Chapter 50
Possibilities, Impediments, and Challenges for Network Security in Big Data

Anuj Kumar Dwivedi
Govt. Vijay Bhusan Singh Deo Girls Degree College, India

O. P. Vyas
Indian Institute of Information Technology Allahabad, India

ABSTRACT

With the time, Big Data became the core competitive factor for enterprises to develop and grow. Some enterprises such as, information industrial enterprises will put more focus on the technology or product innovation for solving the challenges of big data, i.e., capture, storage, analysis and application. Enterprises like, manufacturing, banking and other enterprises will also benefit from analysis and manage big data, and be provided more opportunities for management innovation, strategy innovation or marketing innovation. High performance network capacity provides the backbone for high end computing systems. These high end computing systems plays vital role in Big Data. Persistent and Sophisticated targeted network attacks have challenged today's enterprise security teams. By exploring each aspect of high performance network capacity, the major objective of this book chapter is to present fundamental theoretical aspects in analytical way with deep focus on possibilities, impediments and challenges for network security in Big Data.

1. INTRODUCTION

Since it is an era of information (The Economist, 2011). In this era, due to continuous development in field of electronics and IT, the computational devices and storage becomes inexpensive. With this growing computational capabilities, data is generated from everywhere. These data are stored in databases for future references/decisive purposes. The term Big Data is used for these massive data having varieties, generated with velocity and measured in term of Tera, Peta, Exa, Zetta, Yotta Bytes (Sagiroglu &

DOI: 10.4018/978-1-7998-2466-4.ch050

Sinanc, 2013). As per the Oracle (Dijcks, 2013), big data typically refer these types of data: traditional enterprise data, machine-generated /sensor data, and social data.

With the time, Big Data became the core competitive factor for enterprises to develop and grow. In the age of Big Data (Lohr, 2012), data is generated from everywhere, some enterprises such as, information industrial enterprises will put more focus on the technology or product innovation for solving the challenges of big data, i.e., capture, storage, analysis and application. Enterprises like, manufacturing, banking and other enterprises will also benefit from analysis and manage big data, and be provided more opportunities for management innovation, strategy innovation or marketing innovation. High performance network capacity provides the backbone for high end computing systems. These high end computing systems plays vital role in Big Data. Persistent and Sophisticated targeted network attacks have challenged today's enterprise security teams.

Big Data analytics promises major benefits to the enterprises. Enterprises need to enable secure access to data for analytics, in order to extract maximum value from gathered information, but these initiatives can be a cause for big prospective risks. Handling massive amounts of data increases the risk with magnitude of prospective data breaches. Sensitive data are goldmines for criminals, data can be theft/ exposed, it can violate compliance and data security regulations, aggregation of data across borders can break data residency laws. Thus secure solutions for sensitive data, yet enable analytics for meaningful insights, is necessary for any Big Data initiative (Voltage Security, n.d). Big data analytics will play a crucial role in future for detecting crime and security breaches (Gartner-Research Firm, n.d.).

2. PRIOR RESEARCH WORKS ON NETWORK SECURITY FOR BIG DATA

Enterprises awash in flood of unstructured, semi structured and structured data, which introduced a multitude of security and privacy issues for organizations to contend with. Today's enterprise security teams focused and searching for the root causes of the attack often feels like looking for a needle in a haystack, but as per a white paper (White Paper, n.d.), getting valuable information in context of big data is more than "looking for the needles", security is a serious business and it is "eliminating the hay from the haystack". Security has traditionally been all about the defense. The term network security means providing security when data is on fly, i.e. over network.

Network traffic monitoring remains a decisive component of any enterprise's security strategy, but gaining context into the gigantic amounts of data collected from network, in a timely fashion, is still a hurdle for many enterprise security teams. Incident responders are eventually looking for possible ways to definitively identify threats for evaluating risk of infection and to take the necessary steps to remediate (Arbor Networks Blog, 2014).

A new generation of methods and architectures designed specifically for big data technologies are needed that extract value from gigantic amounts of different data types through high-velocity capture, discovery and analysis. In its review, authors (Matti & Kvernvik 2012) illustrates efficient extraction of value from data and through a figure correlate three associated things: analytics, cloud-based distributed environment/deployment, and Networked Society, and these will be inextricably linked.

It is observed that data generated by the many devices having spatial and temporal characteristics, are part of the networked society. The emergence of complex networks and networks within networks are today's reality (Hurlburt & Voas 2014). When network society, cloud computing and different phases associated with big data are correlated and viewed in a single sleeve, these two figures (Figure 1 and