Hindawi
Security and Communication Networks
Volume 2022, Article ID 3686423, 12 pages
https://doi.org/10.1155/2022/3686423

Review Article

Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network

Se-Joon Park,[1] **Yong-Joon Lee**,[2] **and Won-Hyung Park**[3]

[1] *Department of Information Security Group, SK, Seoul 06750, Republic of Korea*
[2] *Department of Hacking Security, Far East University, Chungbuk 27601, Republic of Korea*
[3] *Department of Information Security Protection, Sangmyung University, Chungnam 31066, Republic of Korea*

Correspondence should be addressed to Yong-Joon Lee; 2020032@kdu.ac.kr

Received 24 October 2021; Revised 5 December 2021; Accepted 14 December 2021; Published 12 January 2022

Academic Editor: Ilsun You

Recently, due to the many features and advantages of cloud computing, "cloud service" is being introduced to countless industries around the world at an unbelievably rapid pace. However, with the rapid increase in the introduction of cloud computing services, security vulnerabilities are increasing and the risk of technology leakage from cloud computing services is also expected to increase in social network service. Therefore, this study will propose an AWS-based (Amazon Web Services) security architecture configuration method that can be applied for the entire life cycle (planning, establishment, and operation) of cloud services for better security in AWS Cloud Services, which is the most used cloud service in the world. The proposed AWS security guide consists of five different areas, Security Solution Selection Guide, Personal Information Safeguard Guide, Security Architecture Design Guide, Security Configuration Guide, and Operational Security Checklist, for a safe social network. The AWS Security Architecture has been designed with three reference models: Standard Security Architecture, Basic Security Architecture, and Essential Security Architecture. The AWS Security Guide and AWS Security Architecture proposed in this paper are expected to help many businesses and institutions that are hoping to establish and operate a safe and reliable AWS cloud system in the social network environment.

1. Introduction

Thanks to the rapid development of ICT technology, the diversification of various types of data and the expansion of data size have accelerated the advent of the Fourth Industrial Revolution based on advanced technologies such as IoT, Big Data, and AI. Since the utilization of such vast amounts of data directly leads to a high level of competitiveness in the industrial field, companies that know how to effectively utilize data in a safe and reliable environment are more likely to gain control over a specific market.

Because the new cloud computing technology, which enables the flexible use of IT resources, can be combined with state-of-the-art IT technologies to provide effective data-related services (i.e., data collection, data analysis, secure data availability, maximization of data sharing, and utilization, etc.) at relatively low costs, many governments and companies around the world are actively considering the introduction of cloud computing services to ensure effective use of data in a secure and safe computing environment. This is because the new cloud computing services, which allow safe storage and management of large amounts of data without any restrictions (anytime, anywhere), can be an alternative to the traditional on-premises environment. Due to these various characteristics and advantages of cloud computing, cloud services are rapidly being introduced to many industries around the world.

However, as the popularity of cloud computing services increases, security vulnerabilities are likely to increase, and technology leaks from cloud computing services are also expected to increase significantly [1–3]. Due to its nature (i.e., resource sharing, virtualization, etc.), cloud computing technology is always exposed to various security threats, which causes many companies to become hesitant in implementing cloud computing services into their system. Therefore, we must find an effective way to solve such reliability issues caused by security vulnerabilities in order to revitalize the cloud industry. Right now, the Korean government is also making various efforts to foster the domestic cloud industry and strengthen its competitiveness by enacting the world's first "Cloud Act (ACT ON THE DEVELOPMENT OF CLOUD COMPUTING AND PROTECTION OF ITS USERS)", implementing a certification system, and developing new guidelines [4]. However, despite such efforts, many companies and institutions are still hesitant to introduce new cloud services into their systems.

In addition, since the traditional on-premises-based security is not ideal for providing quality security in areas that are specialized for cloud services, the need for a specialized security guide (by Cloud Service Provider) is increasing.

Accordingly, this study will look at existing cloud computing security threats and actual incidents that are related to cloud service security issues, then propose an AWS-based security architecture and its utilization method that can be implemented to the entire life cycle such as cloud service planning, implementation, and operation of AWS cloud services, which have been most widely used by countless agencies and businesses around the world today.

2. Related Work

2.1. Cloud Service Model. The most well-known and widely used model in relation to the definition of the "Cloud Computing Model" is the model defined by the NIST (National Institute of Standards and Technology). NIST defines "Cloud Computing" as a service that enables the rapid and convenient delivery of resources that comprise the computing system (network, server, storage, application, service, etc.) with minimal management or service provider's interaction [5, 6]. Depending on the type of service, the cloud service model can be divided into three different categories as shown in Figure 1: IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), SaaS (Software-as-a-Service) [7, 8].

IaaS (Infrastructure-as-a-Service) is a service that provides physical computing infrastructure (i.e., server, storage, network, security, etc.) to the user based on the amount of usage. PaaS (Platform-as-a-Service) aims to provide various computing platforms such as operating systems (Windows, Linux, Android, etc.), which is needed by the users to develop, test, or operate their own applications in the form of a cloud service. SaaS (Software-as-a-Service) is a model that aims to provide standardized application processes or software in the form of a cloud service.

The current status and conditions of the market for each type of cloud service can be seen in Table 1.

2.2. Cloud Computing Security Threats in SNS. The main characteristics of cloud computing include the implementation of virtualization technology, outsourcing of information, sharing of resources, and access from various terminals. Due to these characteristics, cloud computing is vulnerable to many security threats in the social network environment [9, 10]. Therefore, cloud service providers and users must be aware of such security threats and find effective ways to minimize such threats [11–13].

Research on the security threats of cloud computing has been continuously carried out throughout the past decade. In particular, the CSA (Cloud Security Alliance) was always at the center of this research, and they have released a detailed list of security threats that might occur in the cloud environment (2010, 2013, 2016, 2020). The reports released by the CSA are as follows: 7 Top Threats to Cloud Computing in 2010 [14], 9 Top Threats to Cloud Computing in 2013 [15], 12 Top Threats to Cloud Computing in 2016 [16], and 11 Top Threats to Cloud Computing in 2019 [17]. As cloud services are being introduced and implemented in various industries, the security threats of cloud computing in the area of management and operation are also gradually increasing, as shown in Figure 2.

The 11 Top Threats to Cloud Computing in 2019 are as follows: (1) Data Breaches, (2) Misconfiguration and Inadequate Change Control, (3) Lack of Cloud Security Architecture and Strategy, (4) Insufficient Identity, Credential, Access and Key Management, (5) Account Hijacking, (6) Insider Threat, (7) Insecure Interfaces and APIs, (8) Weak Control Plane, (9) Metastructure and Applistructure Failures, (10) Limited Cloud Usage Visibility, and (11) Abuse and Nefarious Use of Cloud Services. According to the CSA's latest release, most security threats were caused by nontechnical issues (i.e., internal moral hazards, insufficient management, carelessness, etc.) rather than technical issues (i.e., system vulnerabilities, DDoS attacks, etc.) [18–20]. This means that even in the case where the service provider (or the user) has the capacity to respond against technical threats, it is difficult to cope with such issues when the threat is caused by internal personnel, which leads to the conclusion that a proper security awareness training course for employees is a crucial factor for achieving a high level of cloud service security.

2.3. Cases of Cloud Service Security Incidents. In a cloud computing environment, the cloud service provider may have access to the users' environments and data, and the threat of data leakage is always present due to the nature (multitenancy) of cloud computing. Due to such unique characteristics of the cloud computing environment, security issues are likely to occur on a regular basis in private/public (hybrid or dedicated) clouds and cloud services. When the cloud service is interrupted or terminated due to unexpected accidents (i.e., mismanagement of the cloud service provider, natural disasters, hacking, etc.), all users of the cloud service become exposed to serious external threats. Table 2 shows the examples of cloud service security incidents (by case).

3. AWS Security Guide

To ensure that the AWS-based systems comply with security compliance requirements, Figure 3 shows the step-by-step security guide throughout the entire lifecycle of the system establishment process in a social network environment.

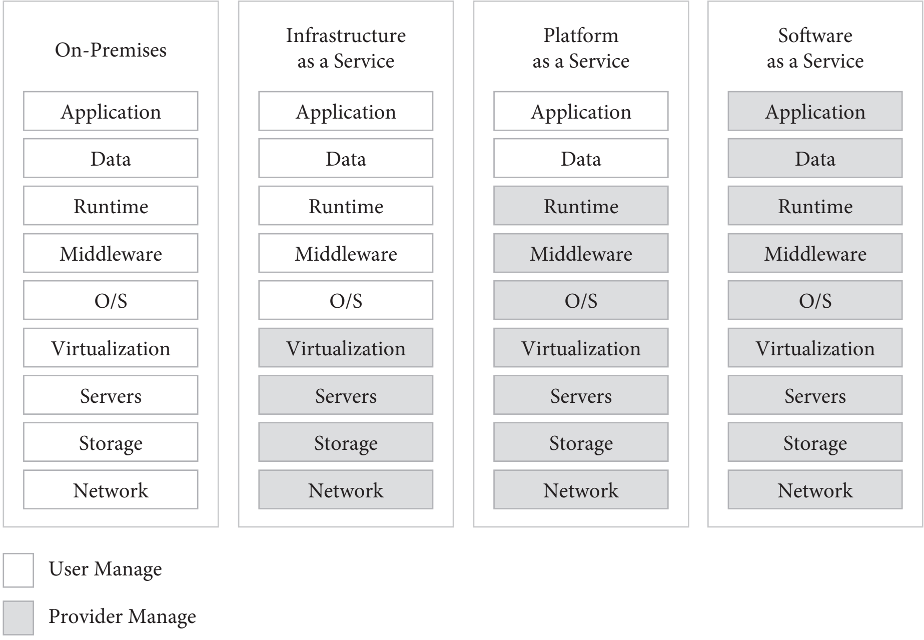


Figure 1: Comparison of cloud service models.

Table 1: Conditions of market for cloud service type.

Service type	Market status
IaaS	(i) Market is led by global companies such as Amazon AWS, Microsoft Azure, etc. Such global powerhouses are cooperating with Korean companies or operating their own data centers in Korea.(ii) In Korea, many telecommunication companies are releasing B2B or B2C services as a combined product, and many Internet companies are also starting to provide cloud services in social network environments.
PaaS	(i) Although the current global PaaS market is not big, many experts are predicting that the companies which dominate the PaaS market will be able to gain the upper hand in IaaS/SaaS businesses in the future.(ii) As a result, major global companies such as Microsoft, Amazon, Google, and IBM are attempting to expand their market presence in the PaaS market.
SaaS	(i) While Google and Microsoft are currently leading the SaaS market, major S/W companies such as SAP, Adobe, etc., are also entering the SaaS market.(ii) In Korea, companies have converted their company resource management, office programs into SaaS to pave their way into the market.

First, during the planning phase, essential security solutions for each purpose must be reviewed and the following guidelines must be proposed to identify the compliance requirements and prevent the omission of costs: Security Solution Selection Guide, Guideline for Securing Personal Information Safety. Second, during the Implementation phase, a Reference Architecture that reflects AWS Well-Architected and Compliance Security Conditions. Third, in the operation phase, an Operational Security Checklist via regular security self-inspections prevents security holes caused by changes in the system.

4. Utilization of AWS Security Guides in SNS

4.1. Security Solution Selection Guide. The Security Solution Selection Guide provides a guideline for configuring the right solution through a case comparison between the AWS native service and the 3rd Party Solution by looking at the limitations and weaknesses of each, as shown in Table 3.

This Security Solution Selection Guide provides a guideline for choosing the ideal solution by comparing AWS native services with 3rd-party solutions in various areas (Network, Application, DB/Storage, Server). Also, it allows you to review the possibility to handle the capacity of the service according to business characteristics while helping you to understand the main key factors that you must consider when building a 3rd-party solution. In order to meet the data security requirements outlined by regulations in the proceeding of personal information, additional considerations on AWS native services are required, such as applying the 3rd-party solution in some security areas, and by minimizing applying 3rd-party solution security architecture can have operational flexibility and cost-effectiveness perspective.

4.2. Personal Information Safety Guide. The Guideline for Securing Personal Information Safety provides a guide about the methods to satisfy the "Technical Protective Actions" of

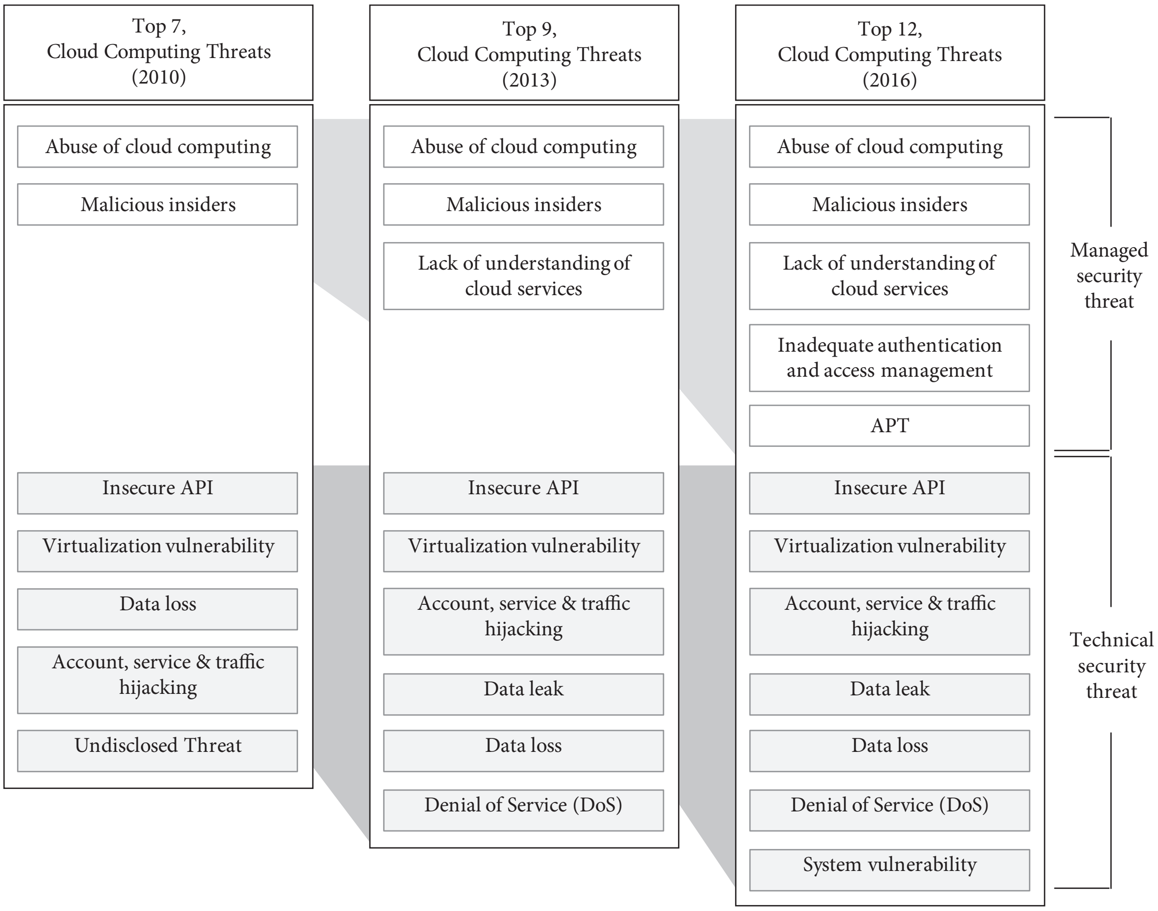


Figure 2: Cloud computing security threats.

the Compliance Requirements via AWS native service & 3rd-party solutions when processing/handling personal information. Table 4 shows the personal information safety guide.

As a guide based on the Personal Information Protection Act, this guide provides a guideline for compliance requirements centering on the measures to secure personal information safety such as the management of permission rights, access control, encryption of personal information, storage and inspection of access records(logs), etc. It also provides a guide on how to implement the AWS native service to apply the requirements of each section.

4.3. Security Architecture Design Guide. The Security Architecture Design Guide provides a guideline for the configuration of AWS native service/3rd-party solutions based on the purposes and form of the system. It also provides a guide for additional reference architecture outside of the basic architecture, such as Standard, Basic, Essential.

In AWS Well-Architected Framework, the security area consists of five security items such as ID & Access Management, Detective Controls, Infrastructure Protection, Data Protection, and Incident Response. Table 5 shows the security items in AWS Well-Architected Framework and the proposed standard security architecture satisfies the five security items.

4.3.1. Standard Security Architecture. Figure 4 shows the design of a Standard Security Architecture Reference Model. The Standard Security Architecture Reference Model is presented as a Security Architecture Configuration based on Personal Information Compliance. It is designed to respond to various security threats by constantly performing security monitoring on IDS/IPS & WAF logs through links with a specialized security monitoring service while detecting attacks from the network/application layer using the Shield, IDS/IPS Solution, and WAF Solution to ensure the users' access to web services. Also, it is configured with network settings and security groups to prevent the Server/DB admins from gaining direct access to the VPC while allowing them to manage the resources by approaching the EC2 Instance/RDS through a Server/DB Access Control Solution. In addition, an antivirus solution is deployed to enable the monitoring of malicious codes and prevent the EC2 from being infected by such codes.

Outside of the 3rd-party solution, various AWS native security services such as the Trust Advisor, Config, CloudTrail, VPC Flow logs, Guard Duty, etc., are implemented to protect the AWS environment.

Figure 5 shows the design of an AWS native service-based Standard Security Architecture Reference Model. AWS native services such as Shield, Security Group, NACL, WAF, ACM, Client VPN, KMS, Session Manager can be configured for

Table 2: Cloud service security incidents in SNS, etc. (by case) [21–24].

Year	Type	Case
2012	Data loss	Loss of personal information through the vulnerability in Apple's 'Find My Mac' feature
	Data leakage	Leakage of personal information (Hacked Dreamhost DB)
	E-mail spamming	Sending spam mails by stealing Dropbox user accounts
	System error	Service failure due to uCloud server switch error
	System error	NA2 service failure due to storage error in Salesforce Storage
	Natural disaster	User service failure (Instagram, Netflix, Pinterest, etc.) caused by Amazon EC2 failure due to power outage caused by a rainstorm
2013	Data loss	Loss of user data (5,698 companies) due to an error during system upgrade
	Data leakage	Leakage of Evernote username, e-mail address, PW hash value
	Data leakage	Leakage of personal information (2.9 million users) & S/W source code due to Adobe server breach
	Data leakage	Leakage of personal information (Twitter, Pinterest, Tumblr, etc.) due to hacked ZenDesk system
	Service exploitation	Existence of a cybercrime portal site that offers cybercrime tools on the web
	System error	Service failure (Netflix, etc.) due to ELB malfunction caused by an AWS administrator accidentally deleting load balancing-related scripts
2014	Data leakage	Leakage & Distribution of photos of cloud service users (including Hollywood actors/actresses) by stealing iCloud accounts
2015	System error	Cloud service user content failure (Netflix, Airbnb, IMDB, etc.) due to an error that occurred during AWS maintenance
2016	Service malfunction	AWS connection failure caused by a DDoS attack to an American Internet hosting company
2017	Data leakage	Top Secret information exposed due to AWS S3 Server Configuration error
2018	Data leakage	Leakage of customer information due to an API bug in the Salesforce Marketing Cloud
	Service exploitation	A notorious hacking group (Muddy Water) exploited the API of a cloud file hosting provider for C&C communication and data leakage
	Data leakage	Leakage of personal information (50,000 users) due to a mistake made by a manager of Honda Car India
	Data loss	Deletion of client company data & backup files due to a mistake made by an employee of Tensent (Chinese company)
2019	System error	DNS Server Setting error (Seoul Region) leads to service failures (Nike, Nexon, Coupang, etc.)
	Unauthorized access	MFA bypasses through IMAP-based password spray attacks on O365 & G-Suite accounts
	Data leakage	Leakage of personal information (24 million users) due to mismanagement of cloud account
	Data leakage	Leak of customer information due to poor configuration of ElasticSearch servers
	Data leakage	Exposure of sensitive information due to a mistake in setting up the Box account

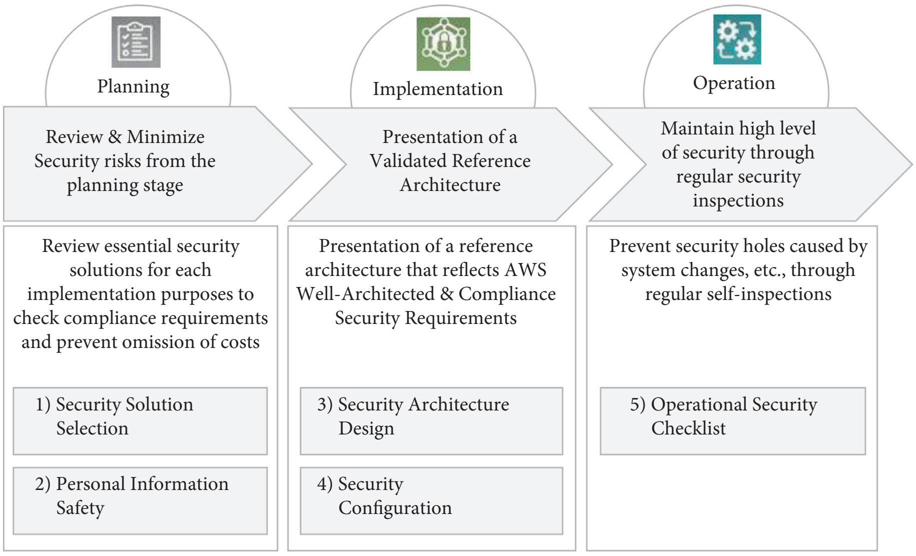

Planning
Review & Minimize Security risks from the planning stage
Review essential security solutions for each implementation purposes to check compliance requirements and prevent omission of costs
1) Security Solution Selection
2) Personal Information Safety
Implementation
Presentation of a Validated Reference Architecture
Presentation of a reference architecture that reflects AWS Well-Architected & Compliance Security Requirements
3) Security Architecture Design
4) Security Configuration
Operation
Maintain high level of security through regular security inspections
Prevent security holes caused by system changes, etc., through regular self-inspections
5) Operational Security Checklist

Figure 3: AWS security guide configuration.

Table 3: Security solution selection guide.

Security area	Security solution	AWS native	AWS native consideration	3rd party review perspective
N/W	DDoS	Shield	—	L3/4/7 Provision
	Firewall	NACL/SG	Limitation in the number of ACL/SG Policies	Ideal for configuring a large-scale service
	Intrusion detection	N/W F/W	Limited Preemptive Detection/Blocking Feature	Mixed use with Guard Duty is recommended
Appl.	Web firewall	AWS WAF	Unable to activate all Management type rules	Replication Configuration recommended
	Channel encryption	ACM/Client VPN	MFA Use Limited	SSL/IPSec VPN Configuration &MFA Provision
DB/Storage	DB access control	—	—	Apply when processing personal information
	Data encryption	KMS	Block Encryption Applied	Apply field encryption
Server	Server access control	System Manager	Use of Log Records Limited	Apply when processing personal information
	Antivirus	—	—	Management server recommended

Table 4: Personal information safety guide.

Requirements		AWS native	Security guide
1. The IT service provider must only grant the access rights to the personal information processing system only to authorized personal information handlers, etc., when it is necessary for the provision of the service.		IAM, Session Manager	Grant minimum authority on access to the personal information processing system through IAM User/Group Policy Allocation
2. The IT service provider must change or revoke the authority to access the personal information processing system WITHOUT DELAY if the personal information handler is changed due to a personnel change, such as a transfer, retirement, etc.		IAM	Grant minimum access rights to the user through IAM Policy Allocation/Removal
3. The IT service provider must record the details of the changes in access rights (alteration, termination, granting) that are made under article #1 or #2 (see above) and keep the records for at least 5 years.		IAM, CloudTrail, S3	Life cycle management by sending the CloudTrail activity log of the IAM user to S3
4. The IT service provider must apply a safe method of authentication when a personal information handler needs to gain access to the personal information processing system from outside through the Information & Communication Network.		IAM, Cloud VPN	Set MFA/IP settings (access conditions) for the IAM user account
5. The IT service provider must install and operate a system including the following functions in order to prevent illegal access and infringement through the Information & Communication Network.	① Restrict unauthorized access to personal information processing system by limiting the access rights to specific IP addresses, etc.	IAM, NACL, Security Group, NW F/W, Client VPN	Set MFA/IP settings (access conditions) for the IAM user account Manage accessible IPs using Security Group & NACL Block illegal access through Shield & WAF
	② Detect illegal attempts to leak personal information by reanalyzing IP addresses, etc. that have connected to the personal information processing system	CloudTrail, Guard Duty, AWS WAF, NW F/W	Detect abnormalities of IAM users by looking at the CloudTrail activity log Analyze & Detect abnormal network activities and IPs using Guard Duty and Detective
6. IT service providers that meet the following conditions must physically or logically separate the network/computer of the personal information handler, who can download or destroy personal information through the personal information processing system and set the access rights to the personal information system, from the main network: IT service providers with more than 1 mil. average users per day whose personal information is stored/managed by the service.		Direct Connect, Cloud VPN, VPC	Use dedicated line via Direct Connect Connect with Private Subnet within VPC by using Cloud VPN Network, Internet Separation by Subnet (in VPC)
7. The IT service provider must establish and implement a specific password-making rule to make sure that the users can create/use safe passwords.		IAM	Set & Apply in IAM Password Policy

Table 4: Continued.

Requirements		AWS native	Security guide
8. The IT service provider must establish, apply, and operate password-making rules for personal information handlers, including the following matters.	① Combination of two or more types from the following: English, Number, Special Characters (min. 10 digits). Or a combination of three or more types from the following: English, Number, Special Characters (min. 8 digits)	IAM	Set to 'Include at least three of the following: English, Number, Special Characters, Min. 8 digits' in IAM Password Policy
	② Recommend to NOT USE passwords that can be easily guessed (consecutive numbers, birthdays, phone numbers, etc.) or similar to the ID IAM Set "Limit Password Reuse" in IAM Password Policy	IAM	Set 'Limit Password Reuse' in IAM Password Policy
	③ Set an expiration date on the password, forcing the users to change their password at least once every six months IAM Set Password Change Cycle to "90 Days" in IAM Password Policy	IAM	Set Password Change Cycle to '90 Days' in IAM Password Policy
9. The IT service provider must take certain measures (i.e., limiting the maximum access time, etc.) to make sure that the personal information that they are handling is not disclosed or leaked to the outside through Internet homepages, P2P, sharing settings, etc.		—	Review the utilization of Terminal Security Solutions such as MDM
10. The IT service provider must take certain measures, such as limiting the maximum access time, only for the time required for the personal information handler to access the personal information processing system.		AWS Console, Session Manager	Use AWS Web Console Session Timeout setting
11. The IT service provider must be regularly identified and supervised by private information handlers for more than one month, and it should maintain and access records for at least a year.		CloudTrail, Session Manger, S3, Cloudwatch logs	Send access activities to S3, Cloudwatch logs for one year of lifecycle management, and monthly log checks.
12. The IT service provider must be kept on a separate physical storage device to ensure that the privacy record is not be changed.		S3, Glacier	Set the lifecycle of log stored in S3 to store and minimize access to Glacier
13. The IT service provider must encrypt and store information such as social number, passport number, driver's license, foreign registration number, credit card number, account number, biometric information.		KMS	Encrypt using KSM key (AES-256) in S3, RDS to store information
14. The IT service provider must encrypt the transmitting information, including personal information, user authentication information.		ACM, Cloud VPN	Configure SSL for API Gateway, Load Balancer, or CloudFront with certificates stored in ACM

AWS security architectures. And DB access control can be configured by Client VPN and IAM access control, antivirus areas that AWS does not provide required 3rd-party solution.

4.3.2. Basic Security Architecture. Figure 6 shows the basic security architecture reference model. The basic security architecture reference model consists mainly of the native security services presented in the AWS Well-Architected Framework for systems that are not subject to the Personal Information Compliance Requirements. Therefore, the 3rd-party network security solution, which is in an inline form, is not applied, and the AWS Guard Duty & AWS WAF are configured to replace them. In addition, it is configured to be accessible via VPN or System Manager, not through a Server/DB Access Control Solution. However, a 3rd-party security solution is used for Antivirus defense, which is a solution that is not provided by AWS.

Table 5: Security in AWS well-architected framework.

Security items	AWS native service
(1) ID & Access Management	IAM
(2) Detective Controls	CloudTrail, VPC Flow logs, Config
(3) Infrastructure Protection	Shield, Security Group, WAF, IDS
(4) Data Protection	KMS, ACM
(5) Incident Response	Security Hub, Security Monitoring

4.3.3. Essential Security Architecture. Figure 7 shows the essential security architecture reference model.

The essential security architecture reference model is a security architecture configuration with minimal security for R&D and PoC systems that are subject to the following four conditions (see in the following), consisting of the native security service provided free of charge by AWS:

(1) Temporarily Open (Assign the period of use)

(2) PoC or Test Purposes (External Service Unavailable)

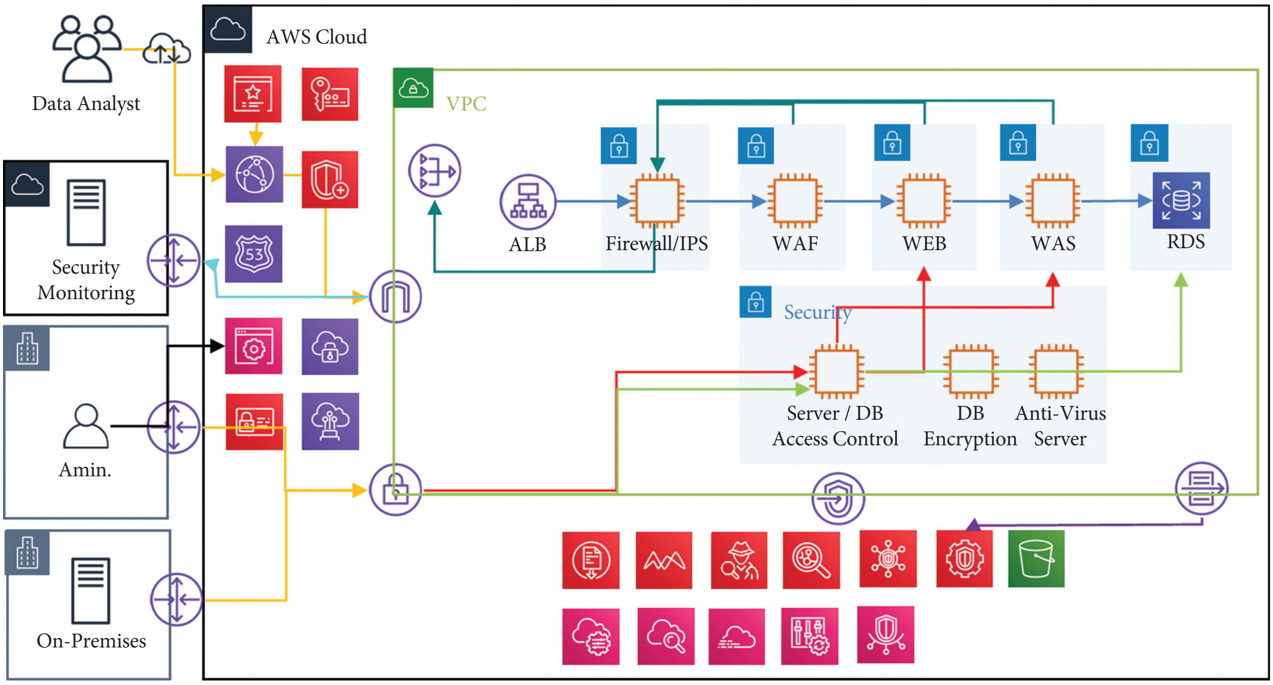


Figure 4: Standard security architecture reference model.

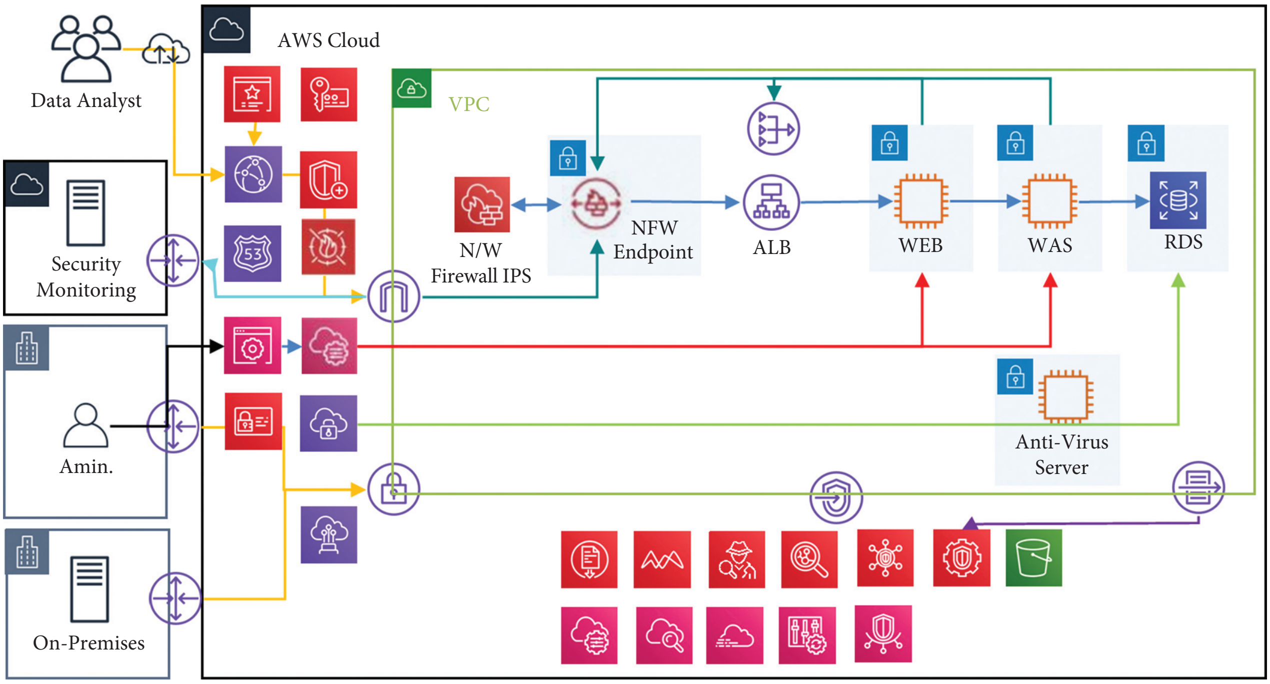


Figure 5: Standard security architecture reference model (native-based).

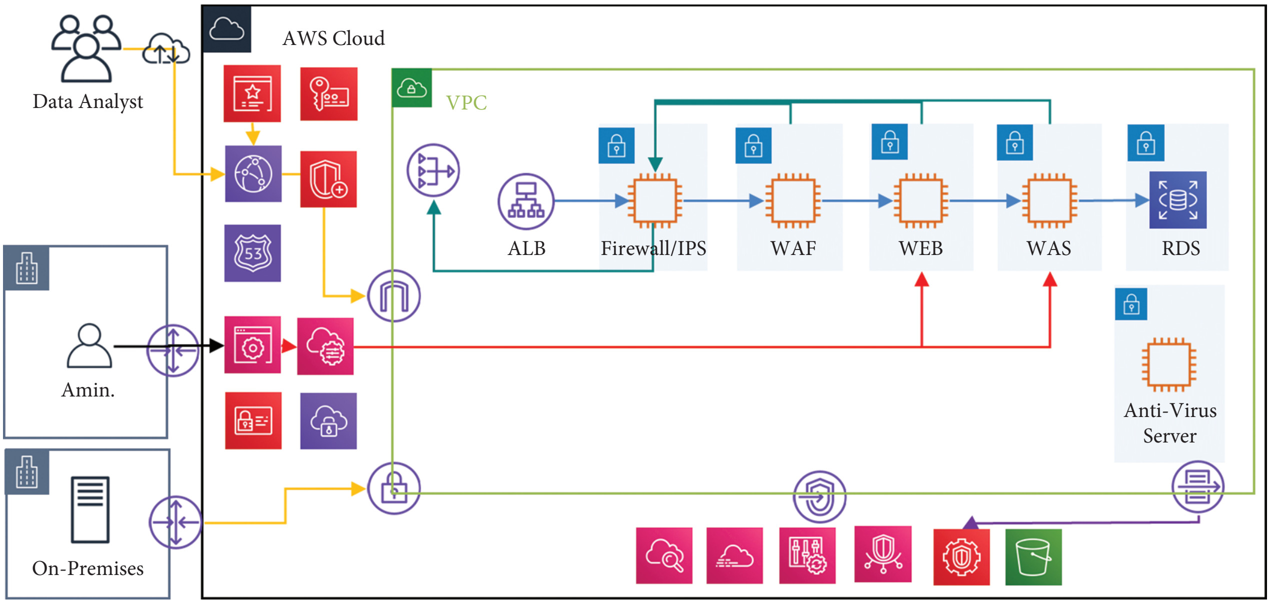


Figure 6: Basic security architecture reference model.

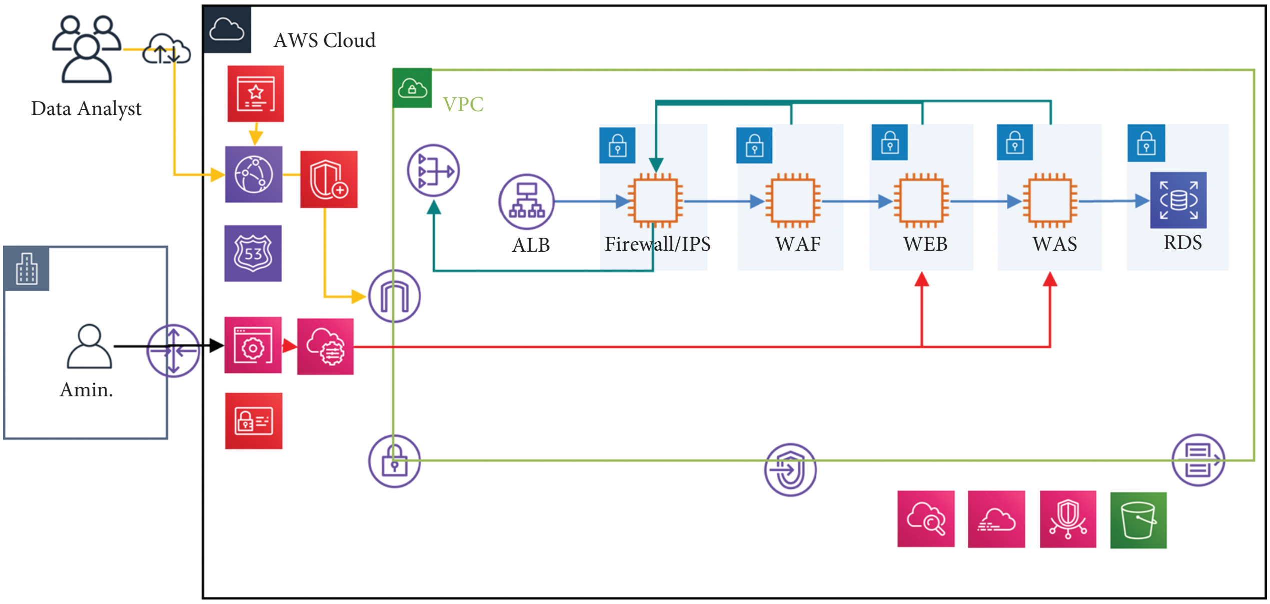


Figure 7: Essential security architecture reference model.

(3) Does not handle/process Personal/Important Information

(4) Not interlinked with Important Systems

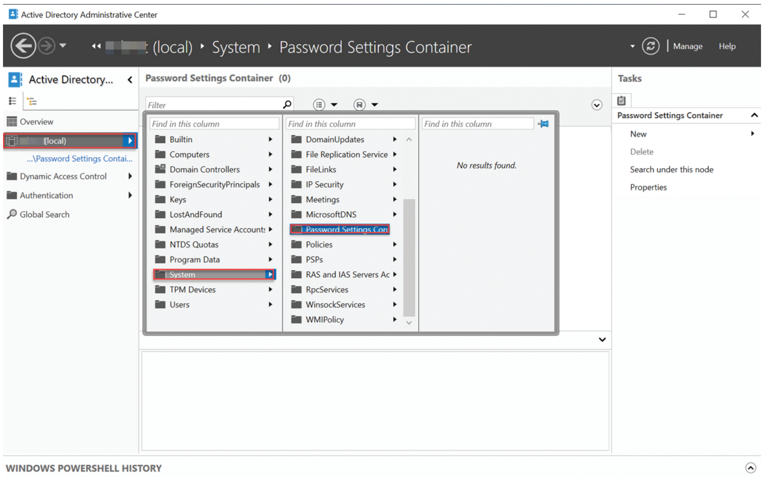
4.4. Security Configuration Guide. Provides a guideline for implementing a safe setting for AWS native service when establishing a system by utilizing the Security Configuration Guide. Figure 8 shows the examples for password policy security configuration.

The security configuration guide is a manual about the security configuration of the AWS native service and provides a guide for an ideal configuration for each service. And based on such configuration, it allows the user to diagnose the current status (safe/vulnerable) of the system.

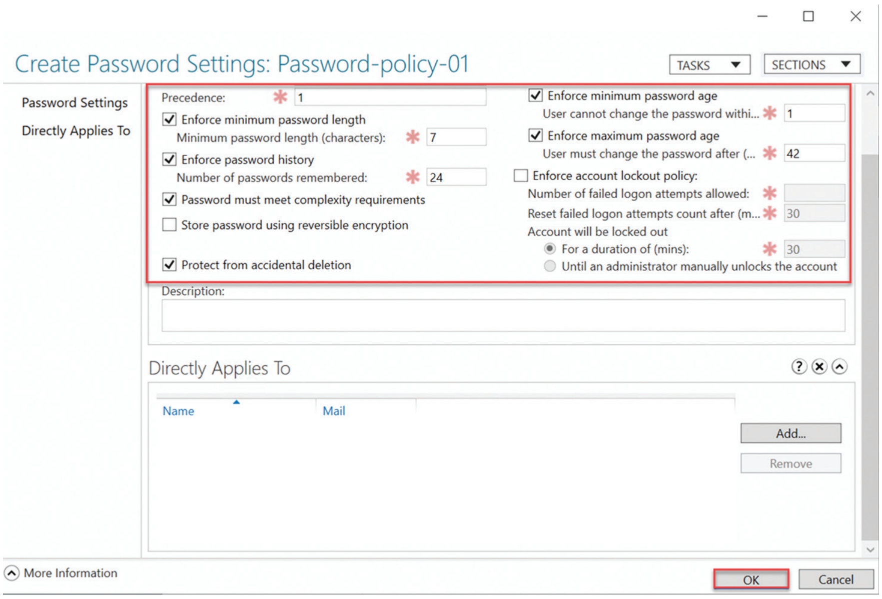
4.5. Operational Security Checklist. The operational security checklist provides a guideline for the measures that must be performed during system operation through an item-by-item Security Diagnosis. As you can see, the example checklist for IAM, CloudTrail, KMS in Table 6, provides a security guide for each service by presenting an AWS native service diagnosis.

Security–Security & Compliance –Amazon Directory Service	Risk Level	High

1) Administrative Tools -> Active Directory Administrative Center-> local -> System -> Password Setting Container



2) Password Policy



Create Password Settings: Password-policy-01

Precedence: * 1

☑ Enforce minimum password length
Minimum password length (characters): * 7

☑ Enforce password history
Number of passwords remembered: * 24

☑ Password must meet complexity requirements

□ Store password using reversible encryption

☑ Protect from accidental deletion

☑ Enforce minimum password age
User cannot change the password withi... * 1

☑ Enforce maximum password age
User must change the password after (... * 42

□ Enforce account lockout policy:
Number of failed logon attempts allowed: *
Reset failed logon attempts count after (m... * 30
Account will be locked out
● For a duration of (mins): * 30
○ Until an administrator manually unlocks the account

Description:

Directly Applies To

Name	Mail

Safe: Configuration & management password policy

Venerable: Not configure password policy

Figure 8: Security configuration guide.

Table 6: Operational security checklist.

Area	Inspection items	Risk level	Security guide
IAM	Is there a complexity setting for the password for the IAM account that is used to connect to the AWS Console?	High	Complexity setting of the password for the IAM account that is used to connect to the AWS Console- - At least one alphabetic character must be included At least one number must be included Must choose at least one character excluding alphanumeric characters- - Safe when all 3 settings above are enabled
	Is there a minimum password length set for the IAM account that is used to connect to the AWS Console?	Medium	Minimum password length setting for the IAM account that is used to connect to the AWS Console - Safe when it is set to 'Password must be at least 8 characters'
	Is it possible to allow the users to change their own password for the IAM account that is used to connect to the AWS Console?	Low	Allow users to change their own password for the IAM account that is used to connect to the AWS Console - Allowing the users to change their own password
CloudTrail	Is the CloudTrail Tracking Creation enabled?	High	Activate CloudTrail Tracking Creation - Performs audits on API Call History by enabling CloudTrail Tracking - Perform monitoring of abnormal behaviors through a routine inspection of VPC Flow Log
	Are integrity checks performed on the CloudTrail logs stored in S3?	Medium	Integrity Validation of CloudTrail logs stored in S3 - Log File verification is enabled - Perform regular reviews of log file integrity
	Are periodic audits performed on the CloudTrail logs?	High	Periodic audit of CloudTrail logs - Monitor unauthorized activities through a periodic (regular) audit of log files - Conduct user interviews of unauthorized activities
KMS	Are the plans for the periodic change of customer management keys (generated by KMS) properly prepared and implemented?	High	Regularly change customer management keys generated through KMS - Manually/automatically performing key changes/management
	Is the permission to use KMS-generated keys reviewed on a regular basis?	High	Regular review of KMS-generated key permission - Perform periodic audits of unused accounts and roles through a regular review of key permission

5. Conclusion

The recent proliferation of cloud computing caused many experts to predict a significant increase in technology leakage in cloud computing services in social network environment due to more security vulnerabilities. Therefore, in order to increase the security level of the AWS Cloud Service, which is the most well-known and widely used cloud service in the world by countless institutions and companies, this research has proposed an AWS-based security architecture and its utilization plan that can be applied throughout the entire life cycle of cloud services such as planning, implementation, and operation.

To this end, we first took a look at other studies about cloud service models, created a list of cloud computing security threats, and analyzed cloud service security incidents that have occurred in the past. Afterwards, we have created an AWS Security Guide by referring to relevant studies and finally proposed an AWS Security Guide Utilization Plan.

The AWS Security Guide consists of a total of five different areas. First, with a Security Solution Selection Guide, it provided a guideline on how to implement the ideal solution through a case comparison between AWS native service and 3rd-party Solutions. Second, through Personal Information Safety, we have suggested a method to satisfy the technical protection measures in compliance with the Compliance Requirements (related to the processing of personal information) when implementing the AWS native service. Third, through the Security Architecture Design Guide, it provided a guideline for configuring AWS native service and 3rd-Party Solutions according to the purpose and form of the system. Fourth, through a Security Configuration Guide, it proposed a safe setting implementation plan for AWS native service when deploying a new system. Fifth, with the Operational Security Checklist, it suggested effective measures that can be taken while operating a system through an item-by-item security diagnosis.

We hope that the AWS Security Guide and Utilization Plan that was proposed in this study can help companies and institutions that are attempting to build a safe and reliable AWS Cloud System in the future.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] T. Wang, J. Zhou, M. Huang et al., “Fog-based storage technology to fight with cyber threat,” *Future Generation Computer Systems*, vol. 83, pp. 208–218, 2016.

[2] M. K. Kim, “The Improvement of Domestic Cloud Security Certification System through the Comparative Analysis with the CSA,” Master’s Thesis, Graduate School of Soon Chun Hyang University, Chungcheongnam-do, Republic of Korea, 2019.

[3] I. Agrafiotis and G. Kul, “Advances in insider threat detection,” *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, vol. 12, no. 2, pp. 1-2, 2021.

[4] KOREA Financial Services Commission, “Plans to Expand the Use of Cloud in the Financial Sector,” KOREA Financial Services Commission, Seoul, Republic of Korea, 2018.

[5] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” National Institute of Standards and Technology, U.S. Department of Commerce, Maryland, MD, USA, SP 800-145, 2011.

[6] NARS, “Current status and challenges of cloud computing,” vol. 313, National Assembly Research Service, Seoul, Republic of Korea, 2017, Issues Report.

[7] E. Maria, “IaaS, PaaS, SaaS – what do they mean?, Cloud on move,” 2017, http://cloudonmove.com/iaas-paas-saas-what-do-they-mean/.

[8] M.-C. Blog, “SaaS vs PaaS vs IaaS: What’s the Difference and How to Choose,” 2020, https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/.

[9] M. Kolomeets, A. Chechulin, and I. Kotenko, “Bot detection by friends graph in social networks,” *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, vol. 12, no. 2, pp. 141–159, 2021.

[10] A. Kumar, S. K. Dhurandher, W. Isaac, J. Joel, and P. C. Rodrigues, “Securing opportunistic networks: an encounter-based trust-driven barter mechanism,” *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, vol. 12, no. 2, pp. 99–113, 2021.

[11] Y. W. Chen, M. Lin, and M. Y. Wu, “Study of data placement schemes for SNS services in cloud environment,” *KSII Transactions on Internet and Information Systems*, vol. 9, no. 8, pp. 3203–3215, 2015.

[12] M. Kim and H. Lee, “SMCC: social media cloud computing model for developing SNS based on social media,” *Convergence and Hybrid Information Technology*, Springer, vol. 206, pp. 259–266, Berlin, Germany, 2011.

[13] Z. Kodric, V. Simon, and L. Jelovcan, “Securing edge-enabled smart healthcare systems with blockchain: a systematic literature reviews,” *Journal of Internet Services and Information Security*, vol. 11, no. 4, pp. 19–32, 2021.

[14] Cloud Security Alliance, *Top Threats to Cloud Computing v1.0*, Cloud Security Alliance, Washington, DC, USA, 2010.

[15] Cloud Security Alliance, *Top Notorious Nine, Cloud Computing Top Threats in 2013*, Cloud Security Alliance, Washington, DC, USA, 2013.

[16] Cloud Security Alliance, *The Treacherous 12, Cloud Computing Top Threats in 2016*, Cloud Security Alliance, Washington, DC, USA, 2016.

[17] Cloud Security Alliance, *Top Threats to Cloud Computing in 2019-the Egregious 9*, Cloud Security Alliance, Washington, DC, USA, 2019.

[18] L. A. Ys, *Cloud Computing Service Security Assurance Programs Comparison Analysis and Improvement Suggestions*, Graduate School of Nam Seoul University, Cheonan, Republic of Korea, 2016.

[19] C. J. Lee, *A Study on Security Requirements for Privacy in a home Cloud Environment*, Graduate School of Soon Chun Hyang University, Asan-si, Republic of Korea, 2017.

[20] M. Ei-Shrkawey, M. Alalfi, and A. I. M. Hassan, “An enhanced intrusion detection system based on multi-layer feature reduction for probe and dos attacks,” *Journal of Internet Services and Information Security*, vol. 11, no. 4, pp. 61–78, 2021.

[21] Y. Jiao, Y. Wang, L. Yuan, and L. Li, “Cloud and SNS Supported Collaboration in AEC Industry,” in *Proceedings of the CSCW Conference*, pp. 842–849, Wuhan, China, May 2012.

[22] Y. G. Lee, “A Study on Improvement of Cloud Security Assurance Program,” Master’s Thesis, Graduate School of Dongguk University, Seoul, Republic of Korea, 2019.

[23] S. Y. Lim, *A Study on the Management System for Domestic Personal Information Protection in the Cloud Environment*, Graduate School of KONKUK University, Seoul, Republic of Korea, 2020.

[24] Y. Lee, B. Son, S. Park, J. Lee, and H. Jang, “A survey on security and privacy in blockchain-based central bank digital currencies,” *Journal of Internet Services and Information Security*, vol. 11, no. 3, pp. 16–29, 2021.