



# International Journal Of Engineering Sciences & Management Research

## IMPLEMENTATION PROCESS FOR ONLINE DYNAMIC LEARNING WITH COST SENSITIVITY IN DATA MINING

Mr. Jadhav Bharat S.\*<sup>1</sup>, Dr. Gumaste S.V. \*<sup>2</sup>

\*<sup>1</sup> M.E. student Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, Maharashtra, India

\*<sup>2</sup> Associate Professor And Head Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, Maharashtra, India

**Keywords:** Cost-sensitive classification, online anomaly detection, online learning

### ABSTRACT

As a rule, execution of the classifier is measure utilize accuracy i.e. on the basis of number of inaccurately anticipated occurrences in testing stage. Cost of what is misclassified is definitely not considered for the measuring execution in general methodologies; cost sensitive classification considers expense of the misclassified label. In online learning, prediction model is upgraded is predicted label also, real mark are not similar in every round, yet in real applications each time getting the real class is unrealistic so there come idea of online element learning. Current online element learning frameworks not consider cost of the misclassification. In this article describes online dynamic learning framework which considers the cost of the misclassification. Spiteful uniform resource locator (URL) recognition is one of the applications where getting actual label of the case is impractical and class conveyance of pernicious and ordinary URL is not the same. To evaluate proposed structure actualized the Malicious URL discovery framework utilizing genuine dataset which beats that existing Malicious URL identification framework.

### INTRODUCTION

The work is mainly related to three groups in data mining and machine learning:

#### 1. Cost-sensitive classification:

Cost-sensitive classification considers the varying costs of particular incorrect sorting. A price grid encodes the regulation of requesting cases from one class as a substitute. Let  $C(i, j)$  demonstrate the cost of predicting an occurrence from class  $i$  as class  $j$ . In this reports,  $C(+; -)$  is the cost of misclassifying a positive case as the negative incidence in addition,  $C(-; +)$  is the price of the inverse compartment. Existing confirmation centrality of positive examples is higher than that of negative occasions. Subsequently, the expense of misclassifying a positive occasion surpasses the expense of misclassifying a negative one (i.e.,  $C(+, -) > c(-, +)$ ); creating a right classification generally demonstrates 0 discipline (i.e.,  $C(+; +) = C(-; -) = 0$ ). The cost-sensitive learning process then tries to minimize the amount of high cost slips and the total incorrect sorting price. A cost-sensitive classification technique considers the cost matrix amidst model building and produces a model that has the most decreased cost. Reported works in cost sensitive learning fall into three class.

#### • Weighting the data space:

The circulation of the preparation set is adjusted with respects to misclassification costs, such that the altered dissemination is one-sided towards the expensive classes. Against the ordinary space without considering the expense thing, cost thing, give us a chance to call a data space with area  $X Y C$  as the cost-space, in that  $X$  stand for a the input space,  $Y$  stand for a the yield space and  $C$  is the cost associated with mislabeling that representation. In case there have cases this prospect structure have drawn from a conveyance  $D$  in the cost-space, by then this prospect structure can have another dissemination  $D$  in the normal space that

$$D(X, Y) \wedge (C/E_{(XY C)} \sim D[C]) \sim D(X, Y, C)$$

Where,  $E_{(XY C)} \sim D[C]$  is the expectation of expense qualities. According to the interpretation hypothesis, those perfect blunder rate classifiers for  $D^\wedge$  will be perfect expense minimizes for  $D$ . Henceforth, when this framework overhaul test weights coordinating the expense things, choosing a speculation to minimize the rate of errors under  $D^\wedge$  is identical to picking the theory to minimize the expected cost under  $D$ .

#### • Making a specific classifier learning algorithm cost sensitive:

Case in point, in the context of decision tree instigation, the tree-building structure is used to minimize the misclassification costs. The cost data is utilized to:



## International Journal Of Engineering Sciences & Management Research

- (1) choose the best attribute to split the data [1, 2]; and
- (2) diagram out if a subtree should be pruned [3].

- By use of Bayes risk theory to assign each sample to its lowest risk class:

For example, average decision tree for a binary classification issue dispenses the class label of a leaf node relying upon the larger part class of the training examples that finish the node. A cost-sensitive algorithm appoints the class label to the node that minimizes the classification cost [4, 5].

Procedures in the first gathering, changing over example ward costs into example weights, are overall called cost sensitive adapting by sample weighting [6].

### 2. Online learning :

Online learning which represents is as family of effective also, adaptable machine learning algorithms [7, 8, 9, 10, 11, 12, 13]. Not under any condition like conventional group learning routines that expect all training instances are accessible before the learning assignment, online learning repeatedly updates the predictive models consecutively, which is more proper for web applications where preparing information frequently arrive consecutively. In literature, an assortment of online learning routines have been proposed in machine learning [14]. One astoundingly noteworthy framework is the Perceptron algorithm [15 16], which updates the model by including another case with some consistent weight into the current arrangement of support vectors when the illustration is misclassified. As of late an extensive gauge of new online learning algorithms has been created in light of the standard of greatest edge [8, 17, 18, 10, 19]. One eminent method is the Passive-Aggressive (PA) strategy [10], which updates the arrangement capacity when another illustration is misclassified on the other hand its classification score, does not surpass some predefined edge. In the proposed system PA calculation is apply to explain the online learning task. Not the same as the general PA learning setting which accept class name of each online approaching occurrence will be uncovered, this proposed framework approach queries the class names of just a constrained measure of online approaching occasions through dynamic learning. Moreover to normal online learning frameworks, this planned structure work is moreover nearly identified with another web learning subject in machine realizing, that is, specific examining [20, 21] or label effective learning [22,23], which additionally questions class names of a subset of online got occurrences by creating suitable testing procedures. On the other hand, conventional label effective learning methodologies frequently plan to optimize the error rate (alternately identically the classification precision), which is unmistakably unseemly for malicious URL location assignments. Interestingly, this proposed framework methodology addresses the test of online malicious URL identification by endeavoring to optimize cost-sensitive metrics (weighted entirety of affectability furthermore, specificity or weighted expense) [24]. Finally, this proposed framework work by and large fits in with the class of "online" lively realizing, which differentiates from a colossal gathering of "batch" dynamic learning studies in literature.

### 3. Anomaly Detection:

Anomaly detection is additionally can say that outlier detection on the other hand interest acknowledgment. The Goal of abnormality recognition is to discover surprising information designs which don't identify with normal patterns. Anomaly detection has been contemplated broadly from most recent many of years. In previous task, innovation recognition in semi supervised setting is naturally solved by decreasing to a binary classification issue. An identifier which has coveted false positive rate can be achieved by decrease into Neyman-Pearson classification. Interestingly of inductive technique, semi-supervised novelty detection (SSND) concedes finders that are ideal regardless of the circulation on novelties. In curiosity identification, there is a considerable impacton the hypothetical properties of the choice tenet of unlabeled information.

### 4. Malicious URL Detection:

In the Malicious URL detection this is identified with how to identify noxious URLs consequently or semi-normally, which has been generally inspected in web and data mining groups for quite a long time when all is said in done, which is segment the current work into two classifications: (i) non-machine learning procedures, for instance, blacklisting [25] or principle based; and (ii) machine learning methodologies. The non-machine learning strategies for the most part experience the ill effects of poor generalization to new malicious URLs and concealed spiteful patterns. In the captivating after, this is focus on investigating essential related work utilizing machine learning techniques. In writing, an collection of machine learning plans have been proposed for malicious URL detection, which can be assembled into two characterization: (i) regular batch machine learning systems [26], and (ii) online learning techniques [27]. Most of the existing malicious URL recognition techniques utilize customary regular batch classification methods to learn a classification model (classifier) from a preparing information set of named examples and after that applies the model to classify a test/unremarkable case. With everything, the categorization problem can be formed as either binary classification (normal vs.

## International Journal Of Engineering Sciences & Management Research

abnormal) [26] or multi-class classification (accepting typical examples originate from numerous classes). In literature, a variety of classification systems have been connected, such as Support Vector Machines (SVM) [26], Logistic Regression [26], most extreme entropy Naive Bayes [26], and so forth. Regardless, these calculations commonly require gathering and storing all the preparation occasions ahead of time and manufacture the models in a batch learning fashion, which are both time and memory wasteful and experiences extremely costly retraining taken a toll at whatever point any new preparing data arrives. Not at all like the clump machine learning calculations,, online Learning [27] has been recently proposed as a scalable way to deal with handling expansive scale online noxious URL recognition tasks .In general, online learning systems are more suitable for colossal scale, genuine online web applications in light of the fact that their high proficiency and flexibility. In any case, most of the past online learning algorithms were intended to upgrade the order exactness, normally by expecting the fundamental preparing information dissemination is class balanced unequivocally or certainly. This is unmistakably unseemly for online malicious URL recognition undertakings since this present reality URL information conveyance is regularly profoundly class-imbalanced, i.e., the quantity of malicious URLs is typically fundamentally littler than the quantity of amiable URLs on the WWW. Along these lines, it is imperative to contemplate this issue at the point when outlining a machine learning and data mining algorithm for understanding a functional URL identification task. Finally, all the existing learning methodologies ordinarily need to mark a genuinely substantial measure of preparing cases with a specific end goal to manufacture a sufficiently great grouping model, which is impractical as the naming expense is regularly extravagant in a genuine word application. This consequently propels us to study a brought together learning plan, which not just has the capacity minimize the naming expense, additionally augment the prescient execution with the given measure of marked preparing examples.

### RELATED WORK

T. Yang et al. [28] investigated new test having, "Online Multiple Kernel Classification", which plans to assault a web learning errand by adapting in a kernel based prediction function from a pool of predefined bits. To handle this issue, they propose a novel composition by combining two sorts of online learning algorithms, i.e., the Perception algorithm that takes in a classifier for a given portion, and the Hedge algorithm that merges various kernel classifiers by straight weighting. The reply for an OMKC task is an appropriate determination method to pick an arrangement of kernels from the gathering of predefined kernels for online classifier updates moreover, classifier mix towards desire. To address this key issue, they display two sorts of choice method: a) Deterministic methodology that picks the all kernels, b) Stochastic strategy that individually tests a subset of kernels according to their weights. Especially, they proposed four varieties of OMKC algorithms by executing unmistakable web upgrading and mix framework. Each of these four OMKC calculations has distinctive advantages for different circumstances. To evaluation the observational implementation of the displayed OMKC algorithms, they did expansive examinations a tried with 15 diverse genuine datasets.

- A. All of OMKC algorithm continually achieve better than predictable Perceptron algorithms with an unbiased linear combination of various kernels, essentially perform better than the Perceptron algorithm with the best kernel detected by utilizing approval, and often perform best over a state-of-the-art online MKL algorithm.
- B. For the two differing improvement overhauling structures, the stochastic updating technique has the limit of in a broad sense improving the viability by keeping up at slightest equivalent execution as differentiated and the deterministic strategy
- C. For the two particular mix frameworks, the deterministic combination technique regularly complete great results, until the stochastic combination methodology has the limit of delivering a through and through additional inadequate classifier.

J. Wang et al. [29] proposed the Soft Confidence-Weighted (SCW) learning, one more second-request online learning framework with cutting edge test execution. Not in any way like the current second-arrange algorithms, has SCW accepted all the four features. a) Extensive margin training. b) Adaptive margin. c) Confidence weighting. d) Ability of taking care of nonseparable information. Tentatively, they found the proposed SCW algorithms perform through and through better than the first CW algorithms, and beat the state-of-the-art AROW algorithm for most cases the extent that both accuracy and capability.

S. C. H. Hoi et al. [30] had exhibited a Library for Online Learning Algorithms, which is called as LIBOL. LIBOL is a simple to use open source bundle for internet learning development in addition, study. The present perceptive of LIBOL comprises of a considerable number of web learning calculations for online classification undertakings. LIBOL is even now being upgraded by criticism from functional customers or genuine clients. They would like to make LIBOL a supportive machine learning instrument, and additionally an impeccable learning stage to do online learning examination. A complete target is to make basic learning with tremendous information streams for taking care of the test of huge information investigation.



## International Journal Of Engineering Sciences & Management Research

R. Jin et al. [31] inspected another exploration issue of Online Feature Selection (OFS), which look for to decide a foreordained numeral of features for forecast by an online learning outline. They acquainting OFS calculation with resolution the learning responsibility, and offered hypothetical examination on the misstep bound of the proposed OFS algorithm. They comprehensively investigated their observational execution on both standard UCI datasets. It is comparative pondered the proposed online feature determination framework with a standard state-of-the art trademark selection algorithm for handling real-world applications: picture portrayal in PC vision and microarray quality translation examination in bioinformatics. Empowering outcome display the planned algorithms are really suitable for feature selection assignments of online applications, what's more, basically more capable and adaptable than some best in class trademark choice framework.

R. Jin, S. C. H. Hoi, and P. Zhao [32] displayed a novel "Double Updating" procedure to web learning named as "DUOL". Double Updating Online Learning (DUOL) not simply adjusts the heaviness of one current bolster vector that the most genuinely clashes with the new help vector, additionally updates the largeness of the misclassified delineation. They show that the mix-up headed for an online-grouping errand can be basically decreased by the proposed DUOL algorithms. They have coordinated a wide arrangement of examinations by algorithms with different calculations for both twofold and multiclass online arrangements. Hopeful experimental results shown that the proposed twofold overhauling online learning algorithms dependably outmaneuver the single-overhaul online learning algorithms.

Nicolo Cesa-Bianchi, Gabor Lugosi in [33] talked about the LEPE algorithms. LEPE implies the mark effective perceptron algorithms. This algorithm is utilized for mark effectiveness.

### IMPLEMENTATION DETAILS

#### 1. System Overview:

Primary target of this paper is to add to a framework which will manage the way that every time getting real class of the example is impractical and will consider the expense of the misclassification to upgrade the classifier in the event of endure misfortune. In proposed the online dynamic learning with cost sensitivity (ODLCS) which will primary target of proposed framework, which is expressed previously. The target of directed malicious URL discovery is to manufacture a prescient model that can unequivocally predict if an approaching URL sample is noxious or not. If all else fails, this can be portrayed as a binary classification errand where malicious URL examples are from positive class ("+1") and typical URL occurrences are from negative ("-1"). For an online pernicious URL recognition responsibility, the objective is to make an online learner to incrementally assemble a arrangement model from a gathering of URL preparing information occasions by method for a online learning fashion. In particular, for every one adapting round, the learner first gets another approaching URL event for location; it then applies the classification model to anticipate in case it is malicious then again not; around the end of the adapting round, if reality class name of the sample can be revealed from the earth, the learner will make usage of the checked case to redesign the characterization model at whatever point the order is erroneous generally speaking, it is normal to apply web figuring out how to comprehend online malicious URL detection. In any case, it is unfeasible to explicitly apply a current online learning framework to settle these issues. This is by virtue of a schedule online classification undertaking typically acknowledge the class label of every approaching event will be revealed keeping in mind the end goal to be used to upgrade the classification model toward the end of every learning round. Plainly it is unfathomable or exceedingly rich if the learner queries the class name of every approaching event in an online malicious URL detection assignment. To address this test, in the proposed framework to research a novel system of ODLCS as demonstrated in Figure 1. Generally speaking, the proposed ODLCS system tries to address two key troubles in a systematic and synergic learning philosophy:

- (i) the learner must choose when it ought to query the class label of an approaching URL case; likewise
- (ii) how to update the classifier in the best path where there is another marked URL event.

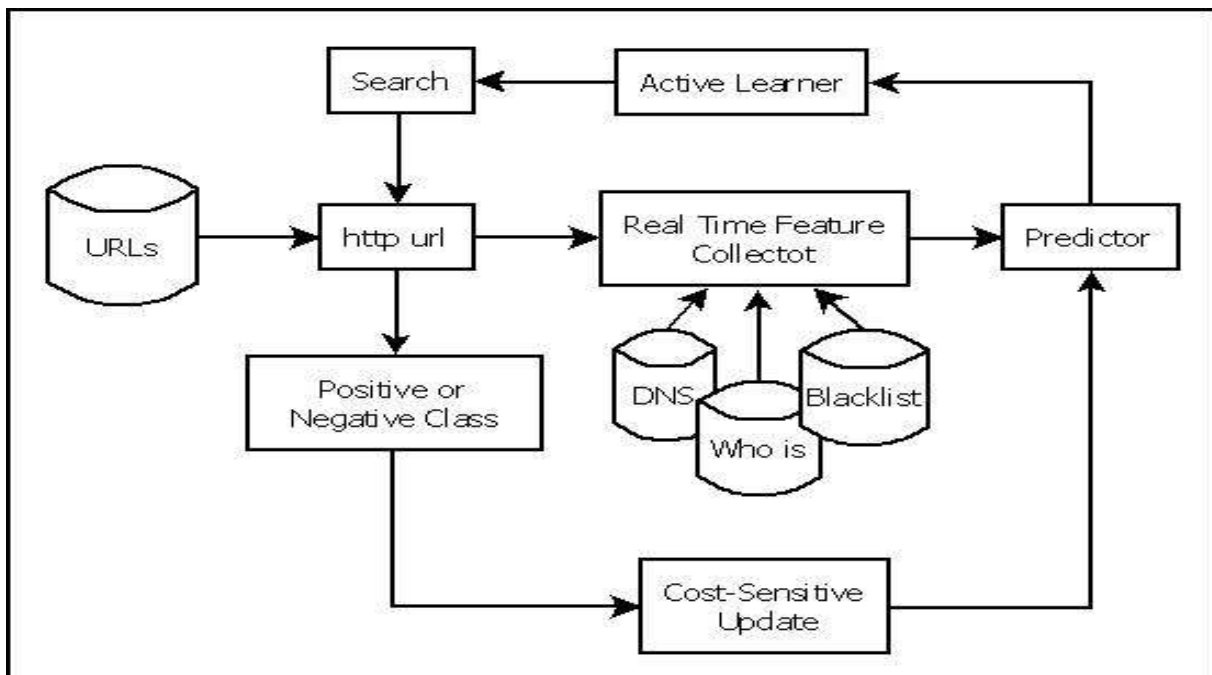


Figure1: System Architecture

**2. Mathematical Model for Proposed Work:**

Sensitivity =  $(T_p - M_p) / T_p$

Specificity =  $(T_n - M_n) / T_n$

Specificity =  $(TM) / T$

Where, M = denote the number of mistakes

$M_p$  = denote the number of false negatives,

$M_n$  = denote the number of false positives

T = to denote the set of indexes of negative examples,

$T_p$  = denote the number of positive examples,

$T_n$  = denote the number of negative examples.

sum of weighted sensitivity and specificity:

- $sum = \eta_p \times sensitivity + \eta_n \times specificity$

Where,  $0 \leq \eta_p, \eta_n \leq 1$  and  $\eta_p + \eta_n = 1$ :

When  $\eta_p = \eta_n = 1/2$

sum is the well-known balanced accuracy.

total cost suffered by the algorithm:

- $cost = c_p \times M_p + c_n \times M_n$

Where,  $M_p$  and  $M_n$  are the number of false negatives and false positives respectively,

$0 \leq c_p, c_n \leq 1$  are the cost parameters for positive and negative classes, respectively

**URL Detection:**

$F_p^b(w) = 1/2 \|w\|_2^2 + C_{-} (t=1)^T l_t(w)$

Where

regularization parameter  $C > 0$ .

loss function  $l_t(w)$ .

**3. Algorithm:**

**A) CSOGD algorithm**

Step 1: INPUT: penalty parameter C, bias parameter  $\rho$  and smooth parameter  $\delta$ .

Step 2: INITIALIZATION:  $w_1 = 0$ .

Step 3: for  $t = 1, \dots, T$  do

Step 4: receive an incoming instance  $x_t \in R^d$ ;

Step 5: predict label  $\hat{y}_t = \text{sign}(p_t)$ , where  $p_t = w_t \cdot x_t$ ;

Step 6: draw a Bernoulli random variable  $Z_t \in \{0, 1\}$  of parameter  $\delta / (\delta + |p_t|)$ ; end

**B) .ODLCS algorithm**

## International Journal Of Engineering Sciences & Management Research

- Step 1: INPUT: penalty parameter, bias parameter, smooths parameter  
 Step 2: INITIALIZATION: classifier as zero  
 Step 3: For every incoming instance  
 Step 4: receiving incoming instance  
 Step 5: predicting label of each instance by using classifier  
 Step 6: draw a Bernoulli random variable of parameter  
 Step 7: if a Bernoulli random variable is 1 and then suffer loss occur in instance then update classifier unless not update  
 Step8: end

#### 4. Experimental Setup:

The system is built using Java framework (version jdk 6) on Windows platform. The Netbeans (version 6.9) is used as a development tool. The system doesn't require any specific hardware to run; any standard machine is capable of running the application.

### RESULTS AND DISCUSSION

#### 1. Dataset:

To examine the performance, in the proposed system test all the algorithms on a large-scale benchmark dataset for malicious URL detection, which can be downloaded from <http://sysnet.ucsd.edu/projects/url/>. The original data set was created in purpose to make it somehow class-balanced. In suggested system to produce a separation by sampling from the original data set to make it close to a more realistic distribution scenario where the number of normal URLs is significantly larger than the number of malicious URLs.

#### 2. Results:

In This experiment will evaluate the performance of the proposed algorithms by varying the ratios of queries for comparing different online malicious URL detection algorithms. Figure 2 and Figure 3 shows the online average sum performance and the online average cost performance under varied query ratios, resp. From the tentative outcome, several observations can be drawn as follows.

Table I. Evaluation of The Malicious URL Detection Performance In Terms Of The Cumulative Sum Measure.

Measures	LEPE	ODLCS
Sum (%)	79.162	92.697
Sensitivity (%)	58.492	88.156
Specificity (%)	99.833	97.237
Accuracy (%)	99.419	97.146

In the following graph System compare the proposed novel class detection method with the existing method. In X axis represent different methods for comparison and Y axis the values.

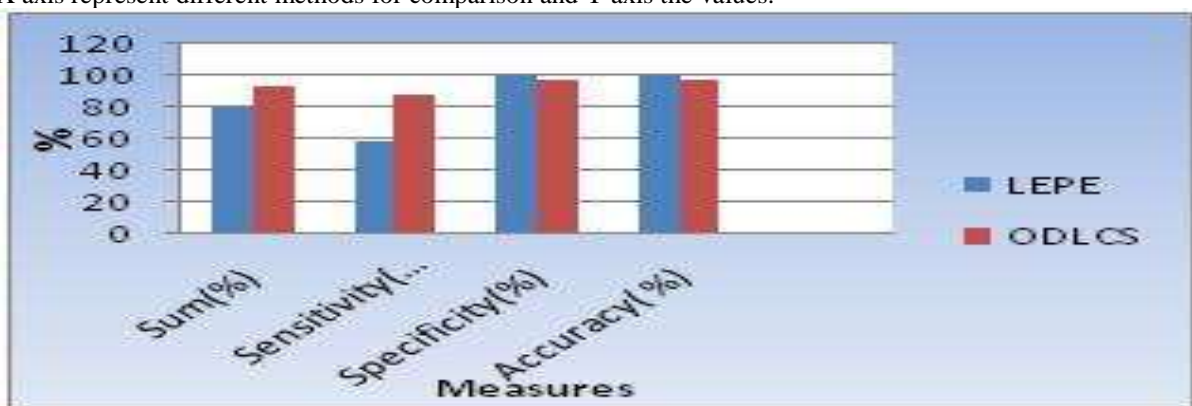


Figure.2: Evaluation of the online cumulative average sum performance with respect to varied ratios

Table II. Evaluation of the Malicious URL Detection Performance.

Measures	LEPE	ODLCS
Sum (%)	57.592	87.742
Sensitivity (%)	99.832	97.285

Specificity (%)	99.41	97.189
-----------------	-------	--------

In the following graph System compare the proposed novel class detection method with the existing method. In X axis represent different methods for comparison and Y axis the values.

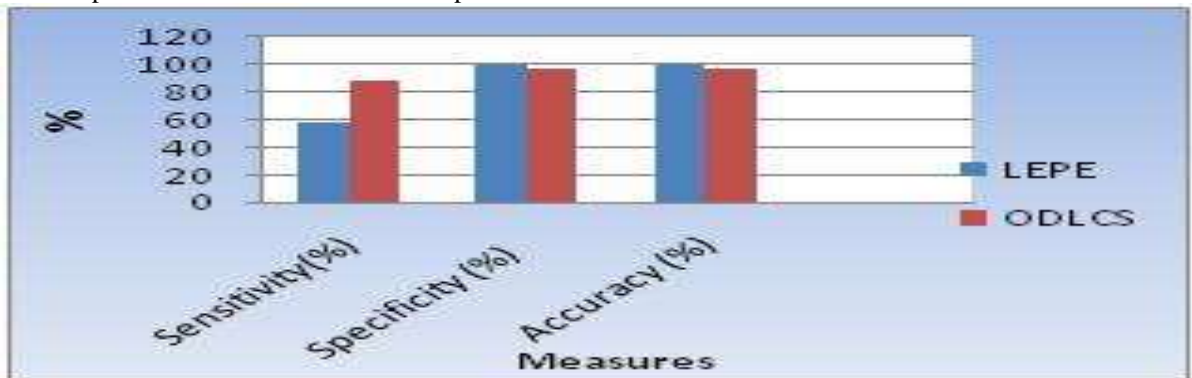


Figure 3: Evaluation of the online cumulative average Cost performance with respect to varied ratios.

## CONCLUSION

In this paper proposed a novel system of Online Dynamic Learning with Cost Sensitivity (ODLCS) to taking care of real-world applications in the classification domain like online malicious URL recognition undertaking. Paper demonstrates the ODLCS algorithms to push cost-sensitive measures and hypothetically analyze the breaking points of the proposed algorithms. in suggested structure result shows:(i) the proposed ODLCS technique has the capacity consider ablyout perform various directed cost-sensitive alternately cost-insensitive online learning algorithms for malicious URL recognition undertakings (ii)the proposed ODLCS algorithms are very proficient and adaptable for web-scale applications.

## REFERENCES

- [1] P. Riddle, R. Segal, O. Etzioni, "Representation design and brute-force induction in a boeing manufacturing domain", *Appl. Artif. Intell.* 8 (1991)125-147.
- [2] C.X. Ling, C. Li, "Decision trees with minimal costs, in: Proceedings of the 21st International Conference on Machine Learning", Banff, Canada, July 2004.
- [3] J. Bradford, C. Kunz, R. Kohavi, C. Brunk, C.E. Brodley, "Pruning decision trees with misclassification costs", in: Proceedings of the Tenth European Conference on Machine Learning (ECML-98), Chemnitz, Germany, April 1998, pp. 131-136.
- [4] B. Zadrozny, C. Elkan, "Learning and making decisions when costs and probabilities are both unknown", in: Proceedings of the Seventh International Conference on Knowledge Discovery and Data Mining, San Francisco, CA, August 2001, pp. 204-213.
- [5] P. Domingos, P. Metacost, "Metacost: a general method for making classifiers cost sensitive, in: Advances in Neural Networks", International Journal of Pattern Recognition and Artificial Intelligence, San Diego, CA, 1999, pp. 155-164.
- [6] N. Abe, B. Zadrozny, J. Langford, "An iterative method for multiclass cost-sensitive learning", in: Proceedings of the tenth ACN SIGKDD International Conference on Knowledge Discovery and Data Mining, Seattle, WA, August 2004, pp. 3
- [7] F. Rosenblatt. "The perceptron: A probabilistic model for information storage and organization in the brain". *Psychological Review*, 65:386-407, 1958
- [8] K. Crammer and Y. Singer. Ultraconservative online algorithms for multiclass problems. *JMLR*, 3:951-991, 2003.
- [9] N. Cesa-Bianchi, A. Conconi, and C. Gentile. "On the generalization ability of on-line learning algorithms". *IEEE Trans. on Inf. Theory*, 50(9):2050-2057, 2004
- [10] K. Crammer, O. Dekel, J. Keshet, S. Shalev-Shwartz, and Y. Singer. "Online passive-aggressive algorithms". *JMLR*, 7:551-585, 2006.
- [11] P. Zhao, S. C. H. Hoi, and R. Jin. "Double updating online learning". *Journal of Machine Learning Research*, 12:1587-1615, 2011
- [12] J. Wang, P. Zhao, and S. C. H. Hoi. "Exact soft confidence-weighted learning". In *ICML*, 2012.



## International Journal OF Engineering Sciences & Management Research

- [13] S. C. H. Hoi, J. Wang, and P. Zhao. "LIBOL: A Library for Online Learning Algorithms." Nanyang Technological University, 2012
- [14] S. Shalev-Shwartz and Y. Singer. "Online learning: theory, algorithms, and applications." In Ph.Dthesis, 2007.
- [15] F. Rosenblatt. "The perceptron: A probabilistic model for information storage and organization in the brain." *Psychological Review*, 65:386-407, 1958
- [16] Y. Freund and R. E. Schapire. "Large margin classification using the perceptron algorithm." *Mach.Learn.*, 37(3):277-296, 1999.
- [17] C. Gentile. "A new approximate maximal margin classification algorithm." *JMLR*, 2:213-242, 2001
- [18] J. Kivinen, A. J. Smola, and R. C. Williamson. "Online learning with kernels." In NIPS, pages 785-792, 2001
- [19] Y. Li and P. M. Long. "The relaxed online maximum margin algorithm." In NIPS, pages 498-504, 1999
- [20] Y. Freund, H. S. Seung, E. Shamir, and N. Tishby. "Selective sampling using the query by committee algorithm." *Mach. Learn.*, 28(2-3):133-168, 1997.
- [21] G. Cavallanti, N. Cesa-Bianchi, and C. Gentile. "Linear classification and selective sampling under low noise conditions." In NIPS 21, pages 249-256, 2008.
- [22] D. Helmbold and S. Panizza. "Some label efficient learning results." In COLT'97, pages 218-230, Nashville, Tennessee, United States, 1997.
- [23] N. Cesa-bianchi, G. Lugosi, and G. Stoltz. "Minimizing regret with label efficient prediction." *IEEE Trans.Inform. Theory*, 51:77-92, 2005.
- [24] J. Wang, P. Zhao, and S. C. H. Hoi. "Cost-sensitive online classification." In ICDM, pages 1140-1145, 2012.
- [25] J. Zhang, P. Porras, and J. Ullrich. "Highly predictive blacklisting." In Proceedings of the 17th conference on Security symposium, SS'08, pages 107-122, Berkeley, CA, USA, 2008. USENIX Association.
- [26] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker. "Beyond blacklists: learning to detect malicious web sites from suspicious urls." In KDD, pages 1245-1254, 2009.
- [27] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker. "Identifying suspicious urls: an application of large-scale online learning." In ICML, page 86, 2009.
- [28] S. C. H. Hoi, R. Jin, P. Zhao, and T. Yang, "Online multiple kernel classification", *Mach. Learn.*, vol. 90, no. 2, pp. 289-316, 2013
- [29] J. Wang, P. Zhao, and S. C. H. Hoi, "Exact soft confidence-weighted learning," in Proc. 29th ICML, Edinburgh, U.K., 2012.
- [30] S. C. H. Hoi, J. Wang, and P. Zhao, "LIBOL: A library for online learning algorithms," *J. Mach. Learn. Res.*, vol. 15, no. 1, pp. 495-499, 2014.
- [31] S. C. H. Hoi, J. Wang, P. Zhao, and R. Jin, "Online feature selection for mining big data," in Proc. 1st ACM Int. Workshop BigMine, Beijing, China, 2012, pp. 93-100.
- [32] Jialei Wang, Peilin Zhao, and Steven C.H. Hoi, Member, IEEE "Cost-Sensitive Online Classification".
- [33] Nicolo Cesa-Bianchi, Gabor Lugosi, "Prediction, Learning, and Games".





## International Journal OF Engineering Sciences & Management Research

### Authors Profile :



**Mr. Bharat S. Jadhav** received the BE degree in Information Technolgy from Pravara Rural Engineering College in 2012. During 2013-2014, he stayed at Late Hon.D.R.Kakade Polytechnic Pimpalwandi as lecturer in Computer Technology Department,.Now he is currently working in Tikona Digital Networks as Network Support Engg. Also he is pursuing Master Of Engineering in Sharadchandra Pawar College of Engineering, Dumbarwadi,Otur, University Of Pune .



**Dr. S.V.Gumaste**, currently working as Professor and Head, Department of Computer Engineering, SPCOE-Dumbarwadi, Otur. Graduated from BLDE Association's College of Engineering, Bijapur, Karnataka University, Dharwar in 1992 and completed Post- graduation in CSE from SGBAU, Amravati in 2007. Completed PhD (CSE) in Engineering & Faculty at SGBAU, Amravati. Has around 22 years of Teaching Experience.