# Development of Integrated Security Control Service Model Using Artificial Intelligence

**Se In Jung**

PAUL MATH SCHOOL

12-11, Dowontongmi-gil, Cheongcheon-myeon, Goesan-gun,

Chungcheongbuk-do, Republic of Korea

(Supervised by teacher **Shin Dong Ho**)

eavatar@hanmail.net

## Abstract

I propose a method that can efficiently apply artificial intelligence technology to integrated security control technology. In other words, it detects cyber attacks and responds appropriately by applying machine learning learning to artificial intelligence based on the big data collected by the integrated security control system. The artificial intelligence-based integrated security service model that analyzes and responds to these behaviors gradually evolves and matures through effective learning methods. In addition, through the proposed security service model, future research directions for security management that can efficiently support the analysis and response of security personnel are presented.

**keywords**

integrated security, service model, AI

## 1. Introduction

### 1-1. Motivation of the Research

It was pointed out at the '2018 RSA Conference' that despite the many advances in attack technology, it is not possible to adequately respond to unknown attacks with only the current technology. Insisted. To this end, it is necessary to expand the cooperation base of related companies and analyze the high-quality threat information collected based on artificial intelligence, and it is necessary to automate it through artificial intelligence technology using machine learning. Through this, it is necessary to respond to the rapidly increasing cyber attack and establish a security task system based on artificial intelligence. At this time, above all, there should be no gaps in the existing

work, and to do so, it can be said that the learning data for learning the existing data using machine learning is the most important. In other words, it is time to strengthen efficiency through the division of human and machine labor, and to apply security technologies such as integrated security control based on artificial intelligence technology. As cyber threats continue to develop technologically, threats such as cybercrime and terrorism are evolving into complex and diverse forms as well as the organization and advancement.

### 1-2. Research Purpose and Scope and method

Security personnel are facing limitations in responding to security events that are increasing exponentially.
Cyber attacks at home and abroad are becoming more intelligent and advanced day by day due to indiscriminate attacks due to the automation of hacking and the heightened risk of cyber warfare. Infringement events are also increasing exponentially, and looking at recent changes in hacking techniques, zero-day attacks and stealth techniques such as ransomware, as well as mobile attacks, are increasing. Attacks such as account hijacking and personal information leakage due to social network hacking are also on the rise. In this paper, an integrated security control model is proposed to effectively implement an artificial intelligence-based integrated security control system as a solution to these complex problems.

## 2. Main contents

### 2-1. Hacking system

1. Hacking system

Hacking security vulnerabilities inherent in operating systems, software, and hardware. It is often called ponable by using pwn from Lit. To learn about system hacking, you need to know the operating system first. Each operating system operates differently, and the source code of the program is also different, so we divide it into Windows and Linux. For hunting for vulnerabilities that the developer has not found, the program must be reverse-engineered to find out the operating principle. This allows you to hack the program. Types of system hacking include password cracking, backdoor, NETBIOS attack, keylogger, buffer overflow, and attack techniques such as race control.

2. Hacker

A hacker made up of a combination of a hacker and a producer means a person who enjoys exploration about it by immersing in computers or networks. However, as people seeking a sense of accomplishment or pleasure emerged from breaking through the tricky intrusion defense system of the network, it began to be used in the negative sense of'computer intruder'. It has even been transformed to mean a criminal who invades a computer to steal information or cause confusion. However, in developed countries, including the United States and Europe, crackers, meaning hackers and malicious intruders, are used separately. Crackers are divided into ″Intruders″, which are simple intruders for information capture, ″attackers,″ which block the service of the system, and ″destroyers,″ which destroy the system

and release copy protection devices of commercial programs or spread viruses.

3. Password security

Encryption refers to a security method that converts information or data into a state that other people cannot read. In order to open the encrypted information, a decryption process that converts the data into its original form using specific data called a key is required. Therefore, even if the password for accessing the computer system is exposed to the intruder, the encrypted data can still be unrecognizable, and the information can be protected.

4. Buffer overflow

It refers to a state in which the service is stopped when sending data of a much larger capacity than the set receiving capacity to a program running on the server at once. If a special execution program is put in the sent data, the special program operates with the administrator authority when the stopped service is moved with the administrator authority. In this way, the server intrudes and performs various attacks. Buffer overflow can be prevented by checking whether the data sent by the application program exceeds the receiving capacity.

## 2-2. Integrated security control system

1. Integrated security control system

In general, integrated security control can be classified into three categories according to the nature of the business. First, it is a ″operation and management″ task to identify failures in security systems and information systems and to grasp compliance with related compliance. The ability to manage and properly operate various security equipment is required, as well as whether the security equipment is properly set up and operating properly and the security policy is properly set. Expert knowledge of various security equipment such as firewall, IPS, IDS, UTM DDoS response equipment, and web firewall is required.Second, there are detection, analysis, and response tasks that quickly detect the behavior of an attacker and quickly judge and respond to threats. In order to respond to various intelligent attacks, it is necessary to quickly understand the flow of data coming through the network and the ability to understand various threats.

Third, it is a preventive task that can minimize damage by preventing infringement accidents in advance and responding promptly in the event of an accident. It checks server, application, network, and SW vulnerabilities in order to promptly respond to known attacks as well as unknown threats, collects external security threat information in real time, and automatically applies it to the integrated security control system to provide harmful IPs and malicious URLs. Update the latest threat information, etc. In addition, it can be seen that it includes training to increase awareness of information security by conducting various mock training for internal employees, establishing response procedures for security threats, and raising awareness about information security. In more detail, the characteristics of security control by service are the dispatch control service, where security control experts provide specialized control services directly from the customer, provide specialized control services directly from the customer, and face-to-face with the

customer's information protection manager. Smooth communication is possible. In addition, immediate action is possible when infringement/failure occurs, and work continuity and efficiency are increased.

1. How to collect artificial intelligence data

   In order to generate learning data and predictive data, it is necessary to collect original logs and history data from the integrated security control system. As a process of converting the original log into a form that is easy for machine learning, it is necessary to extract feature values based on analyst know-how. To this end, information on the capacity of learning and detection data for each collection system should be secured in advance, and issues should be collected in advance when collecting detection data and learning data.

2. Development plan of artificial intelligence integrated security control service model

   For an integrated security control system to which artificial intelligence is applied, it is necessary to prepare a system that predicts, prevents, detects, responds, and evolves itself from a security system that analyzes and responds to after detection. It is necessary to develop a normal-based learning model to strengthen the ability to respond to threats that are not identified as abnormal behaviors. In addition, when applying various techniques to improve the accuracy and performance of the model of the artificial intelligence learning system, the optimal training data is selected through a feature selection algorithm for the training data, weight is assigned to each field, and an optimized model is selected through a sampling technique. Should be applied.

## 3. Conclusion

Data is more important than anything else in integrated security control using artificial intelligence, and such data should be applied to external security issues as well as internal data. In this study, there may be limitations to the method of formalizing various log data. Therefore, research on standard information sharing system for standardization and sharing system should be continued so that external information sharing system can be used in various integrated security control services in a formal data format.

## Reference

Data Oh Yeongtaek and Cho Injun, " A plan to develop an integrated security control service model based on artificial intelligence technology." *Korea Contents Association symposium*, 19.1 (2019): 108-116
.