ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

A Novelty Detection Based on SVM for Malicious File Detection in Cloud Computing Infrastructure

Sandeep H[1], Dr.B.K.Raghavendra[2]

Research Scholar, VTU Belagavi, Department of Computer Science and Engineering, K.S.School of Engineering and Management, Bengaluru, Karnataka,India[1]

Professor and Head, Department of Computer Science and Engineering, K.S.School of Engineering and Management, Bengaluru, Karnataka, India[2]

ABSTRACT:Cloud services are prominent within the private, public and commercial domains. Many of these services are expected to always 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. A detection approach, comprising detection components of the cloud resilience architecture has been implemented. More specifically, the applicability of novelty detection under the Support Vector Machine (SVM) is exhibited. It is a secure and resilient in the face of challenges that include file attacks. 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. . In order to empower the generic properties of our detection approach a secret key generation is implemented using RSA algorithm. It offers reasonable security, usability and fits well with some practical applications for improving the detection. From the experimental results it is observed that SVM improves the overall efficiency of the system and detects the malicious file.

KEYWORDS:Cloud services, transparency, Security, Resilience, Support vector machine.

I. INTRODUCTION

Cloud computing is currently one the leading innovations. Most IT companies have their own cloud computing technologies. Though cloud is still a budding technology it possesses a lot of risk to threats. In the nearest future, cloud will have to undergomany more security exploitation events around cloud computing providers and users, which will lead to many researches on cloud computing security in the next decade. Hence, there has been a rapid change and growth in cloud computing security discipline, with ongoing efforts to cope with the requirements and capabilities regarding privacy and security issues.

The security mechanism aims to improve and adjust the performance of traditional Intrusion Detection Systems (IDS), under signature rule-based strategies which performs Deep Packet Inspection (DPI) on network packets. It monitors system-related features on the Virtual Machine (VM) using Virtual Machine Introspection (VMI) methods in order to analyse and detect threats on the VM Operating System (OS). Outcomes derived by the expert research, aimed to develop a detection strategy that considers both system and network information as seen on each VM. Majority of the used rule based detection policies that depend on pre-defined signatures. Hence, the ability of adapting to new types of anomalies, which usually appear in cloud environments, is extremely limited.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

In machine learning SVMs are called as supervised learning models which is associated with learning algorithms and that is used for classification and analysis of data. For a set of training samples each sample is marked as belonging to one or the other of two categories.SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier. SVM model is a representation, where the input is plotted as points in space, and is mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall. In case of performing linear classification, SVMs can efficiently perform a non-linear classification using what is called the kernel trick that implicitly maps their inputs into high-dimensional feature spaces.

A support vector machine constructs a hyper plane or set of hyper planes in a high- or infinite-dimensional space, which can be used for classification, regression, or other tasks. Intuitively, a good separation is achieved by the hyper plane that has the largest distance to the nearest training-data point of any class (so-called functional margin), in general the larger the margin the lower the generalization error of the classifier.

The work in this paper is divided in three stages.

1) A Frame work is designed on cloud resilience architecture using SVM.
2) Cloud resilience is implemented using virtualization and cloud technologies.
3) Efficiency of the proposed model is evaluated using SVM.

The Paper is organized as follows. Section II describes the related work on anomaly and malicious detection .Section III describes the cloud server and end user. Section IV presents experimental resultsof malicious affected files. Finally, Section V presents conclusion.

II. RELATED WORK

True identification of a file format is a tedious task. There are catalogues containing several thousand of known file types, without having any global standard for the file types. File type detection methods can be categorized into three kinds: extension-based, magic bytes-based and content-based methods, each of them has its own strengths and weaknesses, and none of them are comprehensive or fool proof enough to satisfy all the requirement secure. A number of studies have addressed aspects of cloud security fromdifferent viewpoints (e.g. the network, hypervisor, guest VMand Operating System) under various approaches derived either from traditional rule-based Intrusion DetectionSystems (IDSs) or statistical anomaly detection models.

Anomaly detection is an important problem that has been researched within diverse research areas and application domains; it refers to the problem of finding patterns in data that do not conform to expected beta. Many anomaly detection techniques have been specifically developed for certain application domains, while others are more generic. The existing techniques have been grouped into different categories based on the underlying approach adopted by each technique. For each category, key assumptions have been identified, which are used by the techniques to differentiate between normal and anomalous behaviour. At an abstract level, an anomaly is denied as a pattern that does not confirm to expected normal behaviour [1].

Distributed model of cloud makes it vulnerable and prone to sophisticated distributed intrusion attacks like Distributed Denial of Service (DDoS) and Cross Site Scripting (XSS). To handle large scale network access traffic and administrative control of data and application in cloud, a new multi-threaded distributed cloud IDS model has been proposed. A multi-threaded cloud IDS model is proposed which can be administered by a third party monitoring service for a better optimized efficiency and transparency for the cloud user [2].

Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

another concern of cloud security. Combining the contemporary and historical viewpoints, many cloud computing security problems are not in fact new, but often will still require new solutions in terms of specific mechanisms. Existing contemporary works already explore many pertinent topics. One possible approach would be to formulate the security primitives around defending different stakeholders against different particular threat models [3].

III. IMPLEMENTATION

Cloud Server

Cloud Server provides authentication permission to the Service Provider and to the End User and saves the login details. When the Service Provider uploads a malicious file, the Cloud Server sends an alert message to the Service Provider, and when the End User tries to download that malicious file, the Cloud Server will prevent it from downloading the malicious file. Cloud server also lists the End Users who upload malicious file in the cloud.

The different activities that are performed on cloud server are as follows:

- Admin Profile (Add, Edit).
- Account Details (Add, Provides authentication, Edit, Delete).
- When cloud server receives a login request from the Service Provider and End User, it checks the profile by doing loginauthentication process.
- Login details (Add, Save, Edit).
- Saves the login details of Service Provider and End User.
- Sends alert message.

Cloud Server and End User

Service Provider sends login request to the cloud server. After it receives login authentication, the service provider can view the files in the cloud server and can also upload files. Service provider receives an alert message from the cloud server if the uploaded file has malicious content.

End User sends the login request to the Cloud Server. When it receives the authentication permission, the End User can view and can also download the files. End user has the privilege of passing a query to make a search request. If the requested file has malicious content, the file cannot be viewed after downloading.

The different activities that are performed on cloud server and End user are as follows:

- End User sends a login request to the Cloud Server.
- Cloud Server registers the end users based on the credentials provided, enabling the end users to login to the system.
- End user has the following functionalities such as viewing the uploaded file, and downloading the required file. End user has the privilege of passing a query to make a search request. Prior to downloading the file a secret. key with RSA encryption is sent to the end user by the cloud server.
- End user receives the secret key using which downloading of file is done.
- If the requested file has malicious content, thenthe file cannot be viewed after downloading.

IV. EXPERIMENTAL RESULTS

The Experiments carried out are in the context of an overall cloud resilience architecture under the implementation of SVMs.A novelty detection implementation allows the adaptive SVM-specific parameter estimation for providing better detection accuracy benefits. The resulting experimental findings shows that a malicious content can be effectively

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

detected online, with minimal cost and explicitly address the aspect of malicious file detection in cloud-oriented scenarios as performed by the cloud providers.

Theexperimental results are shown in Figure 1. (a) and (b), where Figure 1(a) shows the malicious contents and figure 1(b) shows an alert message to the end user.The Pie chart in Figure 2 shows the number of malicious affected and malicious free files.

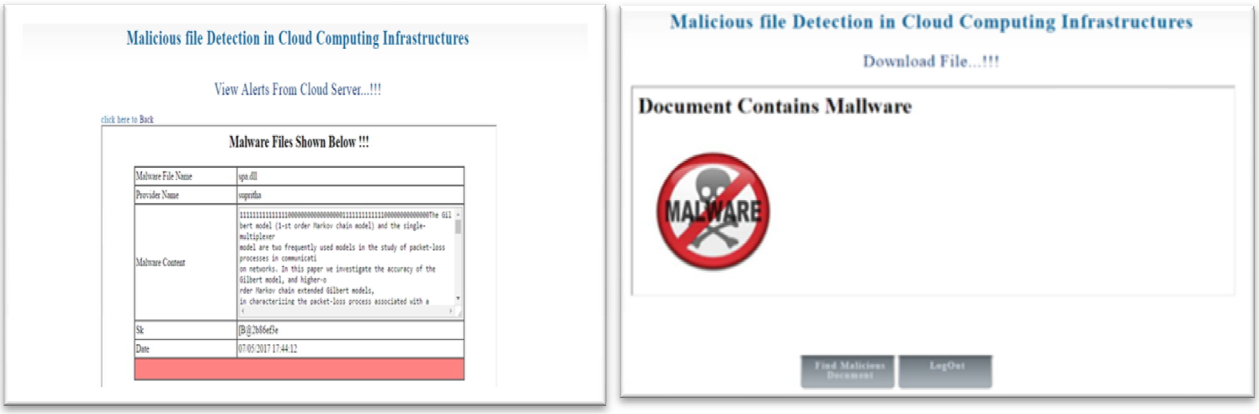

Figure1. Experimental results: a) Malicious file contents b) Warning message

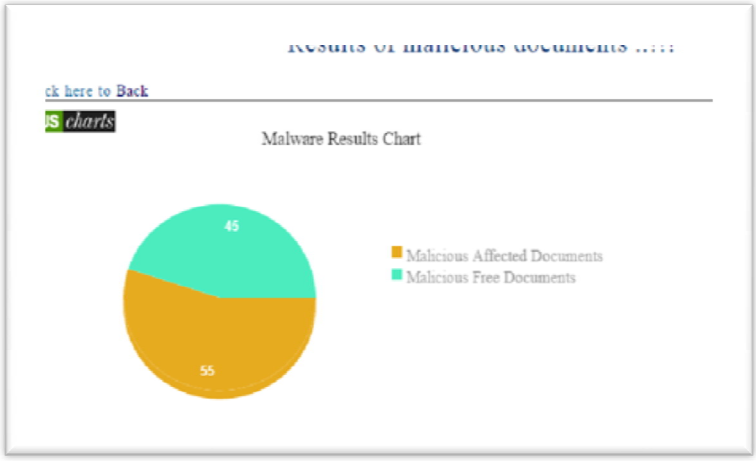

Figure 2.Pie chart depicting malicious affected files

V. CONCLUSION

The proposed novelty detector is a new detection technique which helps in the detection of the malicious file. The architecture of SVM consists of vectors and graph, whichadopts a novelty method of detecting malicious content in a file. In order to empower the generic properties of our detection approach a secret key generation is implemented using

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

RSA algorithm. It offers reasonable security, usability and fits well with some practical applications for improving the detection. Novelty detector hence reduces the probability of downloading the malicious document and provides an estimation of malicious file and non-malicious file

The novelty detector currently detects if the uploaded file is malicious or not, however in the future further enhancement can be made, such that it detects the malicious file and not let it be uploaded. The novelty detector can be made to detect wide variety of malicious file, overcoming the current limitation also; security of the system can be increased by making the system more efficient.

REFERENCES

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

[2] 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.

[3] 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

[4] A. K. Marnerides, M. R. Watson, N. Shirazi, A. Mauthe, and D. Hutchison, "Malware analysis in cloud computing: Network and system characteristics," IEEE Globecom 2013, 2013.

[5] M. R. Watson, N. Shirazi, A. K. Marnerides, A. Mauthe, and D. Hutchison, "Towards a distributed, self-organizing approach to malware detection in cloud computing," 7th IFIP/IFISC IWSOS, 2013.

[6] M. Garnaeva, "Kelihos/Hlux Botnet Returns with New Techniques." Securelist http://www.securelist.com/en/blog/655/ KelihosHlux botnet returns with new techniques.

[7] 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.

[8] T. Brewster, "GameOver Zeus returns: thieving malware rises a month after police actions," Guardian Newspaper, 11, July, 2014, http://www.theguardian.com/technology/2014/jul/ 11/gameover-zeus-criminal-malware-police-hacking.

[9] A. K. Marnerides, P. Spachos, P. Chatzimisios, and A. Mauthe, "Malware detection in the cloud under ensemble empirical model decomposition," in Proceedings of the 6th IEEE International Conference on Networking and Computing, 2015.

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