A Survey of Data Driven Methodologies for Mitigating Cyber Attack in Online Environment

Arati Shahapurkar[1], Dr. S.F.Rodd[2]

[1]Asst. Prof.Dept of CSE KLS GOGTE INSTITUTE OTECHNOLOGY,Belgavi, Email:aratibellary7@gmail.com
[2]Prof. Dept of CSE KLS GOGTE INSTITUTE OTECHNOLOGY,Belgavi, Email:Sfroddgit@git.edu

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract— A large number of users use social networking as a platform for sharing their official and personal information. A spammer will utilize these social platforms for their benefit by flooding malicious links, unwanted information and others. In social networking platform, detecting a spammer is a critical and challenging tasks. For the detection and defending of cyber-attacks analysis of social and internet traffic is fundamental job. Automated approaches that use machine learning are replacing traditional approaches for detection of spammers. This revolution has speeded up by the large datasets that takes the help machine-learning models which gives exceptional performance. In data-driven prototype environment, a review on cyber traffic in social networks and Internet is presented by considering the common parameters like correlation, collective indication, similarity. This work also gives an analysis on classification of network applications or network host and Tweets or users by sharing the goals of security. This article also gives a new methodology of research for data-driven cyber security and its application in social network and Internet traffic study.

Keywords—Concept drift, Class Imbalance, Data distribution, Social Networking Spam Detection, Machine Learning.

1. Introduction

Now a day's internet is an essential part of our daily life. In the meantime, information safety is attacked by various methods of cyber-attacks which are very dangerous. Thus, for several researchers network security in social media environment like Twitter has become the crucial point. Commonly four types of attacks are there: DoS (denial of service), probe, U2R (user to root), and R2L (remote to local). The aim of any spam/anomaly is to divide the network traffic into five categories: normal, DoS, probe, U2R and R2L. When an abnormal attack is detected in the traffic, the traffic maintainers will protect the network by taking measures accordingly. Preprocessing and classification are the two common steps used in these studies. Preprocessing method is the important procedure in the detection of fraud and this method is also called as feature selection process. This process can select important features of raw data, which has significant influence on the results. Preprocessing also reduces the data storage size, improves accuracy of the classifier and training efficiency of the model. It works well for the small input-scale algorithms even for the high dimensional data. There are several machine learning procedures used for network traffic classification. Some of them are DTs (decision trees), SVM (support vector machine), KNN (k-nearest neighbor), ANNs (artificial neural networks), GAs (generic algorithms), fuzzy logic, naive Bayesian and a hybrid model for classification traffic. Based on the features selected, performances of traditional classifiers for fraud detection are studied. In addition, it is challenging to adopt these traditional methods to the huge networks, as they generate enormous traffic data in a day. Machine learning classifiers increase the time and cost of calculation as network traffic data is growing continuously and in rapid manner. They also reduce the anomaly detection accuracy, but these are the most important parameters of anomaly or malicious detection system. The safety of the network is ensured when system employs some amount of time to achieve high accuracy.

In recent times many strategies are using machine learning methods like support vector machine, random forest, KNN, J48 etc. for the detection of spams with better accuracy of detection [1], [2], [3], [4], [5], and [6]. But these machine learning based models does not address the problem of "Spam Drift". Therefore the accuracy gets affected adversely with time. In [7], the authors proposed a posting time model and a language model to address the problems of spam drift. However they failed to create spammer accounts, which are generated deceptively by spammers and they are able to find that is user accounts are hacked or not. To address these problems, the authors of [4] designed a methodology in which knowledge is derived from unlabeled tweet and spam tweets are detected. This overcomes the problem spam drift. Better performance is achieved by the Lfun model proposed by the authors of [3] when compared with [1], [2], [3], and [4]. However, achieved accuracy is not that much efficient because of variation in time. The authors of [8] proposed explicit spam drift detection (ESDD) for feature extraction by the computation of six linear statistical feature set and two nonlinear feature set for concept description. The linear features consist of skewness, auto correlation, variance and kurtosis and nonlinear features consists of common information and bicorrelation. These all feature sets are created with dimensions of input to get the concept vector. Next concept vectors are matched at various intervals of time using total variation distances [10], streaming hashing histograms [9], and cosine distance metrics. But high computation overhead is introduced by ESDD model. To address the problem of computation complexity, the authors of [11], [12] proposed a method for detection of anomaly by method

of relative entropy (i.e., K-L divergence) for distance measurement [13], [14]. On the other hand, already present methodologies are not addressing the problems of class imbalance and concept-drift in an online learning environment. Therefore an extensive literature review done for the design of a method for the detection cyber-attack.

The significance of the work:

- This work presented extensive survey of various existing cyber-attack detection methodology for online and social media environment.
- Survey is broadly focused on addressing class imbalance and concept drift issues affecting cyber-attack detection for online environment.
- Presented efficient cyber-attack detection methodology for online and social media environment.

The paper is arranged as follows. In section 2, this paper carried out extensive survey of various existing cyber-attack detection methodologies. In section 3, future issues and challenges involved in designing efficient cyber-attack detection methodologies. In section 4, problem statement and proposed methodology to design efficient cyber-attack detection framework for online/social media environment. Lastly, the paper is concluded with future research direction.

2. Literature Survey

In this section literature review of different existing methodologies for detection of attacks in online environment is given. First the review for unsupervised methods for detection of attacks carried out in online and social media environment. Second the review is conducted on the basis of blacklisting methodologies and Honeypot for attacks detection in online environment. Finally the review is carried on different machine learning methodologies for attacks detection in online and social media platform.

2.1 Unsuperviced learning based attack detection methodologies:

The new features of Social Web, in which users are the information producers, exposed various problems of information quality (IQ). As an example Twitter and Facebook are most common microblogging sites that have real-time messaging system. This feature makes them to become more popular and is appropriate for handling real-time updates and real-time public events. But due to the simple, flexible usage of these sites and no restrictions on the posting of contents, it gives additional difficulty for the issues of IQ. Certainly social spammers publish the social spam contents are of ill-intentioned one and are the maximum common noise that appears in the online social media (OSM) sites. It is grouped in the category of IQ problems. Social spammers publish nonsense contents like viruses, phishing websites with various other topic or contexts, materials containing pornography, malware and mainly advertisement in a systematic and an automated manner with the bad intention. In addition, these spammers exploit the services available, topics that are in trend or APIs to launch their junk contents for periods of short time say a single day. By this they increase their financial profits and spamming behavior is fastened. As an example, these social spammers influence various sets of services provided for launching spam attacks over the Hashtag, Mention services and URLs. For constructing spam tweets detecting models one of the classical method, supervised learning technique is used in literature. It is popularly known that, these methods require annotated dataset in machine learning (ML) field. But annotated dataset is more costly in terms of human resources or/and time required for annotation. Additionally, categorization of social spam models needs continuous adopting methods using new datasets of training to identify the new patterns of the social spammers' behaviors. Therefore having a training dataset which is static in nature for classification is inefficient method. To overcome this problem the authors of [15] proposed a design of an online collective-based spam tweets classification framework, which uses the advantages of unsupervised ML techniques for providing an annotated dataset automatically and periodically. By using this supervised classifying models are updated. This model implements correlation of tweets of social spammers' in a short time periods for the prediction of spamming behavior.

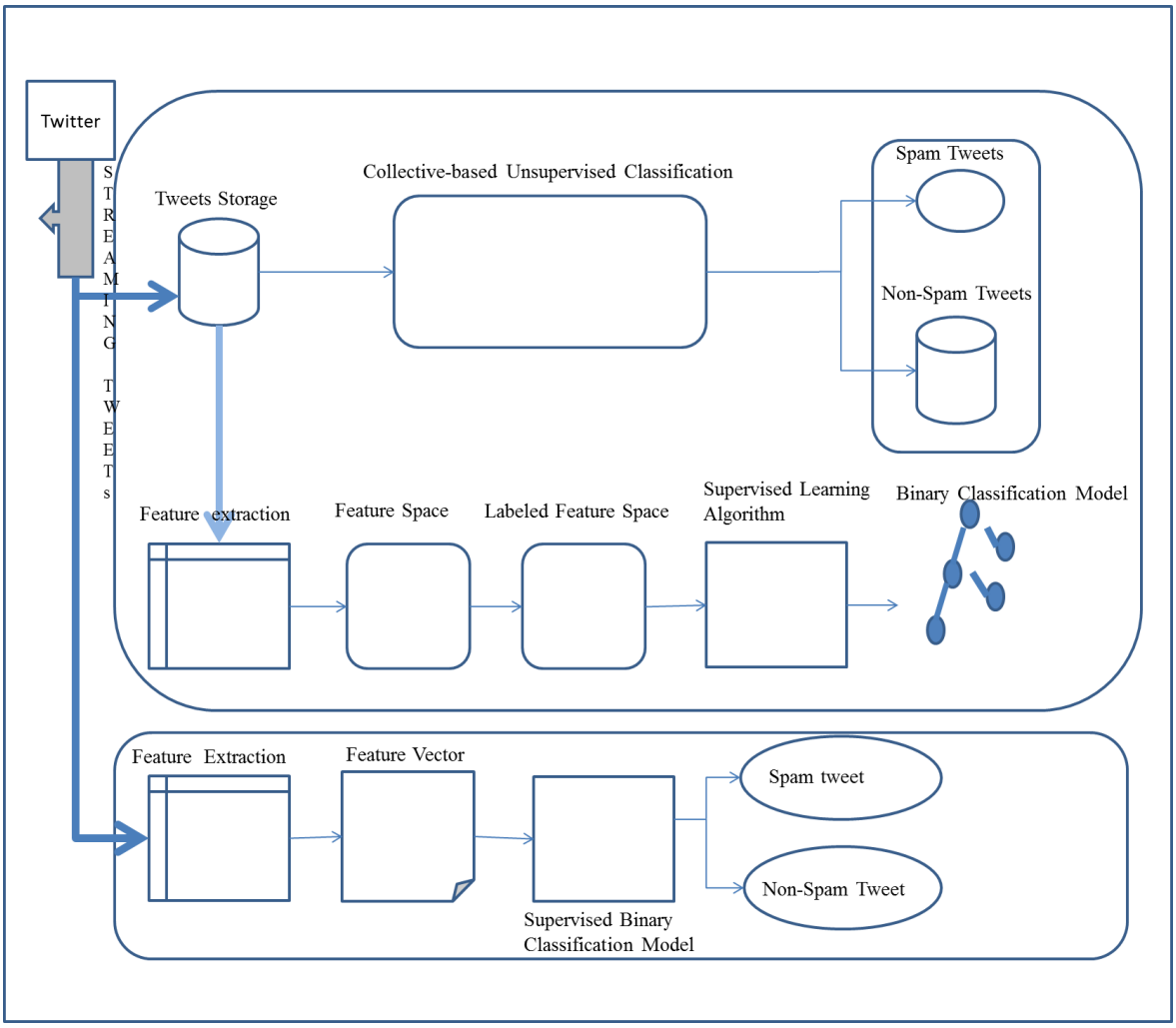

Figure 1. Unsupervised based spam detection methodologies [15].

2.2 Honeypot based attack detection methodologies

Classical supervised learning techniques needs initial dataset which is labeled by human and it cannot handle the spam drift issues in an efficient manner. On the other hand, few spam discovery techniques are based on community reporting methods that uses Social honeypot. The Social honeypot defined as a resource of an information system that monitors the behavior of the social spammers' by getting logged to their information like details of accounts and any information content available. Social honeypots are the tools that are valuable in understanding and gathering the activities of spams. But if we compare social honeypot technique and social media platform anti-spam method, there is no much important difference is there. Both require administrative control to take decisions with respect to accounts that are in honeypot trap for minimizing the false positive rate, which is more time-consuming. But Honeypot was known as a favorable solution for creating accounts manually as traps for the spammers [4], [17], [18], [19], and [20] and is shown in Figure 2. By mimicking as normal account with few specific characteristics which matches the taste of the spammers', a social honeypot stays in the network with the intention of attracting spammers. Even though spammer accounts can be trapped by honeypot, it has significant drawbacks. They include network scalability, attribute variability and deployment flexibility. The reason for this is the manual setup that involves human efforts considerably. Therefore it suffers from huge deployment overhead which is impracticable to scale up in a large- network to trap the spammers. Furthermore, honeypot even acts as an ordinary account and it is possible to identify by the spammers with the development of smart spam methods.

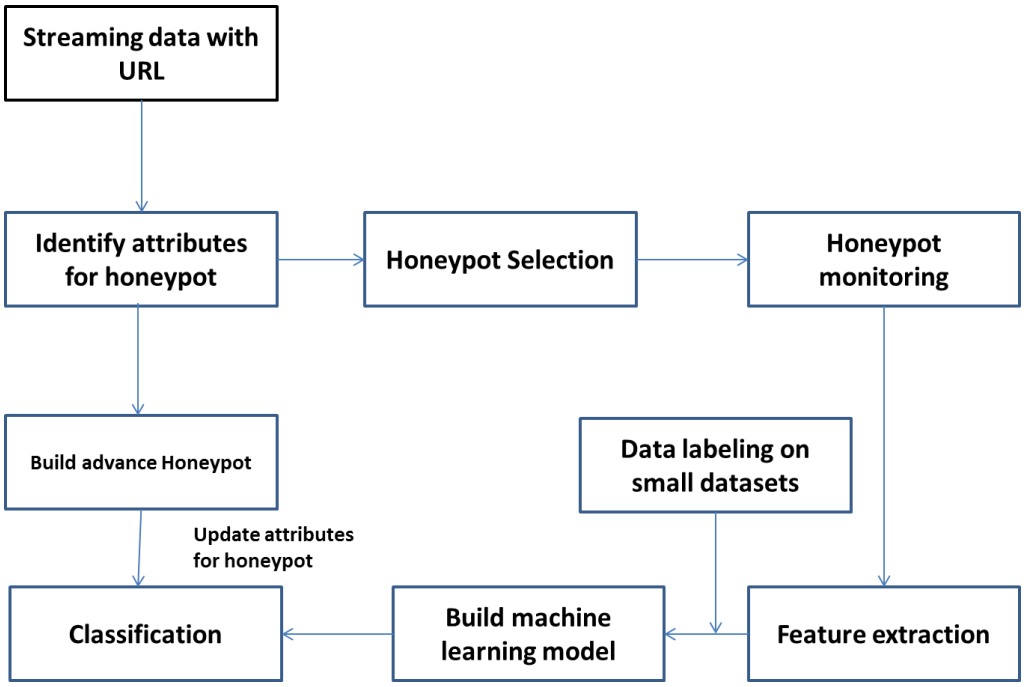

Figure 2. Honeypot based spam detection methodologies.

2.3 Blacklist based attack detection methodologies:

Almost all the spammers support their products and/or services using an embedded URL links in spam data [22]. Thus, a significant method of detecting spam is to identifying the data that contains spam links which are based on third party blacklisting methods. As an example, Googles Safe Browsing API is used to protect from the malicious links by the Twitter and Facebook which are social media platforms. Actually, blacklist techniques are used to detect the spam by searching list. This can be applicable to domain level rather than for the specific URL. Blacklisting methods are generally implemented for labeling the dataset or web filtering services. Additionally, it gives a lightweight method with reduced cost when compared to the existing classifiers. But it cannot handle dynamic behavior activities of spams. Thus it is not suitable for the detection in real-time, because on an average it considers four days for blacklist to add the new spam URLs [23]. Several spammers use shortened URLs to disable the working performance of blacklisting methods. Furthermore, few URLs detecting methods are based on relationship between extracted URLs from many tweets, which need more amount of time for retrieving information from servers of social media platforms.

2.4 Superviced learning based attack detection methodologies:

Many platforms that are in social media are using machine learning methods for automation of detection of spam. But the feature selection is the main criteria that differentiate them. Nearly all the methods give different features which are used in the machine learning techniques for detection of spamming. Features will vary and they change in their level of campaign, tweet, account, method for detection in real-time, formulations, manipulation complexity, and powerfulness. Detecting the spams/anomalies in online environment by data driven methods are increased and are based on algorithms that are used for classification such as SVM (Support Vector Machine), KNN (K-Nearest Neighborhood), random forest and others. These methods [1], [2], [3], [4], [5] and [6] are used to stable the spam in normal tweet information's. The major advantages of data driven techniques is low cost because of reduced labor cost. These can also help in finding new hidden features in twitter spams [23], [24]. By the same time the spammers can produce new types of spam models which will send enormous spam messages into the system to find the filters decision boundary in differentiating a message as abnormal or normal. After spammers established the bugs in the system, the second step is more furtive. As a result of this, models based on historical information, used for twitter spam detection will fail in future. The twitter spams are known as concept drifts as they will change with time [25], [26]. Now a day, understanding the concept drift in streaming areas like twitted has become more important [16], [27]. This can be used in the applications that are used in real world such as twitters. In these applications the statistical properties and their distribution goes on changing with time. Addressing the problems of drifting spams is given in [7] which present posting time model and language model. These models are not able identify the accounts which are deceptively generated by spammers. Also these models establish accounts of users whether they are hacked or not. To address this [4] has designed a method that can derive the knowledge from not labeled tweet, detects tweets that are spam and solve the spam drifting problem. Comparing the works in [1], [2],

[3], and [4], classification of twitter spam is achieved better in the work of [4]. The already present models are failed to address the concept of drifting issues and includes more computations and they also not taken consideration of the problems which are discussed below [28]. Only drift in Posterior probability affects the hyperplane decision. But it is not possible to drift only one drift component to change and the others fixed. All the four drift types are correlated and change simultaneously in real-world with time. Thus the concept of drift is defined as the combination of different drift components as joint concept drift. One more typical problem in data mining is the class imbalance. In class imbalance, all the classes will not have same number of samples, i.e., in one class can have more samples compared to other class [29]. Applying directly the standard machine learning methods to the situations like this will ignore the samples of minority class, as these minority samples affect the overall accuracy. Concept drift and Class imbalance are reinforcing mutual effects. If both problems occur simultaneously, they aggravate one- another. If the data streams in the classes are imbalanced, then it is very difficult to identify the concept drift in minority class and also for adopting online learning to them. On the contrary, class imbalance status can be altered by concept drift, as prior class is one variable in concept drifting environment. Thus so far, a few methods are proposed to manage the problem of concept drifting along with class imbalance. The corresponding literature review was found in [30].

3. Future Issues and Challenges

In this section, we discuss in detail many capable ways for future cyber-attack identification in online environment.

3.1 Class imbalance:

One more typical problem in data mining is the class imbalance. In class imbalance, all the classes will not have same number of samples, i.e., in one class can have more samples compared to other class [29], [31]. Applying directly the standard machine learning methods to the situations like this will ignore the samples of minority class., as these minority samples affect the overall accuracy. Concept drift and Class imbalance are reinforcing mutual effects. If both problems occur simultaneously, they aggravate one- another. If the data streams in the classes are imbalanced, then it is very difficult to identify the concept drift in minority class and also for adopting online learning to them. On the contrary, class imbalance status can be altered by concept drift, as prior class is one variable in concept drifting environment. Thus so far, a few methods are proposed to manage the problem of concept drifting along with class imbalance. The corresponding literature review was found in [30]. The methods which are already exists can be classified into two approaches: Online and the chunk-based. In online approach [32]-[35], for each incoming data sample, prediction model is updated and drift detector is used to monitor data streams. If the concept drift is identified, then the present model of prediction will be reset, and new model for new drift concept will be built. As an example, consider over sampling and under sampling based on online bagging (OOB) [33] which uses time-delayed scheme for obtaining the recent ratio of data stream imbalance. It can be used to incorporate both oversampling and the underdampling in online bagging. This can be related with the drift identifier like Drift Detection Method for Online Class Imbalance (DDM-OCI) [34]. DDM-OCI provides a warning when needed by checking minority class. It recalls and confirm the detection by the use of statistical information. But the main problems with approaches that are based on detectors are the false alarms, detection delays and missed detections. In contrary, chunk based approaches [36]–[39] & [41] data streams are buffered for certain samples and accumulated. Then the classifiers are built based on the accumulated chunks of data. Usually these approaches assume ubiquitous concept drift will occur in data stream and update the present model continuously. Typically, a collaborative framework is used to generate one classifier for every incoming chunk of data. The classifiers weights will be adjusted for new concept [28], [40]. At the same time the issue of imbalance will be overcome by collecting the samples of minority class in past chunks. As an example, importance sampling is used to collect samples of minority class form past chunks in dynamic feature group weighting (DFGW-IS) [38]. And the samples of majority class are bootstrapped to make a bagging-like collection. This approach will work if minority class is of fixed concept in data stream. But when the concept drift environment is complex, the p(y) drift change the imbalance ratio. Thus, if minority class is made to form majority class by expanding, the samples of the minority class which are store in the past cannot be used to refine the present minority class. Along with this it is very difficult to give proper weight for individual classifiers which are trained in different time stamps while restricting the classifiers count not to increase infinitely.

3.2 Concept Drift:

When handling data streams which are nonstationary, concept drifts will become the problems for the models of machine learning. If stationary data producing process is changed, the prior model will become inaccurate or completely useless [42], [43]. An example of concept drift is navigation system, which has to update the map very instantly when it is misleading the vehicles [44]. Another example is an application website which is used for online shopping, has to sense drastic change in the preferences of the customers [45]. Non-adaptive model's performance

will vary periodically when the seasons are changed [46]. These models are used for predicting the demand and supply of local heating energy. They refer the outdated information which is a cause for their failure. It is very time consuming and sometimes it is impossible to manually check the drifts in an environment. Thus a method that automatically identifies the drifts and adopts it to the models is proposed in [47]. These methods are categorized as active approach and passive approach [48]. Active approaches will monitor the performance of models when it is stationary and it will activate the adaptation process when it identifies a drift [49]. Here the main challenge is how to create a drift indicator that represents performance. A good drift indicator is one which is simple in procedure for detection and for computation. Also it should be highly sensitive to identify the drift. To construct the drift indicators two methods are available. One method is based on the real labels in the data sets. The other method uses only unlabeled data.

In the next section, problem statement is presented by considering above said future open issues and the challenges in constructing efficient detection methodology for anomalies in online environment.

4. Problem Statement and proposed methodology to Design Efficient Attack Detection framework for Online/Social media Environment

In last few years, the understanding from online data with concept drifting has gained more significance in online learning field. This is because it happens with real application based on machine learning, where distribution of data underlying changes with respect to time. As an example, the attackers will improve continuously quality of the attack that they post in Twitter so as to prevent the blocking from the fraud detection systems. Thus features and the concepts of attack/spam on Twitter change frequently. Therefore for an online algorithm that process data streaming along with the concept drift should maintain a tradeoff between learning from the previous data collected and adopting into the new concept. This is known as stability-plasticity dilemma. According to the Bayes' theorem, the concept drift will occur in four components. They are: 1) Data Distribution – Is a virtual drift in which distribution of x is changed without modifying decision hyperplane. 2) Class Conditional Probability (Likelihood) – is virtual drift that commonly co-occurs with training data drift and test data drift. 3) Posterior Probability: Is a real drift in which decision hyperplane will be shifted with the changes in conditional probability. 4) Class Prior p(y): Is a virtual drift in which changes in the imbalance ratio is done based on the switching between majority and minority class. The methodologies present in [5], [11], [12], [50], [51] are assumed decision hyperplane is affected by posterior probability drift only. But it is not possible to change only one drift component by keeping the other constant. Thus the four components of drift are simultaneously occurs and are connected to each other. These components can occur in real world streaming data at any time. One more typical problem in data mining is the class imbalance. In class imbalance, all the classes will not have same number of samples, i.e., in one class can have more samples compared to other class [12], [50], [51]. Applying directly the standard machine learning methods to the situations like this will ignore the samples of minority class., as these minority samples affect the overall accuracy. Concept drift and Class imbalance are reinforcing mutual effects. If both problems occur simultaneously, they aggravate one-another. If the data streams in the classes are imbalanced, then it is very difficult to identify the concept drift in minority class and also for adopting online learning to them. On the contrary, class imbalance status can be altered by concept drift, as prior class is one variable in concept drifting environment. Thus so far, a few methods are proposed to manage the problem of concept drifting along with class imbalance. Therefore the aim of the research is to address this problem in creating an efficient fraud detection system by using the methodologies described in the Figure 3.

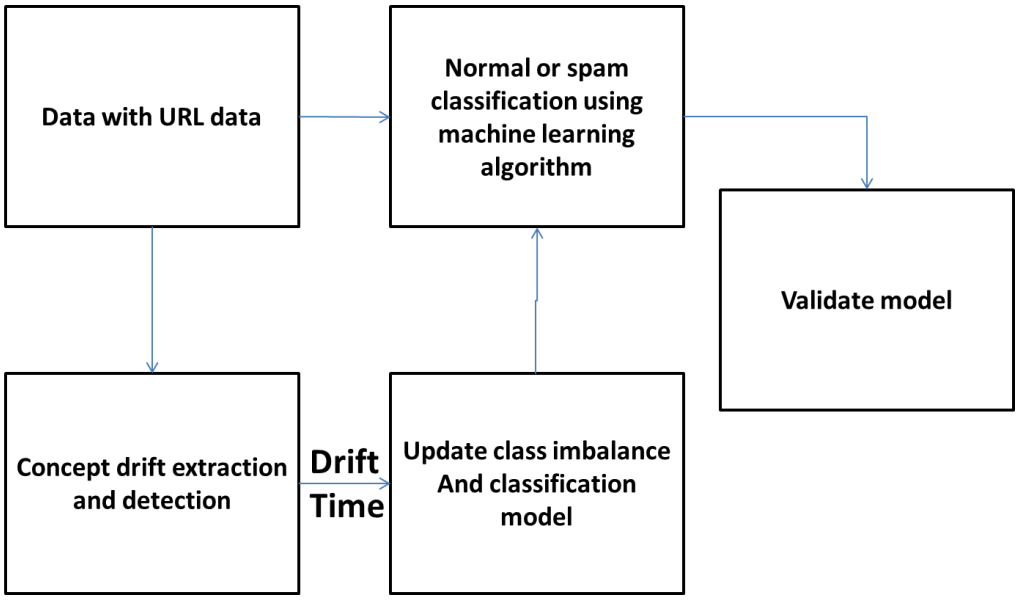

Figure 3. Cyber-attack detection methodology for online environment.

5. Conclusion

One challenging issue in recent trends of distributed environment is workflow scheduling which concentrates on satisfying different constraints of quality of service (QoS). The cloud takes application forms for workflow that contains a set of tasks which are interdependent and are used to solve enterprise and large scale scientific problems. In cloud environment, the workflow scheduling provides broad review of approaches, which are studied comprehensively. Work scheduling article gives the analysis of different workflow scheduling methods and their characteristics. Is also perform the classification based on model of execution and its objectives. Along with this, recent developments in technology like edge-cloud computing are producing new opportunities and requirements for scheduling workflow for background processing tasks like web applications, Internet of-Things (IoT), and event-driven applications in distributed environment. Work scheduling article also gives scheduling of workflow in cloud computing trends. At the end, it presents the future research possible direction in creating an effective utilization of resource with good performance in tolerating the faults, execution of workload in the platform of heterogeneous cloud.

Reference

[1] M. Fazil and M. Abulaish, "A Hybrid Approach for Detecting Automated Spammers in Twitter," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2707-2719, 2018.

[2] M. Jiang, P. Cui and C. Faloutsos, "Suspicious Behavior Detection: Current Trends and Future Directions," in IEEE Intelligent Systems, vol. 31, no. 1, pp. 31-39, 2016.

[3] G. Lin, N. Sun, S. Nepal, J. Zhang, Y. Xiang and H. Hassan, "Statistical Twitter Spam Detection Demystified: Performance, Stability and Scalability," in IEEE Access, vol. 5, pp. 11142-11154, 2017.

[4] S. Sedhai and A. Sun, "Semi-Supervised Spam Detection in Twitter Stream," in IEEE Transactions on Computational Social Systems, vol. 5, no. 1, pp. 169-175, 2018.

[5] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou and G. Min, "Statistical Features-Based Real-Time Detection of Drifted Twitter Spam," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 914-925, 2017.

[6] J. Zhang, R. Zhang, Y. Zhang and G. Yan, "The Rise of Social Botnets: Attacks and Countermeasures," in IEEE Transactions on Dependable and Secure Computing. doi: 10.1109/TDSC.2016.2641441, 2016.

[7] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, “Compa: Detecting compromised accounts on social networks,” in Proc. Annu. Netw. Distrib. Syst. Security Symp., 2013.

[8] R. C. Cavalcante, L. L. Minku, and A. L. I. Oliveira, ``FEDD: Feature extraction for explicit concept drift detection in time series," in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Vancouver, BC, Canada, Jul. 2016, pp. 740-747.

[9] D. Yang, B. Li, L. Rettig, and P. Cudré-Mauroux, ``Histosketch: Fast similarity-preserving sketching of streaming histograms with concept drift," in Proc. IEEE Int. Conf. Data Mining (ICDM), New Orleans, LA, USA, Nov. 2017, pp. 545-554.

[10] G. I. Webb, L. K. Lee, F. Petitjean, and B. Goethals, ``Understanding concept drift," 2017, arXiv:1704.00362. [Online]. Available: https://arxiv.org/abs/1704.00362.

[11] S. Yu, X. Wang, and J. C. Principe, ``Request-and-reverify: Hierarchical hypothesis testing for concept drift detection with expensive labels," in Proc. 27th Int. Joint Conf. Artif. Intell., Stockholm, Sweden, 2018, pp. 3033-3039.

[12] S. Schmidt and P. S. Heyns, ``Localised gear anomaly detection without historical data for reference density estimation," Mech. Syst. Signal Process., vol. 121, pp. 615-635, 2019.

[13] Rout, N. , Mishra, D. , & Mallick, M. K. (2018). Handling imbalanced data: A survey. In M. S. Reddy, K. Viswanath, & S. P. K. M. (Eds.), International proceedings on ad- vances in soft computing, intelligent systems and applications (pp. 431–443). Sin- gapore: Springer Singapore.

[14] Inuwa-Dutse, I., Liptrott, M., & Korkontzelos, I. (2018). Detection of spam-posting accounts on twitter. Neurocomputing, 315 . doi: 10.1016/j.neucom.2018.07.044.

[15] Washha, Mahdi & Qaroush, Aziz & Mezghani, Manel & Sedes, Florence. (2019). Unsupervised Collective-based Framework for Dynamic Retraining of Supervised Real-Time Spam Tweets Detection Model. Expert Systems with Applications. 135. 10.1016/j.eswa.2019.05.052.

[16] G. Ditzler, M. Roveri, C. Alippi, and R. Polikar, "Learning in nonstationary environments: A survey," IEEE Comput. Intell. Mag., vol. 10, no. 4, pp. 12–25, Nov. 2015.

[17] K. Lee, J. Caverlee, and S. Webb. Uncovering social spammers: Social honeypots + machine learning. In Proceedings of the ACM SIGIR Conference on Research and Development in Information Retrieval, pages 435–442, 2010.

[18] M. Nisrine et al. A security approach for social networks based on honeypots. In IEEE International Colloquium on Information Science and Technology (CiSt), pages 638–643, 2016.

[19] C. Yang, J. Zhang, and G. Gu. A taste of tweets: Reverse engineering twitter spammers. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), pages 86–95, 2014.

[20] Y. Zhang, H. Zhang, X. Yuan and N. Tzeng, "Pseudo-Honeypot: Toward Efficient and Scalable Spam Sniffer," 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Portland, OR, USA, 2019, pp. 435-446, doi: 10.1109/DSN.2019.00052.

[21] Lee, S., & Kim, J. (2013). Warningbird: A near real-time detection system for suspicious urls in twitter stream. IEEE Transactions on Dependable and Secure Computing, 10 (3), 183–195. doi: 10.1109/TDSC.2013.3.

[22] Wu, T., Wen, S., Xiang, Y., & Zhou, W. (2017). Twitter spam detection: Survey of new approaches and comparative study. Computers and Security, 76. doi: 10.1016/ j.cose.2017.11.013.

[23] B. Liu, Z. Ni, J. Luo, J. Cao, X. Ni, B. Liu, and X. Fu, ``Analysis of and defense against crowd-retweeting based spam in social networks," World Wide Web, vol. 21, pp. 1-23, 2018. doi: 10.1007/s11280-018-0613-y.

[24] M. Stamp, Introduction to Machine Learning With Applications in Information Security. London, U.K.: Chapman & Hall, 2017.

[25] S. Wang, Z. Ding, and Y. Fu, ``Feature selection guided auto-encoder," in Proc. 31st AAAI Conf. Artif., San Francisco, CA, USA, 2017, pp. 2725-2731.

[26] M. Alrubaian, M. Al-Qurishi, A. Alamri, M. Al-Rakhami, M. M. Hassan, and G. Fortino, ``Credibility in online social networks: A survey," IEEE Access, vol. 7, pp. 2828-2855, 2019.

[27] H. Yuan, J. Gama, I. V. Z. E. Žliobaitˇe, A. Bifet, M. Pechenizkiy, and A. Bouchachia, "A survey on concept drift adaptation," ACM Comput. Surv., vol. 46, no. 4, p. 44, Apr. 2014.

[28] H. M. Gomes, J. P. Barddal, F. Enembreck, and A. Bifet, "A survey on ensemble learning for data stream classification," ACM Comput. Surv., vol. 50, no. 2, p. 23, 2017.

[29] P. Branco, L. Torgo, and R. P. Ribeiro, "A survey of predictive modeling on imbalanced domains," ACM Comput. Surv., vol. 49, no. 2, p. 31, Nov. 2016.

[30] S. Wang, L. L. Minku, and X. Yao, "A systematic study of online class imbalance learning with concept drift," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 10, pp. 4802–4821, Oct. 2018.

[31] H. He and E. A. Garcia, "Learning from imbalanced data," IEEE Trans. Knowl. Data Eng., vol. 21, no. 9, pp. 1263–1284, Sep. 2009.

[32] S. Wang, L. L. Minku, D. Ghezzi, D. Caltabiano, P. Tino, and X. Yao, "Concept drift detection for online class imbalance learning," in Proc. Int. Joint Conf. Neural Netw., Dallas, TX, USA, pp. 1–10, 2013.

[33] S. Wang, L. L. Minku, and X. Yao, "Resampling-based ensemble methods for online class imbalance learning," IEEE Trans. Knowl. Data Eng., vol. 27, no. 5, pp. 1356–1368, 2015.

[34] S. Yu and Z. Abraham, "Concept drift detection with hierarchical hypothesis testing," in Proc. SIAM Int. Conf. Data Mining, Houston, TX, USA, pp. 768–776, 2017.

[35] D. Brzezinski and J. Stefanowski, "Prequential AUC for classifier evaluation and drift detection in evolving data streams," in Proc. 3rd Int. Conf. New Frontiers Mining Complex Patterns. Nancy, France: Springer, pp. 87–101, 2014.

[36] J. Gao, W. Fan, J. Han, and P. S. Yu, "A general framework for mining concept-drifting data streams with skewed distributions," in Proc. SIAM Int. Conf. Data Mining, Minneapolis, MN, USA, 2007, pp. 3–14. [Online]. Available: http://epubs.siam.org/doi/abs/10.1137/1.9781611972771.1

[37] S. Chen and H. He, "Towards incremental learning of nonstationary imbalanced data stream: A multiple selectively recursive approach," Evolving Syst., vol. 2, no. 1, pp. 35–50, 2011.

[38] K. Wu, A. Edwards, W. Fan, J. Gao, and K. Zhang, "Classifying imbalanced data streams via dynamic feature group weighting with importance sampling," in Proc. SIAM Int. Conf. Data Mining, Philadelphia, PA, USA, 2014, pp. 722–730.

[39] Y. Lu, Y.-M. Cheung, and Y. Y. Tang, "Dynamic weighted majority for incremental learning of imbalanced data streams with concept drift," in Proc. 26th Int. Joint Conf. Artif. Intell. Melbourne, VIC, Australia: AAAI Press, Aug. 2017, pp. 2393–2399.

[40] B. Krawczyk, L. L. Minku, J. Gama, J. Stefanowski, and M. Wo´zniak, "Ensemble learning for data stream analysis: A survey," Inf. Fusion, vol. 37, pp. 132–156, Sep. 2017.

[41] G. Ditzler and R. Polikar, "Incremental learning of concept drift from streaming imbalanced data," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2283–2301, Oct. 2013.

[42] V. R. Kompella and W. Laurenz, "Intrinsically motivated acquisition of modular slow features for humanoids in continuous and non-stationary environments," 2017. [Online]. Available: arXiv.1701.04663.

[43] E. Lughofer and M. Sayed-Mouchaweh, "Predictive maintenance in dynamic systems," in Advanced Methods, Decision Support Tools and Real-World Applications, Cham, Switzerland: Springer, 2019.

[44] W. C. Chang and C. W. Cho, "Online boosting for vehicle detection," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 40, no. 3, pp. 892–902, Jun. 2010.

[45] Y. Bao, X. Wang, Z. Wang, C. Wu, and F. C. M. Lau, "Online influence maximization in non-stationary social networks," in Proc. IEEE Symp. Qual. Service, Beijing, China, 2016, pp. 1–6.

[46] I. I. F. Blanco, J. del Campo-Ávila, G. Ramos-Jiménez, R. M. Bueno, A. A. O. Díaz, and Y. C. Mota, "Online and non-parametric drift detection methods based on Hoeffding's bounds," IEEE Trans. Knowl. Data Eng., vol. 27, no. 3, pp. 810–823, Mar. 2015.

[47] I. Khamassi, M. Sayed-Mouchaweh, M. Hammami, and K. Ghedira, "Discussion and review on evolving data streams and concept drift adapting," Evol. Syst., vol. 9, no. 1, pp. 1–23, 2017.

[48] G. Ditzler, M. Roveri, C. Alippi, and R. Polikar, "Learning in nonstationary environments: A survey," IEEE Comput. Intell. Mag., vol. 10, no. 4, pp. 12–25, Nov. 2015.

[49] J. Zhang, Z. Wei, Z. Yan, M. C. Zhou, and A. Pani, "Collaborated online change-point detection in sparse time series with application to online advertising," IEEE Trans. Syst., Man, Cybern., Syst., vol. 49, no. 9, pp. 1141–1151, Jun. 2019.

[50] X. Wang, Q. Kang, J. An and M. Zhou, "Drifted Twitter Spam Classification Using Multiscale Detection Test on K-L Divergence," in IEEE Access, vol. 7, pp. 108384-108394, 2019, doi: 10.1109/ACCESS.2019.2932018

[51] M. Alrubaian, M. Al-Qurishi, M. Al-Rakhami, M. M. Hassan, andA. Alamri, ``Reputation-based credibility analysis of Twitter social network users," Concurrency Comput., Pract. Exper., vol. 29, no. 7, p. e3873, 2017.