Expedite Feature Extraction for Enhanced Cloud Anomaly Detection

Bruno L. Dalmazo, João P. Vilela, Paulo Simões, Marilia Curado
CISUC, Department of Informatics Engineering
University of Coimbra, Coimbra, Portugal
{dalmazo, psimoes, jpvilela, marilia}@dei.uc.pt

***Abstract*—Cloud computing is the latest trend in business for providing software, platforms and services over the Internet. However, a widespread adoption of this paradigm has been hampered by the lack of security mechanisms. In view of this, the aim of this work is to propose a new approach for detecting anomalies in cloud network traffic. The anomaly detection mechanism works on the basis of a Support Vector Machine (SVM). The key requirement for improving the accuracy of the SVM model, in the context of cloud, is to reduce the total amount of data. In light of this, we put forward the Poisson Moving Average predictor which is the core of the feature extraction approach and is able to handle the vast amount of information generated over time. In addition, two case studies are employed to validate the effectiveness of the mechanism on the basis of real datasets. Compared with other approaches, our solution exhibits the best performance in terms of detection and false alarm rates.**

***Keywords*—Security; cloud computing; support vector machine; feature extraction; anomaly detection.**

I. Introduction

Cloud computing is a paradigm that involves service delivery models over the Internet, such as: infrastructure, software and platform. These services can be offered to a wide range of clients through the cloud providers. A recent report by Cisco Global Cloud Index predicts that by 2018, 76% of all data center traffic in the world will come from cloud [1]. According to the same report, the lack of security mechanisms is the top factor that prevents the wide adoption of cloud service models. Moreover, 74% of Information Technology executives believe that security is one of the main issues that needs to be addressed.

Online threats are constantly evolving in the virtual environment. In this context, cloud computing introduces significant new paths of attack. Denial of Service (DoS) is a well-known type of attack that disrupts online operations. The assault is usually carried out by hundreds (or thousands) of requests for a service and has to be detected before it breaks down the server. Owing to the large number of simultaneous requests, this type of attack causes an anomalous behaviour in the network traffic. At the same time, the elastic and scalable nature of cloud environments means that they are also apt to undergo sudden changes [2], [3], which makes it even harder to detect which parts of the incoming traffic are caused by vandalism or are being used legitimately.

Intrusion Detection Systems (IDSs) are complex tools that include a number of concepts, definitions and techniques that may differ, depending on the situation. An IDS usually relies on two main approaches to detect intrusions that differ in the way the data is analysed and processed. The first approach corresponds to a search for evidence of an attack based on signatures of other similar attacks while the second approach consists of a search for deviations from the appropriate behaviour found in periodic observations of the system. The principal advantage of the signature-based detection method is that it leads to a low number of false alarms. However, signature-based IDSs are not able to detect new or variant forms of known attacks. One of the benefits of anomaly-based detection is that a new attack for which a signature does not exist can be detected if it occurs outside of the regular traffic patterns. In our study, we focus on the second class of IDS to detect threats to the network traffic in the cloud environment.

Several techniques have already been proposed to perform anomaly detection in the cloud environment, such as fuzzy logic [4], artificial neural networks [3] and decision tree classifier [5]. Also, different types of network traffic information are used to detect anomalies, such as the behaviour of protocols, CPU utilization and user logs. However, there is an apparent deficiency in their ability to detect anomalies from a large amount of data. In particular, these techniques require extensive tuning to improve their sensitivity and achieve satisfactory results. There is also no consensus about the best way to represent the huge volume of data generated by the cloud infrastructure. As a result, the literature lacks mechanisms that can enable it to improve the accuracy of anomaly detection for cloud environments while reducing false detection rates.

To fill these gaps, a new approach to detect anomalies in a cloud environment is proposed. Our proposal relies on traffic prediction to obtain features that represent the expected appropriate behaviour of the cloud network traffic. This information is then used jointly with a Support Vector Machine (SVM) model that is supplied with these features. The combination of these two tools represents a novel and effective approach for detecting anomalous events in the cloud environment. The forecasting is conducted by a statistical method based on a Poisson process [6], that has proved to be suitable for dynamic environments such as cloud computing. SVM is already known as one of the best learning algorithms for binary classification [7]. Binary classification meets the objectives of this proposal, since our aim is to detect anomalies inside the normal network traffic.

The remainder of the paper is organized as follows. Section II covers some of the most prominent related work. Section III describes the proposed solution and the methodology used

978-1-5090-0223-8/16/$31.00

for this paper, whilst Section IV presents the evaluation and discusses the results. Section V concludes with some final remarks and prospective directions for future research.

II. Related Work

The current state of the art in IDSs contains many different approaches, but due to the focus of our paper, we restrict ourselves to SVM models applied in the IDS context and several models for detecting anomalies in the cloud computing environment. Finally, a discussion about the state-of-the-art and the open issues is provided.

A. Support Vector Machine IDSs

Horng *et al.* [8] proposed a Network Intrusion Detection System on the basis of Support Vector Machine with features selected by a hierarchical clustering algorithm. The SVM uses features such as the type of protocol, the status of the connection, the number of file creation operations, length of the connection and the number of root accesses. In spite of the good results for attacks that generate anomalies, this approach does not present the same effectiveness for other attacks such as User-to-Root (U2R) and Remote-to-Local (R2L). The DARPA dataset was used to evaluate the proposed IDS.

Shon and Moon [9] presented a hybrid machine learning approach to detect anomalies in the network traffic. This model is a blending between supervised and unsupervised SVM model. From this, they aim to increase the performance in detecting new attacks. Besides, they use a Genetic Algorithm for extracting more appropriate packet fields (protocol, IP, TTL). However, in the evaluation section, the proposal presents a high false positive rate with data from the DARPA dataset.

Chen *et al.* [10] did a comparative study between Artificial Neural Network (ANN) and Support Vector Machine to predict attacks on the basis of frequency-based encoding techniques to select the features. The aim of this proposal is to increase the generalization capability of detecting more attacks from less training data. The results have shown that both approaches are able to detect anomalies in the network traffic, but SVM outperforms ANN.

B. Anomaly Detection in Cloud

Kholidy and Baiardi [11] proposed a framework for a cloud-based IDS with features from signature attacks and user logs. This solution presents a distributed architecture without central coordinator to avoid a single point of failure. This framework, based on event correlation, has a drawback in terms of efficiency. According to the authors, this model presents an excessive overhead to update the neural network parameters. Besides, the authors present an own dataset to validate this approach, namely, CIDD dataset.

Song Fu [5] proposed a framework for autonomic anomaly detection in the cloud context. The detection mechanism is fed through an algorithm for metric selection based on mutual information: maximal relevance and minimal redundancy. After that, a semi-supervised decision tree classifier identifies anomalies considering information such as CPU usage, memory utilization, paging fault. Real data from a university campus is employed to assess the feasibility of the solution.

Vieira *et al.* [3] showed some particularities of five IDSs and a comparative study is presented. The IDS proposed uses ANN for anomaly detection in cloud environment, and it improves the security level by integrating two approaches to intrusion detection: behaviour- and knowledge-based. This investigation covers some characteristics such as host- network-based intrusion detection system; data from grid and cloud computing; IDS approach and validation. In the suggested proposal, each node cooperatively participates identifying local events (user logs) that could represent security violations. The authors use simulation to assess this IDS.

Xiong *et al.* [12] surveyed different types of security threats in cloud communication. Furthermore, to reduce security risks, they propose an IDS to detect network traffic anomaly based on synergetic neural networks and the catastrophe theory. The DARPA dataset was used to validate this approach. The results show high detection rates (83% up to 97%) and low false alarm rates (8.3% to 11.4%). Ahmed Patel *et al.* [4] presented a taxonomy and state-of-the-art of intrusion detection and prevention systems for cloud. At the end, they propose an IDS focused on four applicable concepts for cloud-based intrusion detection systems: autonomic computing, ontology, risk management, and fuzzy theory. This proposal lacks of feature extraction approach and evaluation of the feasibility.

C. Discussion

Table I summarizes several IDS approaches and displays their key features. On the one hand, all the SVM models proposed for traditional networks were designed as an individual and centralized module. On the other hand, a couple of the IDSs employed in cloud computing have a collaborative design, but most of them were assessed by synthetic data (simulations) or have a conceptual model that still has to be validated.

Regardless of whether or not anomaly detection methods are reliable, some requirements are still not being met when they are employed in the cloud computing environment, such as finding the best set of features and reducing the amount of information required to describe a large set of data. In the training phase, the SVM spends an amount of time that is proportional to the amount of input data. This means that reducing the amount of data is the key factor for successfully using the SVM in the context of cloud. According to the related work, among the approaches for feature extraction, there is none that is applied to cope with the massive volume of data traffic generated by the cloud infrastructure. Thus, extracting a good set of features that represents the behaviour of the cloud network traffic remains an open issue.

In the following section, a conceptual solution for detecting anomalies in the cloud network traffic is introduced. The mechanism works by means of a SVM model that is fed with features extracted from a predictor based on a Poisson process.

III. Proposal - Anomaly Detection Mechanism

The purpose of our *Anomaly Detection Mechanism* is to provide an efficient method to detect anomalies in the cloud-based network traffic. Figure 1 depicts the basis of our mechanism, by highlighting the application scenario and the main conceptual components.

The cloud provider offers several services by the Internet, such as infrastructure, software and platform to the clients. Real-time cloud traffic data (Flow 1) is continuously being gathered from the cloud environment by the *Cloud Monitoring* module. This information is subsequently processed by the *Feature Extraction Approach* that performs prediction based on information such as the protocol type, the number of network packets and timestamp. After that, the *SVM Model* is fed with features extracted from the aggregated data (Flow 2). Then, the *SVM Model* triggers a warning to the *Event Auditor* when an anomalous behaviour is detected (Flow 3). In the meantime, the *Repository of Outcomes* component stores a detailed output regarding the historic of the Virtual Machine (VM) operation (Flow 4). Furthermore, the *Event Auditor* represents an agent placed in the VM that is able to communicate collaboratively with agents in the other VMs. This agent receives any anomalous event from the *SVM Model* and builds a message with information of all components (Flow 5) for sending alerts to other agents. Having presented an overview of the anomaly detection mechanism, in the following subsections there will be a more detailed description of the components.

A. Cloud Monitoring

Cloud Monitoring has to continuously monitor the service provided by the virtual machine. Thus, the *Cloud Monitoring* is able to take the cloud network traffic patterns during a given period. In other words, this component is responsible for recording all the incoming and outgoing network packets in a virtual machine. As input, raw data is gathered continuously from the cloud network traffic. The next step is building a time series that will be analysed for the following prediction. As output, the *Cloud Monitoring* prepares the collected data by measuring the number of packets in the network traffic at regularly spaced intervals, and thus forms a discrete time series ordered by the time. It is not within the scope of this study to propose a particular approach for monitoring the cloud infrastructure. However, several tools have the potential to monitor the cloud computing environment with the aid of distributed agents in virtual machines, such as Nagios, OpenNebula, and Nimbus [13].

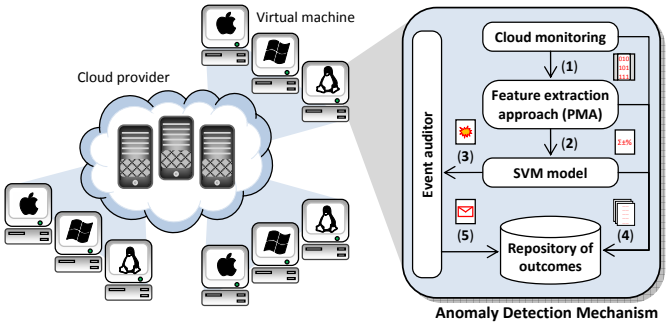


Fig. 1: Application scenario and elements of the proposed mechanism

B. Feature Extraction Approach

Extracting features from the network traffic is of crucial importance for providing a better performance by adopting a non-parametric approach such as using a Support Vector Machine. In our view, feature extraction involves reducing the amount of information required to describe a large set of data, therefore enabling its processing by the SVM. Besides, it creates new features from functions of the original data. In this context, we propose a supervised learning technique that operates through a multi-level representation of data. Our approach uses multiple temporal layers of data for feature extraction so that it can express data in a compact representation by removing redundancy.

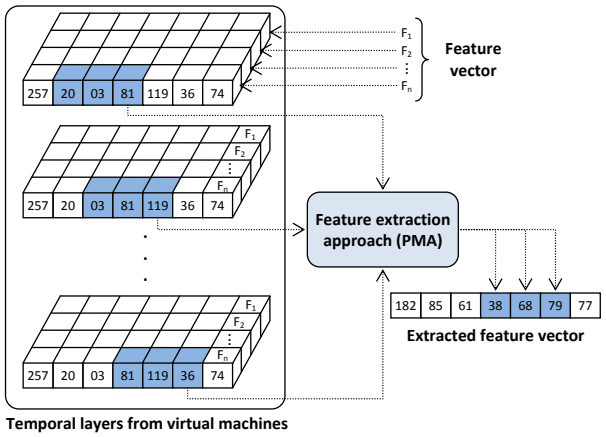


Fig. 2: Feature extraction approach based on PMA

TABLE I: Characteristics of related works concerning Intrusion Detection System

Proposal	Approach	Features	Feature extraction approach	Dataset	Management structure	Cloud scenario
Horng S. *et al.* [8]	SVM	Protocol, duration of connection, status, etc...	Hierarchical clustering algorithm	DARPA	Individual	×
Shon T. and Moon J. [9]	SVM	Protocol, source port, destination port, IP, TTL, etc...	Genetic algorithm	DARPA	Individual	×
Chen W. *et al.* [10]	SVM and ANN	Protocol, source port, destination port, IP, TTL, etc...	Frequency-based encoding	DARPA	Individual	×
Kholidy H. and Baiardi F. [11]	ANN	User logs and signature	Event correlation	CIDD	Collaborative	√
Song Fu [5]	Decision tree classifier	CPU usage, memory and swap utilization, paging and paging faults, etc...	Maximal relevance and minimal redundancy	Own dataset	Individual	√
Vieira K. *et al.* [3]	ANN	User logs	Event correlation	Simulation	Collaborative	√
Xiong W. *et al.* [12]	Neural network and Catastrophe theory	Hurst parameter and dynamic associate factor	Synergetic dynamic equation	DARPA	Individual	√
Ahmed Patel *et al.* [4]	Fuzzy theory	–	–	–	Individual	√

Figure 2 illustrates the process of extracting features. These features ($F_1, F_2, ..., F_n$) are gathered from the *Cloud Monitoring* process described in the last subsection and they characterize the real operation of a virtual machine. The set of features is arranged into vectors. Each layer contains all the feature vectors from a virtual machine at time t. A sliding window of a given size is used to weight past observations of data traffic according to the Poisson Moving Average (PMA) predictor model [14]. Based on the PMA methodology, at each time period, out feature extraction approach produces:

- a unique value that results from condensing the temporal layers by weighting past observations following a Poisson distribution;
- a predicted value for the subsequent time period.

These values are then used as input to the SVM for detection of anomalies.

Kind *et al.* [15] identified a set of relevant features for network anomaly detection. Cloud computing generates large amounts of monitored data, thus calling for a methodology to summarize this information. As detailed in Table II, the set of features from [15] over which we perform our extraction technique consist of: the type of the protocol, the port number, the packet size, the number of packets and the variance between real network traffic and predicted network traffic (Δ-variation).

TABLE II: Details of the extracted features

Feature	Description
Protocol type (f)	Dividing the network traffic by protocols type facilitates identifying anomalies not visible in the global network traffic
Port number (f)	Port number analysis is useful for revealing attacks that attempt to scan ports
Packet size (f)	The rapidly increasing of this feature can indicate a SYN flood attack
Number of packets (c)	Consists of control information and user data used in the prediction
Δ-variation	The absolute difference between the real network traffic and the predicted network traffic

These features are divided into two types: frequency (f) features (*e.g.* the number of times a packet from a protocol appears) and cumulative (c) features (*e.g.* the total number of packets received in a time period). For cumulative features, PMA aggregates values from different temporal layers and estimates the future behaviour of the network; for frequency features, PMA determines which port numbers are most common by a frequency function, and then estimates the occurrences of the port numbers for each slice of time. With the aid of the PMA algorithm, the outcome (*extracted feature vector*) contains just the most accessed port numbers. This operation is analogous to the other frequency features.

The *Poisson-based Predictor* [14] represents the core of our feature extraction approach. PMA has been adopted because of its high accuracy in terms of network traffic prediction, and its ability to generate a subset of representative features. It is worth noting that the feature extraction approach enhances generalisation by reducing the variance in the data. In other words, by employing PMA, the outliers (in a time series) are smoothed inside a sliding window but still noticeable in a global context. The PMA acts as a method of aggregating values over time so that the issue of processing large amounts of information by the SVM can be addressed, while still representing the data with sufficient accuracy.

C. SVM Model

The Support Vector Machine (SVM) is a supervised learning model that evaluates data and identifies patterns with the goal of classifying the data. SVM model uses a methodology for choosing the best hyperplane (among many others) that represents the largest margin between two classes, namely, normal network traffic and anomalies in this work. Then, the hyperplane is chosen such that the distance from it to the nearest support vector on each side is maximized [7].

The Support Vector Machine learning model includes two stages: training and testing. The first learns the two possible patterns of the network traffic (the normal and the anomalous behaviour). The second tests the knowledge achieved in the past stage to detect unknown anomalies. Separating data into training and testing data is an important part of validating the SVM model. At this point, the risk of learning from compromised data is reduced once the SVM can distinguish between the regular traffic and the anomaly. By this, we can minimize the effects of data inconsistencies and better understand the characteristics of the data. Once the SVM model has been processed by using the training set, it is needed to evaluate the prediction capability against the training set. Considering the data in the testing set already contains known values for the attribute that we want to predict, it is possible to determine whether the model's suggestions are correct.

Summing up, the anomaly detection for the cloud network traffic based on SVM with PMA expresses a process of recognizing an unexpected comportment. In this process, the training data represents the standard pattern and the testing data alludes to identify such pattern. The process of identifying a particular behaviour inside of the testing data is a mapping process of the testing data in some existing pattern of the training data.

D. Repository of Outcomes

The component called *Repository of Outcomes* is a database that brings together a set of information used to describe the anomaly detection mechanism activities. This database is done on the basis of the network traffic behaviour and its goal is to keep track of the virtual machine operating history. Furthermore, this information can be used to support the cloud decision-making. In this case, it can be used as subject to investigation by the operator or serves as a foundation to trigger alerts to other agents from other cloud services.

E. Event Auditor

Event Auditor consults the *Repository of Outcomes* periodically looking for unexpected occurrences. Once the *Event Auditor* finds a suspicious action, it will gather information from the *Repository of Outcomes* to build an alert message. The alerts represent that the current course of an event could be in some way dangerous or detrimental to the system. Although

the anomalous pattern is being captured by the *Event Auditor*, other virtual machines may be unaware this event. Thus, the *Event Auditor* can collaborate with agents from other virtual machines so that appropriate actions are taken. This paves the way to identification of distributed attacks.

IV. Evaluation and Discussion

Throughout this section, the anomaly detection model based on SVM that is used to assess this work is presented. Furthermore, we evaluate the effectiveness of the mechanism regarding the most common metrics found in similar studies in the literature. In addition, the results are compared with several SVM models outlined in Section II. We consider two case studies for evaluation: DARPA [16] and CAIDA [17] datasets.

A. Metrics

Typical metrics to evaluate the effectiveness of an anomaly detection system are: detection rate (DR), false positive rate (FPR) and false negative rate (FNR). The DR is the number of correctly classified as normal packets divided by the total number of the data of a test dataset (or true negative plus false positive).The FPR is defined as the total number of normal data traffic, which were classified as anomalies wrongly, divided by the total number of normal data traffic (or true negative plus false positive). The FNR is expressed as the total number of abnormals data that were incorrectly classified as normal traffic, divided by the total number of real abnormals data (or true positive plus false negative).

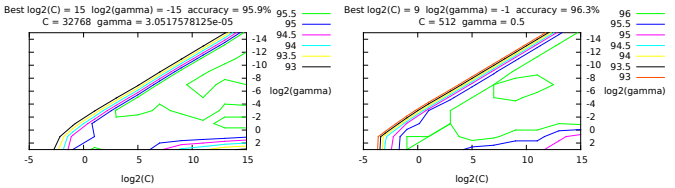
B. DARPA Case Study

The Cyber Security and Information Sciences Group of MIT Lincoln Laboratory, under Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory sponsorship, collected the first standard dataset for evaluation of computer network intrusion detection systems [16]. This dataset was the first formal, repeatable, and statistically significant evaluation of intrusion detection systems. We would like to point out that the DARPA data set is a renowned data set for anomaly detection. Although the data set was created in 1998/1999, it is still being used by many works, including recent works in the context of the cloud [12], [18], [19], [20].

The datasets contains data collected from February 1998 up to October 1999. The data consists of three weeks of training data and two weeks of test data. The first and third weeks of the training data do not contain any attack. The second and the fourth week of the training data contains a select subset of labelled attacks. In this work, we use the first and the second week for the *training phase* and the third and the fourth week for the *testing phase*. In order to make the dataset more realistic, we organized many of the attacks so that the resulting data sets consisted of 10% attacks and 90% normal traffic (for both datasets, *training phase* and *testing phase*).

1) Parameter Setup: The SVM model proposed in this work was implemented with LIBSVM version 3.20. LIBSVM is an integrated software for support vector classification, regression and distribution estimation. We consider the Radius Basis Function (RBF) kernel as SVM algorithm. RBF is a real-valued function that the value depends on the distance from the origin or on the distance from some another point called by *center*. The Euclidean distance is the main example of a Radius Basis Function. In particular, the RBF kernel is suitable when the number of features is not large.This kernel presents two parameters: C and γ. C is the parameter for the soft margin cost function, which controls the influence of each individual support vector. This process involves trading error penalty for stability. The γ is the free parameter of the Gaussian radial basis function, it defines how far the influence of a single training example reaches.

We use a *grid-search* on C and γ using the cross-validation process (performed automatically by the LIBSVM). In this process, several pairs of (C, γ) values are tried and the one with the best cross-validation accuracy is picked. In this process, for the DARPA dataset, the best pair is: (32768, $3.05e^{-5}$), as illustrated in Figure 3a.



(a) DARPA (b) CAIDA

Fig. 3: Grid searching for the best pair (C, γ)

2) Accuracy of the Model: Table III shows the comparison among several approaches that use SVM and DARPA dataset to validate the model. Regarding detection rate (DR) point of view, Soft margin SVM with Radial Basis Function (RBF) kernel obtained 97.48%, but at cost of high false negative rate (FNR), more than 11%. Another model with high DR, but low FPR, is the approach proposed by Chen W. *et al.* [10]. Although the model hits almost 90% of the time, it showed more than 10% of false positive rate (FPR). Other models presented in the Table III present at least one drawback: low accuracy, high FPR or high FNR. In summary, our method on the basis of SVM and RBF kernel with features extracted from Poisson Moving Average predictor presents the best equilibrium in the results. It reaches 98.56% of detection rate and 8% of FNR. Also, our approach displays the lowest FPR among the related work, just 1.44%.

C. CAIDA Case Study

The CAIDA DDoS Attack 2007 Dataset contains a traffic trace of a DDoS attack. This dataset contains pseudonymised traces occurred on August 4, 2007 for approximately one hour (20:50:08 UTC to 21:56:16). The entire CAIDA dataset is divided into 5 minutes packet capture (pcap) files. Only attack traffic to the victim and responses to the attack from the victim are included in the trace. The trace corresponds to a Ping Flood Attack that greatly increases the ICMP packets in the network traffic. The attack in the dataset is not labelled, precluding the training phase of the machine learning algorithms. However, to overcome this gap, the evaluation of the anomaly detection model through the CAIDA dataset was used just in the *testing phase*. We use the DARPA dataset for the *training phase*.

TABLE III: Approaches that use SVM and DARPA dataset

Approach	Kernel	DR(%)	FPR(%)	FNR(%)
LIBSVM and PMA	RBF	98.56	1.44	8.00
Horng S. *et al.* [8]	RBF	95.72	N/A	N/A
Enhanced SVM [9]	Sigmoid	89.59	10.41	27.27
Soft margin SVM [9]	Inner product	89.52	10.48	4.36
Soft margin SVM [9]	Polynomial	94.80	5.20	10.45
Soft margin SVM [9]	RBF	97.48	2.52	11.09
Soft margin SVM [9]	Sigmoid	96.06	3.94	12.73
One-class SVM [9]	Inner product	52.67	47.33	36.00
One-class SVM [9]	Polynomial	54.57	45.43	46.00
One-class SVM [9]	RBF	82.23	17.77	44.00
Chen W. *et al.* [10]	RBF	89.65	10.35	N/A

1) Parameter Setup: For the CAIDA case study, we consider the same RBF kernel as SVM algorithm. The *grid-search* presented (512, 0.5) as the best values for C and γ, as illustrated in the cross-validation process in Figure 3b.

2) Accuracy of the Model: The CAIDA dataset contains around 66 minutes of network traffic monitoring. This dataset exposes a flood attack that begins after 25 minutes until the end of the monitoring process. In this case, the anomaly detection approach was able to entirely identify the attack (100% of DR and 0% of FPR) with delay less than 5 minutes.

V. Final Considerations and Future Work

In this paper, an attempt has been made to shed light on the main obstacle to the adoption of the cloud service models: the lack of security. To address this problem, a novel approach to detect anomalies in the cloud scenario was proposed. Our work differs from previous anomaly detection techniques since it relies on a distributed and collaborative mechanism that combines a Support Vector Machine model with features extracted from a Poisson Moving Average predictor.

By analysing the results of the evaluation, it can be seen that the anomaly detection mechanism was able to detect anomalies by means of two case studies with real data. Our SVM model achieved a high degree of accuracy. In particular, compared with other approaches, we achieved the best level of detection rate and the second best number of false negative rates. Finally, it is worth pointing out that our mechanism outperforms other approaches in the literature, owing to the high quality of the features extracted from the Poisson-based predictor, such as its accurate prediction. Prospects for future research include extending the model so that it can cover other areas not initially envisaged in this work, such as alarm management and policies for reacting to an attack.

Acknowledgment

This work was partially funded by CAPES and CNPq (Brazil) through the Ciência sem Fronteiras Program/2016.

References

[1] Networking, CISCO Global Visual and Index, Cloud, "Cisco visual networking index: Forecast and methodology, 2014-2019 white paper," 2015.

[2] H. Ballani, P. Costa, T. Karagiannis, and A. I. Rowstron, "Towards predictable datacenter networks." in *SIGCOMM*, vol. 11, 2011, pp. 242–253.

[3] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," *IT Professional*, vol. 12, no. 4, pp. 38–43, July 2010.

[4] A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Jnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 25 – 41, 2013.

[5] S. Fu, "Performance metric selection for autonomic anomaly detection on cloud computing systems," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, Dec 2011, pp. 1–5.

[6] B. L. Dalmazo, J. P. Vilela, and M. Curado, "Predicting traffic in the cloud: A statistical approach," in *Third International Conference on Cloud and Green Computing (CGC'13), 2013*, Sept-Oct 2013, pp. 121–126.

[7] N. Deng, Y. Tian, and C. Zhang, *Support vector machines: optimization based theory, algorithms, and extensions*. CRC Press, 2012.

[8] S.-J. Horng, M.-Y. Su, Y.-H. Chen, T.-W. Kao, R.-J. Chen, J.-L. Lai, and C. D. Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *Expert Systems with Applications*, vol. 38, no. 1, pp. 306 – 313, 2011.

[9] T. Shon and J. Moon, "A hybrid machine learning approach to network anomaly detection," *Information Sciences*, vol. 177, no. 18, pp. 3799 – 3821, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025507001648

[10] W.-H. Chen, S.-H. Hsu, and H.-P. Shen, "Application of SVM and ANN for intrusion detection," *Computers & Operations Research*, vol. 32, no. 10, pp. 2617–2634, 2005.

[11] H. Kholidy and F. Baiardi, "CIDS: A framework for intrusion detection in cloud systems," in *Ninth International Conference on Information Technology: New Generations (ITNG), 2012*, April 2012, pp. 379–385.

[12] W. Xiong, H. Hu, N. Xiong, L. T. Yang, W.-C. Peng, X. Wang, and Y. Qu, "Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications," *Information Sciences*, vol. 258, pp. 403–415, 2014.

[13] G. Aceto, A. Botta, W. de Donato, and A. Pescap, "Cloud monitoring: A survey," *Computer Networks*, vol. 57, no. 9, pp. 2093 – 2115, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613001084

[14] B. L. Dalmazo, J. P. Vilela, and M. Curado, "Online traffic prediction in the cloud: A dynamic window approach," in *The 2nd International Conference on Future Internet of Things and Cloud (FiCloud'2014)*, Aug 2014, pp. 9–14.

[15] A. Kind, M. Stoecklin, and X. Dimitropoulos, "Histogram-based traffic anomaly detection," *IEEE Transactions on Network and Service Management*, vol. 6, no. 2, pp. 110–121, June 2009.

[16] J. Haines, L. Rossey, R. Lippmann, and R. Cunningham, "Extending the darpa off-line intrusion detection evaluations," in *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings*, vol. 1, 2001, pp. 35–45 vol.1.

[17] P. Hick, E. Aben, K. Claffy, and J. Polterock, "The CAIDA DDoS Attack 2007 Dataset," 2007.

[18] P. Ganeshkumar and N. Pandeeswari, "Adaptive neuro-fuzzy-based anomaly detection system in cloud," *International Journal of Fuzzy Systems*, pp. 1–12, 2015.

[19] W. Xiong, H. Hu, N. Xiong, L. T. Yang, W.-C. Peng, X. Wang, and Y. Qu, "Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications," *Information Sciences*, vol. 258, pp. 403–415, 2014.

[20] Y. Liu, K.-K. Tseng, and J.-S. Pan, "Statistical based waveform classification for cloud intrusion detection," in *2012 International Conference on Computing, Measurement, Control and Sensor Network (CMCSN)*, July 2012, pp. 225–228.