A Prediction-based Approach for Anomaly Detection in the Cloud

Bruno L. Dalmazo[1,2], João P. Vilela[2], Marilia P. Curado[2]

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil

[2]CISUC, Department of Informatics Engineering
University of Coimbra – Coimbra – Portugal

{dalmazo, jpvilela, marilia}@dei.uc.pt

Abstract. *This document provides an at-a-glance view of the main contributions of my Ph.D. work. This work aims at improving security and trustworthiness of cloud computing environments by developing a model for predicting cloud network traffic, an approach for detecting anomalies in cloud network traffic that relies on traffic prediction, as well as a mechanism for aggregating similar alarms from an IDS in the context of the cloud network traffic. All the benefits and drawbacks of the contributions were demonstrated in realistic simulations using public data from real network traces. Furthermore, the evaluations were conducted with well-known metrics and the results show that all the proposed mechanisms were able to outperform similar proposals in literature.*

Resumo. *Este documento fornece uma visão geral das principais contribuições do meu trabalho de doutorado. Esse trabalho objetiva aumentar a segurança e a confiabilidade do ambiente de computação em nuvem através do desenvolvimento de um modelo para predição do tráfego de rede, uma abordagem para detectar anomalias que depende da predição do tráfego de rede, bem como um mecanismo para agregar alarmes similares oriundos de um sistema de detecção de intrusão no contexto de computação em nuvem. Os benefícios e desvantagens das contribuições foram demostrados com simulações usando dados públicos coletatos de monitorimento de redes reais. Além disso, a avaliação foi conduzida a partir de métricas conhecidas e os resultados mostram que os mecanismos propostos foram capazes de superar propostas similares na literatura.*

1. Introduction

Computer networks are present everywhere, making them a key aspect to the proper functioning of products and services that are often served exclusively through the Internet. The pervasive nature of computer networks makes them particularly suitable to attacks. Therefore, more than just functional systems, we are also looking for systems that are reliable, available, scalable and secure [Dalmazo et al. 2013].

A solution to meet the growing demands of industries and customers alike is cloud computing. Among several other advantages of this paradigm, the possibility of increased profits by reducing costs with infrastructure and software licenses, while allowing for virtually unlimited growth is particularly relevant [Dalmazo et al. 2014]. However, these advantages are many times shadowed by the increased security risks that steam from having

different entities involved, with relationships and responsibilities not properly identified. This may lead to misuse or malicious attacks against cloud computing, which may compromise sensitive information that is stored in shared third party facilities, and many open issues still prevail [Dalmazo et al. 2016a]. Due to these and other issues, it is important to devise new solutions that increase the trustworthiness of cloud computing environments and help to keep the continued growth in demand for virtualized resources. Facing this challenge, this work aims to study, analyse, propose, develop and evaluate several models and mechanisms to fill these gaps [Dalmazo et al. 2017b].

Firstly, a systematic approach for selecting a group of candidate predictors that is suitable for cloud network traffic prediction is proposed. On the basis of this scenario, a predictor model for cloud network traffic that involves a tradeoff between prediction error, historical data dependence, computational costs, and timely response is proposed [Dalmazo et al. 2017a]. Next, an Anomaly Detection System to support decision-making and counter attack malicious actions against cloud computing systems is presented [Dalmazo et al. 2015, Dalmazo et al. 2016b]. This contribution relies on network traffic prediction to obtain features that represent the expected appropriate behaviour of the cloud network traffic used jointly with a Support Vector Machine (SVM) model for detecting anomalous events in the cloud environment. Finally, a mechanism for determining the similarity level between features of the alarms is proposed. This mechanism aims to optimize the efficiency for generating alarms, decreasing the network data traffic to manage the IDS and its associated transfer costs [Dalmazo et al. 2018].

1.1. Motivation and Problem Statement

A study performed by the Carbon Disclosure Project attests that large IT companies could achieve expressive cost savings and carbon reductions by 2020 if they move their IT assets to the cloud [Baumast 2013]. This study claims that these companies could benefit from billions in savings. Furthermore, another study published in *The New York Times* [Gilmer 2011] went deeper: they estimate that companies in the U.S.A. using cloud computing can save $12.3 billion per year by 2020. In addition, these companies could make an annual reduction in carbon emissions equivalent to 200 million barrels of oil.

Cloud computing enables the adoption of a promising computing model that allows consuming a computer resource rather than having to build and hold their own computing infrastructure. However, a widespread adoption of this paradigm has been hampered by the lack of security mechanisms. For instance, it is predicted that cybercrimes will cost the world $6 trillion annually by 2021. Furthermore, 74% of Information Technology executives believe that security is the top factor that needs to be addressed to expand the use of cloud computing [Networking, CISCO Global Cloud Index 2018].

In this context, the last several years have been the most remarkable period from a cloud security threat perspective. For illustrative purposes, in 2017 there were at least two high-profile incidents involving gaming platforms. Firstly, Blizzard Entertainment reported a flood of junk traffic that caused problems for players of Overwatch and World of Warcraft. Another situation involves the UK National Lottery that was seriously damaged for being unable to place their stakes online or via applications for hours. These two organizations were victims of a Distributed Denial of Service (DDoS) performed by botnets powered by cloud infrastructures [Khalimonenko et al. 2017].

The cloud network is prone to several kinds of threats. Although some of these threats are able to leave traces, the task of identifying them is not trivial. To give an example, there are attacks that cause an anomalous behaviour in the network traffic which allows the threat to be detected. However, at the same time, the elastic and scalable nature of cloud environments makes them prone to undergo sudden changes [Ballani et al. 2011], which makes it even harder to detect which parts of the incoming traffic are caused by vandalism or are being used legitimately.

It is therefore imperative that the cloud provider monitors and analyses a huge number of devices and virtual machines (VMs). In doing so, relevant information about network traffic can be collected and used to support decision-making processes. Later, it is possible to identify and analyse suspicious network traffic patterns to prevent similar situations from occurring in the future [Dainotti et al. 2012]. This calls for network traffic predictions mechanisms that favour timely detection of issues in the network, which is particularly challenging in cloud environments due to the volume and volatility of traffic and resources available, as addressed in Chapter 3 of the thesis.

In addition to the network traffic prediction, several techniques have already been proposed to perform anomaly detection in the cloud environment, such as fuzzy logic, entropy-based, artificial neural networks and decision tree classifier. However, there is an apparent deficiency in their ability to detect anomalies when analysing a large amount of data. In particular, these techniques require extensive tuning to improve their sensitivity to 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 improve the accuracy of anomaly detection for cloud environments while reducing false-positive detection rates, as addressed in Chapter 4 of the thesis.

A further aggravating factor is regarding to the number of alarms generated. Alarm management approaches have been proposed in the literature such as alarm correlation, regular expression matching and clustering alarms. However, these works are more concerned with increasing the number of true alarms. As a result, they fail to meet a low number of false alarms as well as decreasing the number of control messages in general. To make matters worse, it is known that around 99% of the alarms are false both in cloud computing [Patel et al. 2013] and in traditional environments [Hubballi and Suryanarayanan 2014]. The wide disparity between the true and false alarms generated has certainly compromised the performance of IDS. From this, two significant problems arise, as addressed in Chapter 5 of the thesis: the huge volume of control messages between the VMs and the servers and the associated transfer costs.

1.2. Objectives and Contributions

The goal of the thesis is to enhance security aspects of the cloud computing environment by addressing security aspects including areas such as network traffic prediction models, intrusion detection systems and methodologies for aggregating alarms. This task brings attention for specific activities, for instance, characterization of the needs, design new solutions, implement and evaluate such proposals.

In particular, the thesis contains a comprehensive analysis of the state of the art in these fields in order to identify and mitigate numerous open issues. The proposed solutions were evaluated by using traces from real network operations. In addition, the

entire methodology presented in the thesis allows a systematic comparison of results from a general perspective among several research efforts found in the literature. The specific goals of the thesis are as follows:

Goal 1 – Proposing a new network traffic prediction model and a methodology for selecting and evaluating a set of prediction models that is suitable for the highly dynamic cloud computing environment;

Goal 2 – Extracting features that represent the expected appropriate behaviour of the cloud network traffic, then used jointly with a Support Vector Machine (SVM) for detecting anomalous events in the cloud environment;

Goal 3 – Grouping similar alarms that may correspond to the same attack (or attack attempt) in order to optimize the efficiency for generating alarms, decreasing the network data traffic to manage an IDS and its associated transfer costs.

Taking the specific goals into consideration, the thesis has succeeded in producing the follow main contributions:

Contribution 1 – Poisson Moving Average Model (PMA): A moving average approach based on the Poisson distribution is proposed and used to determine the probable minimum and maximum number of transactions that can occur within a given time period, from a series of discrete values.

Contribution 2 – Dynamic Window Size Algorithm (DyWiSA): To reduce the complexity of predicting network traffic, time-bounded past information is considered by means of a sliding window with size defined by the DyWiSA, which makes it suitable for online prediction in a cloud computing context.

Contribution 3 – Feature Extraction Approach: Feature extraction uses multiple temporal layers of data for feature extraction so that it can express data in a compact representation by removing redundancy.

Contribution 4 – Anomaly Detection Mechanism: The purpose of this mechanism is to provide an efficient method to detect anomalies in cloud-based network traffic. This mechanism works on the basis of a SVM and prediction of the network traffic.

Contribution 5 – Triple-Similarity Mechanism (T-SyM): This mechanism aims to group similar alarms that may correspond to the same attack to reduce the number of messages sent from the VMs to the servers.

Contribution 6 – Severity Adjustment of Alarms Algorithm: It allows to analyse the output of the T-SyM in order to seeking for alarms and classifies them according to a database. Then, the algorithm assigns a level of severity.

The remainder of this paper points out the key outcomes of the thesis. Section 2 presents an analysis mechanism for evaluating network traffic predictors in the cloud. Section 3 details a mechanism that combines SVM with features extracted from a PMA predictor, whilst Section 4 presents a systematic approach for aggregating similar alarms. Section 5 concludes with some final remarks and potential directions for future research.

2. Network Traffic Prediction in the Cloud

This section alludes to Chapter 3 on the thesis that presents the state of the art and a taxonomy for network traffic prediction models, as well as an analysis mechanism that provides a standardized approach for evaluating network traffic predictors based on global and local data analysis. The outcomes of this mechanism enable the performance comparison

of several predictors in the cloud, particularly in terms of accuracy, historical dependency, time and computational overhead. Figure 1 depicts the steps of the mechanism, by highlighting its main conceptual components, the personnel involved, and their interactions.

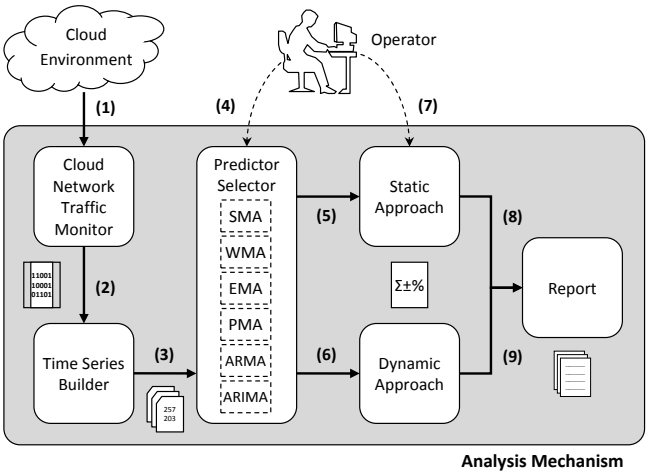

Figure 1. Elements of the proposed mechanism and interactions

From the observation of the evaluation, it can be seen that all the predictions based on local analysis present a considerable improvement after using the DyWiSA. The accuracy of the all traffic predictors considered, have been increased from 6% up to 495.51% (Normalized Mean Square Error) 7% up to 101.21% (Mean Absolute Percent Error). Furthermore, besides the good results, the Poisson Moving Average has maintained the same computational complexity of the predictor models assessed in the thesis. Considering a dataset with traffic from a diverse set of common cloud services, the ARIMA model shows a slight advantage over the other predictors in terms of accuracy. However, this is achieved at the cost of high computational complexity and time consumption. Poisson Moving Average, which is more attractive due to its lower computational complexity, has shown itself to be more suitable for dynamic cloud environments than the other predictor models assessed. The outcomes of this chapter include the following publications:

- Dalmazo, Bruno L. **"Abordagem dinâmica para cálculo de tamanho de janelas deslizantes através da variância teórica máxima"**, registration date: 22/01/2019, Patent: Computer Program. Register number: BR512019000076-5, Registration institution: INPI - Instituto Nacional da Propriedade Industrial
- Dalmazo, Bruno L. and Vilela, João P. and Curado, Marilia, **"Performance Analysis of Network Traffic Predictors in the Cloud"**, Journal of Network and Systems Management, vol. 25, 2, pp. 290-320, Springer, 2017. Impact factor: 1.75
- Dalmazo, Bruno L. and Vilela, João P. and Curado, Marilia, **"Online Traffic Prediction in the Cloud"**, International Journal of Network Management, vol. 26, 4, pp. 269-285, John Wiley & Sons, 2016. Impact factor: 1.34
- Dalmazo, Bruno L. and Vilela, João P. and Curado, Marilia, "**Online Traffic Prediction in the Cloud: A Dynamic Window Approach**", in The 2nd International Conference on Future Internet of Things and Cloud, 2014
- Dalmazo, Bruno L. and Vilela, João P. and Curado, Marilia, "**Predicting Traffic in the Cloud: A Statistical Approach**", in IEEE International Conference on Cloud and Green Computing, 2013

3. Anomaly Detection for Cloud Network Traffic

This section point out Chapter 4, where an attempt has been presented to shed light on the main obstacle to the adoption of the cloud service models: the lack of security. To address this problem, an approach to detect anomalies in the cloud scenario was proposed. This work differs from previous anomaly detection techniques since it relies on a collaborative mechanism that combines a SVM model with features extracted from a Poisson Moving Average predictor. Figure 2 depicts the basis of the mechanism, by highlighting the application scenario and the main conceptual components.

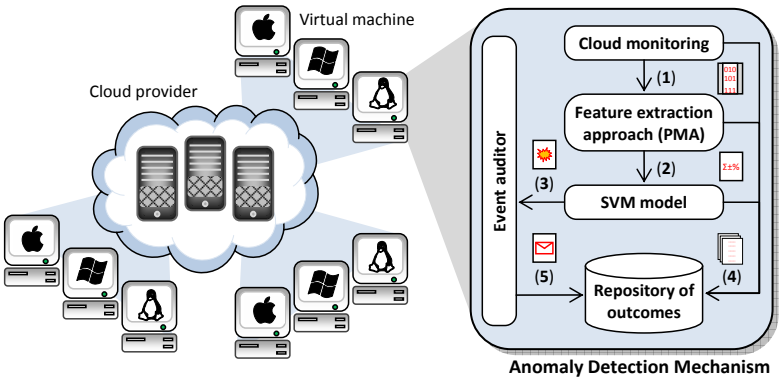

Figure 2. Application scenario and elements of the proposed mechanism

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. In comparison with other approaches, the SVM model achieved a high degree of accuracy. In particular, the best level of detection rate (98.56%) and the second best number of false negative rates were achieved (8%). The sensitivity analysis has shown the tradeoff between the time granularity and the accuracy of the model, showing that the scheme performs accurate detection within a short time-frame. Finally, it is worth pointing out that the 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. This chapter resulted in the following papers:

- Dalmazo, B. L. and Vilela J. P. and Curado M., "**Security and Trustworthiness in Cloud Computing**", in Meeting with Science and Technology in Portugal, 2017
- Dalmazo, B. L. and Vilela J. P. and Simões, P. and Curado M., "**Expedite Feature Extraction for Enhanced Cloud Anomaly Detection**", in NOMS - IEEE/IFIP Network Operations and Management Symposium, 2016
- Dalmazo, B. L. and Vilela J. P. and Curado M., "**A SVM Model based on Network Traffic Prediction for Detecting Anomalies**", in 21th edition of the Portuguese Conference on Pattern Recognition, 2015

4. Triple-Similarity Mechanism for Alarm Management

This section refers to Chapter 5, where the main issues generated by IDS for cloud computing are presented. For instance, the huge number of alarms generated over time and how this impacts on the number of control messages between VMs and servers. To address these problems, the Triple-Similarity Mechanism (T-SyM), a systematic approach for aggregating similar alarms in the context of the cloud network traffic and an algorithm

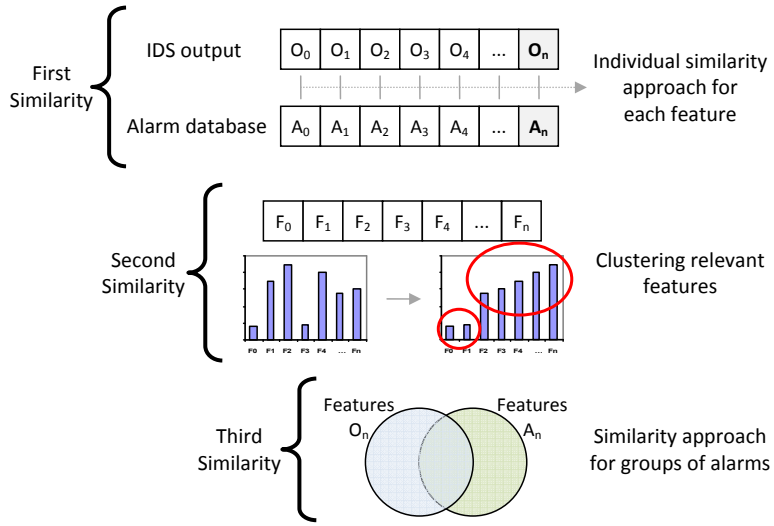

Figure 3. The triple-similarity mechanism

to assign severity level for alarms were proposed. Figure 3 illustrates the *First Similarity*, the *Second Similarity* and the *Third Similarity*.

From the observation of the evaluation, we can see that the mechanism was able to (*i*) reduce the generation of alarms by from 73% to 90% and; (*ii*) decrease the network data traffic to manage IDS and its associated transfer costs by more than 80%. Moreover, aggregating similar alarms produces fewer alarms but with higher levels of severity, supporting the network traffic monitoring of the cloud providers. The outcomes of this chapter generated the following journal:

- Dalmazo, Bruno L. and Vilela, João P. and Curado, Marilia, **"Triple-Similarity Mechanism for Alarm Management in the Cloud"**, Computers & Security, vol. 78, pp. 33-42, Elsevier, 2018. Impact factor: 2.65

5. Conclusions and Future Work

Cloud computing presents an impressive potential to provide rapid access to flexible and low cost IT resources on the fly, over the Internet. However, these benefits are subject to be harmed by the failure to guarantee an appropriate level of security when using cloud services, resulting in higher costs and potential loss of business.

The main contributions of the thesis are as follows. Firstly, a network traffic prediction model was proposed, that is suitable for the highly dynamic cloud computing environment. Secondly, an approach for extracting features based on the network traffic prediction model jointly with a SVM in order to detect anomalies in the cloud network traffic. Finally, a similarity approach to aggregate alarms that may correspond to the same attack for minimizing generation of alarms, thus decreasing the network data traffic and its associated transfer costs.

Nevertheless, there are still several aspects that need further work and could be addressed in the future including, but not limited to, evaluating the prediction models in other scenarios, extending the anomaly detection model so that it can cover other areas not initially envisaged and implementing these mechanisms in a real environment including the launching of real attacks against the network.

References

Ballani, H., Costa, P., Karagiannis, T., and Rowstron, A. (2011). Towards predictable datacenter networks. In *Proceedings of the ACM SIGCOMM 2011 Conference (SIGCOMM'11)*, volume 41, pages 242–253.

Baumast, A. (2013). *Carbon Disclosure Project. Encyclopedia of corporate social responsibility*, volume 21. Springer Berlin Heidelberg.

Dainotti, A., Pescape, A., and Claffy, K. (2012). Issues and future directions in traffic classification. *Network, IEEE*, 26(1):35–40.

Dalmazo, B. L., Vilela, J. P., and Curado, M. (2013). Predicting Traffic in the Cloud: A Statistical Approach. In *Third International Conference on Cloud and Green Computing (CGC'13), 2013*, pages 121–126.

Dalmazo, B. L., Vilela, J. P., and Curado, M. (2014). Online Traffic Prediction in the Cloud: A Dynamic Window Approach. In *The 2nd International Conference on Future Internet of Things and Cloud (FiCloud'2014)*, pages 9–14.

Dalmazo, B. L., Vilela, J. P., and Curado, M. (2015). A SVM Model based on Network Traffic Prediction for Detecting Anomalies. In *21th edition of the Portuguese Conference on Pattern Recognition*.

Dalmazo, B. L., Vilela, J. P., and Curado, M. (2016a). Online Traffic Prediction in the Cloud. *International Journal of Network Management*, 26(4):269–285.

Dalmazo, B. L., Vilela, J. P., and Curado, M. (2017a). Performance Analysis of Network Traffic Predictors in the Cloud. *Journal of Network and Systems Management*, 25(2):290–320.

Dalmazo, B. L., Vilela, J. P., and Curado, M. (2017b). Security and trustworthiness in cloud computing. In *Meeting with Science and Technology in Portugal*.

Dalmazo, B. L., Vilela, J. P., and Curado, M. (2018). Triple-Similarity Mechanism for Alarm Management in the Cloud. *Computers & Security - Elsevier*, 78:33–42.

Dalmazo, B. L., Vilela, J. P., Simoes, P., and Curado, M. (2016b). Expedite Feature Extraction for Enhanced Cloud Anomaly Detection. In *IEEE/IFIP Network Operations and Management Symposium (NOMS'16)*, pages 1215–1220.

Gilmer, E. M. (2011). Is There a Silver Lining for the Environment in Cloud Computing? *The New York Times*, 10 August.

Hubballi, N. and Suryanarayanan, V. (2014). False alarm minimization techniques in signature-based intrusion detection systems: A survey. *Computer Communications*, 49:1–17.

Khalimonenko, A., Kupreev, O., and Ilganaev, K. (2017). DDoS attacks in Q3 2017. Securelist.com. {Online resource} Available at: https://securelist.com/ddos-attacks-in-q3-2017/83041/. [Accessed 20/03/18].

Networking, CISCO Global Cloud Index (2018). Cisco Global Cloud Index: Forecast and Methodology, 2016-2021 White Paper.

Patel, A., Taghavi, M., Bakhtiyari, K., and Junior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*, 36(1):25–41.