International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 217-226
http://dx.doi.org/10.14257/ijsia.2015.9.6.21

A Study on the Development of Next Generation Intelligent Integrated Security Management Model using Big Data Technology

JeongBeom Kim

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

Abstract

In this article, the development of integrated security model for the next generation using big data technology is proposed. The main objective of this model is to make a paradigm shift from managing separate security to managing integrated security with real time basis monitoring of hacking attacks which are coming from all kinds of security input channels, using big data analysis technology. This new model technology can be a more enhanced approach than conventional security technology in terms of detection and response speed. This new model will contribute to governance and management of security in many areas significantly.

Keywords: *Security, Big Data, Integrated security management, Security Monitoring, Log Analysis, Security Channel, Hacking Attack, Security Information*

1. Introduction

The effective management of the total security information management is a fundamental concern for the long-term growth of each organization or company in competitive markets. There is no organization which is not keen to security issue and efficient growth. The most pressing issues about security management in these days are quick response to various kinds of hacking attacks. Hence, many organizations are concerned with business enablement architecture to avoid impact and damage from outside security attacks. Information security is practiced in daily operation as people respect the policies and principles related with it. [2] Although people are provided with sufficient and detailed guidance and are encouraged to participate in security alerts, they are faced with the challenge of situations of new security attacks. Everyone is accountable for protection and stakeholders are also involved in the identification and response to the threats to the enterprise in many cases. [1] Management proactively supports innovations of security infra structure as one of competitive edge. In this paper, the development of next generation intelligent integrated security management model using big data technology is mainly discussed to solve this kind of issue seamlessly. The basic value of this model is to change the very nature of security information from passive cargo that arrives, when queried, via paved cow path, to an active enzyme that circulates throughout an security ecosphere in which all points are instantly accessible from all other security points. [11] In this paper, new approach of next generation intelligent security management model using big data analysis technology has been proposed.

2. Related Study

2.1. Information Security Factors: There are general approaches based on basic factors as the following. First, information security should support the mission of organization. Second, Information security is an essential factor for the management of organization. Third, Information security should be cost effective. Fourth, Information security should

ISSN: 1738-9976 IJSIA

be definite for the responsibility and accountability. Fifth, each owner of system is responsible for security management about their external organization as well. Sixth, Information security needs comprehensive and integrated approaching method. Information security should be reevaluated regularly. Seventh, Information security tends to have limitation from social factors [9].

2.2. Infrastructure for Information Security Model: The Infrastructure of security system should provide a security architecture, security development, adequately secured and configured system, user access and access right, prompt protection against external attacks and intrusion attempts, adequate incident response, security testing, and monitoring with alert services. [3] There are three models related with this category. Hybrid integrated model is integration of individual security system into one sever or hardware, integrating firewall, IDS, and VPN. Interoperation model is interoperability of individual security system and integration by predefining protocol methodology. Broker model is using broker which enables interoperability and integration of separate security systems. So, each individual system can only focus on its own agents and connectivity. System stability and strong recovery from the security incidents are the key factors of infrastructure in security model with continued advancement of related technologies. This will surely hold high customer loyalty [7].

2.3. Existing Integrated Security Management System which are using Relational Data Base Model: The existing integrated security system is based on relational data base architecture, slow in speed if the log volume is huge, detects only traditional incidents, needs high level skill in operation.

3. Requirements of New Integrated Security Model

3.1. General Requirements: Because of the existing integrated security system's limitation as described above, blocking the security threats fundamentally using all kinds of security tools is very difficult while security related incidents are happening continuously. Also there is another requirement about mutual connecting deployment of various security products (*i.e.*, firewall, IPS, VPN) and networks on hand. Since most hacking attacks vary and are also being accelerated continuously, a quick response system is needed inevitably. Other issues about DDOS threat and APT(Advance Persistence Threat) would be representative security threats in these days. APT tend to remain in internal IT system for a long time, and this is one of harmful threat with characteristics of unnoticeable attack [5]. DDOS attacks disturbs the service and business operation, and they have been evolved into multi-vector attacks which using diversified and mixed techniques. There should be some approach to defend against this kinds of new multi-vector attacks effectively by deploying more enhanced security infrastructure with integrity, availability and reliability [7, 13].

3.2. Technical Requirements: There is a requirement of establishing new process for the real time detection of security threats in security infrastructure system based on accurate analysis of collected security log files using big data. There is another tendency that the functions concerning log collection and search are being lowered remarkably when large size log data are accumulated on the security system. Since the existing integrated security system is based on relational data base architecture, they are having problems with low speed if the log volume is huge, also they detect only traditional incidents. Distributed security systems mean more machines and a more complicated systems administration problem. This problem can be addressed through automation. Security management without real time monitoring can't meet business requirement in terms of

agility. Monitoring security system needs intelligent architecture to detect and defend diversified security attacks [16].

4. Next Generation Intelligent Integrated Security Model using Big Data Technology

There is more to business intelligence than simply deploying security management technology or system. We need a comprehensive, strategic approach to designing, implementing, managing, tracking, and supporting Integrated Security System initiatives. Lacking intelligent framework, enterprises would end up with a patch work of good intentions but no meaningful enterprise-wide intelligence in security management. [4] The next generation of intelligent integrated security model using big data technology consists of intelligence, integration, monitoring, search and analysis using big data technology, and reporting functions. If the log data is high volume, this will impact the analysis and search the related data in terms of speed and performance. Using big data technology can solve this issue easily and quickly. As a new approach, using natural language in search can help with detection of unknown security attacks as well as hacking incidents. Considering these view points, this paper suggests the need for development of intelligent integrated security model using big data technology as following [6, 8].

4.1. Total Architecture of Next Generation Intelligent Integrated Security Model using Big Data Technology: Through the development of next generation intelligent integrated security models based on big data, we can detect new types of security attacks more easily and intensively, finding out the existing dead zone of security area, as well as managing various security channel ultimately. The main differences from the existing system are as following. Firstly, this model is using big data analysis technology, not relational data base technology which existing security systems are using currently. Secondly, since this model has parallel structure, processing speed is very quick even when log volumes are increasing. The processing speed of existing system is proportional to the amount of log. Thirdly, this model utilizes natural language base technology in detection of new and old incidents, while existing system can only detect precedent incident. The existing system cannot detect normally if the security policy set up does not match the cases even slightly..Fourthly, this model is ease of use for the responsible staff regardless of security related management knowledge level, while existing system requires high level of security knowledge skill to manage it. Fifthly, this model contains legal compliance requirement in secure. The main functions of this model are log management, weak point detection, lifecycle management of vulnerability, analysis of network packet, detection of abnormal network status, response management for the incident cases.[3] The total architecture of next generation intelligent integrated security model using big data is identified in Figure 1, as below.

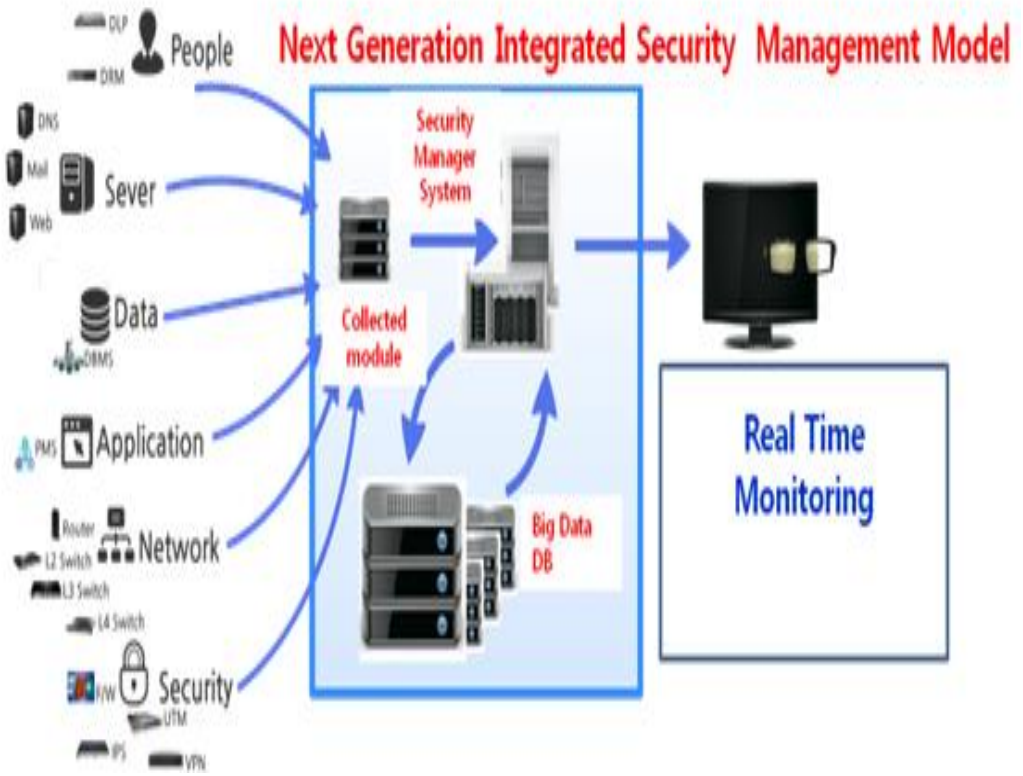

Figure 1. Total Architecture of Next Generation Intelligent Integrated Security Management Model using Big Data Technology

4.2. Functions about Next Generation Intelligent Integrated Security Model using Big Data Technology: The function of new model is as follows. First, this model is using and processing big data analysis for searching and reporting with high speed, and also supports flexible expansion of system up to required resources. When there is a need of new resource increase, this flexible architecture can expand another security process engine. Second, this model analyzes packet network based on L4 and L7. L4 based packet do the analysis focused on packet header data. L7 based packet do the analysis focused on packet main data for the details and exploit of network. Third, this model does the log management with data encryption and forgery prevention programs. Fourth, this model detects abnormal status quickly by tracking destination base. This can detect and monitor whether some data move to the same destination continuously to detect unusual cases. [6] This also detects abnormal protocol and status based on data flow by analyzing usage trends. This model can detect abnormal symptoms in early stage by analyzing network packet usage status. Fifth, this model detects all the threats based on new technology of natural language algorithm. This model analyzes all log types based on IP address alignment which are security side data. And leverage the results from detection lesson for future review for accidental threats. Sixth, this model can detect weak points of security related systems and applications. This model find out the weak spots of sever systems and network equipments which are consisting security infrastructure. This model also checks intensively weak points of application area which are running the business process. Seventh, this model does the lifecycle management in weak point area. This model monitors frequent weak portion and reaction cases for the compliance purpose by assigning the responsible staff to handle the weak point management. Eighth, this model does the analysis activities about the security incidents by means of profiling response management as well as provision of solved or not solved criteria. This model alerts

whenever incidents happen, and conveys SMS message or email responsible manager to react on the spot. Ninth, this model can produce reports of statistics about infringement prevention, firewall, VPN, change of system file, and virus types in details along with collection events. [12]

4.3. System Architecture of Next Generation Intelligent Integrated Security Model using Big Data Technology: The key points of system architecture about this model are integration of existing security systems, monitoring and measurements, and using big data analysis technology.

Below figures shows the system architecture of this model. The main objective of system architecture is ease of use for the users in terms of operation and security management. Risk analysis consist of information assets, factors of threats, and security vulnerability. Risk management contains security threats and measurements for security using big data analysis and integration of existing security systems which are intrusion detection system, intrusion prevention system, intrusion tolerance system and firewalls [7].

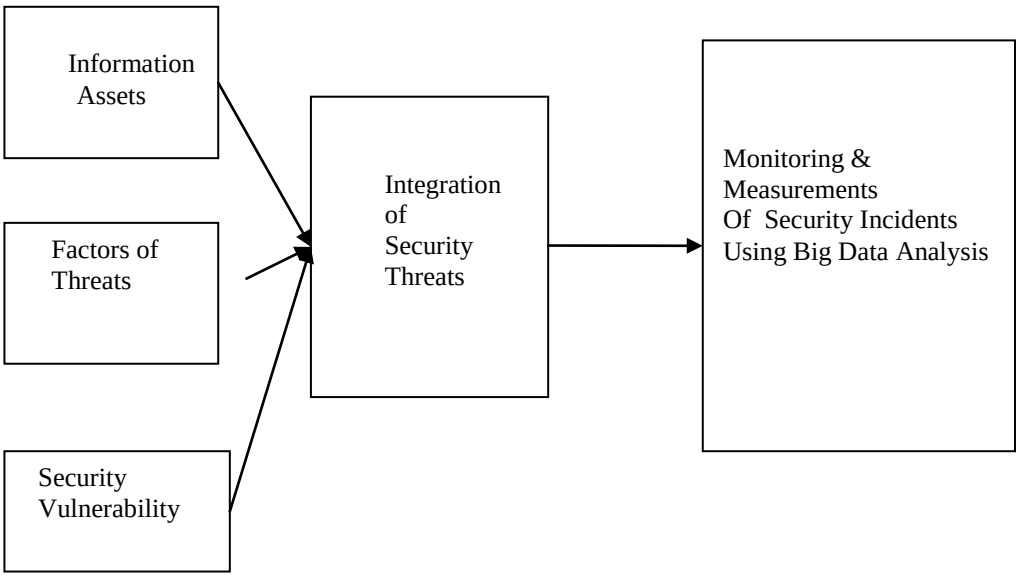

Figure 2. System Architecture

There are four core technologies for this model as following. 1) Event normalization which collects events and normalizes all the events from each security equipments 2) Analysis and risk classification methodology which analyzes detection pattern per each security products, classifies detected danger, vulnerability, and set up the guidelines of risk category according to security system. 3) Anomaly detection and response which are doing misuse/anomaly detection and response passively and actively. 4) Integrated Policy Management which are doing automatic policy management according to all security products involved in security management. From the perspective view of advanced security management, security management team should perform as following. Security program champions define corporate security intelligence strategy, ensure alignment with corporate objectives, consolidate and prioritize for the new security requirements throughout the enterprise and track project success. Advanced analytic experts perform complex data mining and modeling in response to requests from business units and conduct research with models to explore correlations and interdependencies of security issues. [8] Security application developers develop, test, and maintain security

applications for the enterprise – both user-facing applications and those that directly interface with expansion and flexibility infrastructure. [9] The major data flow about this data flow architecture are identified in Figure 3 [6].

Figure 3. Data Flow Architecture

4.4. Value of Next Generation Intelligent Integrated Security Model using Big Data Technology:

We can streamline various security solutions and monitoring function which have been scattered in many areas. This study found out the difference of existing security system and this new architecture as following. Monitoring work load will be changed from 40% to 10%. Monitoring the security status with real time is one of the key important activities. Report generation work load will be changed from 30% to 5%. Report about the abnormal cases can improve the ability of prevention next time. Exact reporting with decision factors will be helpful to enhancement of system. Analysis and solving new incident work load will be changed from 12% to 5%. One of the difficult jobs about security management is solving new incident quickly to deliver secure service to customers. Planning work load will be changed from 5% to 10%. This means that planning work should be increased because of important portion. Security system planning is the most crucial activity for the management with short term and long term planning. Ad hoc work load will be changed from 8% to 6%. Ad hoc job can be administration work by responsible staffs. Policy management and rolling out of new action work load will be changed from 6% to 12%. Policy management and rolling out the new security action is also important work for security managers. So, the total cost saving would be 52%. This

can be huge improvement of productivity in security management compared to existing ones. This can be big gains changing from conventional system to new model. The major effectiveness of this model are as following the first one is total integrated security management which increase the security management efficiency by doing alert activity for each security solution and log information management in central integrated system through integrated monitoring and control. The second one is synergy effect which reduce the cost duplication and reinvestment cost by assigning minimum number of responsible staff who control security system as well as reducing cost of deploying security systems with the help of management productivity. The third one is preparatory measure which is not follow-up action. This can provide prior prevention plan through analysis of each log management and integrated management. This can also analyze system status regularly by using statistical process functions. The last one is agility which enables real time response per incidents. Quick response for the incidents can survive the companies in these hot competition market situation. Security organization is one of critical success factors for business management in terms of providing better customer services. The main value of this model can be dramatic economic effects by reducing management cost and human resource cost as well as, also increase of efficiency in security management, as shown below Figure [8].

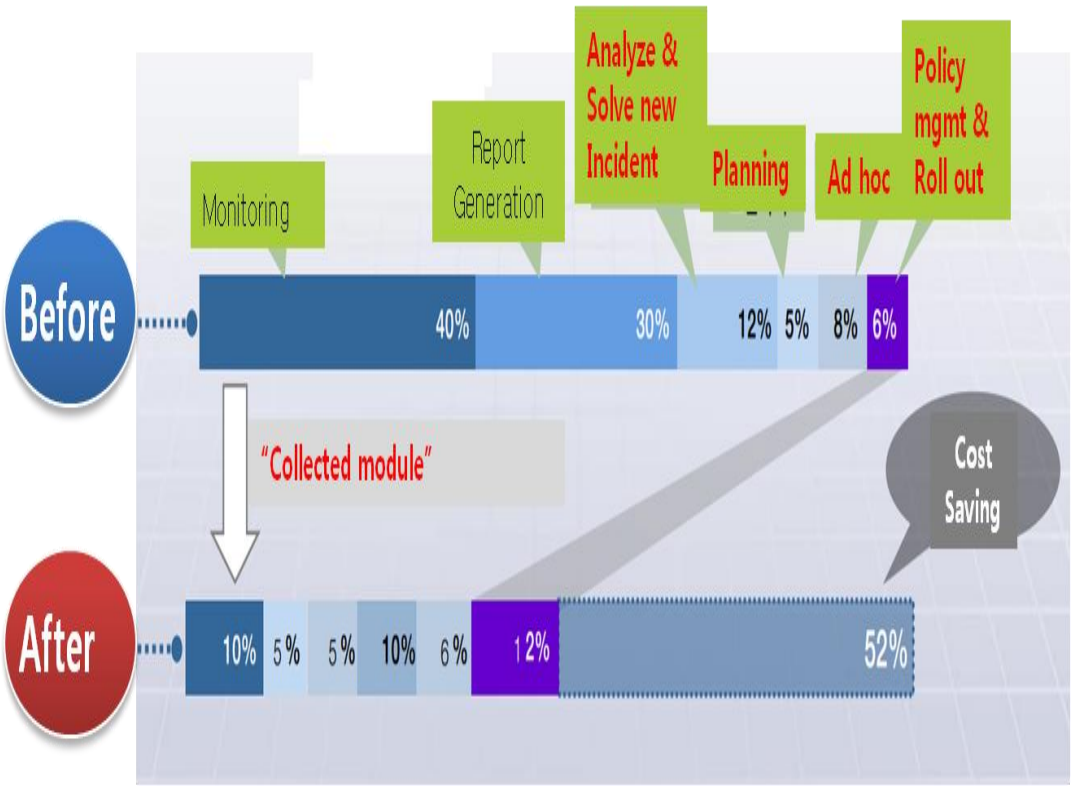

Figure 4. Value of Next Generation Intelligent Integrated Security Management Model using Big Data Technology

5. Conclusion

Companies improve their product, system or services because they want to serve more profitable groups of customers who are willing to pay higher prices for these improved products or services. Often, it is more than a want. It is need. [11] If an innovation does not take place at a point of modularity, it is one of the two other forms of sustaining innovations-radical or incremental-that both happen at points of interdependence. Radical sustaining innovations are at the complex end of continuum. Integrated companies can

master the myriad interdependencies involved in wrestling with compatibility, interoperability, and legacy issues in security management. Without the reliable security infrastructure any company or organization can't survive to meet customer support requirements. This model can improve security infrastructure to provide better services to customers. The development of next generation intelligent integrated security management model using big data technology can support various protocols to collect all 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. Therefore, this model can be a new trend of integrated security management technology which has evolved from separated security management to converged security management system with an aim of optimal management concept. [14] This model can be a new platform for Security Monitoring System with quick response in times of security attacks and incidents and also provide prompt security information for related analysis with ease of use. Firstly, collect all log files from various security channels. 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, The main objective of this model is doing log management using big data, detection of weak points, life cycle management, analysis of network packet, detection of network abnormal condition, prevention of attacks from security threats by means of real time analysis and response. The development of this model is a transformation that can be considered as a journey toward new ways of next generation intelligent security management. Some users, put off by the more challenging new environment, are tempted to point out what's wrong with becoming intelligent rather than anticipating the benefits once new complexity is mastered. The best way to make accurate sense of the present, and the best way to look into the future, is through the analysis of big data. Good analysis provides a robust way to understand important developments, even more when data is limited. And big data analysis in security management is even more helpful when there is abundance of data. This can be critical challenge of this model. This model also suggests intelligent integration of security system with monitoring function. Sustaining innovations play two important roles in security industry change: They define the path of incumbent improvement and they provide the fuel for disruptive companies to march up their own improvement trajectories. This model can be one of the best ways to improve security management productivity as a new approach. I conclude from many experiences with implementation of information infra structure that converting it to integrated and intelligent have increased its productivity at a rate which are comparable to great growth in the larger economy.

There are some limitations of this research that should be considered. Firstly, the verification of this total architecture through questionnaire and survey has not been proposed. Further study can do this research from real reference cases. Secondly, the value of this model can be compared with real cases if we have statistical result analysis of before and after implementation of this model. Thirdly, application of this research can be extended in many security management areas through the implementation of this model as a validity. Thirdly, all of the diverse factors about intelligent security model have not been mentioned in this paper. These limitations can be studied for future research, which can be contributed to the development of security management areas.

Acknowledgements

Funding for this paper was provided by Namseoul University.

References

[1] J. Valouch Ing, "International Journal of Disaster Recovery and Business Continuity", Publisher: Science and Engineering Research Support Society, Integration of Alarm Systems, IJDRBC, vol. 3, **(2012)** November, pp. 21-30.
[2] Y. Zhang and K. Wu, "Software Cost Model Considering Reliability and Time of Software in Use", Journal of Convergence Information Technology, vol. 7, no. 13, **(2012)**, pp. 135-142.
[3] H. S. Nalwa, Editor, Magnetic Nanostructures, American Scientific Publishers, Los Angeles, **(2003)**.
[4] Method of Data Resource Secure and Quality Management in Big Data Era, NIA, **(2012)**.
[5] P. Denning, "Computer Under Attack Intruders", Worms and Virus, Addision Wesley, **(1990)**.
[6] C. P. Pfleeger and S. L. Pfleeger, "Security in Computing", Prentice Hall, **(2003)**.
[7] H. Lim and S. Park, Security 3.0, IDam Publisher, **(2011)**, pp. 305-307.
[8] IT Governance Institute, COBIT: Governance, Control, and Audit for Information and related Technology, **(2000)**.
[9] W. Soo Cho, "Information System Security", HongRyung Science Publishers, Seoul, vol. 1, **(2003)**, pp. 399.
[10] J. Davis, G. J. Miller and A. Russel, "Information Revolution", Published by John Wiley &Sons, Inc,. New Jersey, **(2006)**, pp. 133-139.
[11] V. Ranadive, "The power of now", published by Mcgraw-Hill, **(1999)**, pp. 62-64.
[12] W. S. Cho, "Information System Security", HongRyung Science Publishers, Seoul, vol. 1, **(2003)**, pp. 19-25.
[13] A. Hoog, translated by K. Yoon, "Android Forensic", Acorn Publishers, Seoul, vol. 1, **(2013)**, pp. 209-213.
[14] C. M. Christensen, S. D. Anthony and E. A. Roth, "Seeing What's Next", published by Harvard Business School Press, **(2004)**, pp. 30-31.
[15] J. Kim, "A study on the development of Integrated Security Technology based on Big Data", Advanced Science and Technology Letters, (Security, Reliability and Safety **2015**), http://dx.doi.org/10.14257/astl.2015.93.09, vol. 93, pp. 40-43.
[16] K. Son, "Information Security Industry Trend and Forecast", Proceeding of Korea Information Processing Society Review, vol. 17. 6th, **(2011)** November, pp. 72-74.

Author

Name: JeongBeom, Kim
Profile:
B.A. degree from Seoul National University
MBA degree from Yonsei University
Ph.D. degree from Soongsil University
Manager, IBM Korea
Sales Director, SAP Korea
CEO, TIBCO Software Korea
CEO, Ariba Korea
CEO, Interwoven Korea
Vice President, DASSAULT SYSTEMS Korea
Currently, Professor at Namseoul University