Advanced Science and Technology Letters
Vol.93 (Security, Reliability and Safety 2015), pp.40-43
http://dx.doi.org/10.14257/astl.2015.93.09

A Study on the development of Integrated Security Technology based on Big Data

JeongBeom Kim

Professor, Industry-Academic Cooperation Foundation,
Namseoul University,
jbkim@nsu.ac.kr

Abstract. The purpose of this paper is to study the integrated security technology based on big data. The concept of new technology is to change individual security to integrated security with a view to finding new format of hacking attack, and also to manage many kinds of security threat through effective monitoring system. Using big data analysis, this new technology can be more enhanced approach than conventional security technology. This new concepts have been required by business entities and also by government organization as a approach to newly integrated security management.

Keywords: Big Data, Security, Integrated Security Management, Security Motoring, Security Channel, Log Analysis

1 Introduction

In this paper, enhanced integrated security management technology using big data was presented. With the help of the rapid development of security technology, many business entities and government organizations have solved many issues and problems about many security attacks. In order to cope with highly skilled threats regarding security, new process of management infrastructure concerning security system based on big data have raised these requirements recently to compensate the defect of traditional security system [1].

2 Integrated Security Management Model based on Big Data

The integrated security management model based on big data can be widely used in security reliability field. The aspects focused on intensity and value function of the model is as below: [2].

2.1 View point of Security Management

ISSN: 2287-1233 ASTL

Through the development of integrated security management model based on big data, we can detect new types of security attacks more intensively, and find out existing dead zone of security area, and intensively manage various security channel moving from individual security to merged security, ultimately [3].

2.2 View point of Economic Management

We can streamline various security solution and monitoring function which are scattered in many areas for the purpose of dramatic economic effects by reducing management cost and human resource cost as well as by increase of efficiency in security management.

3 Needs about the Development of integrated security management technology based on big data

3.1 Social Need

Although we are trying to block the security threats fundamentally using all kinds of security tools, security related accidents are happening continuously. Also there is a trend of newly development about mutual connected deployment of various security products (i.e. firewall, IPS, VPN) and networks on hand. The technology of hacking attack ways are being upgraded and accelerated continuously, and this cause the confrontation of not automatic and positive counter-attack. Another issues about DDOS and APT(Advance Persistence Threat) can be representative security threats trends. APT tends to remain in internal IT system for a long time with characteristics of unnoticeable attack [4].

3.2 Technical Need

There is a need to establish new process to do real time detect of security threats from internal infrastructure system based on accurate analysis of collected security log files. Also there is a tendency that the functions concerning log collection and search are being lowered remarkably when large size log data are accumulated on the security system.

4 The Architecture & Function of integrated security management technology based on big data

The architecture of this model is as below. Firstly, collect all log files from various security channels [5]. Secondly, restore in deposit place and take process of analysis. And finally, draw the results about correlation from various channel input, having the architecture of real time detecting and monitoring, which is described in below figure.

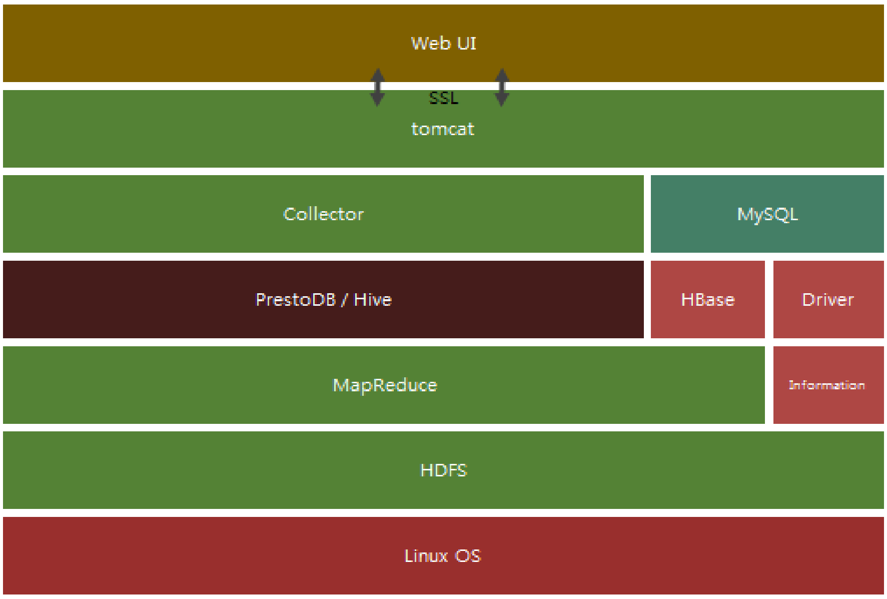

Fig. 1. Model Architecture

The functions of this model is doing log management, detection of weak points, life cycle management, analysis of network packet, detection of network abnormal condition, counter attack from security threats by means of real time analysis [6].

5 Conclusion

The development of this integrated security model based on big data technology can support various protocols to collect all many kinds of log information for the purpose of flexible action. This model is an integrated technology of natural language based analysis, ease of use for users, convenient users interface, automation of log management, analysis of network packet, real time detection of security threats. Hence, this model can be a new trend of integrated security management technology which has been evolved from separated security management to converged security management system with an aim of optimal management concept.

References

1. Method of Data Resource Secure and Quality Management in Big Data Era, NIA, (2012.5)
2. Big Data is only the beginning of extreme information management, Gartner
3. Search, From Big Data to Big Insight Finding Enterprise and Future, Wisenuts (2012, Feb)
4. Data Quality for Big Data : Principle Remain, But Tactics Change, Gartner
5. Security 3.0 Lim HoJin, 462 (2011)
6. Information System Security, Cho WanSoo, 11-15 (2003)