A FRAMEWORK FOR DETECTING SPAM REVIEWS IN ONLINE SOCIALMEDIA

[1]D.Madhumitha Reddy, [2]Dr. R. Jegadeesan [3]V.Tejaswi, [4]T.Sahruday, [5]Dr.M.Sujatha, [6]G.Nikitha
[1,3,5,6]Final year Student Computer science and Engineering, [2,5]Associate Professor-CSE
[1,2,3,4,5]Jyothishmathi Institute of Technology and Science, Karimnagar, India

ABSTRACT:

Today's, a major part of everyone trusts on content in social media like opinions and feedbacks of a topic or a product. The liability that anyone can take off a survey give a brilliant chance to spammers to compose spam surveys about products and services for various interests. Recognizing these spammers and the spam content is a wildly debated issue of research and in spite of the fact that an impressive number of studies have been done as of late toward this end, yet so far the procedures set forth still scarcely distinguish spam reviews, and none of them demonstrate the significance of each extracted feature type. In this investigation, we propose a novel structure, named Net Spam, which uses spam highlights for demonstrating review datasets as heterogeneous information networks to design spam detection method into a classification issue in such networks. Utilizing the significance of spam features help us to acquire better outcomes regarding different metrics on review datasets. The outcomes demonstrate that Net Spam results the existing methods and among four categories of features; including review-behavioral, user-behavioral, review linguistic, user-linguistic, the first type of features performs better than the other categories. The contribution work is when user search query it will display all top-k products as well as recommendation of the product.

KEYWORDS: Social Media, Social Network, Spammer, Spam Review, Fake Review, Heterogeneous Information Networks.

I. INTRODUCTION

Online Social Media gateways assume an influential part in data proliferation which is considered as an imperative hotspot for makers in their publicizing efforts and additionally for clients in choosing items and administrations. In the previous year's [1], individuals depend a ton on the composed audits in their basic leadership procedures, and positive/negative reviews empowering/debilitating them in their choice of items and administrations. Moreover, composed surveys additionally help specialist co-ops to improve the nature of their items and administrations. These reviews in this way have turned into an imperative factor in accomplishment of a business while positive audits can bring benefits for an organization, negative audits can possibly affect validity and cause financial misfortunes[2]. The way that anybody with any personality can leave remarks as spam, gives an enticing chance to spammers to compose counterfeit reviews intended to delude clients' conclusion. These deceptive audits are then duplicated by the sharing capacity of online networking and spread over the web. The reviews written to change clients' impression of how great an item or an administration are considered as spam and are regularly composed in return for cash. The general idea of the proposed structure is to demonstrate a given review dataset as a Heterogeneous Information Network (HIN) [3] and to outline issue of spam recognition into a HIN classification issue. Specifically, here display review dataset as a HIN in which audits are associated through various node types, (for example, highlights and clients). A weighting calculation is then utilized to ascertain each element's significance (or weight).

These weights are used to ascertain the final names for reviews utilizing both unsupervised and directed methodologies.

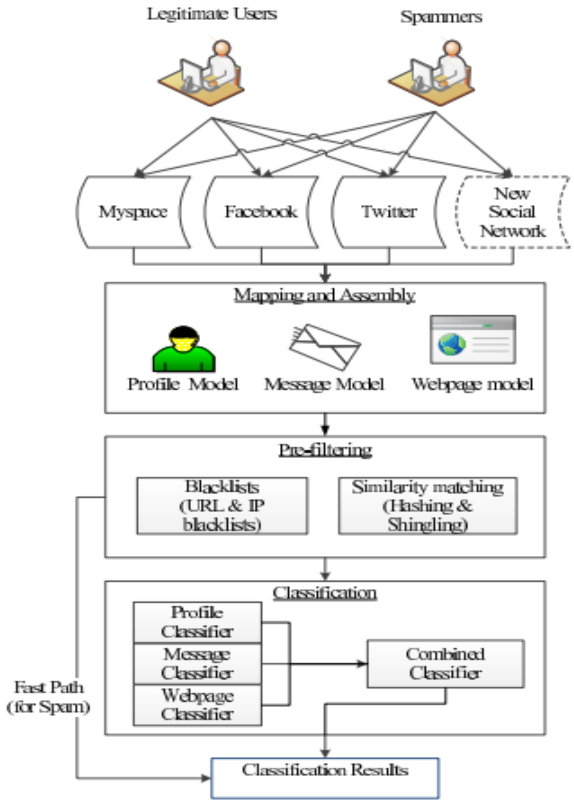


Figure 1: Overview of the spam detection framework

In outline, the fundamental commitments are as per the following: (I) Here propose NetSpam structure that is a novel network -based approach which models reviews organizes as heterogeneous information systems. The classification step utilizes distinctive metapath writes which are creative in the spam identificationarea.(ii)Another spam highlight weighting technique is proposed to determine the relative s ignificance of each component and to show how feasible each of the highlights is to recognize spam from ordinary surveys. As clarified in the unsupervised approach, NetSpam can find highlights significance even without ground truth, and just by depending on metapath definition and in view of qualities ascertained for each survey.[4] (iii) NetSpam enhances the precision contrasted with the state of-the workmanship as far as time many-sided quality, which very depends to the quantity of highlights used to recognize a spam audit; consequently, utilizing highlights with more weights will brought about distinguishing counterfeit surveys less demanding with less time intricacy. The paper's remaining is organized as follows.

The framework for social spam detection can be divided into three major components. Figure 1 shows an overview of the system and we provide a brief explanation for each part here: 1) Mapping and Assembly: Mapping techniques are used to convert a social network specific object into a framework defined standard model for the object (e.g., profile model, message model, or webpage model). If associated objects can be fetched based on this object, it is assembled here; 2) Pre-filtering: Fast-path techniques (e.g., blacklists, hashing, and similarity matching) are used to check incoming objects against known spam objects; 3) Classification: Supervised machine learning techniques are used to classify the incoming object and associated objects. We use a Bayesian technique to combine the classification results into spam or non-spam[5].

More concretely, we make the following contributions:

- Build a social-spam detection framework to filter spam on multiple social networks. We build the three main components of the system and demonstrate the use of the system on data from Twitter, MySpace, and the Web Spam Corpus.
- Demonstrate cross social-corpora classification and measure the feasibility of doing so. Namely, we show that we can build a classifier for a particular model on one social network and apply it to another social network. We then use existing datasets to approximate this technique's accuracy.
- Demonstrate associative classification or classification in which the results depend not only on the object being classified, but also on objects associated with it. e.g., classification of a message object takes into account classification outcomes of the associated webpage objects that may be linked inside the message. We also measure the feasibility of this technique[6].

II. RELATED WORK

In authors going for giving a proficient and compelling strategy to recognize review spammers by consolidating social relations in view of two suspicions that individuals will probably consider reviews from those associated with them as reliable, and review spammers are less inclined to keep up a substantial relationship coordinate with ordinary clients. The commitments of this are twofold:
(1) We expound how social connections can be joined into audit rating forecast and propose a trust-based rating expectation demonstrate utilizing nearness as put stock in weight; and
(2) We outline a trust-mindful identification show in terms of rating fluctuation which iteratively ascertains client particular general dependability scores as the marker for spamicity. Since not every single online survey are honest and reliable, it is vital to create strategies for recognizing audit spam. By extricating significant highlights from the content utilizing Natural Language Processing (NLP), it is conceivable to lead audit spam discovery utilizing different machine learning procedures used. Moreover, commentator data, aside from the content itself, can be utilized to help in this procedure[7]. In this paper, we overview the unmistakable machine learning systems that have been proposed to take care of the issue of audit spam recognition and the execution of various methodologies for order and discovery of survey spam. In authors propose utilizing unsupervised oddity discovery systems over client conduct to recognize possibly awful conduct from typical conduct. Here presenting a procedure in view of Principal Component Analysis (PCA) that models the conduct of typical clients precisely and distinguishes noteworthy deviations from it as abnormal. It tentatively approved that typical client conduct (e.g., classifications of Facebook pages preferred by a client, rate of like movement, and so forth.) is contained inside a low-dimensional subspace agreeable to the PCA strategy. By utilizing the perplexing conditions among audits, clients and IP addresses, in[8] authors initially proposed an aggregate arrangement calculation called Multi-wrote Heterogeneous Collective Classification (MHCC) and afterward extend it to Collective Positive and Unlabeled learning (CPU). Results demonstrate that the proposed models can particularly enhance the F1 scores of solid baselines in both PU and non-PU learning settings. Since the models just utilize dialect free highlights, they can be effectively summed up to different dialects. In [9] authors expect to distinguish clients creating spam audits or review spammers. It recognized a few trademark practices of review spammers and model these practices to identify the spammers. Specifically, try to display the accompanying practices. To start with, spammers may target particular items or item bunches keeping in mind the end goal to expand their effect. Second, they tend to go amiss from alternate analysts in their appraisals of items. Here propose scoring techniques to quantify the level of spam for every commentator and apply them on an Amazon survey

dataset. At that point select a subset of exceedingly suspicious analysts for encourage examination by the client evaluators with the assistance of an online spammer assessment programming uncommonly created for client assessment tests. In [10] authors proposed a novel idea of a heterogeneous review chart to catch the connections among commentators, reviews and stores that the analysts have checked on. Here investigate how communications between hubs in this diagram can uncover the reason for spam and propose an iterative model to distinguish suspicious commentators. This is the first run through such unpredictable connections have been distinguished for survey spam location. It additionally builds up a viable calculation strategy to measure the trustiness of analysts, the genuineness of audits, and the dependability of stores. Unique in relation to existing methodologies, it didn't utilize survey content data. So the model is along these lines integral to existing methodologies and ready to discover more troublesome and unpretentious spamming exercises, which are settled upon by human judges after they assess our outcomes. In [11] authors build up a deliberate technique to consolidation, analyze, and assess surveys from different facilitating locales. It centered around lodging surveys and utilize in excess of 15 million audits from in excess of 3.5 million clients spreading over three noticeable travel destinations. This work comprises of three pushes: (a) create novel highlights equipped for recognizing cross-site disparities adequately, (b) direct seemingly the principal broad investigation of cross-site varieties utilizing genuine information and build up a lodging character coordinating strategy with 93% precision, (c) present the True View score, as a proof of idea that cross-site examination can better advise the end client. This work is an early exertion that investigates the focal points and the difficulties in utilizing numerous auditing destinations towards more educated basic leadership. In [8] authors adopt an alternate strategy, which abuses the burstiness idea of reviews to distinguish review spammers. Blasts of audits can be either because of sudden prominence of items or spam assaults. Commentators and surveys showing up in a burst are frequently related as in spammers tend to work with different spammers and honest to goodness analysts has a tendency to seem together with other honest to goodness commentators. This prepares for us to manufacture a system of commentators showing up in various bursts. Then display analysts and their co occurrence in blasts as a Markov Random Field (MRF), and utilize the Loopy Belief Propagation (LBP) strategy to deduce whether a commentator is a spammer or not in the chart. It likewise proposed a few highlights and utilize include actuated message going in the LBP structure for arrange surmising. Here further propose a novel assessment strategy to assess the distinguished spammers naturally utilizing administered grouping of their audits. Furthermore, utilize space specialists to play out a human assessment of the recognized spammers and non-spammers. In [12], exploration is a stage forward in enhancing the precision of recognizing abnormality in an information chart speaking to availability between individuals in an online interpersonal organization. The proposed mixture strategies depend on fluffy machine learning methods using distinctive sorts of auxiliary information highlights. The techniques are exhibited inside a multi-layered structure which gives the full prerequisites expected to discovering irregularities in information charts created from online interpersonal organizations, including information demonstrating and investigation, marking, and assessment. In [13] authors misuse machine learning techniques to recognize survey spam. Around the end, physically fabricate a spam accumulation from crept audits. At first dissect the impact of different highlights in spam distinguishing proof. It likewise watched that the review spammer reliably composes spam. This gives another view to recognize audit spam: it can distinguish if the creator of the survey is spammer. In [14] authors proposed another comprehensive approach called SPEAGLE that uses pieces of information from all metadata (content, timestamp, rating) and in addition social information (system) tackle them all in all under a *unified* structure to spot suspicious clients and surveys, and in addition items focused by spam. In addition, our technique can effectively and flawlessly incorporate semi-

supervision, i.e., a (little) arrangement of marks if accessible, without requiring any preparation or changes in its hidden calculation.

III.SOCIAL-SPAM DETECTION FRAMEWORK

We present the framework for social spam detection in this section. An overview of the framework is shown in Figure 1 and we present the three main parts in the following subsections.

3.1 Mapping and Assembly

We need to create a standard model for the objects within the social network to build a framework that is social network agnostic. We define an object model as a schema that contains the object's most common attributes across social networks. Once a model is defined, we need to map incoming objects from the social networking into objects of the model. We discuss both these steps in more detail below.

3.1.1 Models

Our framework defines three models representing the most important objects in social networks, namely: profile model, message model, and web page model. We omit other models, as they are not required to demonstrate the feasibility of the framework. The profile model we defined has 74 attributes and is derived from the Google Open Social Person API [13]. The attributes we selected cover attributes most commonly used in user profiles across websites like Facebook, MySpace, Twitter, and Flickr. The message model we defined has 15 attributes based on common attributes used in messages – such as "To", "From", "Timestamp", "Subject", and "Content". We also include in the message model a few attributes which would be common for a social-network to have and also found in e-mail messages, e.g., "Sender-IP", and other header attributes. The web page model we defined has attributes based on common HTTP session header information (based on work done by Steve et al. [29]) and content. For example, "Connection", "Content-length", "Server" and "Status" et al. are common features in HTTP session header. For the content of web pages, we extracted visible text (non-HTML tags) from them and focused on text classification. A model is akin to a class, and an object is an instance of the model (or class). All models are stored in XML, so they are extensible and can be modified easily.

3.1.2 Mapping

Mapping transforms incoming social network objects into the respective object model in the framework. This mapping is mostly done automatically by providing to the framework a list of incoming attributes and their attributes in the respective model. These are specified in an XML file due to easy updatability and simplicity. Name mappings are the simplest to handle and type mappings are also straight-forward except in illegal cases, which we disallow (e.g., "Date" to "Categorical"). For some data types such as categorical type, we need to specify the mapping for each value in the domain of the data type. The handling of semantic mapping is done by manual code written within a special XML tag to perform the necessary conversion. An example of name mappings is shown in Table 1 (shown in table format for simplicity)[14].

3.1.3 Assembly

Assembly is the process of probing each model object for associated objects and then subsequently fetching those model objects. For example, if we are dealing with a message object and the content contains URLs, we fetch the web pages associated with those URLs and create web page objects which are then assembled together with the message object. This additional information is often critical for spam detection as it can provide a rich source of information for the further stages.

3.2 Pre-filtering

In order to reduce classification cost, we adopt fast-path techniques to quickly filter out previous classified or similar spam in incoming social network objects. Some of these techniques involve:

- Blacklists: lists of entries, such as URL, DNS, and IP address, which are to be immediately rejected. Entries are added to these lists due to prior spamming or bad behavior, and thus it is expected that objects which contain such entities should be rejected.
- Similarity matching: Hashing and shingling can be used to quickly calculate similarity against previous spammy entries. The number of previous spammy entries an object is checked against can be limited in order to avoid high lookup costs. These techniques may have shortcomings due to their lagtime in detecting new spam, although their significantly improve time taken to classify an object as spam or non-spam.

3.3 Classification

We build one classifier for each model and use over 40 different types of supervised machine learning classifiers, including standard algorithms such as Naive Bayes [13], Support Vector Machine (SVM) [9] and Logit Boost [6, 10]. Incoming objects to be classified can have associated objects which will be retrieved in the Assembly stage (see Section 3.1.3). For instance, a profile is passed to the profile classifier for classification followed by associated messages being passed to message classifier to do the classification. If the message object contains a URL (such as a Tweet), then the associated object will be a web page object which will be passed to the web page classifier. This process is illustrated in Figure 2. We apply combination strategies to the results of the classifiers after obtaining all results. After the classifier for each model involved return a decision, it is passed on to the combiner. There are four different combination strategies available for us to adapt in our framework: AND strategy, OR strategy, Majority voting strategy, and Bayesian strategy. AND strategy classifies an object as spam if all classifier, for each model, classifies it as spam. OR strategy classifies an object as spam if any classifier, for each model, classifies it as spam. Majority voting strategy classifies the object as spam only when majority of classifier, for each model, classifies it as spam. Bayesian strategy is a slightly modified version of a strategy from previous research

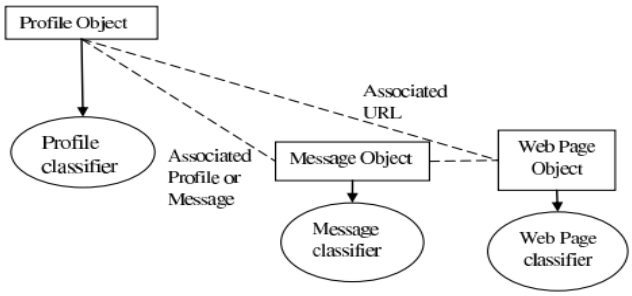


Figure 2: Using associated objects to assist in classification.

on creating an anti-spam filter combination framework for text-and-image emails [15]. We use a subscript i to distinguish different models and t to denote incremental learning cycles at time t. Suppose we receive a object x and ω is the class associated with x, either being spam or legitimate. Then, assuming a hidden variable Z for an event to select one model, a probability for a class ω given x, P (ω|x), can be expressed as a marginal probability of a joint probability of Z and ω.

$$P(\omega|x) = \sum_i P(\omega, Z_i|x) = \sum_i P(\omega|Z_i, x)\, P(Z_i|x)\,.$$

To express each classifier's confidence given x, we use external knowledge P (Zi|x). For instance, if a certain classifier model becomes unavailable, we will set the corresponding P (Zi|x) to be zero. Also if one classifier dominates over other classifiers, one could assign a large probability for the corresponding P (Zi|x). Most data types are supported directly by the classifiers we use, except for the String data type. We use bag of words to change the string into a list boolean attribute (where each boolean attribute represents the presence or absence of a word) after using stemming and removing stop words[15]. Before classification, we represent each object (or model instance) as a attribute vector f of n attributes: hf1, f2, fni. All of attributes are boolean; hence, if fi = 1, the attribute is present in a given object; otherwise, the attribute is absent in a given object.

IV. EXPERIMENTAL RESULTS

In this section, we present the results of the two core parts of our detection framework, namely the cross social-copora classification and associative classification.

4.1 Cross Social-Corpora Classification

During practical usage of our framework, we expect our classifier models to be built using a number of social networks. Incoming objects from the same social networks or other social networks can then be classified using these models. We evaluate an extreme case of this classification, where we build a classifier using one social-network dataset and test the results using another dataset. We first show cross social-corpora classification based on web page model as the web page model can be used in conjunction (via associated objects) with both profile and message models in our framework. We will use the web page model classifier to improve the accuracy of the other models.

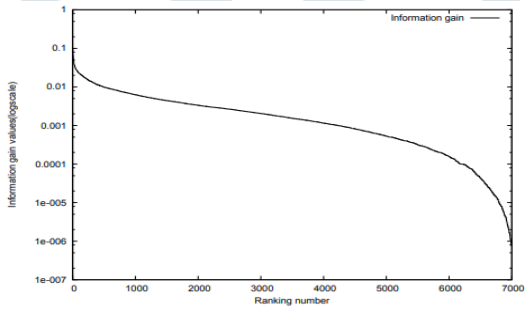


Figure 2: The information gain values of 7,000 features for Web Spam Corpus and Web Base web pages

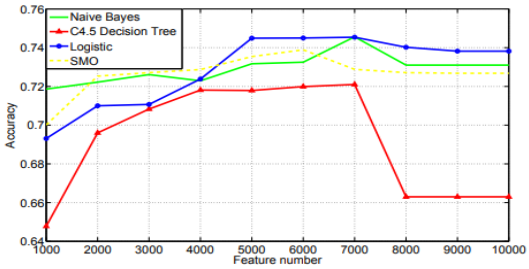
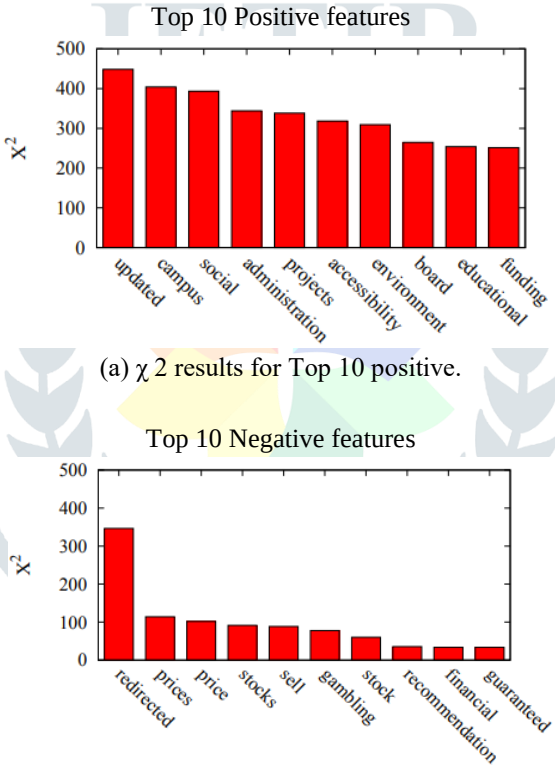


Figure 3: Classifier performance results for Cross corpus learning on web page model

To build (train) the web page model classifier, we use the Webb Spam Corpus (contains spammy pages) and Web Base (contains legitimate pages). We apply the classifier to labeled web pages associated with Tweets from the Twitter dataset. These datasets previously described in Section 4.1 consist of HTTP session headers and content web pages. Previous work [14] used HTTP session headers to detect spam for web pages, but based on our datasets we found that HTTP session headers are not robust to temporal differences in the cross-corpora classification. This is likely due to HTTP session headers containing transitory features that become exiting due to the arms-race between spammers and spam-researchers. We therefore perform classification on content of web pages for cross-corpora and cross-temporal datasets.

Table 1: The results of Na¨ıve Bayes classifier

	Predicted Legitimate	Predicted Spam
True Legitimate	3286	1714
True Spam	830	4170



(a) χ 2 results for Top 10 positive.

Figure 4: Top 10 positive and negative attributes for Webb Spam Corpus and Web Base.

Using a bag of words approach on the content of web pages results in over 50,000 words (after stripping HTML tags, removing stop words, and removing words which occur less than 10 times). As this attribute set is too large to use practically, we explore the impact of feature set size and corpus sample size on the effectiveness of our classifiers. We vary the feature set size between 1,000 and 10,000, based on the features with most information gain, and varied the corpus sample size similarly, with a unified random sample of spam and legitimate instances to generate an equal class distribution (thereby minimizing the class-specific learning biases). The size of total features in datasets influences the size of feature set we choose. After performing this evaluation, we found the majority of our classifiers consistently exhibited their best performance with 7,000 retained features and a corpus sample size of 10,000 instances. Their information gain values are shown in Figure 2. We use these settings for the rest of our experiments involving the web page model.

V. CONCLUSION

To detect spam on multiple social networks, we have implemented a spam detection framework. Through the experiments, we demonstrate that our framework can be applied to multiple social networks due to the spam arms race and is resilient to evolution. We plan to test and evaluate the framework for live feeds from social networks in the future. Furthermore, integrate detection of the behavior of spammers.

REFERENCES

[1] P. Wang, C. Domeniconi, and J. Hu. Cross-domain text classification using wikipedia. IEEE Intelligent Informatics Bulletin, 9(1), 2008.
[2] S. Webb, J. Caverlee, and C. Pu. Introducing the web spam corpus: Using email spam to identify web spam automatically. In Proceedings of the Third Conference on Email and Anti-Spam (CEAS 2006), 2006.
[3] S. Webb, J. Caverlee, and C. Pu. Characterizing web spam using content and http session analysis. In Proceedings of the Fourth Conference on Email and Anti-Spam (CEAS 2007), pages 84–89, August 2007.
[4] S. Webb, J. Caverlee, and C. Pu. Predicting web spam with http session information. In Proceedings of the Seventeenth Conference on Information and Knowledge Management (CIKM 2008), October 2008.
[5] B. Byun, C. Lee, S. Webb, D. Irani, and C. Pu. An anti-spam filter combination framework for text-and-image emails through incremental learning. In Proceedings of the the Sixth Conference on Email and Anti–Spam (CEAS 2009), 2009. [6] X. Carreras and L. Marquez. Boosting trees for anti-spam email filtering. Arxiv preprint, 2001.
[7] J. Caverlee, L. Liu, and S. Webb. Socialtrust: tamper-resilient trust establishment in online communities. In Proceedings of the 8th ACM/IEEE-CS joint conference on Digitial libraries, 2008.
[8] J. Caverlee and S. Webb. A large-scale study of MySpace: Observations and implications for online social networks. Proceedings of the International Conference on Weblogs and Social Media, 8, 2008.
[9] H. Drucker, D. Wu, and V. Vapnik. Support vector machines for spam categorization. Neural Networks, IEEE Transactions on, 10(5):1048–1054, 1999.
[10] J. Friedman, T. Hastie, and R. Tibshirani. Additive logistic regression: a statistical view of boosting. The annals of statistics, 28(2):337–407, 2000.
[11] Gosier and Guadeloupe. Social networks as an attack platform: Facebook case study. In Proceedings of the Eighth International Conference on Networks, 2009.
[12] Z. Gyongyi, H. Garcia-Monlina, and J. Pedersen. Combating web spam with trustrank. In Proceeding of the Thirtieth international conference on Very large data bases, volume 30, 2004.
[13] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. Witten. The WEKA data mining software. ACM SIGKDD Explorations Newsletter, 11(1):10–18, 2009.
[14] J. Hirai, S. Raghavan, H. Garcia-Molina, and A. Paepcke. WebBase: A repository of web pages. Computer Networks, 33(1-6):277–293, 2000.
[15] D. Irani, S. Webb, J. Giffin, and C. Pu. Evolutionary study of phishing. eCrime Researchers Summit, 2008, pages 1–10, 2008.
[16].Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[17]. Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013 "A Recent Approach to Organise Structured Data in Mobile Environment" R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

3. Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

4. Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013)

"Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

5. Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014

"NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD" Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

6. Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014

"SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups" Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

7. Jegadeesan,R.,SankarRam,T.Karpagam March-2014 "Defending wireless network using Randomized Routing process" International Journal of Emerging Research in management and Technology

8.Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

9. Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

10. Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

11. Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

12. Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

13. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., "Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission" International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018

14. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G "Health Monitoring System Using Internet of Things" International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.