

Design of an Integrated Cyber Defense Platform for Communication Network Security of Intelligent Smart Units

Jung-Ho Eom(✉), Dong-Won Yoon, and Jung-Ho Choo

Daejeon University, 62 Daehakro, Dong-Gu, Daejeon 300-716, Republic of Korea
eomhun@gmail.com

Abstract. The key to building an intelligent smart unit promoted by military advanced countries is to strengthen security based on new technologies of the 4th Industrial Revolution. It should be manageable the security of information system and network in real time by applying new information and communication technologies such as artificial intelligence and big data. As various new technologies are applied to the information and communication networks of smart units, vulnerabilities will increase, and sophisticated cyber threats using these vulnerabilities will also increase. Artificial intelligence and big data technologies are essential for the integrated security control system of a smart city currently being built. They are also needed for the cyber security orchestration and security control system developed by a company. So, it processes, classifies, and analyzes massive data in real time, detects threats more accurately, and reduces false detection rates. In this study, we proposes an integrated cyber defense platform design that can process data, detect threats, and judge true/false detection in real time based on the functions of the existing integrated security control system and the characteristics of the information communication network of intelligent smart units.

Keywords: Integrated Cyber Defense Platform · Threat Detection · True/False Detection Rate · Intelligent Cyber Attack · Intelligent Smart Unit

1 Introduction

Military advanced countries are converting existing units into intelligent smart units, advanced combat units, so that they can conduct military operations quickly and efficiently by applying new technologies of the 4th Industrial Revolution (IR) [1]. In particular, South Korea is promoting Defense Innovation 4.0 with the aim of fostering an AI science and technology powerful military through advanced science and technology-based military innovation. Its purpose is to equip swift and accurate operation/mission capability and smart organization/system/procedure through intelligence of weapon system, high efficiency of operating environment, and advancement of technology and infrastructure [2]. Currently, new technologies such as artificial intelligence and big data are being applied to advanced weapon systems including military operation systems, base defense systems, and operation support systems in the intelligent smart units. In addition,

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14106, pp. 218–230, 2023.
https://doi.org/10.1007/978-3-031-37111-0_16

the weapon system to be introduced in the future will be equipped with advanced intelligent software. As the high-tech application system is diversified and advanced, security problems have begun to emerge. Security systems such as firewalls, intrusion prevention system (IPS), network access control (NAC), and antivirus systems for integrated networks and terminals that have been previously installed cannot secure the safety and reliability of various mission systems that are becoming advanced and large-scale.

The aspect of recent cyber threats is utilizing intelligent and sophisticated attack techniques. In particular, as artificial intelligence and big data technology are applied to cyber-attack techniques, it is becoming difficult to identify and detect cyber threats with cyber security systems. Therefore, it is necessary to install an integrated cyber defense platform to comprehensively control the information communication network of intelligent smart unit and respond to intelligent cyber threats [3].

We propose an integrated cyber defense platform design that can protect mission system of Korea's intelligent smart unit, respond to various cyber threats, and manage each security system and information system. We explains the building status of Korea's intelligent smart units in Sect. 2, and describes the security threats of intelligent smart units in Sect. 3. We propose the design of an integrated cyber defense platform in Sect. 4 and conclude in Sect. 5.

2 The Building Status of Intelligent Smart Units in South Korea

In the era of the 4th Industrial Revolution (IR), military advanced countries such as the United States are already converting and promoting military innovation based on advanced science and technology. The Ministry of National Defense of Korea is promoting Defense Innovation 4.0 in order to actively respond to the paradigm shift in defense and warfare following the innovative development of the 4th IR technology. Defense Innovation 4.0 intends to redesign and remodel all areas of national defense such as defense R&D, power reinforcement system, defense science and technology, military strategy and operational concept, and military structure and operation in order to retain and operates core advanced forces based on 4th IR science and technology such as AI, unmanned robots, etc. Finally, it aims to build a powerful AI science and technology force with a competitive advantage. In accordance with Defense Innovation 4.0, each military is building intelligent smart units using new technologies of the 4th IR [2].

The Army is building advanced and strong units that can monitor the current operational status of all units in real time by applying new technologies of the 4th IR, such as artificial intelligence, big data, augmented/virtual reality, 5G, and the Internet of Things (IoT). The Army's smart unit consists of a super-intelligence platform, a super-convergence intelligence information center, and a hyper-connected network. The super-intelligence platform consists of a warrior platform, an intelligent personnel management/military maintenance system, an intelligent LVCG (Live, Virtual, Constructive, and Game) system, an automated unmanned security system, and a smart troop management system. The super-convergence intelligence information center is based on artificial intelligence and consists of an open algorithm, a high-speed processing shooter computing system, and a data platform for learning. The hyper-connected network establishes

an integrated network system by connecting all platforms, and constitutes an Army-only communication network that can visualize the battlefield by connecting communication networks, means of maneuver, means of surveillance and strike in real time. And Army Tiger 4.0(Army Transformative Innovation of Ground forces Enhanced by the 4th IR technology), the Army's future core combat system, is equipped with optimal detection, determination, and strike capabilities with mobility, networking, real-time hyper-connectivity, and super-intelligence technology [4].

The Navy applies the advanced ICT-based technology to ships to integrate the loading system, reflect the automation system, connect advanced manned / unmanned naval platforms with an intelligent network, and reinforce response capability of maritime accidents and disasters in order to build a smart naval combat system. The smart naval system consists of a system-integrated battleship, a maritime unmanned system, and a wide sea area battlefield surveillance system. System-integrated combat ships build an integrated ship computing environment so that various systems can be operated in a single server environment, and apply automation technology to reduce combat response time and increase maintenance efficiency. The maritime unmanned system is the core of manned/unmanned forces along with combat ships, and consists of three types: unmanned surface boats, unmanned submarines, and unmanned aerial vehicles. And the function will be developed from surveillance/reconnaissance to combat. The wide sea area surveillance system is planned to be built as a system that can detect and monitor long-distance maritime and underwater targets by establishing an over-the-horizon (OTH) radar and a fixed/buoy type underwater surveillance system [5].

The Air Force intend to build a smart air force based on the advanced of the 4th IR as building system such as an intelligent command decision system and aerial unmanned system based on big data and artificial intelligence, an unmanned access control system based on AI and the IoT, a base security system using drones/robots, and demand prediction system for aircraft repair parts based on AI and big data, and a remote base environment management system based on the IoT. The Air Force's super-intelligent smart flight wings is consisted of infrastructure, a platform that processes information collected from the infrastructure, and an application system that utilizes data. The standard platform consists of a standard collection/linkage system that integrates and links networks for each operating systems/equipment, a data integration/distribution system that integrates, classifies/summarizes, and searches/converts various application system data, a content linkage system that exchanges various service linkage (API, etc.) and application system data. The application system consists of a unit situation sharing system that monitors/controls all situations within the command center unit, a base boundary monitoring system that performs real-time monitoring & control and manned/unmanned complex alert operations, facility remote monitoring system for real-time remote monitoring and control of equipment/materials (ammunition, oil, etc.) and so on. The intelligent smart flight wings is a new ICT-based high-tech flight wings that integrates individual operating systems and equipment such as computers and CCTVs in the base through a network to control the operation situation of aircraft, facilities, and equipment in a three-dimensional manner anytime, anywhere. The below figure shows the concept of an intelligent flight wing being promoted by the Air Force. The Air Force intends to be intellectualized all systems with functions

such as monitoring/surveillance/prediction/detection/management/training by utilizing the 4th IR technology [6, 7] (Fig. 1).

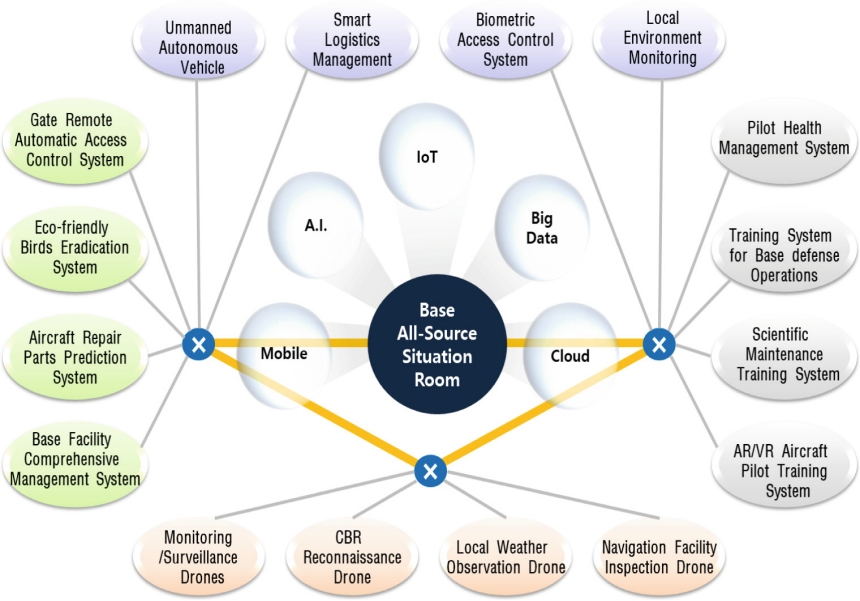

Fig. 1. The concept of an intelligent smart Air Force unit using 4th IR technology

3 Security Threats of Intelligent Smart Units

3.1 Security Vulnerabilities of Intelligent Smart Units

The communication network of the intelligent smart unit is composed of a closed network, so security threats from the outside will be limited. However, if the network is connected to the Air Force headquarters, the Ministry of National Defense, or military organizations connected to the external network, there is a possibility of threat from the outside. The security threats of smart cities, which are similar to the composition and service of intelligent smart units, are classified into outsiders, insiders, and internal/external connection points for security management [8]. Since intelligent smart units operate as a closed network, security threats from an insider's point of view are most likely to occur among security threats in smart cities. In particular, the most serious vulnerabilities are threats arising from internal infrastructure and communication networks. Internal infrastructure threats can occur by exploiting vulnerabilities in the IT infrastructure or by using unauthorized users' internal systems. Threats to the internal communication network may leak internal information through stealing identification and authentication information in the data processing section. An additional security threat is a security threat that can occur in collusion with an insider. Insiders include

employees working in the smart unit, external employees residing within the unit, and external employees who periodically come in and out for system/communication management. If an external employee for checking system/communication connects a PC or USB with ransomware or APT attack programs to the unit's communication network, the most serious damage will occur. Also, supply chain attacks can occur. When a new system is introduced to replace an old system in the unit, a developer or supplier may implant malicious code into the new system for malicious purposes. When a new system infected with malware is installed in the unit, connected to the network and operated, all connected systems are infected.

3.2 Possible Cyber-Attacks Scenarios in Intelligent Smart Units

As mentioned above, since the network of intelligent smart unit is composed of a closed network, a security threat scenario is presented by using cyber-attack techniques with a high possibility of cyber threat targeting the internal network in recent cyber-attack cases. Closed networks have limitations in intruding directly from the outside through the network, so most cases use insider-based attack techniques or supply chain attack [9].

First, it is to use the laptop of an external employee who regularly come in and out the unit for checking system/network (Fig. 2). A hacker injects malware into the laptop

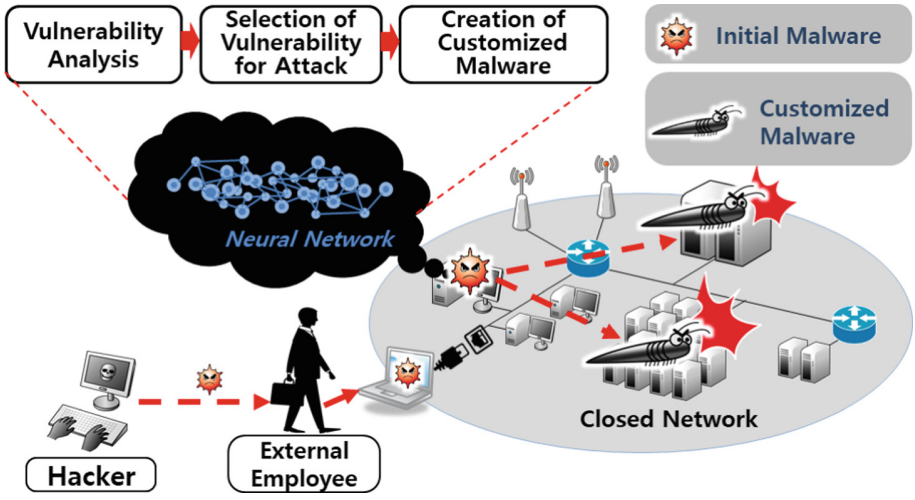

Fig. 2. AI-based malware infection using insiders

of an external employee. And when an external employee connects his laptop to the closed network to check the unit's system and network, the malware code installed in the laptop infects the closed network. Recently, malware perform more intelligent and autonomous functions by applying artificial intelligence. In the past, all processes were programmed by hacker (human), but now, it can be produced quickly and precisely by automating everything from analyzing vulnerabilities to programing malicious codes through artificial intelligence. AI-based malware infects only one system even if it does

not know specific network configuration information inside the closed network, and then uses artificial intelligence to scan surrounding systems and exploits vulnerabilities. After that, it creates a secondary malicious code and infects all systems through self-propagation inside the closed network.

Second, it is a supply chain attack that has recently become a security issue (Fig. 3). Supply chain attacks are mainly used when attacking systems and data that are not easy to attack directly from the outside. When hackers plant malware in the software or systems of software developers and vendors, and when that software or system is installed on the internal network, all connected systems are infected with the malware [10]. Therefore, it is mainly used when attacking systems or data within a closed network that is difficult to intrude from the outside. However, it takes a long time for the software to be developed and installed on the closed network to be attacked. A variety of software or firmware is installed in the closed network of intelligent smart unit, from the infrastructure system to the main asset management & support system and control/command system. In order to always keep them up to date, they are downloaded by connecting to the update server of each software/firmware manufacturer, or an outside company manager directly accesses the base and installs them. Using this point, an attacker can secretly intervene in the software/firmware development process and perform a supply chain attack in order to infect systems inside the closed network with malicious code. The supply chain attack utilizes the following techniques.

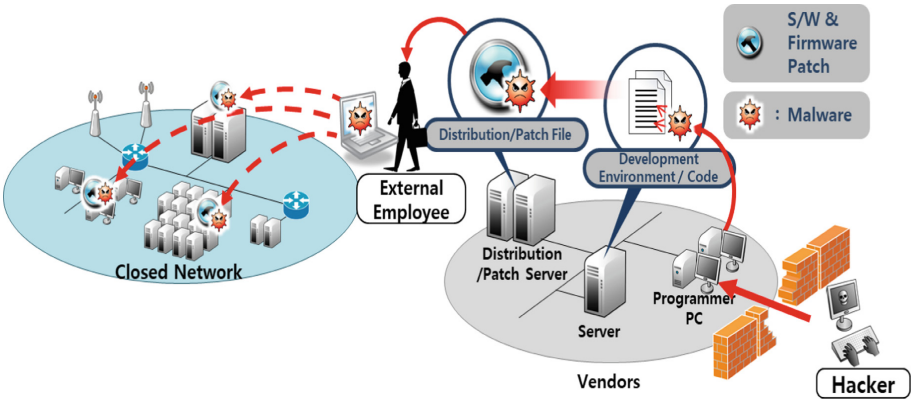

Fig. 3. Penetrating closed networks using supply chain attacks

- A method of infiltrating and tampering with software development (build/update) infrastructure
- A method to sign and distribute certificates of malicious software created by hijacking legitimate certificates used to verify the integrity of software
- A method of infiltrating the internal network by modifying the firmware of network equipment such as switches and routers

4 Design of an Integrated Cyber Defense Platform

The integrated cyber defense platform should include functions to monitor, detect, analyze, and share cyber threats occurring in the mission system such as military operation system, base defense operation system, operation support system, and education and training system. In this chapter, we derive the requirements for designing an integrated cyber defense platform, and propose the design of overall integrated cyber defense platform and the functions of modules.

4.1 Requirements for Designing an Integrated Cyber Defense Platform

As various new technologies are applied to the mission system of intelligent smart units, vulnerabilities will increase, and cyber threats using these vulnerabilities will increase. Recently, the aspect of cyber threats uses intelligent and sophisticated techniques. It is necessary to design an integrated cyber defense platform that can ensure the safety and reliability of the mission system, manage heterogeneous security systems, and monitor/detect/analyze/respond to sophisticated cyber threats in real time. Therefore, it is necessary to derive requirements prior to designing an integrated cyber defense platform.

First, it is necessary to know the type and function of the mission system as well as the applied technology and system configuration operated in the intelligent smart unit. By analyzing the types and functions of the mission system, it is possible to identify a system that performs similar functions in the private sector and to identify the system's vulnerabilities, possible errors or threats. Also, by analyzing the applied technology and configuration status, it is possible to know the vulnerabilities of the applied technology and cyber threats that may occur to the applied technology. In addition, it is necessary to accurately understand the configuration of all network infrastructures to manage networks reliably and to block only those networks when cyber threats occur.

Second, it is necessary to identify the types, performance, and applied technologies of security systems and software installed in closed network and system. It is necessary to analyze whether a security system capable of responding to each type of cyber threat is installed and how well it performs. It is also necessary to check if security functions are duplicated or if a security system capable of responding to threats is not installed. In addition, it is necessary to check whether security functions such as prevention, detection, analysis, sharing, and recovery are missing, and it is necessary to check whether the latest version of the security system is maintained. And it is necessary to check whether new technologies are applied to the security system to respond to sophisticated cyber threats.

Third, it is necessary to be aware of the latest intelligent cyber threats. Among recent cyber threats, intelligent cyber-attacks using convergence tools combining ransomware and APT attack methods and cyber-attack tools with artificial intelligence are difficult to detect with existing security techniques. These cyber threat methods will evolve into more powerful cyber-attack tools through mutual convergence in the future. In addition, artificial intelligence technology will be applied to various cyber-attack tools to achieve more sophisticated and covert attacks. It is necessary to understand the aspects of these intelligent cyber threats in advance so that prevention/detection/analysis functions can be performed accordingly.

Fourth, it is necessary to check linkage between the integrated cyber defense platform and heterogeneous security systems, management methods, and overlapping functions. In other words, it has to determine whether to send only data detected as abnormal behavior in heterogeneous security systems to the integrated cyber defense platform, or send all data except normal behavior data. If all heterogeneous security systems send data to the integrated cyber defense platform, performance degradation and overload problems of the integrated cyber defense platform may occur. In addition, it is necessary to compare whether the functions of the modules of the integrated cyber defense platform overlap with the functions of heterogeneous security systems.

Finally, it should be considered the scalability of the integrated cyber defense platform. An intelligent smart unit can be additionally installed with other mission systems and can be linked with other units. And he future cyber threats that can act as a game changer may occur. As the scope of monitoring cyber assets and threats expands, the platform's functions and modules must also be added.

4.2 Design of an Integrated Cyber Defense Platform

The proposed integrated cyber defense platform was designed by referring to models such as smart city integrated security control system, intelligent integrated security control model, cyber security orchestration, and next-generation security control system. Recently, intelligent/next-generation integrated security control systems utilize artificial intelligence and big data technologies to enable faster data processing, classification, and analysis, more accurately detect threats, and reduce false detection rates [11–13]. The proposed platform also applies big data technology to data collection, processing, classification, and analysis, and applies artificial intelligence technology to analyze and block threats and determine true and false detection.

The integrated cyber defense platform receives security events and suspicious data from heterogeneous security systems installed in the information and communication system of intelligent smart units. And if a threat is detected by analyzing the data, it automatically blocks the threat immediately. In addition, true/false detections are judged once again for the results determined by the individual security system and threat detection module of the platform. If it is judged to be a true positive, it is reported to the base all-source situation room and notified to the incident response team to conduct an accident investigation.

The integrated cyber defense platform consists of seven modules and performs functions such as big data collection and analysis, threat detection and blocking, true/false decision, security system management. The database stores and manages data related to integrated security policies, artificial intelligence and big data (Fig. 4).

The big data collection module collects and processes all security events generated from various heterogeneous security systems based on big data technology. Since various types of events occur in heterogeneous security equipment, various raw data are classified/sorted/refined and classified into structured data and unstructured data. And it interprets and transforms the data so that it can be used in the integrated cyber defense platform. Since raw data is composed according to each language or form, it must be reproduced as meaningful data through data preprocessing techniques.

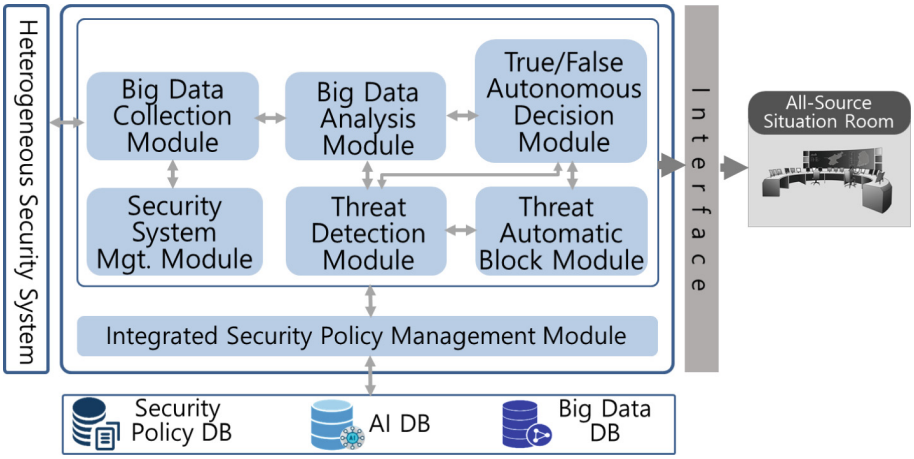

Fig. 4. Design of Integrated Cyber Defense Platform

The big data analysis module performs real-time automatic high-speed search for data related to security threats among data received from the collection module, and performs various big data analysis functions such as threat-related data classification and association (correlation) analysis. In the analysis module, the relationship between threat-related data and between the data set and other data is analyzed in terms of time and causal correlation.

The security system management module manages the operating status of heterogeneous security systems installed to protect various mission systems. When a new or changed security policy is received from the integrated security policy management module, it is sent to the relevant security system so that the security policy can be modified. In addition, the normal operation of heterogeneous security systems is monitored to continuously check for abnormalities. If a problem occurs in the security system, the information is sent to the situation room so that action can be taken.

The threat detection module analyzes the data received from the big data analysis module to determine threats. When judging threats, an algorithm that can quickly and automatically process a large number of security events and an intelligent algorithm that can detect highly complex security events must be applied to reduce false detection rates. Among AI technologies, if supervised/unsupervised learning algorithms are used, large-volume security events and complex security events can be automatically processed and threats can be determined. Since intelligent cyber threats are not one-time, but continuously change the attack type for a long period of time, it is difficult to detect them with a matching algorithm such as a string or pattern (a signature-based algorithm). These intelligent cyber threats must be detected by unsupervised learning algorithm of an AI. AI's unsupervised learning algorithm is a learning model in which AI classifies and judges by itself when various problems are input and derives the result value. In other words, when security events acquired by various security systems are trained with an unsupervised learning algorithm, the algorithm classifies similar types of actions

into cluster units, and determines large clusters as normal actions and small clusters as abnormal actions.

The true/false autonomous decision module judges threats simultaneously with the threat detection module, and re-judges the threats determined by the threat detection module. The judged result is sent to the integrated security policy management module after classifying true and false detection. The integrated security policy management module updates the security policy and sends it to the threat detection module, and the threat determination standard is modified according to the updated security policy. The automatic decision algorithm for true and false detection also uses supervised learning algorithms and unsupervised learning algorithms. The true detection rate is improved through supervised learning algorithm, and the non-detection rate and false detection rate are reduced through unsupervised learning algorithm.

The threat automatic block module blocks the operation of the system or network once the event is judged to be a threat in the threat detection module. In addition, security systems are taken according to the result of the true/false autonomous decision module. Each type of security event is processed by predefined threat response processor step by step, and the processor executes according to the information received from the big data analysis module, threat detection module, and true/false autonomous decision module. For example, an automatic firewall's blocking action is executed for an event having a malicious IP, and this execution action is sent to the integrated security policy management module to update the integrated security policy database.

The integrated security policy management module manages security policies including all security rules and standards processed in the integrated cyber defense platform. When a new event or threat occurs in the module of the integrated cyber defense platform, it is sent to the database through the integrated security policy management module, and when a changed or added security policy also occurs, it is received from the database to the corresponding module of the integrated cyber defense platform. In addition, when a new intelligent threat occurs, the necessary data to configure the learning data is requested to the module, and the received data is sent to the artificial intelligence and big data database.

The database consists of an integrated security policy database, an artificial intelligence database, and a big data database. The integrated security policy database contains security rules, procedures, standards, etc. for the operations by all modules of the platform. When a new or modified threat or security event and new detection mechanism are discovered through the platform's modules, the integrated security policy database is updated through the integrated security policy management module. The artificial intelligence database manages AI algorithms used by modules within the platform and saves data such as learning data. It manages the evolution and change of algorithms to detect new threats or security events as new threat or security event occurs. In particular, it also manages such operations as threat detection/blocking using AI algorithms, malware/domain/IP identification, abnormal behavior auto-blocking, artificial intelligence-based self-mutation, deep learning-based similarity analysis, machine learning-based correlation analysis, real-time threat level analysis, etc. Big data database includes big data collection (big data search, collection, conversion), big data storage (distributed file system, distributed database, distributed system access control, etc.), big data analysis

(distributed parallel processing system, big data analysis language, data visualization) and big data management and saves related data.

4.3 Process of an Integrated Cyber Defense Platform

The modules of the integrated cyber defense platform collect, analyze, and process data and respond to threats as shown in the figure below (Fig. 5).

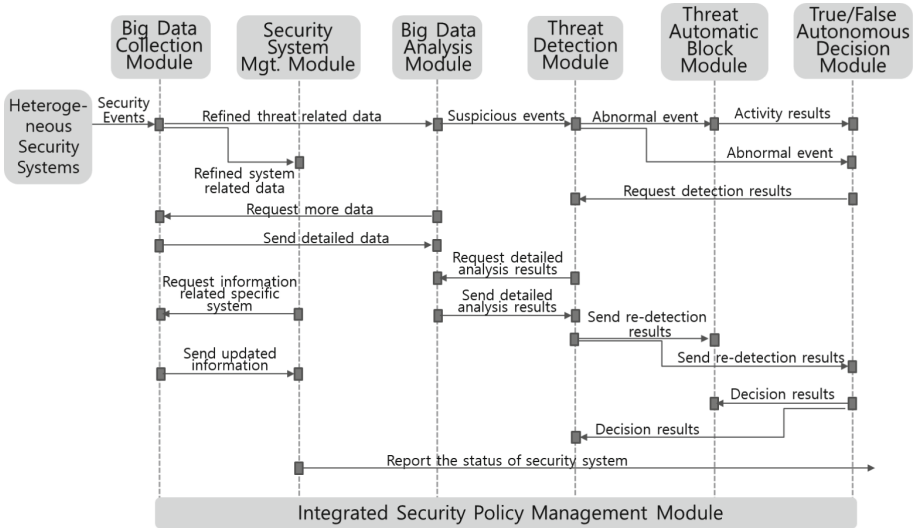

Fig. 5. Process of Modules in an Integrated Cyber Defense Platform

The big data collection module collects abnormal or suspicious events and error data from heterogeneous security systems. Then, such events are refined and sent to the analysis module and security system management module so that the modules of the platform can process them. The security system management module checks the security system in which an error has occurred and identifies the problem. And if action is required, it is reported to the all-source situation room. The analysis module extracts events that can be judged as threats through big data analysis among security events and sends them to the threat detection module. The threat detection module determines abnormal events that can lead to a cyber-attack among suspicious events and sends them to the threat automatic block module and the true/false autonomous decision module. The threat automatic block module blocks the system or network to prevent abnormal events from progressing further into a cyber-attack. The true/false autonomous decision module re-analyzes the detection result determined by the threat detection module to accurately determine whether a threat occurs. If detailed data is needed for judgment, data is requested from the threat detection module. The threat detection module requests the detection result data and additional data to the big data analysis module, executes re-analysis, and sends the result to the threat automatic block module and the true/false autonomous decision module. The big data analysis module also requests the collection

module to collect additional data when the data requested by the threat detection module is insufficient. All execution results from each module are sent to the integrated security policy management module and saved in each database according to the type of data. In addition, the policy management module also performs change management such as modification, addition, and deletion of policies.

5 Conclusion

The proposed integrated cyber defense platform is a security platform customized for military smart units to protect various intelligent mission systems of smart units. Since the network of the military smart unit is composed of a closed network, cyber threats from the outside can be limited. However, if a cyber-attack occurs, such as a supply chain attack or insider threat, the damage will cause enormous damage not only to the unit but also to the all units connected to the unit. Recently, cyber-attack technology has a sophisticated and covert attack form by applying artificial intelligence algorithms. These intelligent cyber-attacks have limitations in protecting them with the existing installed and operating security systems. Therefore, artificial intelligence and big data were applied to the cyber defense platform to quickly detect errors or indications of threats and accurately detect cyber-attack. In particular, we applied big data technology that can quickly collect, analyze, process, and process enormous data generated from various mission systems and security systems. And we also applied supervised/unsupervised learning algorithm to detect threats quickly and accurately and block them preemptively. The true/false autonomous decision function allows to accurately determine the characteristics of a threat by using an artificial intelligence algorithm after detecting a threat.

In the future, it plans to identify the type and form of threats occurring in smart units to strengthen threat detection and true/false autonomous decision function.

Acknowledgement. This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2022S1A5C2A03093531).

References

1. Clark, B., Patt, D., Schramm, H.: Mosaic Warfare. Center for Strategic and Budgetary Assessments, New York (2020)
2. KIMA: Republic of Korea Defense Innovation 4.0 Focus and Major Tasks. KIMA Newsletter **1332**, pp. 1–2 (2022)
3. Eom, J.-H.: Active and context-resilient cyber defense operation applying the concept of performing mosaic warfare. J. Convergence Security **21**(4), 41-48 (2021)
4. Shin, K., Choi, H.-J., Park, S.: Developing a digital twin and extended reality based future integrated combat training platform under 5G. J. Digital Contents Society **22**(4), 727–735 (2021)
5. Park, D.-S.: 'SMART Navy' grand voyage plan based on advanced of the 4th industrial revolution. Bulletin of the Society of Naval Architects of Korea **57**(1), 7–10 (2020)
6. Lee, J.: Air Force and the 4th Industrial Revolution from New Technology Policy Division', Monthly Air Force, No. 493, pp. 6–11 (2019)

7. Lee, J.-S.: Intelligent Smart Flight Group No. 1, 20th Fighter Wing, Monthly Air Force, No.493, pp. 12–14 (2019)
8. KISA: Smart City Security Model, KISA White paper (2020)
9. Eom, J.H., Choi, Y.S., Kim, H.J.: A method for establishing a security platform for air force intelligent smart unit cyber protection. Air force Research paper (2022)
10. Kim, D., Kang, D., Choi, Y., Lee, S., Choi, B.: Trends in supply-chain security technologies. Electronics Telecommun. Trends **35**(4), 149–157 (2020)
11. Oh, Y.-T., Jo, I.-J.: Development of integrated security control service model based on artificial intelligence technology. J. Korea Contents Association **19**(1), 108-116 (2019)
12. Hong, J.-H., Lee, B.Y.: Artificial intelligence-based security control construction and countermeasures. J. Korea Contents Association **21**(1), 531-540 (2021)
13. Lee, S.-H., Jo, I.-J.: Proposal of security orchestration service model based on cyber security framework. J. Korea Contents Association **20**(7), 618–628 (2020)