Chapter 17
A Review of Machine Learning Methods Applied for Handling Zero-Day Attacks in the Cloud Environment

Swathy Akshaya M.
Avinashilingam Institute for Home Science and Higher Education for Women, India

Padmavathi Ganapathi
Avinashilingam Institute for Home Science and Higher Education for Women, India

ABSTRACT

Cloud computing is an emerging technological paradigm that provides a flexible, scalable, and reliable infrastructure and services for organizations. Services of cloud computing is based on sharing; thus, it is open for attacker to attack on its security. The main thing that grabs the organizations to adapt the cloud computing technology is cost reduction through optimized and efficient computing, but there are various vulnerabilities and threats in cloud computing that affect its security. Providing security in such a system is a major concern as it uses public network to transmit data to a remote server. Therefore, the biggest problem of cloud computing system is its security. The objective of the chapter is to review Machine learning methods that are applied to handle zero-day attacks in a cloud environment.

INTRODUCTION

Cloud Computing (CC) is an international collection of hardware and software from thousands of computer network. It permits digital information to be shared and distributed at very less cost and very fast to use. Cloud Computing has become popular in organizations and individual users. Cloud Computing is the foremost technology which has been emerging in all fields of network applications.

Cloud Computing and web services run on a network structure and they are open to network type attacks. Security issues such as data loss, phishing and botnet pose serious threats to organization's data and software. It has become a serious challenge to contain security threats and vulnerabilities. Of all

DOI: 10.4018/978-1-5225-9611-0.ch017

the security threats Zero-Day attacks are the most vulnerable and complex one. Zero-Day Attack (ZDA) could not be easily detected. Zero-Day attack may be from outside or inside. Managing Zero-Day attack is a challenging task.

Cyber Security Ventures recently predicted that there will be one new zero-day exploit per day by 2021. Zero-day attacks are purposively created and developed by many companies and they are sold for profits. For instance, Trend Micro and Zerodium offer up to $500,000 for zero-day attacks.

The number of zero-day exploits detected keeps increasing at an alarming rate. The well-known WannaCry Ransomware attack that hit the majority of the world in May 2017 is an example of the worst-case scenario that could happen due to a Zero-day attack. Zero-Day attacks are difficult to detect as they are not known. Zero-Day attacks usually exploit vulnerabilities that unknown to public including network defenders.

Cloud Environment Attacks

Cloud Computing: A New Vector for Cyber Attacks - Cloud computing technology provides a shared pool of computing resources over the internet at any time for little to no cost. Using cloud computing, many individuals and businesses have already improved the efficiency of their operations while reducing IT costs (Ammar, Gupta, et.al, 2013). While cloud computing models are full of advantages compared to on-site models, they're still susceptible to both inside and outside attacks. Therefore, cloud developers need to take security measures to protect their users' sensitive data from cyber-attacks are shown in table. 1.

Attack Vectors for Cloud Computing

The main goals of cyber-attacks against cloud computing are getting access to user data and preventing access to cloud services. Both can cause serious harm to cloud users and shatter confidence in the security of cloud services. When arranging attacks in the cloud, hackers usually intrude into communications between cloud users and services or applications by:

- Exploiting vulnerabilities in cloud computing.
- Stealing users' credentials somewhere outside the cloud.
- Using prior legitimate access to the cloud after cracking a user's passwords.
- Acting as a malicious insider.

ATTACKS ON CLOUD

There are many ways to attack cloud computing services, and hackers are constantly working on developing more sophisticated ones. However, becoming aware of at least the most common will help cloud developers design more secure solutions. Here's a list of most common types of cyber-attacks performed against cloud users which are shown in figure 1.