

## Article

# Security Architecture for Cloud-Based Command and Control System in IoT Environment

Jahoon Koo <sup>1</sup>, Se-Ra Oh <sup>1</sup> , Sang Hoon Lee <sup>2</sup> and Young-Gab Kim <sup>1,\*</sup> 

<sup>1</sup> Department of Computer and Information Security, Security Engineering laboratory, Sejong University, Seoul 05006, Korea; sigmao91@sju.ac.kr (J.K.); terious551@sju.ac.kr (S.-R.O.)

<sup>2</sup> Agency for Defense Development, Seoul 05006, Korea; shlee@add.re.kr

\* Correspondence: alwaysgabi@sejong.ac.kr

Received: 26 November 2019; Accepted: 24 January 2020; Published: 4 February 2020



**Abstract:** With the development of the fourth industrial technology, such as the Internet of Things (IoT) and cloud computing, developed countries including the U.S. are investigating the efficiency of national defense, the public sector and national innovation, and constructing the infrastructure for cloud computing environments through related policies. The Republic of Korea is enacting the related legislation and considering the fourth industrial technology in various fields. Particularly, it is considering the adaptation of the cloud to the command and control system in the national defense sector; hence, related research and pilot projects are being conducted. However, if the existing information system is converted to a cloud computing system by introducing IoT devices, existing security requirements cannot solve problems related to the security vulnerabilities of cloud computing. Therefore, to build a cloud-based secure command and control system, it is necessary to derive additional cloud computing-related security requirements that are lacking in the existing security requirements, and to build a secure national defense command and control system architecture based upon it. In this paper, we derive security requirements for a cloud-based command control system, propose a security architecture designed based thereupon, and implement a security architecture with an open-stack-based cloud platform, “OpenStack”.

**Keywords:** command and control system; C4I system; security architecture in national defense cloud; internet of things; everything as a service; EaaS; OpenStack

## 1. Introduction

Recently, the entry into a hyperconnected society, in which everything caused by the Internet of Things (IoT), big data and cloud technology are connected to the Internet, is progressing rapidly. Research is being conducted to implement everything as a service (EaaS) by combining the IoT and the cloud. EaaS easily integrates technologies, such as databases and distributed caches, on top of an infrastructure as a service (IaaS), which can be used by many government departments. Accordingly, major countries such as the U.S. have released standards and policies related to the IoT and the cloud. For example, they are developing guidelines and standards for managing and operating major IoT issues, such as safety, security, privacy and interoperability. Furthermore, they are rapidly expanding the use of cloud in government and corporations based on the “Cloud First” policy, and building infrastructures to improve national defense and public sector efficiency, to promote national innovation, and to improve the environment of cloud computing. The department of defense (DoD) predicts that the future battlefield will be defined by the Internet of Battlefield Things (IoBT) and the Internet of Military Things (IoMT) that continually spill data such as smart devices, soldier wearable sensors, and drones. IoBT and IoMT involve the full realization of pervasive sensing, pervasive computing, and

pervasive communication, resulting in an unprecedented scale of information produced by networked sensors and computing units.

Additionally, they are transitioning to cloud computing through a joint information environment (JIE) to physically and logically integrate data centers across regions. In Korea, according to the “Basic Plan of the Internet of Things (‘14)”, the “Cloud Computing Activation Plan (‘09)”, and the “Cloud Computing and Competitiveness Reinforcement Strategy (‘11)”, their government departments are adapting the IoT technologies and transitioning to a cloud computing environment. The Korean military recognized the necessity of adapting cloud computing to efficiently manage national defense resource information, and therefore established a defense integrated data center (DIDC) that integrates the computer centers of the army, navy and air force. Moreover, the DIDC provides cloud computing services for systems that are common to all military units.

However, the informatization policy of the Korean Defense Ministry is aimed at cloud computing and the introduction of the IoT; however, the policy is still in its infancy, and no detailed policies and systems exist on the cloud to manage the information collected from IoT devices. In addition, because the security platform, security communication protocol and security solution used by each system of the Korean military are different, it is difficult to comprehensively and enterprise-wide control the command and control system (C4I; command, control, communication, computers and intelligence). Particularly, it is difficult to respond simultaneously at the military level, because each system operates different identity and access managements (IdAMs) that provide different methods of authentication, authorization, and access control. For example, even if the IdAM for each system uses a cryptographic module as the common authentication method, the authentication process may be different for each IdAM, and requires separate maintenance. In addition, it is necessary to unify the use of authentication factors, such as identity information, credentials, and attributes when interworking between systems. The current cloud computing environment is similar to the existing computer system environment; however, other new security vulnerabilities are occurring, and the existing security system cannot respond properly. Therefore, additional security requirements should be derived and applied for a secure national defense information system based on cloud computing.

Hence, it is necessary to derive the security requirements for a cloud-based information system, by analyzing the security requirements applied by the U.S. military when adapting to cloud computing, analyzing the existing security requirements of the Korea military information system, and also the security requirements of the cloud computing system. In addition, it is necessary to design a security architecture to build a cloud-based secure C4I system in an IoT environment based on the derived security requirements. Therefore, we derived security requirements for countermeasures against security threats related to the cloud environment in the previous work [1]. In the previous work, we analyzed the instructions of security requirements for the Korean military information system and the security requirements in the U.S. military for cloud computing. In this paper, we focus on implementation for authentication and authorization as an IdAM module. Based on the analyzed security requirements, we design a security architecture and implement the IdAM module for authentication and authorization in the cloud-based command and control system. Additionally, we propose the operational view (OV) of the C4I system that focuses on access control. The proposed security architecture has a cloud-based and centralized IdAM. Unlike the general system environment, in the C4I system, the usage of a different authentication system for each branch (i.e., the army, navy and air force) is inefficient in performing real-time operations, and therein occurs the inconsistency problem. The proposed centralized IdAM based on cloud computing provides consistent authentication, authorization, and access control to achieve the easy management of identity information and credential. Moreover, it affords a lower maintenance cost by each system. In addition, we implement a testbed that performs the authentication and authorization of the designed security architecture. The testbed uses biometrics for multifactor authentication. We focused on implementing the specific test example as a method of authentication and authorization. It represents the applicability of several scenarios that include various authentication methods, such as biometrics, certificates and cryptographic modules.

This paper is organized as follows. Security factors such as the interworking, security architecture, and the security requirements of the Korean and U.S. national defense C4I system, are analyzed in Section 2. Security requirements of the cloud-based C4I system are derived in Section 3. The cloud-based security architecture for the Korean military based on the derived security requirements is proposed in Section 4. The test scenario and implementation of a testbed based on “OpenStack” is proposed in Section 5. In Section 6, the existing C4I system is compared with the proposed security architecture, and Section 7 presents the conclusions of our study.

## 2. Background

In this section, we analyze the environment of the national defense C4I system for the U.S. and Korean military. In Section 2.1, we analyze the security architecture and security requirements of the cloud certification system used by the DoD. In Section 2.2, we analyze the security requirements of the Korean military information system and the interoperability among the C4I systems.

### 2.1. DoD C4I System

#### 2.1.1. Security Architecture in DoD

As depicted in Figure 1, the JIE single security architecture (SSA) is a DoD security architecture designed to establish a secure network for defense cyber infrastructure operation, and to develop a common countermeasure against cyber threats through control. By integrating distributed servers and services around the core data center, a joint security structure is realized through a joint regional security stack (JRSS), which transforms the distributed security structure into a standardized single security structure [2,3]. The JRSS is a key element of JIE network security. It strengthens the security of DoD networks and functions as a firewall. Additionally, it performs intrusion detection and prevention, enterprise network management and virtual routing and forwarding. It provides a common approach to network defense for all military organizations such as the army, navy, and air force.

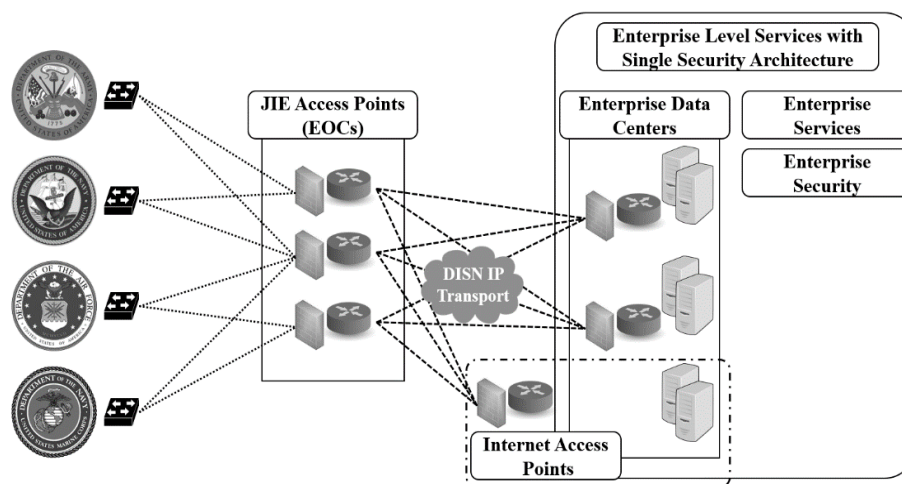


Figure 1. Joint information environment (JIE) Single Security Architecture (SSA) [2].

The U.S. Army, Navy, Air Force, and Marine Corps intend to use enterprise-level services protected by the SSA. Requests for the use of military enterprise-level services first reach JIE access points (enterprise operation centers). The request includes an IP conversion process from the JIE access point to the enterprise data center.

The user then accesses the SSA-protected enterprise-level data center and uses email, cloud computing, identity manager, access management, the enterprise portal and enterprise licensing services. This centralized security architecture eliminates redundant countermeasures, thus minimizing the complexity of overlapping and redundant roles and responsibilities, and hence the exposure to

cyber-attacks. Furthermore, it provides global context awareness through centralized network security control, enabling a rapid command and control of mission commanders in cyberspace.

### 2.1.2. Security Requirements of National Defense Cloud Service in DoD

The DoD has implemented IdAM services on a “per-application, enclave, or per-system basis” [4]. Furthermore, the DoD used the common access card (CAC), which is a common means of authentication, such as the current Korean military’s cryptographic module. However, inconsistency problems occurred owing to the different authentication, authorization, and access control processes for each system. Consequently, the U.S. military is currently building a cloud-based national defense information system through a JIE, and deploying the JRSS to enhance the security of information exchange and data access. Additionally, it is deriving and directing the security requirements of cloud computing through the security requirements guide of cloud computing from the federal risk and authorization management program (FedRAMP) and the defense information system agency (DISA). Table 1 summarizes the security requirements published by the FedRAMP, and Table 2 summarizes the cloud computing security requirements published by the DISA [5,6]. The DoD provides a standard approach to security assessment, certification, and continuous monitoring of cloud products and services through the FedRAMP. Cloud service providers that provide products and services to the U.S. government must certify their compliance with the FedRAMP, which is a requirement specified in NIST 800-53; i.e., security and privacy for federal information systems and organizations. In addition, more than 2000 U.S. government agencies currently use various Amazon web services (AWS), and the DoD applies AWS to process, store and transmit data. AWS obey the security requirements through the certification of the DISA under the DoD. It defines security requirements guides, as summarized in Table 2, and provides a standard assessment and certification process.

**Table 1.** Federal risk and authorization management program (FedRAMP) Security Controls Baseline [5].

Name	Requirements
FedRAMP Security Controls Baseline	Access Control
	Security Alert and Education
	Inspection and Responsibility
	Evaluation and Authorization
	Configuration
	Emergency Management
	Identification and Authentication
	Incident Response
	Maintenance Management
	Media Security
	Physical Environment Defense
	Plan
	Personnel Security
	Calculate Threat
	Add System and Service
	System and Communication Security
	System and Information Integration

**Table 2.** Defense information system agency (DISA) Cloud Computing Security Requirements Guide [6].

Name	Requirements
DISA Cloud Computing Security Requirements Guide	Availability assurance
	Usage of SSL/VPN
	Recovery (Duplexing, Backup)
	Security Team Composition
	Resilience, on-Demand Scalability
	Maintain Operational Transparency
	Personnel Security
	Logical Separation of Information Data
	Physical Separation of Information Data

## 2.2. Existing C4I System in Korea

In this subsection, the interworking among the existing Korea C4I systems and the “National Defense Cyber Security Instruction”, which specifies the security requirements of existing information systems in the Korean military, is analyzed. However, the interworking process among the Korean C4I systems and the “National Defense Cyber Security Instruction” are not fully disclosed; therefore, we present the analysis of only a few factors.

### 2.2.1. Security Requirements for Existing Information System

Currently, security-related instructions of the Korean military include the “National Defense Cyber Security Instruction”, the “National Defense Security Task Instruction” and the “National Defense Informatization Task Instruction”. Each instruction is related and referenced in other laws. Among them, the security requirements of the Korean military information system are attached to the “National Defense Cyber Security Instruction”, and five fields of information security and 237 detailed requirements exist. The “National Defense Cyber Security Instruction” aims to establish guidelines and procedures for all tasks for creating, maintaining and protecting an accurate, safe and effective national defense cyber space. The five fields of security requirements include network security, server security, personal computer security, application system security and security management. The national defense information system is classified as “A”, “B” and “C” by the importance and risk of assets based on confidentiality, integrity, and availability. Therefore, the detailed requirements of each field are classified according to the importance of the national defense information system. The security requirements of the national defense information system specified in the “National Defense Cyber Security Instruction” are currently lacking the security requirements for cloud integration. It is necessary to add security requirements for virtualization and cloud service asset management.

### 2.2.2. Interworking among the C4I Systems

Currently, the C4I system of the Korean military is composed of the allied Korea joint command and control system (AKJCCS), Korean joint command and control system (KJCCS) and the army tactical command information system (ATCIS), Korea naval command control system (KNCCS), air force command control system (AFCCS) and the C4I system below the battalion level. The internal systems (authentication and authorization systems, etc.) operated by each C4I system are different. In addition, the army, navy, and air force C4I systems have limited direct interworking with each other, and can currently perform data sharing through interworking with the KJCCS. Security measures necessary for interworking with the KJCCS and ATCIS are analyzed in this subsection. In the current Korean military, users must receive a cryptographic module first and register it in the system. In addition, because the key management system for each C4I system is established, the ID, password and cryptographic module for each system must be used, and each system must have an interworking-router and interworking-server, separately.

Therefore, for users of the ATCIS C4I system to access the KJCCS C4I system, they must be authenticated with the ATCIS ID, password and cryptographic module first, and additionally authenticated with the KJCCS ID and password. Such a process, which does not involve direct interworking among the army, navy, and air force C4I system, lacks security and convenience during operation owing to decryption when exchanging data for each C4I system.

### 2.2.3. Related Works

Singh et al. [7] propose the visualizing of a military health service (MHS) platform, which is based on hierarchical IoT architecture and the semantic edge-based network model, which plays a significant role in communicating tactical and nontactical pieces of information over the network. They made the command and control center as the semantic edge component that correlates the events happening in real time. The center is entrusted with making vital decisions on the tactical arena of



the battlefield, and the proposed architecture aims to provide a secured zone to monitor health and weapons conditions. They have introduced the semantic edge computing mechanism to deal with a large amount of health data in terms of processing, storing and sharing information. In addition, they give general requirements the impetus of military health services (MHS), based on the semantic Edge for the IoT architecture, and present remarks of the proposed scenario and challenges of security and privacy in edge computing-enabled IoT systems.

Castiglione et al. [8] analyze the importance of static and dynamic biometrics in IoMT or IoBT. In these environments, an increasing number of ubiquitous sensing and computing devices are worn by military personnel and embedded within military equipment (combat suit, instrumented helmets, weapon systems, etc.) are capable of acquiring a variety of biometrics (e.g., face, iris, periocular, fingerprints, heart-rate, gait, gestures, and facial expressions), and they also emphasize the importance of cloud computing and edge computing in managing the data collected by various sensors in these IoMT and IoBT environments. This edge computing can potentially play a crucial role in enabling user authentication and monitoring through context-aware biometrics in military/battlefield applications.

Smith et al. [9] propose and analyze an architecture that adopts cloud computing design methodologies and adapts existing cloud implementations to the tactical environment. They aim to develop technical approaches to mitigate the difficulties in a tactical environment and increase the effectiveness of the military. Because the military often operates in tactical environments with limited resources that reach back, their communications may be low bandwidth and intermittent. Additionally, in this work, they distinguished the layers, such as the application layer, cloud layer, network layer and the compute and energy layers. They also identify and analyze the key functions of each layer.

There have been some projects related to the use of cloud computing technology in the military by a few countries. Traditionally, national defense forces operate using systems designed for using proprietary protocols. However, the researchers at the communications electronics research, development and engineering center (CERDEC) of the U.S. army are working on a cloud-based command and control platform. This platform enables soldiers to access crucial command control and intelligence services with a wide variety of military computers of variable link capacities located anywhere in the battlefield [10]. Another initiative is being carried out by the DoD, and it is called the rapid access computing environment (RACE), which is a private cloud providing IaaS and PaaS for the DoD, and is predominantly used for development and testing [11].

Currently, the Korean Ministry of the National Defense has been promoting various pilot projects and policies to adopt cloud computing. The “National Defense Cloud Proliferation Policy Study” analyzes international cloud-related policies and presents national defense cloud promotion strategies. Promotion strategies that propose the fourth industrial revolution and cloud application plans include the analysis of national defense cloud application cases, which suggests the need to improve laws, institutions and instructions to spread defense cloud adaption, and the need to establish application plans for each cloud type.

The DoD aims to provide enterprise-level commercial cloud services including IaaS and platform as a service (PaaS) to the DoD and mission partners through a joint enterprise defense infrastructure (JEDI) project. Additionally, it discusses JEDI cloud requirements and attempts to achieve the major goals of the national defense cloud. Kim et al. [12] reported the necessity and solution of building a Korean combat cloud. A combat cloud refers to data distribution and information sharing network, where all combatants, combat platforms and nodes transparently utilize essential information across the entire military operation in multiple combat spaces. Furthermore, they explained the structure of a combat cloud and discussed its future direction. Jeong et al. [13] reported that cloud adaption in the national defense sector is difficult because of many limitations, such as the characteristics of the national defense task and the diversity of information system operations in each military. Therefore, they suggested policy directions and strategies for the proliferation of national defense clouds.

### 3. Security Requirements of Cloud-Based C4I System

In this section, we explain the derived security requirements for the cloud-based C4I system by referencing the security requirements of the Korean military information system and the cloud-related security requirement of the DoD and Korea institute. We derived security requirements for countermeasures against security threats related to the cloud environment in the previous work, that must be considered when the current military environment adapts cloud computing. In order to derive the new security requirements, we referenced the security requirements identified by the ‘Security Controls Baseline (FedRAMP)’ [5], ‘Cloud Computing Security Requirements Guide (DISA)’ [6], ‘Security Certification Guide for Cloud Service (Korea Internet and Security Agency)’ [14], ‘Security Requirements for Server Virtualization System (Telecommunications Technology Association)’ [15] and ‘Security Guidelines of National and Public Institution for Cloud Computing (National Intelligence Service)’ [16]. The derived security requirements are divided into five fields and contain 28 items, as shown in Figure 2. The fields include virtual security, data protection, network security, access control and risk management. Security requirements related to virtualization technology require factors for virtual resources, such as virtual machines, virtual storage, virtual servers and virtual software. Virtualization security applies to servers, PCs and applications. Server virtualization security includes hypervisor security and public server security, and application security includes virtual software security. Public server security demands the requirements of physical and technical security measures for websites to provide a virtual resource and a server to distribute virtual software, such as applications. Virtual software security is a requirement where the cloud computing service provider must provide a virtual environment comprising a clear source, a distribution channel and manufacturers. In addition, the three fields typically include malware control, interface security and API security in a virtual environment. Security requirements for the resource management of cloud computing systems include identifying information assets such as information systems and information security systems used in cloud computing, management by security level, and continuous monitoring. In addition, it is necessary to manage the creation, modification and withdrawal of virtual resources to ensure the integrity of the virtual resource and to monitor the change of virtual resource. Separate authorizations and procedures for users or terminals accessing cloud computing services are required, and risk management for cloud computing is required by establishing appropriate control policies and security technology plans. The detailed contents can be referenced in our previous paper [1].

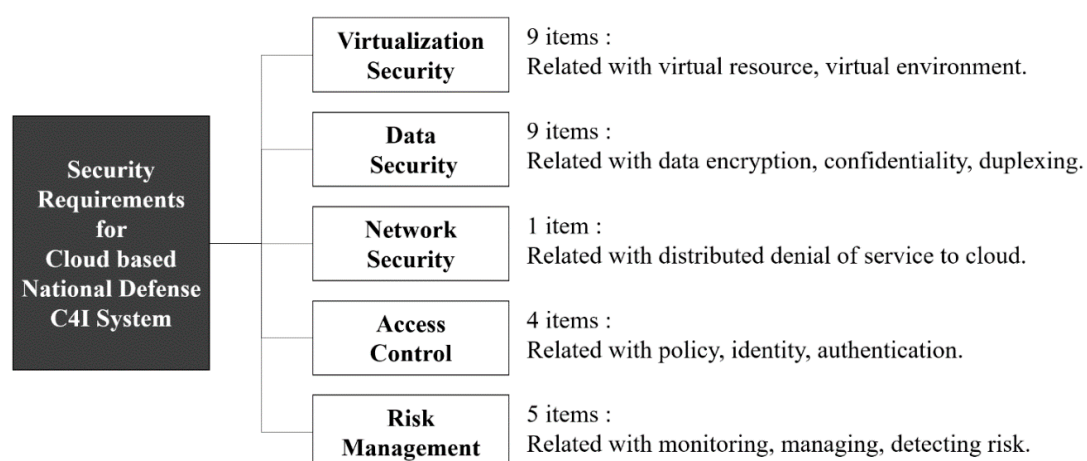


Figure 2. Security Requirements for the Cloud-based National Defense C4I System.

### 4. Security Architecture for Cloud-based C4I system

In this section, the security architecture design of the cloud-based C4I system based on the analyzed security requirements is presented, and the operation procedure emphasizing the authentication and

access control is described. The security architecture proposed in this paper comprises three layers, as shown in Figure 3. The security architecture comprises the virtualization and physical layers, both of which comprise the operating layer for managing all layers. The virtualization layer is divided into a virtual application layer and a virtual infrastructure layer. The virtual application layer is the software as a service (SaaS) of a cloud computing system, and the virtual infrastructure layer is the IaaS of a cloud computing system. The “cloud-based C4I system” on the left side of Figure 3 represents the components of the future cloud-based Korean C4I system.

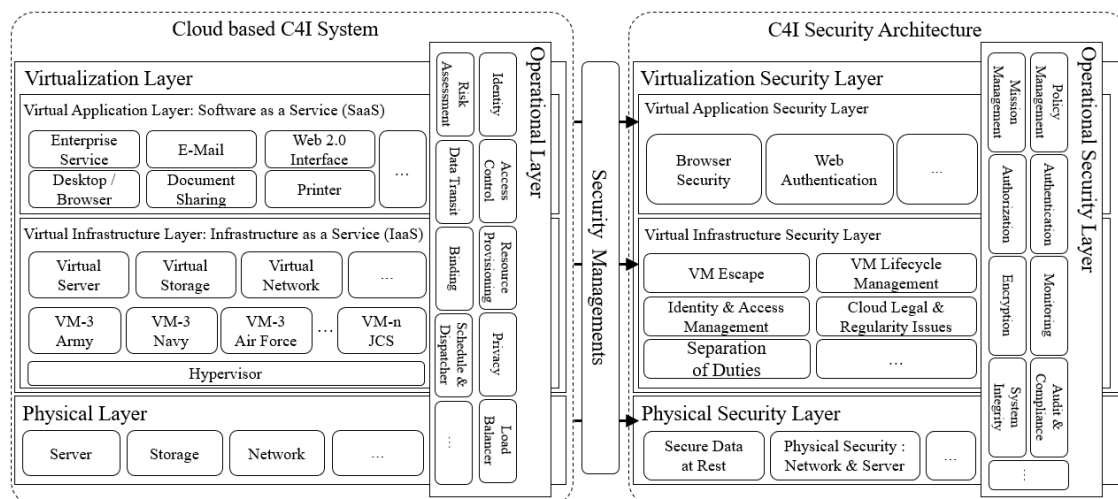


Figure 3. Proposed Security Architecture for Cloud-based C4I System.

And the “C4I Security Architecture” on the right side of Figure 3 represents the security factors for each layer of the C4I system. The virtual application layer includes service factors that can be used by system users such as enterprise services, document sharing, email and web servers. The security factors for the layer include web browser security and web authentication.

The virtual infrastructure layer includes the virtual environment, virtualization network, storage and server, which can be allocated in each C4I system; the security factors for this layer include elements such as virtual machine (VM) sprawl and VM escape attack. The physical layer includes physical devices in the physical data center. Additionally, this layer includes the security of stored data and physical elements, such as networks and servers. The operational layer manages these three layers and contains security elements including access control, such as policy and task management, authentication and authorization, monitoring and auditing, and secure encryption of stored and transmitted data. We aim to develop an IdAM module that serves as authentication, authorization and access control in the functions of the operation security layer. Authentication, authorization and access control are the processes of confirming the user suitability for using a service and granting authority. These processes are important for blocking unauthorized users from accessing a service.

Therefore, referring to the derived security requirements and architecture, the authentication, authorization and access control functions of the cloud-based C4I system in the IoT environment are shown in a use case diagram, as shown in Figure 4. Actors in the use case diagram include “users”, “services”, “national defense integrated policy managers”, “national defense integrated security managers” and “administrator for each military information system”. A “user” includes user registration, credential registration and management, login, user authentication, authorization and access control, and service access. The “national defense integrated information security policy manager” manages security policies related to authorization when users access a service. The “national defense integration security manager” manages information such as identity information, credential values, and user missions. The “administrator for each military information system” manages the information on the army, navy, and air local systems. The proposed use case diagram and the existing



C4I system differ vastly in terms of two aspects. First, the existing C4I system requires a complicated user registration process. The administrator registers the physical credentials with the key management infrastructure, issues them, and delivers them directly to the user. The user applies for registration using the physical credentials and the specified logical credentials.

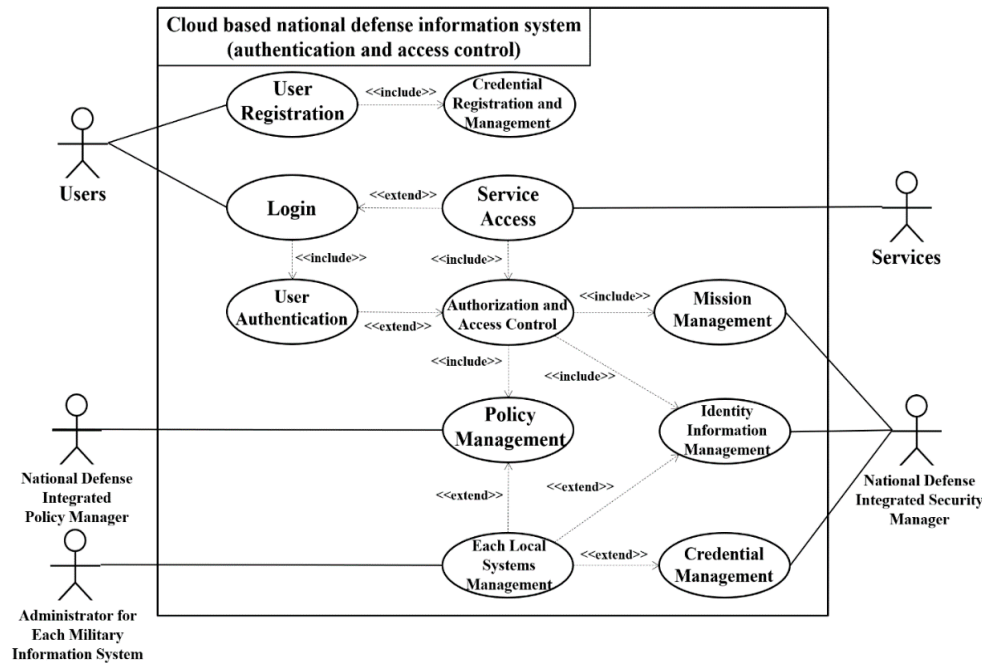


Figure 4. Authentication and Access Control Use Case Diagram for Cloud-based C4I System.

However, in the proposed system, users can apply for user registration directly through the cloud service, and after the administrator's approval, the service according to the authority can be used. Second, the existing C4I system requires the permission of each unit manager for the remote access of the user and requires a limited environment; however, the proposed system aims to provide cloud services through the terminal, anytime and anywhere. The sequence is created based on the use case created and is shown in Figure 5.

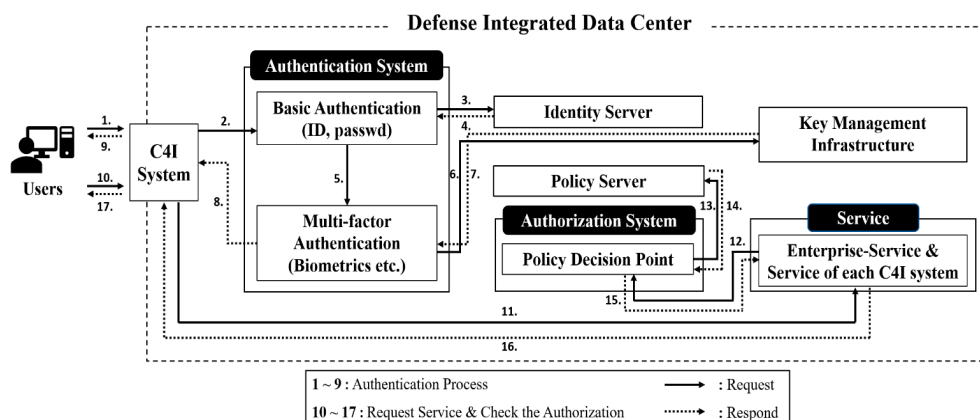
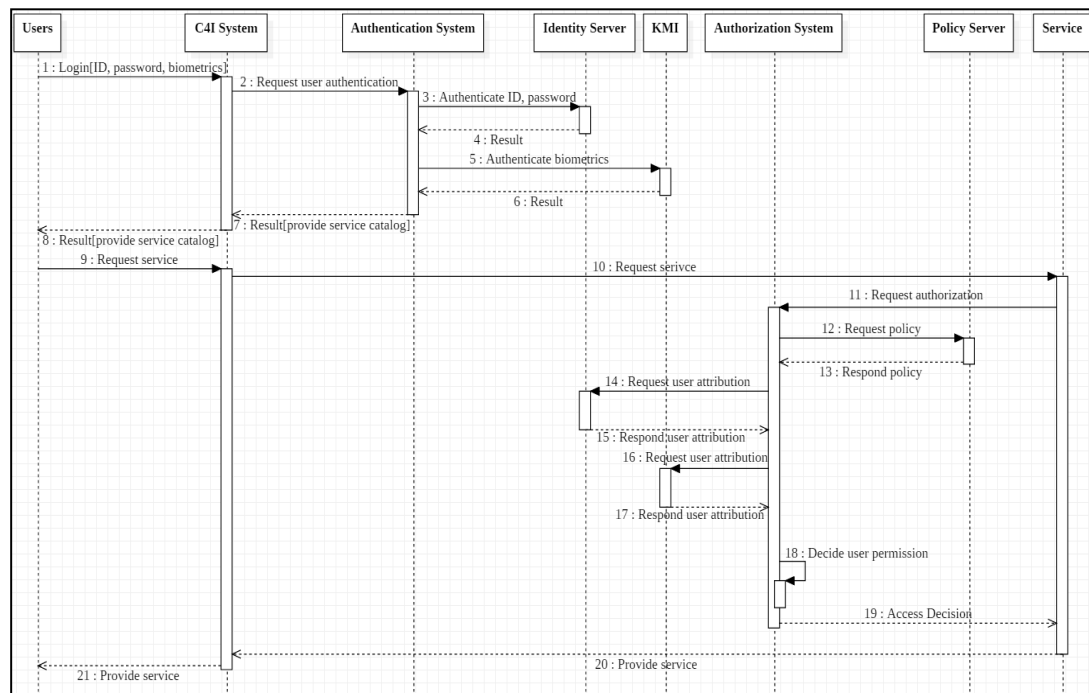


Figure 5. Authentication and Access Control for Cloud-based C4I System.

The elements in Figure 5 include users of the entire army, the C4I system, authentication system, authorization system, identity information server, policy server, key management system and military service. The C4I system allows users to access the integrated data center similarly as web browsing. In addition, numbers 1 to 9 in Figure 5 show the authentication process of registered users, and numbers

10 to 17 show the request for military services and the authority verification process. The authentication system includes basic authentications such as ID and password, and multifactor authentications such as biometric information. For basic and multifactor authentications, an identity server and key management system are used. The authorization system verifies the authority of a user utilizing the policy server, and permits the use of the service. In addition, a multifactor authentication should be additionally performed according to the confidentiality level of the service; in this case, reference information such as mission information and rank of the military for users may be referred to. Additionally, the detailed sequence diagram of authentication and access control for the cloud-based C4I system is shown in Figure 6.



**Figure 6.** Sequence Diagram of Authentication and Access Control for Cloud-based C4I System.

1. The user logs in using the registered account information. The user inputs the ID, password and fingerprint through a client device such as a web browser, and sends them to the C4I system (web server).
2. The C4I system requests authentication (ID, password and fingerprint) to the authentication system.
3. The ID and password are compared with the identity server.
4. The authentication system confirms the authentication result.
5. The biometrics are compared with the key management infrastructure (KMI).
6. The authentication system confirms the authentication result.
7. The authentication system sends the authentication result to the C4I system.
8. The C4I system shows the login result to the user through the client device, and when the user login is successful, it shows the available services (service catalog) to the user.
9. The user requests a service through the client device and sends it to the C4I system.
10. The C4I system sends the request to the service.
11. The service requests the authorization system to verify user permission.
12. The authorization system requests the policy for the service to the policy database.
13. The policy database returns the policy for the service to the authorization system.
14. The authorization system verifies the policy for the service and requests the user attributes such as identity information to the identity server.

15. The identity server returns the user attributes requested by the authorization system.
16. The authorization system requests the user attributes such as biometrics to the KMI.
17. The KMI returns the user attributes requested by the authorization system.
18. The authorization system compares the combination of user attributes with the policy for the requested service to determine the permission.
19. The authorization system sends the result for the access decision to the service.
20. The service verifies the access decision authorization system and provides the service to the C4I system when the permission is appropriate.
21. The C4I system provides service to the user through the client device.

## 5. Proof of Concepts

In this section, we create the test scenario and implement the testbed for the authentication and authorization of the designed security architecture. The authentication and authorization are the main functions of IdAM in the national defense information system and determine whether a user can access to confidential services. We use the open-source cloud platform “OpenStack”. In this platform, we use the user ID and password as our basic authentication, and use the fingerprint information as the multifactor authentication. We focused on implementing the specific test example as a method of authentication and authorization. It represents the applicability of several scenarios. However, our scenario can be adapted to other scenarios by changing the authentication method. For example, authentication methods include biometrics, certificates and cryptographic modules. In this paper, we have created and implemented a scenario of authentication methods that use fingerprint information among them.

The environment of the testbed for authentication and authorization is explained in Section 5.1, and the test scenarios are described in Section 5.2. The implementation of authentication and authorization based on the testbed environment and scenario are described in Section 5.3.

### 5.1. Implementation Environments

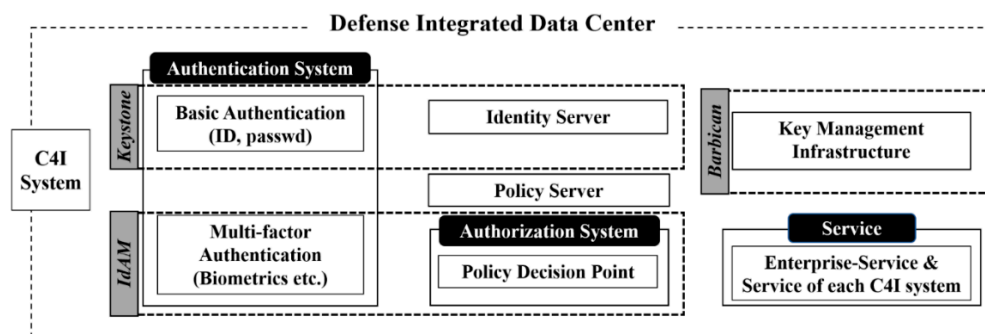
Table 3 shows the test environment and configuration used in this implementation. As a cloud platform, we used “OpenStack”, which is an open-source cloud operating system that enables cloud computing services to be created and operated on common servers. Consequently, it can build and manage cloud computing environments in the form of IaaS, which affords infrastructure resources. “OpenStack” contains many components in addition to the core components necessary to compose a cloud environment. Hence, various functions for the cloud environment configuration can be installed and used as required, thus providing flexibility and scalability. The components used in this implementation are “Keystone” and “Barbican”. “Keystone” is a service that proves the authenticity of all users and services in “OpenStack”, and provides an endpoint for all “OpenStack” services. “Barbican” is an “OpenStack” key management service that provides the secure storage, provisioning and management of secret data. We selected the fingerprint identification information as an element of multifactor authentication, and the FPM10A sensor that identified this fingerprint information was used. In addition, to implement a fingerprint identification function in the IoT environment, a fingerprint identification sensor was attached to the Raspberry Pi.

When implemented using “OpenStack”, the created OV and role mapping are as shown in Figure 7. Basic authentication and identity management, such as IDs and passwords, are performed in “Keystone”. The basic authentication uses the basic components of “OpenStack”; however, additional environment configurations are required for multifactor authentication. When accessing the proposed C4I system, multifactor authentication using biometric information, as well as ID/password is used for multifactor authentication. However, the basic environment configuration provided by “OpenStack” does not satisfy a multifactor authentication, because user authentication is performed using only the ID/password. Additionally, it provides only a time-based, one-time password function using Google Authenticator. Therefore, it is necessary to additionally implement an IdAM module that performs

multifactor authentication and authorizes user requests based on policies. “Barbican” manages the credential information used for multifactor authentication.

**Table 3.** Test Environment and Configuration.

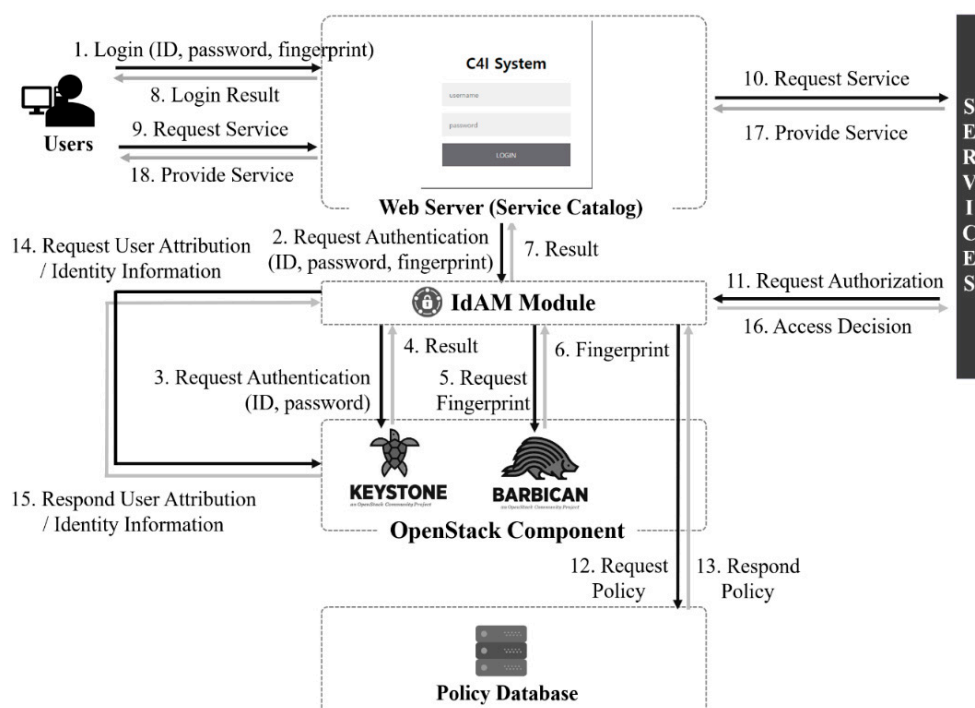
	Name	Language
Web Server	Flask Framework	Python
Cloud Platform	OpenStack Queens Ver	Python
Sensor	Raspberry Pi 3 Model B+ Chrome Extension Fingerprint Scanning Program FPM10A	Python JavaScript Python, PyQt5



**Figure 7.** Authentication and Access Control Function in OpenStack C4I system.

## 5.2. Scenario

Figure 8 shows the big picture of authentication and access control in the OpenStack C4I system. The user must create an account through the registration before using the service. Furthermore, the user ID, password and identity information, such as military rank and fingerprint, must be registered. The administrator confirms the validity of the user registration and approves it.

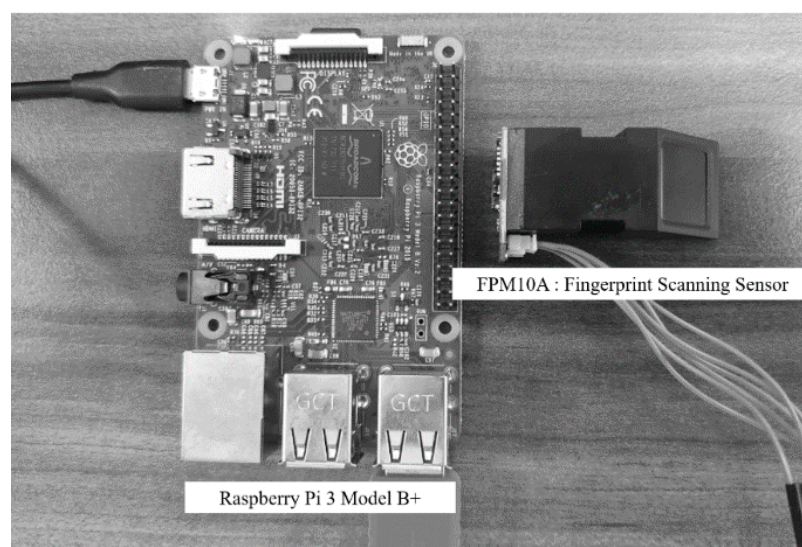


**Figure 8.** Authentication and Access Control in the OpenStack C4I system.

1. The user logs in using the registered account information. The user inputs the ID, password and fingerprint through a web browser, and sends them to a web server.
2. The web server requests for authentication (ID, password and fingerprint) to the IdAM module.
3. The ID and password are sent to “Keystone” for authentication.
4. “Keystone” sends the authentication result to the IdAM module.
5. The IdAM module requests the fingerprint information that maps the input ID to “Barbican”.
6. “Barbican” sends the fingerprint information that maps the ID to the IdAM module.
7. The IdAM module compares the fingerprint received from “Barbican” with the input fingerprint and sends the authentication result to the web server.
8. The web server shows the login result to the user through a browser and when the user login is successful, it shows the available services (service catalog) to the user.
9. The user requests the service through a browser and sends it to the web server.
10. The web server sends the request to the service.
11. The service requests the IdAM module to verify the user permission.
12. The IdAM module requests the policy for the service to the policy database.
13. The policy database returns the policy for the service to the IdAM module.
14. The IdAM module verifies the policy for the service, and requests the user attributes such as identity information and fingerprint to “Keystone” or “Barbican”.
15. “Keystone” or “Barbican” returns the user attribute information requested by the IdAM module.
16. The IdAM module compares the combination of user attributes with the policy for the requested service to determine the permission and sends the result to the service.
17. The service verifies the access decision by the IdAM module and provides the service to the web server when the permission is appropriate.
18. The web server provides the service to the user through the browser.

### 5.3. Implementation

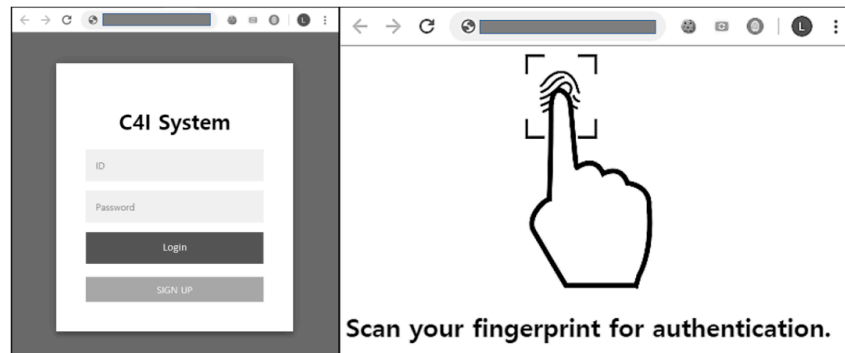
We have created the test scenario for the authentication and authorization of the designed security architecture, and this subsection describes the implementation of this scenario. The testbed was implemented using fingerprint authentication for multifactor authentication. To scan the fingerprint information, we used the FP10A sensor. The FP10A was attached to Raspberry Pi for composing the low computing environment, such as the IoT environment, as shown in Figure 9.



**Figure 9.** Fingerprint Scanning Sensor.

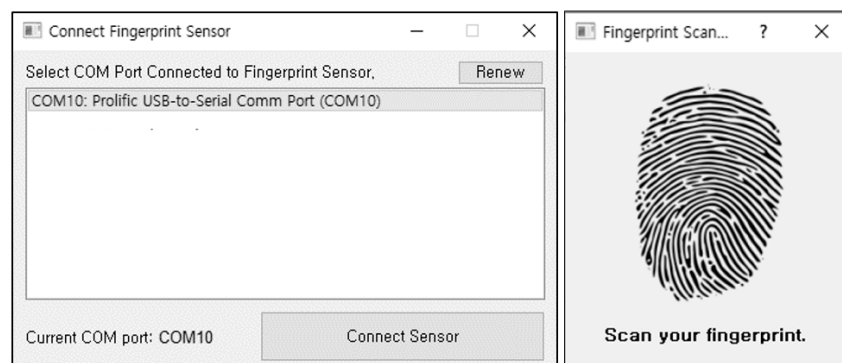


The user connects to a web server and inputs the ID, password and fingerprint information. To implement this testbed, we built a web server as shown in Figure 10. When the user enters the ID and password, the user is directed to a page where fingerprint information can be input.

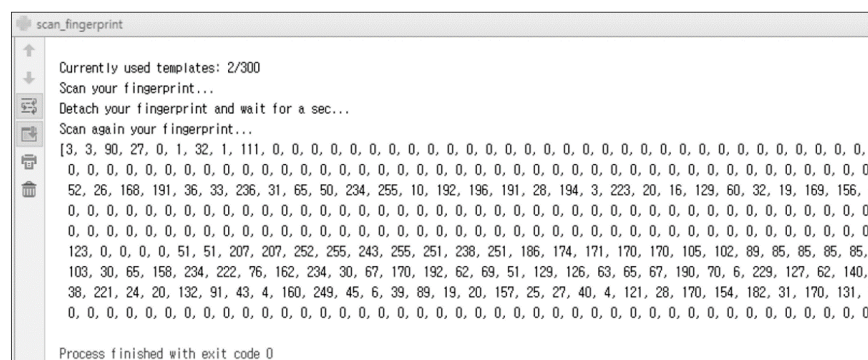


**Figure 10.** Web Server for Cloud-based C4I System.

After the user visits the page where the fingerprint is input, the fingerprint scanning module is automatically executed, as shown in Figure 11. The user selects the appropriate USB port in the module, clicks the sensor connection, and clicks a window to scan the fingerprint. The scanned fingerprint information is in the stream format, as shown in Figure 12. The user fingerprint information is scanned at the time of user registration in advance, and is stored in “Barbican”. The IdAM module compares the registered fingerprint information with the scanned fingerprint information to allow user login. After a successful login, the user is shown a list of available services. When the user requests a service, the IdAM module grants permission by combining the fingerprint and identity information.



**Figure 11.** Scanning Fingerprint Module.



**Figure 12.** Characteristic of Scanned Fingerprint.

## 6. Evaluation and Discussion

In this section, we compare the security requirements published by FedRAMP, DISA and the derived security requirements that should be newly added to the Korean military. In addition, based on this comparison, it also evaluates which parts of the security architecture correspond to the security requirements, as shown in Table 4. It includes access control, risk management, and data security requirements. These security requirements related with security elements in the operational security layer, virtual infrastructure security layer, and physical security layer of the security architecture. In Table 4, “Physical environment defense” and “Physical separation of information data” correspond to the physical security layer in the security architecture.

**Table 4.** Comparison between Security Requirements and Security Architecture.

Security Requirements of FedRAMP and DISA	Security Requirement for Cloud-Based National Defense C4I System	Security Architecture for Cloud-Based National Defense C4I System
Access control and authorization	Access control: related with policy, identity, authentication	Operational security layer: authorization and authentication
Identification and authentication		
Security alert and education	Risk Management: related with monitoring, managing, detecting risk.	Operational security layer: audit and compliance, monitoring, system integrity, etc.
Emergency management		
Incident response		
Maintenance management		
Calculate threat		
Recovery (duplexing, backup)	Data security: related with data encryption, confidentiality, duplexing	Operational security layer: encryption, system integrity
Logical separation of information data		Physical security layer: secure data at rest
Physical environment defense	Existing security requirement: physical security	Virtual infrastructure security layer: Separation of duties
Physical separation of information data		
		Physical security layer: secure data at rest, physical security, etc.

However, these physical security requirements are not included in the list of newly derived security requirements because they exist in existing Korean military security requirements.

We also compare and evaluate the interworking process between the existing C4I systems and the newly proposed security architecture OV. Table 5 shows the differences in interworking among the army, navy, and air force C4I systems, IdAM, and authentication factors. The existing C4I system has limited interworking with the army, navy and air force, and exchanges data through interworking with the KJCCS. In addition, different IdAMs exist for each C4I system, and the authentication, authorization, and access control methods and processes provided by each IdAM are different. However, in the cloud-based C4I system, the data of each system can be interworked through the cloud. It can provide consistent authentication, authorization, and access control because it has a centralized IdAM. Therefore, it is easy to manage identity information and credential values. In addition, the existing C4I system requires each user ID, password and cryptographic module for the KJCCS. Meanwhile, in the cloud-based C4I system, multifactor authentication factors such as ID, password and biometric information or cryptographic modules are required.

However, the proposed scenario can be applied to other systems, but it has a limitation that only a specific test scenario is implemented. In the implementation section, the user ID, password and fingerprint information is authenticated, and the attributes are compared to allow access to confidential services. The credentials such as user ID, password and fingerprint must be protected in an appropriate method when stored in the database and transmitted. These methods include ‘encryption of stored and transmitted credential values’ and ‘usage of defined and encrypted networks.’ The limitation of this paper is that the implementation does not include any factors other than the authentication and

authorization of the designed security architecture. These security factors are important but difficult to describe in one implementation test. Therefore, we will group several factors and have future works. In addition, we will work on how the proposed security architecture, scenarios and solutions can be easily deployed to all clients, and how the proposed security requirement can be implemented flexibly in a real C4I system.

**Table 5.** Comparison between Existing C4I System and Cloud-based C4I System.

Name	Existing C4I System	Cloud-Based C4I System
Inter-working among Army/Navy/Air Force C4I	Limited Interworking: Interworking between KJCCS and other C4I systems is possible.	C4I service can be accessed depending on the user's authority.
IdAM	Separated IdAM on each C4I system.	Centralized IdAM
Authentication Factor	ID, password for the user's C4I system, ID, Pwd for the KJCCS system and encryption module.	ID, password, and secondary authentication factor (biometric information, cryptographic module, etc.)

## 7. Conclusions

The Korean military is considering the integration of cloud computing technology into the defense command control information system with the development of cloud computing technology. However, the security requirements of the existing Korean military information system cannot effectively solve security vulnerabilities owing to cloud computing. Therefore, it is necessary to refer to the U.S. military to apply new cloud security requirements. That is, the current defense information system security requirements lack the security requirements for cloud integration, and the security requirements for virtualization and cloud service asset management should be additionally applied. In addition, data security, network security, access control, and risk management requirements are required in the cloud environment. Therefore, we analyzed various security requirements for national defense and cloud computing, and then proposed a security architecture of a cloud-based Korean C4I system based on the security requirements derived. The future cloud-based Korean C4I security architecture is divided into the virtualization, physical and operational layers, and comprises security aspects for each element. The authentication and access control of the OV, unlike the existing C4I system, include a sequence of authenticating users and access services with a centralized IdAM. Furthermore, in order to show the feasibility of our proposed security architecture, we developed and tested an authentication and access control module for C4I service examples using "OpenStack", an open-source cloud platform.

As mentioned previously, the main contribution of this research is to propose a new security architecture for the cloud-based C4I system. Despite the considerable research relating to cloud computing and IoT, little attention has focused on applying these technologies to the C4I system in the IoMT environment. Furthermore, most research has focused on the capabilities of cloud technology rather than any security concerns of national defense. In addition, research topics dealing with confidential information, such as the national defense sector, make it difficult for researchers to obtain relevant information. In particular, the C4I system is a closed and protected environment, and can only be accessed and used by pre-authorized users. Hence, it is difficult to propose a new security architecture for the future C4I system in IoMT and IoBT environments.

**Author Contributions:** The authors contribute of this paper as follows: J.K. wrote this article, analyzed and derived the security requirements; Y.-G.K. supervised and coordinated the investigation; S.-R.O. performed and coordinated the implementation; S.H.L. inspected this article and coordinated the investigation. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported by C2 integrating and interfacing technologies laboratory of Agency for Defense Development (UD180012ED).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Koo, J.; Lee, S.H.; Kim, Y.G. Design of Security Architecture for the Cloud-based Korea Military Command and Control System. *J. Korean Inst. Commun. Sci.* **2020**, *45*. (accepted).
2. The Department of Defense Strategy for Implementing the Joint Information Environment. Available online: [https://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13\\_DoD\\_Strategy\\_for\\_Implementing\\_JIE\\_\(NDAA\\_931\)\\_Final\\_Document.pdf](https://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implementing_JIE_(NDAA_931)_Final_Document.pdf) (accessed on 25 November 2019).
3. Additional Information about the Joint Information Environment (JIE). Available online: <https://dodcio.defense.gov/Portals/0/Documents/JIE/Additional%20Info%20on%20the%20Joint%20Information%20Environment%20-%20DISTRO.pdf> (accessed on 25 November 2019).
4. U.S. Army Identity and Access Management (IdAM) Reference Architecture (RA). Available online: [https://www.dragon1.com/downloads/20140507-US\\_Army\\_IdAM\\_Reference\\_Architecture\\_V3-0.pdf](https://www.dragon1.com/downloads/20140507-US_Army_IdAM_Reference_Architecture_V3-0.pdf) (accessed on 25 November 2019).
5. FedRAMP Security Controls Baseline. Available online: <https://www.fedramp.gov/documents/> (accessed on 25 November 2019).
6. Cloud Computing Security Requirements Guide. Available online: <https://public.cyber.mil/dccs/dccs-documents/> (accessed on 25 November 2019).
7. Singh, D.; Tripathi, G.; Alberti, A.M.; Jara, A.J. Semantic Edge Computing and IoT Architecture for Military Health Services in Battlefield. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 185–190.
8. Castiglione, A.; Choo, K.K.R.; Nappi, M.; Ricciardi, S. Context aware ubiquitous biometrics in edge of military things. In *IEEE Cloud Computing*; IEEE: Piscataway, NJ, USA, 2017; Volume 4, pp. 16–20.
9. Smith, W.; Kuperman, G.; Chan, M.; Morgan, E.; Nguyen, H.; Schear, N.; Vu, B.; Weinert, A.; Weyant, M.; Whisman, D. Cloud Computing in Tactical Environments. In Proceedings of the 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MA, USA, 23–25 October 2017; pp. 882–887.
10. Buyya, R.; Yeo, C.S.; Venugopal, S.; Broberg, J.; Brandic, I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Gener. Comput. Syst.* **2009**, *25*, 599–616. [CrossRef]
11. Rapid Access Computing Environment (RACE). Available online: <https://whatis.techtarget.com/definition/Rapid-Access-Computing-Environment-RACE> (accessed on 25 November 2019).
12. Kim, J.B.; Park, J.H. National Defense Cloud Strategy and Direction of Development. *J. Korea Soc. Inf. Technol. Policy Manag. ITPM* **2019**, *11*, 1213–1220.
13. Jeong, C.I. Smart Strategy for National Defense in the Fourth Industrial Revolution. *J. Korean Inst. Commun. Sci.* **2019**, *36*, 47–54.
14. Security Certification Guide for Cloud Service. Available online: [https://www.kisa.or.kr/public/laws/laws3\\_View.jsp?cPage=1&mode=view&p\\_No=259&b\\_No=259&d\\_No=91&ST=&SV=](https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=91&ST=&SV=) (accessed on 16 December 2019).
15. Security Requirements for Server Virtualization System. Available online: [http://www.tta.or.kr/data/ttas\\_view.jsp?rn=1&pk\\_num=TTAK.KO-10.0708](http://www.tta.or.kr/data/ttas_view.jsp?rn=1&pk_num=TTAK.KO-10.0708) (accessed on 16 December 2019).
16. *Security Guidelines of National and Public Institution for Cloud Computing*; National Intelligence Service: Seoul, Korea, 2016; pp. 101–103.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).