which in turn differentiates the mail as spam or non-spam [5]. Only a trained classifier can generate the needed functions which help to detect the spam. With the help of this methodology, whole procedure of training is improved to a better extent.

Loredana Firte et. al. [8] proposed a new but different method to easy the detection process and filters the spam mails. Unlike other application, this technique works offline and collects the data for the training process. K-Nearest neighbor or KNN algorithm is the base algorithm in this paper along with already classified mails for the training procedure. All the mails then sorted out with the help of trained classifier and KNN algorithm. Various mails are taken from the inbox of the account. All these mails are analyzed carefully. Then the characteristics are taken and stored in the database such as the size of the mail, recipients address, number of replies, number of attached files in the mail etc. After all this feature extraction process, resampling is done and F-measure is calculated and the outcome is evaluated.

A different method for spam detection is proposed by M. Basavaraju et.al [9]. Text clustering and vector space model are used for spam detection. Spam and non-spam mails can easily be distinguished with this technique. The technique discussed in this paper takes advantage of the fact that there is a gap in the attributes of an email. A new unit of features is described in this paper. This is called Word. On the basis of occurrence or non-occurrence of the words, values or weightage is assigned to specific features. BIRCH (Balanced Iterative Reducing and Clustering using Hierarchies) along with K-Nearest neighbor is used for the classification of data. Porter's algorithm is also used for pre-processing of noisy data. Now vector space model comes into the scene. Vocabulary is developed through VCM and then data clustering is completed. Correctness of the result is evaluated in the last.

Siddu et. al. [10] suggested a model through that can detect the phishing in the web pages. Content and link spam detection method has been discussed in this paper. Unsupervised machine learning is used here to detect the web spam. As mentioned earlier, there are two sections for detection. They are Content and Link. These modules combine and search for the facts which are somehow related to one another in the target Uniform resource locator. Both these modules again splits into five sub modules which works together to return the spamcity value which is evaluated against the pre-calculated threshold value calculated by statistical means.

Mohammed Mikki et. al. [2] suggested a better performed spam detection method. This method combines two algorithms to find out the spam mails. They are DBSCAN (Density based spatial clustering of applications with noise) clustering algorithm and a new improved digest algorithm. Instead of features collection, digest of emails has been collected and stored. Then, clustering of data is achieved through DBSCAN algorithm. Minimum number of points that can generate a cluster is calculated by DBSCAN algorithm.

Vandana et. al. [4] proposed a method which can detect the spam messages hidden in the images. Discrete Markov design is made to find all the spam images in a given mail or message. Spams are being differentiated depending on the type of content. Excel files and text files are used for the training process. Removal of stopping and stemming words will lead to characteristics extraction.

Saadat Nazirova [11] presents a plain survey on different types of anti-spamming techniques that are in use and their comparisons are mentioned in detail in the paper.

Longfei Wu e al. [6] suggests a novel approach for defending mobile utilities from the dangerous phishing invasion, web pages. It is a lightweight anti-phishing technique for mobile tools. It has the capability to protect the mobile webpages, data, and applications against the mobile phishing attacks done in order to steal the private information. Logically, it is based on the principle of identity extraction in which a full page or important portion of the page is captured and saved in one screenshot [22]. After taking the screenshot, it is converted into the text file which can be used to get the declared uniqueness. Real self of the mobile page can be extracted through the SLD. If the system finds any difference in the two identities which were obtained earlier then it produces a warning which will alert the user to take appropriate action. Optical character recognition method is used to obtain text from the snapshot of a login page and it achieves higher efficiency on the mobile devices. Varieties of mobifish technique are Webfish , Appfish , and Accountfish .

Jae Woong Joo et al. [12] suggests S- Detector Smishing security model that uses the concept of Naive Bayesian

classifier which is used as a counter attack against the phishing attack done on the mobile text messages. It analyzes two types of data, text message content and URL. S-Detector comprises of SMS monitor, SMS analyzer, SMS determinant, and a database. There are many types of safety concerns in mobiles which should be taken care of. These issues could arise from the applications installed, web pages surfed or from the network.

Bottazzi et. al. [13] described MP-Shied design for finding out the malicious mails or the corrupt links. The whole design comprises of modules which are equally responsible for the phishing detection. They are blacklist, machine learning oriented device and watchdog. It works closely with the Google and helps it to find harmful URLs.

Zhang et al. [14] suggested an application which works online and produces the result at that moment. It inspects the URLs that are being asked in real time and will find out some malicious URLs from the features like characters, domain and path of the address. Device can detect the suspicious activity through statistical machine learning.

Foozy et. al. [15] suggested a classification approach required in detecting spam in mobiles. There are numerous ways through which a mobile can be attacked. Phishing can be observed through some application, web, Bluetooth, SMS etc. The author also mentions other technologies for antiphishing and produces a comparison between them.

Jiayi et al. [16] explained security concerns and attacks in the Android and proposed methods to overcome the loopholes in the security. There are variety of threats that are discussed in the paper such as loss of mobile, unauthorized reach to data present in mobile, harmful code or phishing. The author reaches out to each and every threat and explained the requirements in detail. That's why it is very beneficial for the user to counter act against each and every attack. There is one application which provides security against the SMS phishing. It is called the Smishing block app. It reduces the harmful effects of the phishing attacks done in order to gain some private information from the SMS. It also enables the users to handle their device securely against any type of attack. This application blocks all the SMS which have ill purpose of stealing the information.

Chaitrali Amrutkar et al. [17] suggested a speedy and trustworthy technique to handle all the phishing attacks in the mobiles. It works offline or we can say statically. It extracts the static characteristics of the mobile pages from the Uniform resource locator, HTML, strings etc. Then these features are fed to the machine to differentiate between trustworthy pages and the corrupt pages.

In Nour Abura et al. [18] suggested a method to overcome the phishing attack in the Android system. A trojan virus is deliberately installed in the mobile devices which activates the phishing attack through the old applications which were previously installed. Trojan procedure then makes fool of the user and make him to enter his personal details through pop up and user falls into this trap.

In [19] the researchers implemented an anti-phishing technique that is based on the single sign on design QR code. Single sign on process is quite easy to understand. It relieves the user from having several usernames and passwords which can lead to unwanted leak of information. User can sign in to all the websites through a single username and single password. This is much simpler to handle instead of having more number of usernames and passwords. This could only be possible through QR technique. Two modules are present in this model i.e. first module works at operating system level and second module runs at secure socket layer. The trojan attack technique comprises of five major parts. Each part has some major role to play. These provide a security to the attack so that the user cannot realize that there is some attack happening in the mobile phones. This attack keeps an eye on the applications which are being used by the users currently. There are two modules present the whole procedure. They are User registration phase and user verification phase. User gets a hidden or private key which gets utilized later in verification module.

Asmeeta Mali performed an experiment," Spam Detection using Bayesian with Pattern Discovery". In the proposed approach, author creates patterns from data set collected through any legitimate source and she used these patterns by updating them for finding spam. Bayesian classifier and effective pattern Discovery techniques are used to detect spam mails from the email dataset with great accuracy [21].

Table 1: Summary of significant mobile SMS spam detection methods

S.No	Reference	Proposed approach	Source of Dataset	Results Comparison	Remarks
1	Adrian[25]	Challenge response based (Turing test)	Not disclosed	Humans	Performed with accuracy between 94% and 100%
2	Joe and shim[28]	SVM	Around 200 non spam messages and 100 spam messages used for the training purpose.80 spam and same number of non-spam messages were used for the	No evaluation	Optimum efficiency having a feature vector value of 150, a constant value around 20.

			testing.		
3	Sohn et al.[30]	Stylistic content	Real messages from Kore having both spam and non-spam texts.	Bayesian	The content-based technique works efficiently than Bayesian method.
4	Cao et al.[26]	Ontology	Not available	No evaluation	The ontology predicts high quality in detecting phishing attacks.
5	Vural and Venter[29]	Artificial immune systems (AIS)	Real world SMS text messages	AIS, Threshold and AIS, Affinity	This is proved that the botnet detection system correctly filters spam up to 86% with threshold.
6	Yadav et al.[27]	SMS Assassin and Bayes	Real world SMS text messages	Bayesian learning and SVM	97% efficiency in messages detection accuracy.
7	Coskun and Giura[31]	Network based online detection technique	Comments from the you tube	Bloom filter	In order to achieve high detection rates, there is no need to use costly bloom filters.
8	Rafique et al.[32]	SLAVE	5000 real world SMS and grumble text website	Naive Bayes, RIPPER, SVM, UCS	The SLAVE achieves a detection correctness of over 93%.
9	Skudlark[35]	Content based	Mobile terminating (MT) , International Mobile equipment identity (IMEI)	No evaluation	A view into content classification of spam characteristics based on geological position.
10	Chen et al. [34]	TruSystem	NUS SMS Corpus	Not mentioned	Quite effective in case of enhancing efficiency.
11	Almeida et al. [20]	Text Processing Approach(TPA)	SMS spam collection which is a public data comprises of 5574 SMS	Bagging of decision Trees, SVM, KNN, Markov Compression, Prediction by Partial match and Probabilistic Suffix Trees Compression.	For the Wilcoxon Signed ranks Test, the null hypothesis is rejected and with high confidence value.

III. CONCLUSION

Phishing is posing an immense threat to internet and with advancements in tools and techniques attackers are constantly growing their skills in discovering new ways of carrying out phishing. We have studied so many papers in above section where we realized that there are numerous technologies available around us through we can reduce the harmful effects of the phishing but every technique is not complete in itself that can guarantee a perfect robust solution against phishing and anti-spamming. Attacker is always takes the advantage of user's trust on a content provider or a legal site and continuously growth of social media facilitate attackers in multiple ways. The techniques which are described in this paper mainly exploit the concept of the feature engineering.

REFERENCES

[1] Junod .J, "Serves to Spam: Drop Dead", Computer and Security Elsevier, Vol.16, 1997

[2] Alaa H. Ahmed and Mohammed Mikki, "Improved Spam Detection using DBSCAN and Advanced Digest Algorithm", International Journal of Computer Applications, Vol. 6 May 2013.

[3] Faraz Ahmed and Muhammad Abulaish, "An MCL Based Approach for Spam Profile Detection Social Network", IEEE 11th International Conference on Trust, Security and Privacy.

[4] J. Vandana and Nidhi Sood, "Spam Detection System Using Hidden Markov Model", International Journal of Advanced Research in Computer Science and Software Engineering, Volume-3,Issue-7, July-2013

[5] R.Malarvizhi and K.Saraswathi, "Content – Based Spam Filtering and Detection Algorithms-An Efficient Analysis and Comparison", International Journal of Engineering Trends and Technology, Vol.4,Issue 9,Septmber 2013

[6] LongfeiWu, Xiaojiang Du, Jie Wu. "Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY , AUGUST 2016.

[7] Guang-Gang Geng, Qiu-Dan Li and Xin-Chang Zhang, "Link Based Small Sample Learning for Web Spam Detection", ACM, April 2009

[8] Loredana Firte, Camelia Lemnaru and Rodica Potolea, "Spam Detection Filter Using KNN Algorithm and Resampling", IEEE Conference, 2010

[9] M.Basavaraju and Dr.R.Prahakar, "A Novel Method of Spam Mail Detection using Text Based Clustering Approach",

International journal of Computer Applications, Volume-5, August 2010

[10] Siddu p.Algur and Neha tarannumPendari, "Hybrid Spamicity Approach to web Spam Detection", IEEE Conference on Pattern Recognition, Informatics and Medical Engineering, March 2012

[11] Saadat Nazirova, "Survey on Spam Filtering Techniques", Communication and Network, August 2011

[12] Jae Woong Joo , Seo Yeon Moon, Saurabh Singh, Jong Hyuk Park. "S-Detector: an enhanced security model f for detecting Smishing attack for mobile computing" ,Springer 2017.

[13] Bottazzi, G., Casalicchio, E., Cingolani, D., Marturana, F., & Piu, M. (2015). MP-Shield: A framework for phishing detection in mobile devices. In 2015 IEEE International Conference on Computer and Information Technology.

[14] Zhang, J., & Wang, Y. (2012). A real-time automatic detection of phishing URLs. In: 2012 2nd International Conference on Computer Science and Network Technology (ICCSNT), IEEE (pp. 1212–1216).

[15] Foozy, C. F. M., Ahmad, R., & Abdollah, M. F. (2013). Phishing detection taxonomy for mobile device. International Journal of Computer Science Issues (IJCSI), 10(1), 338–344.

[16] Jiayi, M., Cui, A., & Rao, J. (2013). Android mobile security– threats and protection. In International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013) (pp. 683-686). Atlantis Press, Paris

[17] Chaitrali Amrutkar, Young Seuk Kim, Patrick Traynor. "Detecting Mobile Malicious Webpages in Real Time", IEEE Transactions on mobile computing, 2017.

[18] Abura'ed, Nour, et al. "Mobile phishing attack for Android platform." Innovations in Information Technology (INNOVATIONS), 2014 10th International Conference on. IEEE, 2014.

[19] Mukhopadhyay, Syamantak, and David Argles. "An Anti-Phishing mechanism for single sign-on based on QR-code." Information Society (i-Society), 2011 International Conference on. IEEE, 2011.

[20] T. A. Almeida, T. P. Silva, I. Santos, and J. M. G. Hidalgo, ''Text normalization and semantic indexing to enhance instant messaging and SMS spam filtering,'' Knowl.-Based Syst., vol. 108, pp. 25–32, Sep. 2016.

[21] Asmeeta Mali, "Spam Detection Using Baysian with Pattren Discovery", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-3, July 2013.

[22] T.-J. Liu, W.-L. Tsao and C.-L. Lee, "A High Performance Image-Spam Filtering System", 19th International Symposium on distributed Computing and Application to Business, Engineering and Science, August 2010

[23] Ann Nossier, khaled kagati, and Islam Taj-Eddin, "Intelligent Word- Based Spam Filter Detection Using Multi Neural Networks", International Journal of Computer Science Issues, Vol 10, Issues 2, No 1, March 2013 ISSN(Print): 1694 -0814|ISSN(Online): 1664- 0784

[24] Geerthik. S and Anish .T.P, "Filtering Spam: Current Trends and Techniques", International Journal of Mechatronics, Electrical and Computer Technology Vol. 3(8), Jul, 2013, pp 208-223, ISSN: 2305-0543 © Austrian E-Journals of Universal Scientific Organization

[25] A. M. Adrian, ''A challenge response system for filtering automated SMS spam,'' M.S. thesis, Dept. Comput. Sci. Inf. Eng., Nat. Taiwan Univ. Sci. Technol., Taipei, Taiwan, 2010.

[26] L. Cao, G. Nie, and P. Liu, ''Ontology-based spam detection filtering system,'' in Proc. Int. Conf. Bus. Manage. Electron. Inf. (BMEI), May 2011, pp. 282–284.

[27] K. Yadav, P. Kumaraguru, A. Goyal, A. Gupta, and V. Naik, ''SMSAssas- sin: Crowdsourcing driven mobile-based system for SMS spam filtering,'' in Proc. 12th Workshop Mobile Comput. Syst. Appl., 2011, pp. 1–6.

[28] I. Joe and H. Shim, ''An SMS spam filtering system using support vector machine,'' in Future Generation Information Technology. Berlin, Germany: Springer, 2010, pp. 577–584.

[29] I. Vural and H. Venter, ''Detecting mobile spam botnets using artificial immune systems,'' in Advances in Digital Forensics VII. Springer, 2011, pp. 183–192.

[30] D.-N. Sohn, J.-T. Lee, S.-W. Lee, J.-H. Shin, and H.-C. Rim, ''Korean mobile spam filtering system considering characteristics of text messages,'' J. Korea Acad.-Ind. Cooper. Soc., vol. 11, no. 7, pp. 2595–2602, 2010.

[31] B. Coskun and P. Giura, ''Mitigating SMS spam by online detection of repetitive near-duplicate messages,'' in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp. 999–1004.

[32] M.Z.Rafique,N.Alrayes,andM.K.Khan,''Applicationofevolut ionary algorithms in detecting SMS spam at access layer,'' in Proc. 13th Annu. Conf. Genet. Evol. Comput., 2011, pp. 1787–1794.

[33] Gupta, S., & Sanghwan, S. (2015). Load balancing in cloud computing: A review. International Journal of Science, Engineering and Technology Research (IJSETR), 4(6).

[34] B. Reaves, L. Blue, D. Tian, P. Traynor, and K. R. B. Butler, ''Detecting SMS spam in the age of legitimate bulk messaging,'' in Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw., 2016, pp. 165–170.

[35] E.-S. M. El-Alfy and A. A. AlHasan, ''Spam filtering framework for multimodal mobile communication based on dendritic cell algorithm,'' Future Generat. Comput. Syst., vol. 64, pp. 98–107, Nov. 2016.

[36] Gupta, S., & Sanghwan, S. (2015). Load balancing in cloud computing: A review. International Journal of Science, Engineering and Technology Research (IJSETR), 4(6).

