

Detection of Malware in Cloud Computing using Sparse Autoencoders

Doddi Srilatha

School of Computing & Information Technology,
REVA University, Bengaluru, India,
doddisrilatha@gmail.com

Gopal Krishna Shyam

School of Computing & Information Technology,
REVA University, Bengaluru, India,
gopalkrishnashyam@reva.edu.in

Abstract: *Cloud computing is a most inclining world view that gives conveyance of physical and intelligent assets as administrations over the Internet on request. Numerous malwares focus at customized personal computers (PCs) in cloud condition to obtain secret data and obstacle the cloud appropriation by organizations and clients. In this paper, we consider a way to deal with shielding the cloud from being assaulted by nearby PCs. Because of this issue, in view of the Windows Application Programming Interface (API) calls are removed from the Portable Executable (PE) files, we propose a novel Behavior-based Machine Learning Framework (BMLF) using Sparse Autoencoder (SpAE) which is worked in cloud stage for detection of malware. In the proposed BMLF, first we develop conduct graphs to give effective data of malware practices utilizing extricated through. We at that point utilize SpAEs for removing elevated level highlights from conduct graphs. The layers of SpAEs are embedded in a steady progression and the last layer is associated with an additional classifier. The design of SpAEs is 5,000-2,000-1000. The experimental results show that the proposed BMLF yields the semantics of more elevated level noxious practices and increments the normal detection accuracy by 2%.*

Keywords: *Cloud Computing; Malware Detection; Machine Learning; Behavior based Machine Learning Framework (BMLF); Sparse Autoencoders (SpAEs)*

I. INTRODUCTION

At present, cloud computing is a innovative technology that provisions physical and logical resources as services to the end users for necessary operation of data processing and management tasks. Organizations such as Amazon, Google, IBM, Microsoft, Facebook and Yahoo! are investing on data centers to offer cloud services that aim to utilize virtualization capabilities[1]. Cloud frameworks pull in numerous clients with its attractive features such as flexibility to access the services, easy to use, pay as per use, simple registration process etc. Undoubtedly, this increased flexibility in the cloud encounters a number of security attacks.

As mentioned in [2] cloud service models suffer from a large number of security threats that break the security

enclosed within the inherent features of cloud such as rapid elasticity, flexibility to access and service transparency. Hence, a security is great challenging issue that exists in cloud is associated with the efficient detection of abnormal behaviors such as perpetrate web fraud, steal personal information, and for many other abuse and nefarious activities caused either by legitimate or malicious intent. In particular, the malware detection is a most challenging issue since malwares results in starting point for launching of Distributed Denial of Service (DDoS) assaults in cloud [3].

Malware is a trend that tends to increase and will remain as the greatest security threat faced by computer users. Symantec report [4] demonstrated that new malwares have developed by 36% before in 2015 with all out examples surpassing 430 million. Everyday lives can be caused risk because of exponential development of malware threats.

Customized PCs acquire a great deal of assaults cloud condition. Malware assaults PCs and utilizations, the tainted PCs to assault other associated gadgets in cloud condition. For example, Mirai can taint windows and use the hosts to contaminate different gadgets. The tainted windows can take private data and change the affected systems into a botnet to dispatch another DDoS assault. Numerous existing customized PCs' malware assaults may likewise reach out to other cloud. Lamentably, there are no perfect answers for keep away from Mirai and other cloud dangers. One methodology intends to debilitate these dangers by ensuring the security of conventional PCs in cloud condition.

Because of rapid development of malware in the information technology, the knowledge of new or unknown malware detection based on machine learning methods is an important challenge for researchers.

Malware can be detected basically with two techniques. Signature based and behavior based detection techniques[5]. The popular anti-malware software's such as Kaspersky, Symantec, and Comodo etc. use signature-based detection in order to guard legal users from the hackers, The signatures may be operation codes (opcode), the sequences of byte codes, system calls etc. However, this method can be easily escaped by hacking through

