Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Malware Detection in Cloud Computing Infrastructure

G. Swathi
Department of Computer Science & Engineering,
NS Raju Institute of Technology,
Visakhapatnam, Andhra Pradesh-531173, India.

L.V.Krishna Sai
Department of Computer Science & Engineering,
NS Raju Institute of Technology,
Visakhapatnam, Andhra Pradesh-531173, India.

P.B.M.G.B.Kumar
Department of Computer Science & Engineering,
NS Raju Institute of Technology,
Visakhapatnam, Andhra Pradesh-531173, India.

T.V.S.Sriram
Department of Computer Science & Engineering,
NS Raju Institute of Technology,
Visakhapatnam, Andhra Pradesh-531173, India.

Abstract
Cloud services are prominent within the private, public and commercial domains. Many of these services are expected to be always on and have a critical nature; therefore, security and resilience are increasingly important aspects. In order to remain resilient, a cloud needs to possess the ability to react not only to known threats, but also to new challenges that target cloud infrastructures. In this paper we introduce and discuss an online cloud anomaly detection approach, comprising dedicated detection components of our cloud resilience architecture. More specifically, we exhibit the applicability of novelty detection under the one-class support Vector Machine (SVM) formulation at the hypervisor level, through the utilization of features gathered at the system and network levels of a cloud node. We demonstrate that our scheme can reach a high detection accuracy of over 90 percent whilst detecting various types of malware . Finally, the paper shows that our approach to detection using dedicated monitoring components per Virtual Machines (VM) is particularly applicable to cloud scenarios and leads to a flexible detection system capable of detecting new malware strains with no prior knowledge of their functionality or their underlying instructions.

Keywords:
Malware Detection, Security, Resilience and Protection.

1. Introduction
Cloud datacenters are beginning to be used for a range of always-on services across private, public and commercial domains. These need to be secure and resilient in the face of challenges that include cyber attacks as well as component failures and mis-configurations[1-2]. However, clouds have characteristics and intrinsic internal operational structures that impair the use of traditional detection systems. In particular, the range of beneficial properties offered by the cloud, such as service transparency and elasticity, introduce a number of vulnerabilities which are the outcome of its underlying virtualized nature[3-5]. Moreover, an indirect problem lies with the cloud's external dependency on IP networks, where their resilience and security has been extensively studied, but nevertheless remains an issue [6-8]. The approach taken in this paper relies on the principles and guidelines provided by an existing resilience framework [9-10]. The underlying assumption is that in the near future, cloud infrastructures will be increasingly subjected to novel attacks and other anomalies, for which conventional signature based detection systems will be insufficiently equipped and therefore ineffective.

Cite this article as: G. Swathi, T.V.S.Sriram, P.B.M.G.B.Kumar & L.V.Krishna Sai, "Malware Detection in Cloud Computing Infrastructure", International Journal of Research in Advanced Computer Science Engineering, Volume 4, Issue 10, 2019, Page 31-37.

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Moreover, the majority of current signature-based schemes employ resource intensive deep packet inspection (DPI) that relies heavily on payload information where in many cases this payload can be encrypted, thus extra decryption cost is incurred [11]. Our proposed scheme goes beyond these limitations since its operation does not depend on a-priori attack signatures and it does not consider payload information, but rather depends on per-flow meta-statistics as derived from packet header and volumetric information (i.e. counts of packets, bytes, etc.) [12-13]. Nonetheless, we argue that our scheme can synergistically operate with signature-based approaches on an online basis in scenarios were decryption is feasible and cost-effective. Overall, it is our goal to develop detection techniques that are specifically targeted at the cloud and integrate with the infrastructure itself in order to, not only detect, but also provide resilience through remediation.

2. System analysis

2.1 Existing system

Cloud computing is an increasingly popular platform for both industry and consumers. The cloud presents a number of unique security issues, such as a high level of distribution and system homogeneity, which require special consideration. In the proposed system, the system introduces a resilience architecture consisting of a collection of selforganising resilience managers distributed within the infrastructure of a cloud. More specifically we illustrate the applicability of our proposed architecture under the scenario of malware detection. The system describes our multi-layered solution at the hypervisor level of the cloud nodes and considers how malware detection can be distributed to each node.

2.1.1 Limitations of the Existing System

1. The existing cloud servers cant able to access the data in a encrypted manner rather than they are stored directly in a plain text manner.
2. All the data which is stored inside the cloud server will be directly stored into the server space despite of verifying the presence of any malware or virus content inside it.
3. There is no technique to automatically identify the presence of malware content inside the documents which is going to be uploaded or downloaded.
4. There is no proper technique in the existing cloud server or service providers to block the malware content files not to downloaded for the end users.And there is no concept like Support Vector Machine (SVM) technique integrated with the cloud server for finding the presence of data storage inside the cloud server.

2.2 Proposed system

The elements presented here form the basis in which different detection techniques can be hosted and fur the allow the identification and attribution of anomalies. In this paper we discuss the detection of anomalies using a novelty detection approach that employs the one-class Support Vector Machine (SVM) algorithm and demonstrate the effectiveness of detection under different anomaly types. More specifically, we evaluate our approach using malware and Denial of Service (DoS) attacks as emulated within a controlled experimental test-bed. The malware samples used are Kelihos and multiple variants of Zeus.

2.2.1 Advantages of the Proposed System:

1. The proposed cloud servers can able to access the data in a encrypted manner rather than in a plain manner.
2. All the data which is stored inside the cloud server will be directly stored into the server space and they will be verified by the cloud server if there are any malware content available in that file.
3. This proposed SVM integrated cloud computing technique can automatically identify the presence of malware content inside the documents which is going to be uploaded or downloaded.

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

4. The proposed technique can block the malware content files not to downloaded for the end users.

3. SYSTEM SPECIFICATION

3.1 SYSTEM REQUIREMENTS:

3.1.1 HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz. Or More Configuration
- Hard Disk : 40 GB.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 1 GB.

3.1.2 SOFTWARE REQUIREMENTS:

- Operating system : Windows XP/7.
- Coding Language : JAVA/J2EE
- IDE : Eclipse -- Galileo
- Database : MYSQL

3.1.3 FUNCTIONAL REQUIREMENTS:

Functional requirements describe what the system should do, i.e. the services provided for the users and for other systems.

INPUT

- The service provider tries to register first into the application.
- The end user try to register into the application.
- The service provider try to login into its account for uploading files into the cloud server.
- The end user try to login into their account with the valid credentials.
- The cloud server need to activate the service providers and end users who got recently registered into the application.
- The service provider try to upload the file into the cloud server.
- The cloud server identifies the malicious file inside the storage server.

OUTPUT

- The Service Provider gets an output window as" Service provider Registered Successful"
- The End user gets an output window as" End User Registered Successful"
- The End User gets an output window as" End User Login Successful"
- The Service Provider gets an output window as" File Uploaded Successful"
- The Cloud Server gets an output window as" Malicious File Found in the Server"
- The Cloud gets an output window as" Block Malicious Files"
- The End User gets an output window as" Data Decrypted and Viewed Successful"

DATA STORAGE

- Here we use MY Sql as back end so we use a GUI tool like Heidi sql as back end for implementing the current application with easy of use. application.Here we use MY-SQL as back end data base that is due to because of various advantages,they are as follows:
- It has featured like auto commit.
- It is GUI in nature (Common line Interface).
- It occupies very size for installation.
- It is cross platform in nature

3.1.4 Non Functional Requirements

In non-functional requirements the following are the things that come under .They are as follows:

- **Reusability:** As we developed the application in java, the application can be re-used for any one without having any restrictions in its usage. Hence it is re-Usable.
- **Portability:** As the application is designed with java as programming language, we know java can be run on any operating system. Hence the application is portable to run on any operating system.
- **Extensibility:** The application can be extended at any level if the user wish to extend that in future

Volume No:4, Issue No:10 (March-2019)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

this is done because java is a open source medium which doesn't have any time limits for expiry or renewal.

3.2 SYSTEM STUDY

3.2.1 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

4. OUTPUT SCREENS

FIG. 1 Home page

FIG .2 Registration page Of Service Provider

FIG. 3 Registration Successful page

FIG. 4 Cloud server Login page

FIG. 5 service provider list

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

FIG. 6 Enduser list

FIG. 7 Service Provider login

FIG. 8 File Uploading page

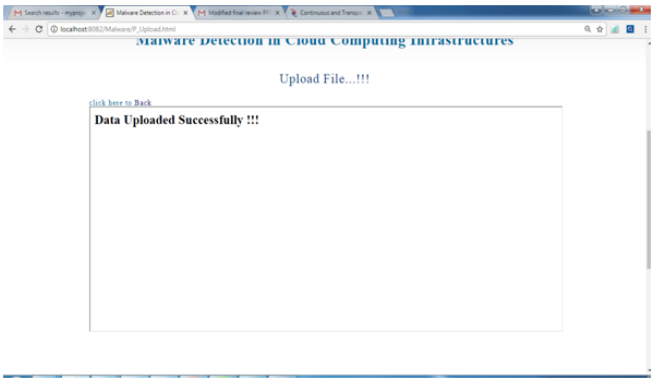

FIG. 9 Uploading file successfully page

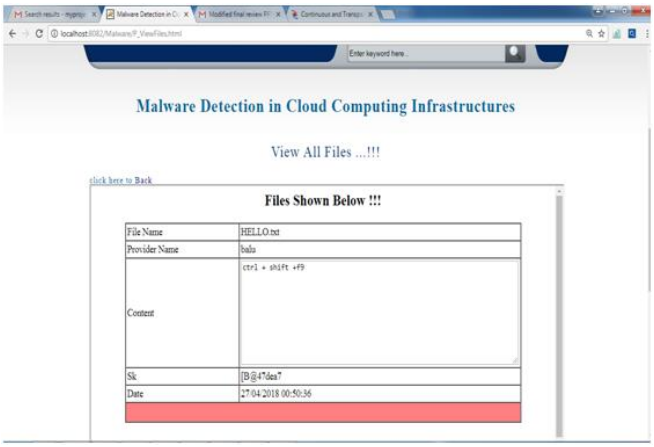

FIG. 10 File list

5. Conclusion

In this paper we introduce an online anomaly detection method that can be applied at the hypervisor level of the cloud infrastructure. The method is embodied by a resilience architecture that was initially defined in [4], further explored in [11], [12] and which comprises the System Analysis Engine (SAE) and Network Analysis Engine (NAE) components. These exist as submodules of the architecture's Cloud Resilience Managers (CRMs), which perform detection at the end-system, and in the network respectively. Our evaluation focused on detecting anomalies as produced by a variety of malware strains from the Kelihos and Zeus samples under the formulation of a novelty detector that employs the one-class Support Vector Machine (SVM) algorithm. Moreover, in order to empower the generic properties of our detection approach we also

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

assess the detection of anomalies by the SAE and NAE during the onset of DoS attacks.

6. REFERENCES

[1] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "Bothunter: Detecting malware infection through ids-driven dialog correlation," in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, ser. SS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 12:1–12:16. [Online]. Available: http://dl.acm.org/citation.cfm?id=1362903. 1362915

[2] M. Bailey, J. Oberheide, J. Andersen, Z. Mao, F. Jahanian, and J. Nazario, "Automated classification and analysis of internet malware," in Recent Advances in Intrusion Detection, ser. Lecture Notes in Computer Science, C. Kruegel, R. Lippmann, and A. Clark, Eds. Springer Berlin Heidelberg, 2007, vol. 4637, pp. 178–197. [Online]. Available: http://dx.doi.org/10. 1007/978-3-540-74320-0 10

[3] B.Hay and K. Nance, "Forensics examination of volatile system data using virtual introspection," SIGOPS Oper. Syst. Rev., vol. 42, no. 3, pp. 74–82, Apr. 2008. [Online]. Available: http://doi.acm.org/10.1145/1368506.1368517

[4] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 41, no. 3, p. 15, 2009.

[5] L. Kaufman, "Data security in the world of cloud computing," Security Privacy, IEEE, vol. 7, no. 4, pp. 61–64, July 2009.

[6] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, and D. Zamboni, "Cloud security is not (just) virtualization security: A short paper," in Proceedings of the 2009 ACM Workshop on Cloud Computing Security, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 97–102. [Online]. Available: http://doi.acm.org/10.1145/1655008.1655022

[7] S.Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in Dependable, Autonomic and Secure Computing, 2009.DASC '09. Eighth IEEE International Conference on, Dec 2009, pp. 729–734.

[8] Y. Chen, V. Paxson, and R. H. Katz, "Whats new about cloud computing security?" EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2010-5, Jan 2010. [Online]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/ EECS-2010-5.html

[9] J. P. G. Sterbenz, D. Hutchison, E. K. C¸ etinkaya, A. Jabbar, J. P. Rohrer, M. Sch¨ oller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," Comput. Netw., vol. 54, no. 8, pp. 1245–1265, Jun. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet. 2010.03.005

[10] N. Gruschka and M. Jensen, "Attack surfaces: A taxonomy for attacks on cloud services," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, July 2010, pp. 276–279.

[11] H. Binsalleeh, T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, and L. Wang, "On the analysis of the zeus botnet crimeware toolkit," in Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on, Aug 2010, pp. 31–38.

[12] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network ids into an open source cloud computing environment," in Information Assurance and Security (IAS), 2010 Sixth International Conference on, Aug 2010, pp. 265–270.

[13] A. Marnerides, C. James, A. Schaeffer, S. Sait, A. Mauthe, and H. Murthy, "Multi-level network

Volume No:4, Issue No:10 (March-2019)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

resilience: Traffic analysis, anomaly detection and simulation," ICTACT Journal on Communication Technology, Special Issue on Next Generation Wireless Networks and Applications, vol. 2, pp. 345–356, June 2011.