Analysis of Cloud Migration Trends and Security Threats in the South Korean Financial Sector

Daemin Shin[1], Jiyoon Kim[2*], and Ilsun You[3]

[1] Financial Security Institute, Seoul, Republic of Korea
dmshin@fsec.or.kr
[2] Department of Computer Science, Gyeongsang National Univeristy, Jinju, Republic of Korea
jykim92@gnu.ac.kr
[3] Department of Financial Security, Kookmin University, Seoul, Republic of Korea
isyou@kookmin.ac.kr

Abstract

Recent changes in cloud regulations have led to the widespread adoption of cloud technology in the South Korean financial sector, making it a pivotal infrastructure. Prior to October 2016, stringent regulations, including the mandatory physical network separation for all computing systems in financial institutions, presented challenges for utilizing public cloud services. However, as electronic financial supervisory regulations gradually eased, the adoption of cloud services gained momentum and continues to thrive. To ensure secure cloud utilization in the financial field, it is imperative to establish business continuity plans, exit strategies, and security enhancement measures in line with the guidelines for financial sector cloud computing services. This also entails adhering to internal controls, such as safety assessments of cloud service providers, deliberation and approval by internal information security committees, and reporting to regulatory authorities. This study, based on case studies of cloud adoption in the South Korean financial sector, examines adoption trends, driving factors, industry-specific characteristics, and regulatory changes. Furthermore, it analyzes security threats in response to evolving cloud usage environments through an inductive approach, drawing from real-world incidents, and presents a threat classification model.

Keywords: Cloud, Security, South Korean Financial

1 Introduction

Recently, as new IT technologies like 5G, artificial intelligence, big data, and the cloud have emerged, services harnessing these innovations are gaining prominence. Consequently, there's an escalating interest in these developments within the South Korean financial sector. By introducing these advanced technologies, the financial industry can effortlessly integrate the high-performance, high-cost infrastructure offered by cloud service providers with their internal platforms. This facilitates the application of various PaaS (Platform as a Service) and SaaS (Software as a Service) services to operations, allowing for efficient utilization of cutting-edge tech such as AI/ML (Artificial Intelligence/Machine Learning) and big data analysis platforms [1–4]. The core system managing pivotal financial transactions is currently undergoing a phased transition to the cloud. Moreover, a range of innovative services, from the My Data service and insurance claims automation to auto-response and product sales monitoring, are

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No. 51
*Corresponding author: Department of Computer Science, Gyeongsang National Univeristy, 501 Jinjudaero, Jinju, Gyeongnam, 52828 Republic of Korea, Email: jykim92@gnu.ac.kr

now leveraging cloud capabilities [5–16]. The South Korean financial sector's cloud environment is transitioning into a hybrid/multi-cloud setup, where on-premises, private clouds, and public clouds operate concurrently. With this shift, there's heightened complexity in infrastructure operation, sparking increased focus on integrated infrastructure management and driving operational efficiency and optimization [17–20].

The South Korean government has been progressively easing regulations related to cloud and network separation. They are contemplating the allowance of SaaS-type clouds for non-critical tasks within internal networks [21, 22]. Table 1 illustrates the evolving cloud regulatory landscape in the South Korean financial industry.

Table 1: Changes in Cloud Regulations for the South Korean Financial Sector

Date	Associated Regulation	Contents
June 2016	Advance notice of changes to proposed provisions for partial revision of electronic financial supervisory provisions	- The use of the cloud is permitted for non-critical information, excluding personal credit information and unique identification information of financial companies and electronic financial business operators
July 2018	Financial cloud usage expansion plan	- Advancement of the system to expand the scope of use - Establishment of standards for service use and provision - Strengthening of service supervision and inspection
January 2019	Revision and enforcement of electronic financial supervisory provisions	- Allowing the use of personal credit information and unique identification information in the cloud - Preparation of cloud service guidelines - Establishment of a supervision and inspection system
January 2020	Revision of the Data 3 Act	- Application of cloud environments for credit evaluation businesses and specialized product development, following the allowance of MyData
January 2023	Improved regulation of cloud and network separation in the financial sector	- Specification of the criteria for importance evaluation - Relaxation of the usage procedures for non-critical tasks - Maintenance of evaluation items for the safety of CSP (Cloud Service Providers) - Transition to post-use reporting and simplification of submitted documents

Given the critical nature of data such as personal credit information in the financial sector, the adoption of public cloud has faced challenges. Fundamental issues stem from the inherent characteristic of the cloud being a resource-sharing infrastructure based on virtualization, regulatory concerns regarding the overseas handling of financial information, and the burden of adhering to guidelines for using the cloud. However, with the rising demand for cloud services

in the market and progressive government deregulation, coupled with advancements in cloud security services and technologies, it's anticipated that the adoption of cloud in the financial sector will gradually expand [23–25].

As businesses increasingly shift to cloud workloads and data migration accelerates, cloud services have become prime targets for attackers, leading to a steady rise in security breaches. Examples of cloud security incidents can be seen in Table 2 [26]. A primary cause of these incidents is improper configuration settings of cloud resources, which expose them to the internet, making them accessible from anywhere by anyone with the appropriate access key [27].

Table 2: Recent Cloud Security Incident Cases

Date	Contents
December 2018	Disclosure of dozens of corporate and government assets and sensitive materials worldwide to corporate MSP companies (Cloud Hopper Campaign)
July 2019	Capital one credit card customers and personal information disclosure (106 million)
January 2021	VIP Games, improper cloud configuration reveals 23 million records of over 60,000 users
November 2021	Vulnerability in Log4j could allow encryption, ransomware, botnet, and spam attacks
January 2022	LAPSUS$ hacker group hacks NVIDIA's internal network to steal sensitive data
March 2022	70% of ServiceNow instances, customer management access controlIncorrect configuration of strike (ACL) results in guest user over-allocation and security issues
April 2022	Threat hunting by Broadcom's symantec division finds signs of a long-term cyber espionage campaign targeting MSPsa

For the safe use of the cloud, security must be prioritized. ITU-T, in [28], analyzes security threats and challenges in the cloud computing environment, proposing a security framework to mitigate them. [29] delves into security threats and tasks related to virtualization containers in the cloud computing environment, providing a reference framework that includes security guidelines. CSA, in [30], offers security guidelines to manage and mitigate risks associated with adopting cloud technologies and, in [26], conducts a survey targeting cloud industry security experts, identifying and analyzing 11 primary security threats. The NSA, in [31], discusses concepts of vulnerabilities within the cloud environment and offers necessary security guidelines. CISA shared a reference architecture utilizing Cloud Security Posture Management (CSPM) in [32] to support the federal government migrating to a cloud environment. While existing studies comprehensively explain security in a general cloud computing environment, they fall short in detailing specific security threats and alternatives, considering the Korean financial sector's cloud usage environment. Scattered and listed-level information necessary for regulatory compliance in the financial sector makes it inefficient to directly use for tasks such as threat identification and security review.

This paper collected and examined approximately 90 South Korean press releases to analyze the transition to the cloud in the South Korean financial sector and to model security threats in a financial cloud usage environment. Chapter 2 categorizes and describes trends in the financial sector's transition to the cloud and its security by time periods, exploring the main factors driving the transition. It also summarizes the characteristics and commonalities that appear in

each subsector. Chapter 3 looks at changes and prospects in the cloud usage environment. In Chapter 4, we inductively analyze cases of security incidents in major cloud environments and describe the threat classification model and security threats.

2 Cloud Adoption Trends and Security in the South Korean Financial Sector

South Korean financial sector's cloud adoption trends can be categorized into three phases: the initiation phase (before 2019), the transition phase (2019-2020), and the stabilization phase (2021-2022). The initiation phase, prior to the revision of the electronic financial supervision regulations, faced constraints due to physical network separation regulations and regulations on the use of clouds for essential tasks. In this period, cloud usage was limited primarily to overseas corporations and non-essential financial tasks. During the transition phase, the use of unique identification information and personal credit information in the cloud was permitted. The introduction of open APIs in banks and the revision of the government's "Data 3 Law" meant that cloud usage increased in the data utilization market. The stabilization phase targeted improvements to the workflow in the existing cloud operating environment of various companies, optimizing work efficiency, and focusing on cloud performance and cost. In particular, the need for non-face-to-face services became prominent due to the effects of COVID-19. This spurred the acceleration of digital transformation strategies in companies and had an impact on the increased adoption of public cloud services, which offer rapidity, flexibility, and scalability, to cope with the surge in non-face-to-face traffic data.

2.1 Initiation Phase (Before 2019)

During the initiation phase[1], the cloud in the financial sector of South Korea began as a pilot application for private cloud technology, alongside preparations for the future digital finance environment, primarily through the introduction of virtualization equipment. The transition towards a low-power x86-based Linux environment, commonly provided by the cloud, commenced as there was a desire to utilize various open-source technologies while conserving power costs of server infrastructure resources.

The 2011 incident involving the paralysis of the NH (NongHyup) computer network led to the mandatory physical network separation of the financial sector in 2013. Adhering to the network separation policy, the sector constructed its own cloud computing resources based on virtualization solutions and began using cloud technology at the level of PC virtualization for internal operations. However, before 2019, domestic regulations strictly limited the use of personal credit information and unique identification information on the cloud. As a result, operations transitioned to public clouds were primarily limited to non-essential tasks that did not fall under domestic regulations, such as overseas corporate websites. Furthermore, to pilot new cloud technologies, companies constructed and operated private clouds within their data centers. The operation of these private cloud platforms allowed for the efficient use of idle resources (such as CPU, memory, and storage). There was also a focus on achieving infrastructure flexibility for applications using container-based virtualization techniques, thereby streamlining and improving productivity in service development, deployment, and operations. Subsequently, as a logical alternative to the growing infrastructure demands of the financial sector, public clouds were considered.

[1] Drawing from references [33–39], the characteristics of the initiation phase (before 2019) are described.

2.2 Transition Phase (2019 ∼ 2020)

In 2019[2], regulations on cloud computing were relaxed, allowing the use of unique identification information and personal credit information on public clouds. The adoption of OpenAPI in the financial sector and the revision of the "Data 3 Law" had a positive influence on the activation of cloud usage in the data utilization market. Consequently, financial institutions established IT governance related to cloud usage, encompassing internal organization, regulations, guidelines, procedures, security, and standards. This led to the efficient standardization of the cloud usage work process, ensuring that the guidelines for using cloud computing services in the financial sector were consistently managed and integrated into internal IT business processes. With market changes, the entrance of big tech and fintech companies into the financial service competition prompted financial institutions to intensify their own capabilities. Specifically, the cloud was utilized as an infrastructure-building strategy for a successful digital transition, aligned with enhancing customer experience, securing early customer acquisition, addressing limitations in IDC space and network capacity, replacing obsolete equipment, and propelling post-next-generation business initiatives.

The cloud usage structure of financial companies evolved into a hybrid environment, wherein customer data was securely stored in internal on-premises or private clouds, while customer interface services and analysis platforms leveraged public clouds. This allowed for secure data storage, scalable responses to increasing traffic from various promotions and events, and efficient use of storage, computing resources, and analytical tools required for big data analysis. Moreover, in preparation for traffic surges and as a strategy to address service outages, transitioning the core system of financial transaction processing, the ledger system, to the cloud was considered. This transition aimed to improve the low scalability and elasticity of the traditional on-premises approach, which required physical standby servers to be prepared in advance and connected as needed. It also sought to proactively prevent human errors that may occur during service development and deployment processes in core systems. On another front, through collaboration with fintech companies, financial institutions explored new businesses. They provided support for OpenAPI, development tools, IaaS, PaaS, and other necessities for new technology and service development. This effort aimed to narrow the technological gap with big tech companies and enhance the customer experience.

2.3 Stabilization Phase (2021 ∼ 2022)

With the advent of the stabilization phase[3], cloud services became prevalent in all operations of financial companies, emphasizing work efficiency and optimization in the cloud. The use of the cloud was a priority for the operational infrastructure of new services, and it was also applied in new services using AI non-face-to-face technologies, digital property insurance, and "My Data" among others. Moreover, the cloud was adopted in services such as insurance reviews, insurance claim automation, auto-response services, and product sales monitoring services.

While traditional private clouds, based on commercial platforms, had the downside of not being easily interconnected with other platforms, public clouds were actively embraced. They presented advantages such as effortless integration with various new technology platforms and the capability to establish a high-availability environment at a lower cost. In light of these trends, some financial companies opted to transition parts or the entirety of their core systems, like the accounting systems, to both public and private clouds.

[2]Drawing from references [40–51], the characteristics of the transition phase (2019-2020) are described.
[3]Drawing from references [52–97], the characteristics of the stabilization phase (2021-2022) are described.

The emergence of cloud-native applications played a significant role in propelling application modernization. Financial companies implemented automation across infrastructure and application development, testing, and deployment by adopting Infrastructure as Code (IaC), infrastructure cataloging, standard CI/CD pipelines, and introducing DevOps. Especially, the establishment of CI/CD and DevOps environments catered to an immediate response framework for market shifts, like reactions to new services or changes in service demands. Through this, financial companies enhanced their business agility. The development and deployment of infrastructure and applications were automated, encompassing activities like static and dynamic vulnerability checks on code, infrastructure configuration assessments, and error checks in configurations. This meant maximizing automation in infrastructure setup and application deployment, thereby curbing human errors and fortifying security. Regarding cloud usage, measures ensuring safety such as network isolation, access control, account management, logging, auditing, encryption, and key management were codified and automated using services like the AWS Landing Zone. This strategic approach drastically reduced the recurrent workload typically associated with cloud usage. Applications incorporated a microservices architecture (MSA), optimizing database load distribution and enabling cost-effective autoscaling by segmenting into more granular, autonomous services. Systems hosted on the cloud underwent improvements in cost and performance metrics, previously overlooked due to rapid deployments, by leveraging resource monitoring, logging, and transaction analyses.

2.4 Financial Sector Cloud Usage Regulations and Security

In October 2016, the government introduced a new provision, Article 14-2 of the Electronic Financial Supervisory Regulations, designating systems with a low impact on electronic financial transactions as non-critical information processing systems [21]. Systems designated under this provision were allowed to use cloud services, provided they adhered to the cloud service usage guidelines. At that time, financial companies and the like were subject to Article 15 of the Electronic Financial Supervisory Regulations, which required anti-hacking measures. They had to ensure physical network separation from the internet and other external communication networks for internal information processing systems and terminals that directly connected for operational development purposes. This posed constraints on the use of cloud services. However, with the amendment to the Electronic Financial Supervisory Regulations, exceptions to the physical network separation regulations became possible for systems that did not handle customer information, such as product development, risk management, and business support [22]. The guidelines for using cloud computing services in the financial sector included details on the target systems for cloud usage, criteria for designating non-critical information processing systems, and system protection measures. Furthermore, the guidelines covered the soundness and safety evaluation criteria for cloud service providers, measures for data backup and disaster preparedness, securing redundancy or backup equipment, training and accident management, and establishing emergency response plans. The guide also addressed account management, access control, network security, integration between the internal systems of financial companies and cloud systems, encryption and key management, logging, virtual environment security, security monitoring and vulnerability analysis/evaluation, and measures to ensure human security [23–25].

Cloud service providers are supervised as electronic financial auxiliary businesses in a limited manner. Financial companies, acting as delegators, complied with Article 60, Paragraphs 1 and 2, of the Electronic Financial Supervisory Regulations. This entailed establishing security measures against threats like hacking and personal information leaks, putting in place emergency

measures for system failures and other service disruptions, formulating backup strategies for essential computerized data to ensure business continuity, implementing and operating internal control measures to maintain information security, and assessing the financial soundness and service quality levels of electronic financial auxiliary businesses at least once a year, reporting the results to the supervisory authorities. The obligations of financial companies as delegators had overlapping content and procedures with the measures for business continuity planning. Therefore, improvements were made by integrating the duplicated matters.

Following the revision of the Electronic Financial Supervisory Regulations in January 2019, the use of cloud services for critical information processing systems became permissible. Procedures for information security in the cloud concerning critical information were established. Due to concerns about legal disputes, consumer protection oversight, and personal data protection in case of incidents, the physical location of cloud systems and data was restricted to domestic territories when utilizing public cloud services for crucial tasks. Additionally, the government provided standards for the safety of cloud services in the financial sector. The established information protection procedures encompass granting financial companies and delegated third parties investigation access rights, setting up a financial backup system in anticipation of cloud service disruptions and data loss, vulnerability analysis and evaluation, emergency response training, integrated security control environment support, compliance with reporting procedures and response to security breaches and failures, and ensuring safety management equivalent to financial companies for facilities like buildings, power and HVAC, and computer rooms. Personal credit information and unique identification information are protected and managed according to laws such as the Credit Information Act and the Personal Information Protection Act, regardless of cloud utilization. The Credit Information Act demands compliance with protective measures like encryption when entrusting credit information, prohibits the use beyond the scope of the entrusted tasks, and forbids the re-delegation and requires training for custodians. The Personal Information Protection Act, Articles 26, 24, and 24-2, mandates prohibition of personal information processing outside the entrusted purpose, adherence to technical and managerial protective measures, and obligatory supervision and encryption for custodians. Moreover, CSPs must meet security standards equivalent to existing financial computer systems and undergo safety evaluations.

Financial companies have established internal control procedures, including evaluations of business importance, CSP (Cloud Service Provider) safety assessments, and reviews and decisions by the information protection committee. These companies evaluate the importance of information, confirm whether personal credit information is being processed, and conduct self-assessments of the cloud's technical and managerial safety measures to ensure secure cloud usage. The company's information protection committee reviews and decides on business continuity plans, safety assurance measures, and safety assessment results. Any decisions are then reported to the supervisory authority. The Financial Security Institute has supported financial companies in CSP safety evaluations. To streamline the process and avoid redundancy, the institute has taken the lead in evaluating the CSPs, allowing financial companies using the same CSP to utilize the results.

The government has presented countermeasures for major risks associated with cloud usage, such as CSP service interruptions, service failures, service lock-ins, and overseas business delegation. To mitigate CSP service disruptions, the government mandated the establishment and adherence to business continuity plans, such as the redundancy of key systems, emergency response systems, and conducting mock drills reflecting real-life situations. Financial companies have implemented malicious code prevention, crisis response procedures, spread prevention strategies for any failure, and risk management measures. This includes security patches for vir-

tual machines and hypervisors, monitoring, suspending and isolating in case of anomalies, and strengthening training for those responsible for the cloud environment. Moreover, they have fostered internal experts and managed user account permissions to strengthen crisis response systems and expertise. To prevent dependency or lock-ins to specific cloud providers, the government recommended financial companies to ensure flexibility by operating high-importance services on multi-cloud platforms. Additionally, for overseas business delegation, the government suggested identifying risks in advance when using overseas clouds, reflecting financial companies' requirements, such as jurisdiction, in contracts, and analyzing the political, social, and legal risk factors of the respective country while establishing a corresponding response system.

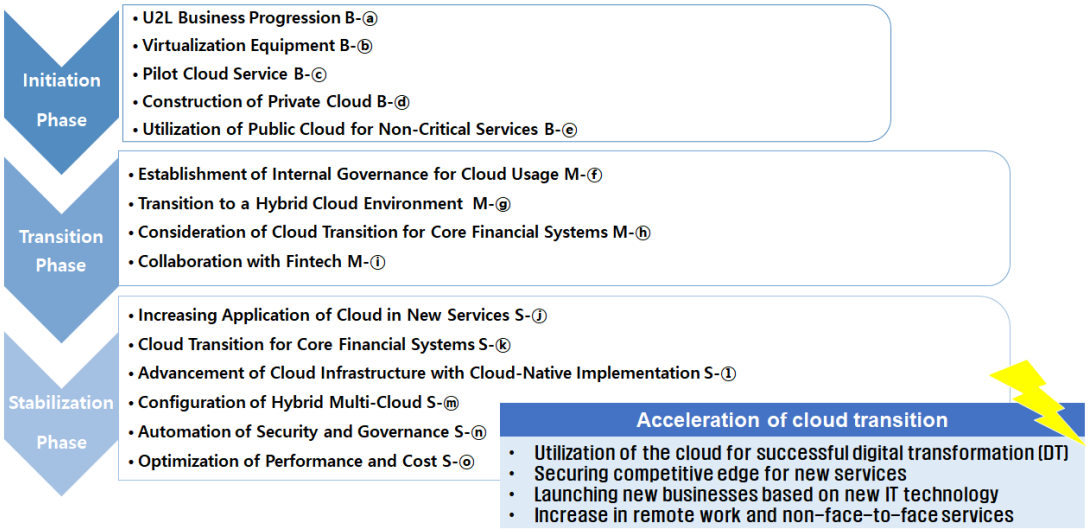

Figure 1: Phased Categorization of Cloud Adoption in the South Korean Financial Sector

Recently, the government has prepared supplementary measures to minimize security incidents, such as personal data breaches, resulting from the relaxation of physical network separation regulations. Through the financial regulatory sandbox, after conducting a self-risk assessment, financial institutions can apply information protection control methods as alternatives to network separation set by the supervisory authority. Exceptions to network separation are permitted for research and development purposes that are unrelated to financial transactions or do not handle customer transaction information. Also, they are considering allowing the use of SaaS for non-critical tasks within the internal network through additional conditions of the regulatory sandbox, preparing compensatory devices for information protection to apply network separation exceptions. With the gradual relaxation of cloud regulations and the transition of financial services, necessary policies, technologies, and devices for security are also changing. Various efforts have been made to satisfy both performance and security aspects. However, since the transition to the cloud is still ongoing, security also needs to adapt and change according to the evolving environment and structure.

Figure 1 depicts the main characteristics of the cloud transition in the financial sector over time. The symbols (B-, M-, S-) were used to link the features over time with the main factors identified for cloud transition. Table 3 summarizes the main factors for cloud transition in the

financial sector. Differences and commonalities observed in the transition cases by sector, such as banks, cards, insurance, securities, mutual finance, and fintech companies, are as shown in Table 4. When linking the characteristics by time, the overall use of the cloud in the South Korean financial sector showed characteristics of the stabilization phase.

Table 3: Key Factors for Cloud Transition in the South Korean Financial Sector

Category	Factor	Details
Efficient Utilization of New Technology (M-ⓖ, S-ⓙ)	Efficient utilization of new technologies such as AI/ML, big data analysis, and blockchain	Integration of various PaaS and SaaS related to new technologies offered by cloud providers and marketplaces
	Use of convenient high-performance, high-cost infrastructure	Ease of use of massive storage, high-performance analysis servers, and big data analysis tools
Infrastructure Operation and Cost Efficiency (B-ⓓ, B-ⓔ, M-ⓖ, M-ⓗ, S-ⓙ, S-ⓚ)	Flexible infrastructure operation through auto-scaling	Scale up to improve server specifications, scale out more servers and auto-scaling to handle promotions, events and runaway IPO traffic
	Utilization of Pay-as-you-go model	Cloud services such as serverless services reduce the cost burden associated with building an initial infrastructure
Securing Business Agility (S-ⓛ, S-ⓝ)	Launching services faster in competition with BigTech and FinTech	Accelerated launch of new MyData services to preoccupy customers
	High-speed application development and deployment through CI/CD pipeline and DevOps	Rapid application change deployment in response to changing market conditions
Strengthening Collaboration with Fintech (M-ⓘ, S-ⓙ)	Collaboration with FinTech companies through cloud open APIs, data linkage, etc	Building and operating a cloud platform consisting of data repositories, IaaS, data analysis platform (PaaS), open APIs, etc., to establish an efficient work collaboration environment between financial companies and FinTechs
	Creation of new businesses through the development of customized financial products and service partnerships	Utilizing the financial data of financial companies and the non-financial data of FinTech companies, along with the integration of AI/ML technologies, for the creation of new business opportunities and more

Table 4: Industry-specific Transition Trends and Key Differences

Industry	Key Differences (Cases)	Category
Bank	① Establish and operate a hybrid and multi-cloud strategy to utilize the best cloud services, reduce dependency on specific CSPs (Cloud Service Providers), and achieve objectives such as disaster recovery centers and enhanced security ② Establish governance and devise methods for work automation for efficient cloud operation	M-ⓕ, S-ⓜ, S-ⓝ
Credit Card	① Utilizing the cloud with the aim of offering not just payments but also personalized asset management, financial recommendations, and even non-financial services as part of an integrated financial platform ② Leveraging the cloud to secure service competitiveness in the easy-payment market in which big tech and fintech participate	S-ⓙ, S-ⓛ
Insurance	① Improving business processes through the management of vast amounts of data, insurance assessments, and the automation of claim processes ② Applying cloud AI services for non-face-to-face Happy Call services (Complete Sales Monitoring)	S-ⓙ
Securities	① Using the cloud for efficient infrastructure operation in anticipation of transaction surges due to events like IPOs, promotions, etc ② Utilizing the cloud so that operational teams can analyze derivative products in real-time as needed	M-ⓖ, S-ⓙ
Mutual Finance and Fintech	① Employing public cloud to develop a wide range of services swiftly and economically even with a small workforce, and to cut costs in infrastructure operation and management ② Focusing on innovative service development based on analyzing a vast amount of customer feedback and requirements	B-ⓔ, M-ⓘ, S-ⓙ
Common	① Adopting the cloud for swift infrastructure setup and service launch, aiming for early customer acquisition ② Using the cloud for cost-effective setup of high-availability infrastructure and for integration with AI/ML, big data analysis platforms ③ Continuous increase in adopting the public cloud for a flexible and resilient infrastructure and for the application of various new technologies ④ Applying cloud-native to maximize the benefits of the cloud ⑤ Considering data security and the integration with legacy systems, opting for a hybrid model ⑥ Gradual cloud adoption or review for core financial systems, such as account systems	B-ⓔ, M-ⓖ, M-ⓗ, M-ⓘ, S-ⓙ, S-ⓚ, S-ⓛ

3 Changes and Prospects in the Use of Cloud in the South Korean Financial Sector

The characteristics and factors for change, as observed through transition cases, are summarized to depict the evolution and prospects of cloud usage, as shown in Figure 2. The use of cloud in the financial sector is anticipated to grow further due to the increasing need to enhance customer experience and secure technical expertise, and the increasing need to create innovative customer-centric services. The operational complexity of the infrastructure is expected to increase with the operation of hybrid and multi-cloud. Therefore, it seems crucial to manage the schedule for active and inactive states by identifying idle resources through cloud inventory and identification. The need for integrated management using a cloud management platform is likely to increase. Moreover, there's a need for a strategy to standardize and commonize IT and security compliance based on consistent criteria, minimizing operational management costs and automating them. The modernization of existing applications will lead to rapid cloud-native adoption, enabling quicker service launches and a faster response to market environment changes.

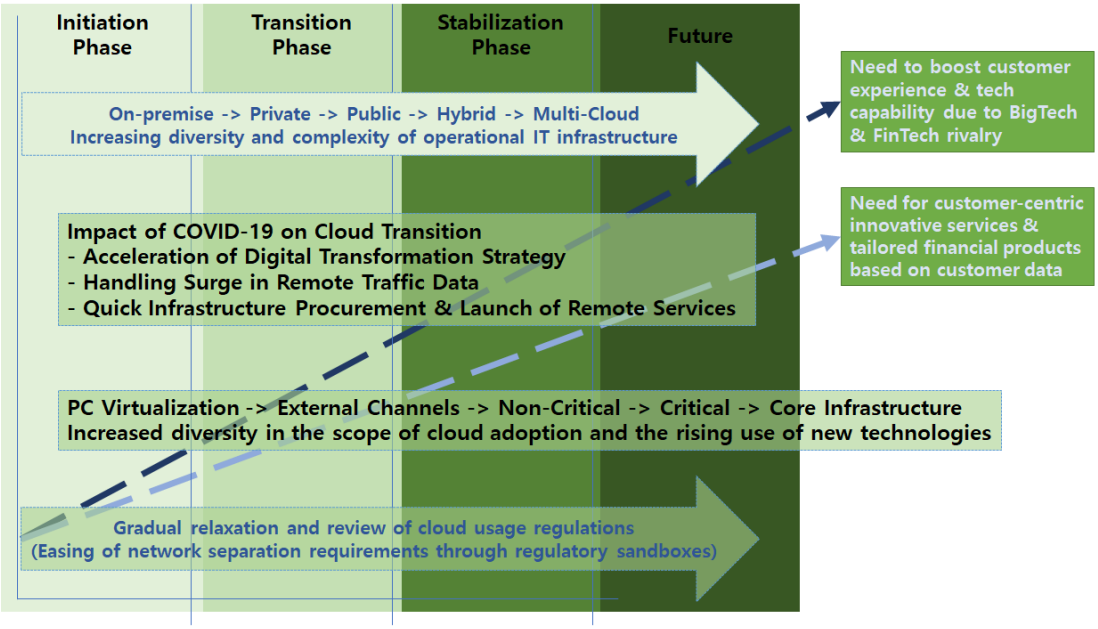

Figure 2: Changes in the Environment of the South Korean Financial Sector by Period and Prospects for Cloud Usage

The global outbreak of COVID-19 dramatically changed how businesses and individuals operate, emphasizing the need for digital transformation. The cloud played an essential role in accommodating these changes, and here are the major impacts of the pandemic on the cloud transition:

Acceleration of Digital Transformation Strategy: The pandemic underscored the importance of having a robust digital infrastructure. As face-to-face interactions became limited, organizations rapidly sought ways to shift their operations online. This led to a more aggressive approach towards adopting digital strategies, and the cloud became a pivotal component in

this shift.

Handling Surge in Remote Traffic Data: With the majority of the workforce transitioning to remote work and an increase in online shopping, education, and entertainment, there was a significant surge in online traffic. Traditional IT infrastructure could have struggled to cope with this sudden increase in demand. Cloud infrastructures, with their scalable nature, allowed businesses to quickly adapt and handle the unexpected spike in data traffic.

Quick Infrastructure Procurement & Launch of Remote Services: As the need for remote services grew, companies needed to launch new applications and platforms promptly. The cloud offered a quick and efficient way to procure the necessary infrastructure without the need for physical hardware setups. This meant businesses could deploy remote services faster, ensuring continuity and minimizing disruptions.

In response to market changes, cloud regulations are expected to gradually relax. With the loosening of cloud regulatory policies, both critical and non-critical financial information, which was previously restricted, will be utilized in cloud-based services. This shift underscores the anticipated need for enhanced security measures. Meanwhile, as the public cloud is being adopted across all areas of financial operations, including the core systems that handle customers' financial transactions, there's a growing trend among companies. These companies are considering building their own cloud infrastructure. However, as cloud service providers start offering various open-source solutions as services, companies will likely lean towards public clouds. This shift is due to the technical support for open-source solutions and the operational efficiency and cost-effectiveness advantages that public clouds present.

4 Security Threat Analysis and Classification Model

4.1 Use Environment of Cloud-Native Hybrid Multi-Cloud

Upon examining the preceding transition trends, the cloud usage environment in the South Korean financial sector is transitioning to a hybrid multi-cloud. The components are structured as illustrated in Figure 3, and Table 5 describes these components.

Financial companies are striving for operational efficiency and optimization of performance and cost in cloud-native and multi-cloud environments. In particular, to protect data, financial information such as customer information, credit information, point information, and transaction information is stored and managed on-premises. This data is encrypted and transmitted through dedicated lines to data analysis platforms. The data then undergoes ETL (Extract Transform Load) and anonymization processes before being stored in separate analysis marts for model development or EDA (Exploratory Data Analysis). The cloud infrastructure is configured using virtualization technologies like SDC (Software Define Computing), SDN (Software Define Network), and SDS (Software Define Storage). SDC supports bare-metal servers, virtual machines, and container computing resources, SDN supports L4 switches, L4 and L7 load balancers, and security resources, while SDS supports RBD (Raw Block Device), NFS (Network File System), and object storage resources. Containers are OS-based virtualization technology that provides an isolated service execution space while sharing the server's kernel. Kubernetes is used for container orchestration. Operating multi-cloud increases management complexity as the number of clusters and containers increases and services diversify, leading to rising management costs and a need for efficient management approaches. Multi-cluster operations based on Kubernetes help establish a centralized integrated resource visibility foundation by deploying consistent resource management policies across various clusters, such as on-premises, private, and public. Table 6 shows the multi-cluster management functions based on Kubernetes, which

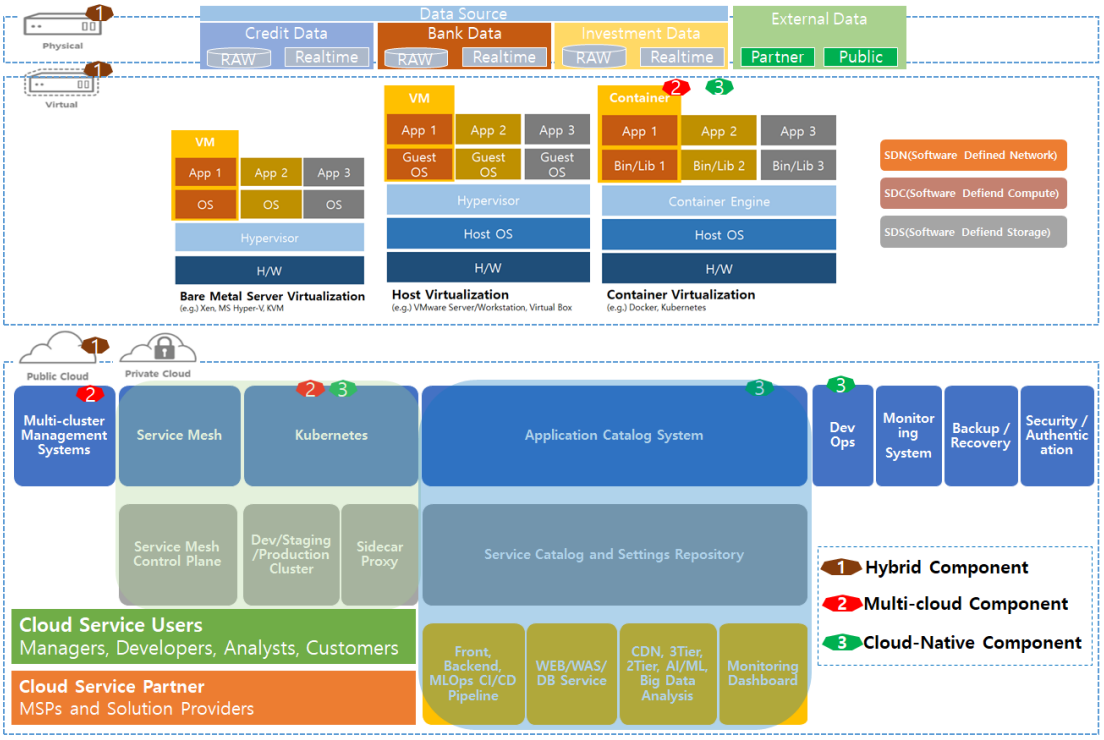

Figure 3: Cloud Native Hybrid Multi-Cloud Structure Abstract Diagram

reduces the burden of individually managing various Kubernetes clusters based on infrastructure.

Financial companies automate repetitive tasks through the operation of various standard CI/CD pipelines for infrastructure construction, application development, and deployment. This prevents human errors and boosts development productivity. They also utilize IaC (Infrastructure as Code) to manage infrastructure by catalog in repositories and provision infrastructure by selecting from the catalog when needed. Applications are split and organized into domain-specific service units that can be deployed independently. Each service communicates through APIs by setting up a service mesh. Cloud users consist of customers using the service, internal employees such as data analysts, infrastructure managers, developers, MSP staff, and service operators. Depending on the cloud usage environment, each system and service can either use services provided by CSPs, employ 3rd party solutions, or build using open source.

4.2 Security Threat Classification Model through Incident Case Analysis

Based on major cloud incident case studies [98–103], threats associated with the presented environment were derived through inductive analysis. Through the incident analysis, the cyber attack classification model was structured as shown in Figure 4, categorizing by purpose, means, method, risk factors, target, and attacker. Risk factors were differentiated into vulnerable operational structures, internal factors, and external factors, as depicted in Table 7. Attack methods

Table 5: Description of Cloud Components

Component		Description
Hybrid Multi-cloud	On-premise	Data storage for each subsidiary, with encrypted transmission through dedicated lines for data analysis utilization
	Kubernetes	Container irtualization orchestration
	Multi-cluster Management System	Support for multi-Kubernetes clusters in public, private, and on-premises environments (multi-tenancy management and monitoring)
	Monitering System	Collection, integration, and visualization of various information such as CPU usage, memory usage, API server response time, and pod status
	Backup / Recovery System	Cluster backup and restoration based on object storage
	Security / Authentication System	Authentication and key management module
	Logging System	Log format configuration, loading, and integrated analysis
Cloud-Native	DevOps	Source version management, build library management, image registry, code inspection, deployment tools, and standard CI/CD pipelines
	Service Mesh	Dedicated infrastructure layer built into applications to enable communication and data sharing between microservices
	Sidecar Proxy	Proxy container for communication between microservices
	Application Catalog System	Easy creation, sharing, management, and deployment of enterprise solutions
	MSA	Split a single large application into multiple independent service units, allowing for changes and combinations

Table 6: Example of Kubernetes-based Multi-Cluster Management Capabilities

Division	Example
1	Integrated monitoring of CPU, memory, pod usage, etc.
2	Cluster lifecycle management
3	Centralized access control and security policy management - Easy integration with existing enterprise authentication providers and any Kubernetes environment (AD, LDAP, etc.) - Central management of Kubernetes RBAC - Multi-tenant cluster management - Security and network policy management - CIS Benchmark Compliance Scan Inspection
4	Deployed workloads, cluster resource management and monitoring - Efficient service installation through the application service catalog function (marketplace operation, etc.)

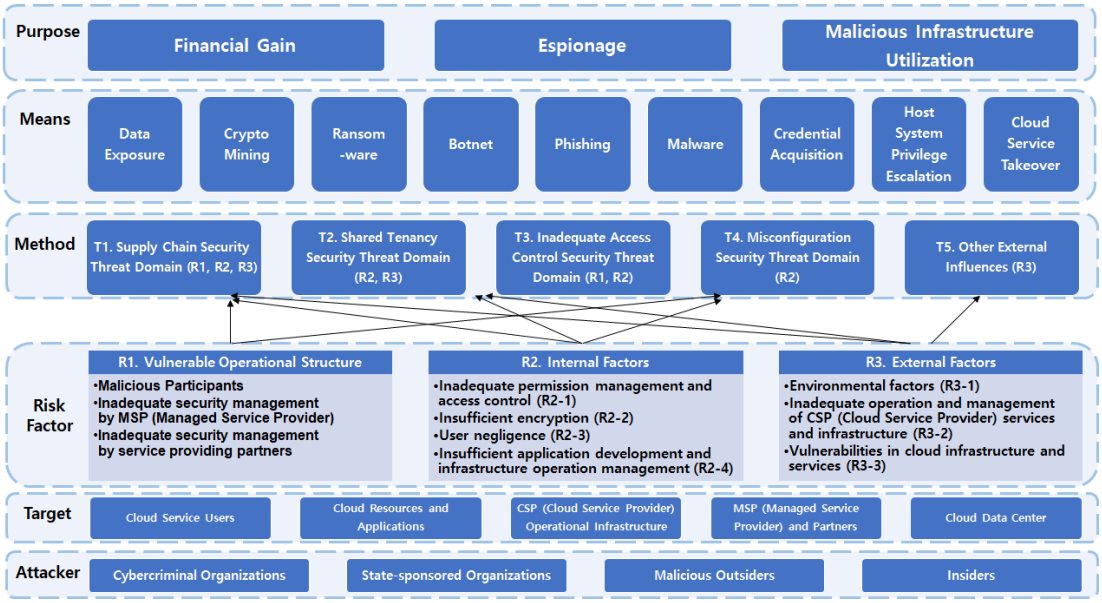

Figure 4: Cloud Cyberattack Classification Model

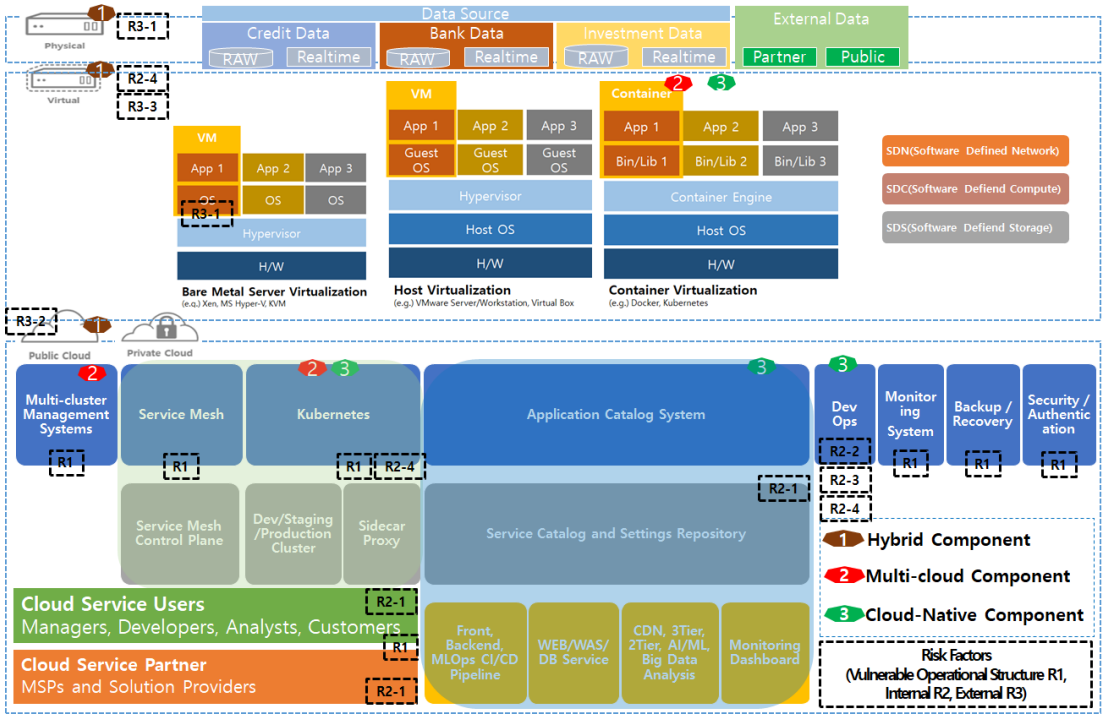

Figure 5: Identification of Threat Areas Relevant to the Classification Model

for each risk element were derived as security threats. The identified security threats represent methods to exploit the system's vulnerabilities, and the related system domains appeared as illustrated in Figure 5. Cloud security threats arise due to four vulnerabilities inherent to the cloud. Threats were categorized according to the related vulnerability domains, as shown in Table 8. Measures are taken to mitigate each vulnerability to prevent exposure to the respective security threats.

Table 7: Analysis of Risk Factors

Risk Factors (R)		Details
R1. Weak Operating Structure		- Malicious Participant - Lack of MSP Security Management - Lack of Security Management of Cloud Services (Backup Service, OA)
R2. Internal Factors	R2-1. Authority Management and Access Control	- Inappropriate Account Management and Authority Management - Inappropriate Cloud Resource and Service Security Settings - Lack of Cloud Security Governance Management
	R2-2. Encryption	- Critical Information Encryption Not Applied
	R2-3. User Negligence	- Lack of User Account Management - Insufficient Security Measures for User Terminals
	R2-4. Lack of Application Development and Infrastructure Operation Management	- Inherent Application Vulnerabilities - Shadow IT - Developer Negligence - Lack of Backup Management - Lack of DNS Server Management - Insufficient Web Firewall Settings - Lack of Network Access Control - Lack of Instance and Container Operation Management - Insufficient System Component Security Management
R3. External Factors	R3-1. Environmental Factors	- Natural Disasters such as Lightning, Fire, Flood, and Earthquake - BGP Setting Error of Router Device - Hostile Aggressor
	R3-2. Lack of CSP Service and Operation Management	- Operational Mistakes - Errors in the Data Center Management Automation Process

Each security threat area mentioned in Table 8 is elaborated upon below. Also, case studies for each security threat are shown in Table 9.

Supply Chain: The vulnerability of the supply chain in a cloud environment is considered a significant security issue. Threats can arise due to the presence of internal attackers or backdoors deliberately injected into hardware and software. Key causes of these threats include global CSP (Cloud Service Provider) workforce outsourcing, intentional backdoor injections by developers, and the intentional placement of industrial spies within the cloud supply chain. Such threats could compromise the entire cloud computing environment. To address these,

Table 8: Analysis of Security Threats

Security Threat Area	Security Threats (Method)
T1. Supply Chain	- T1-1. Malicious Insider Abuse of Power - T1-2. Spear Phishing for MSP employees - T1-3. Exploit Supply Application Vulnerabilities - T1-4. Open Source S/W Supply Chain Attack - T1-5. Exploitation of Cloud Service Vulnerabilities
T2. Shared Tenancy	- T2-1. Exploit Hypervisor Vulnerabilities - T2-2. Security Threats in Container Runtime - T2-3. Security Threats in Container Orchestration - T2-4. Security Threats in Container Networks
T3. Inadequate Access Control	- T3-1. Exploitation of Admin Application Vulnerabilities (bypassing Authentication Procedures, etc.) - T3-2. Abuse of Trust Relationship (Insufficient Authentication and Verification Procedures)
T4. Misconfiguration	- T4-1. Internet Exposure Cloud Resources Unauthorized Access and Scanning - T4-2. Serverless and Container Exploits - T4-3. Social Engineering
T5. Other External Influences	- T5-1. Mistakes in CSP Maintenance (Automatic Management Process, Internal DNS Change, Authentication System Change, Data Deletion during Operation, etc.) - T5-2. Exploit Computing Chip Vulnerabilities - T5-3. Natural Disaster (Lightning, Fire, Flood, Earthquake) - T5-4. BGP Setting Error (External ISP Official Mistake) - T5-5. Cloud Data Center Damage (such as the Physical Impact of a Data Center Fire) - T5-6. Loss of Backup Data Resiliency (Setting up Asynchronous Replication Backup) - T5-7. SSL Certificate Expiration

various alternatives are proposed, including recognizing supply chain risks, software and hardware verification, procurement of certified resources, adherence to secure coding standards, and more.

Shared Tenancy: Cloud platforms provide a multi-tenancy environment through various software and hardware components. In such an environment, security threats may arise from vulnerabilities in cloud hypervisors or container platforms and hardware flaws in processors. Such threats could compromise workload isolation features or expose another tenant's information to risk. Preventative and responsive measures include separating an organization's resources from other cloud tenants, encrypting data, and utilizing bare-metal instances.

Inadequate Access Control: When cloud resources and services employ weak authentication or authorization methods, they pose significant security risks. The lack of, or vulnerabilities in, authentication and authorization procedures are primary causes of such threats. Due to inadequate access control, attackers might escalate privileges or compromise cloud resources. To counter this, strong authentication and authorization protocols, zero-trust approaches, log auditing, and API key management are recommended.

Misconfiguration: Incorrect configuration of cloud services can lead to various security threats. Mistakes in setting cloud service policies or misunderstandings about shared responsibility can result in issues like service denials or account compromises. To prevent and address such problems, it's essential to rigorously implement cloud governance, apply encryption, utilize application gateways, IDS, VPN, and build a well-designed cloud architecture using technical alternatives.

Table 9: Descriptions and Cases of Security Threats

Security Threat	Description	Case
T1-1	Deviating from the principle of minimum privilege according to the roles and responsibilities of the given task or abusing authority	Malicious actors gaining read and write access to Twillo's AWS S3 bucket and abusing it to leak data
T1-2	Phishing emails impersonating CSPs and stakeholders to hijack accounts or spread malware	APT10 sending spear-phishing emails to MSPs to gain system access
T1-3	Attacks exploiting vulnerabilities in commercial applications	Solarwinds facing supply chain attacks that leaked customer network credentials and personal data from their products and networks
T1-4	Exploiting vulnerabilities in open-source used in services and applications	Malware attacks, like cryptomining and ransomware, using zero-day vulnerabilities found in the Java logging framework log4j
T1-5	Security threats arising from vulnerabilities in cloud providers, managed services, and SaaS products	Exploiting zero-day vulnerabilities in virtual storage appliances used by MSP cloud services to distribute ransomware to endpoints
T2-1	Exploiting hypervisor vulnerabilities to break out of virtual machines	Executing arbitrary code to escape the confines of VMs using vulnerabilities in VMware and Oracle virtualization software
T2-2	Security threats exploiting compromised virtualization containers	Gaining host access from container environments using vulnerabilities like CVE-2022-0811 in container runtimes
T2-3	Security threats due to poor orchestration management	Gaining container host access using vulnerabilities like CVE-2022-0185 arising in container orchestration
T2-4	Security threats from container network communications	Exploiting compromised containers to launch DDoS attacks on other containers in the same network or flooding serverless applications with excessive requests, causing financial burdens for cloud customers

Security Threat	Description	Case
T3-1	Attacking exposed admin applications	Unauthorized use of administrative features due to exposed administrator pages, API, and compromised user authentication
T3-2	Exploiting permissions of vulnerable services or servers	Abusing excessive IAM roles of EC2 instances through SSRF vulnerabilities to access S3 buckets
T4-1	Security threats abusing resources by accessing vulnerable cloud services identified through public repositories, dark web, or various OSINT	Unauthorized calls and information gathering on exposed cloud resources
T4-2	Malware operations on serverless services through compromised accounts	Distributing malicious code like crypto-mining through serverless AWS Lambda using malware like Denonia
T4-3	Security threats exploiting basic trust among people	Lapsus hacker group employing social engineering tactics to hijack accounts
T5-1	Security threats due to maintenance errors at CSP data centers	AWS engineer mistake causing a region outage
T5-2	Security threats from CPU hardware vulnerabilities	CSP patching for Spectre and Meltdown vulnerabilities
T5-3	Security threats due to natural disasters damaging data centers	MS Azure data center affected by lightning causing cooling system failures
T5-4	Security threats from BGP configuration errors by external ISPs	Connectivity issues in Google Cloud traffic due to BGP misconfigurations
T5-5	Security threats from physical attacks	Physical damages to data centers or communication cutoffs due to damaged optical cables
T5-6	Data loss issues during restoration using backup data	Data loss during recovery using asynchronously replicated backup data
T5-7	Unnatural connectivity issues due to SSL certificate expiration	Service connectivity issues when renewed certificates aren't properly integrated

5 Conclusion

This paper examined the cloud transition and security trends in the South Korean financial sector and forecasted the usage environment. Moreover, it explored the security threat classification model required to establish a safe cloud usage environment, as well as alternatives against security threats. The South Korean financial sector, in compliance with government regulations, is increasingly operating cloud-native hybrid multi-clouds, adhering to the financial sector cloud service usage guide proposed by the government. Consequently, the security threat classification model and the security threats discussed in this paper, based on major incident

case studies, provide a comprehensive view of security across infrastructure. This is anticipated to assist in reducing cyber risks in complex application operational environments. In the future, the authors of this paper plan to identify all foreseeable threats in the aforementioned environment and derive the necessary security requirements. They intend to perform threat modeling using the STRIDE method, identify threats, and evaluate them through graphs.

Acknowledgments

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. RS-2023-00210767).

References

[1] N. Bin. K-bank turns to 'big data system' cloud for the first time in the banking sector. https://www.hankyung.com/economy/article/202301301747i, January 2023.

[2] H. Hong. K-bank joins the public cloud line. https://byline.network/2022/06/02-69/, June 2022.

[3] E. Cha. Nh investment & securities opens big data cloud platform. https://www.hankyung.com/finance/article/2022022597536, February 2022.

[4] J. You. Kyobo life insurance builds big data cloud system. https://www.kbanker.co.kr/news/articleView.html?idxno=200530, September 2021.

[5] H. Hong. [interview] why lotte card turned its account system into a cloud. https://byline.network/2020/12/26-119/, December 2020.

[6] S. Lee. Lotte Card, which has switched to the 'account system' cloud, successfully responds to the "open banking - My Data environment.". https://ddaily.co.kr/page/view/202104210914206506 5, April 2021.

[7] H. Hong. [insite] why does kookmin bank change its account system to cloud? https://byline.network/2022/05/17-193/, May 2022.

[8] H. Hong. [financial in] core banking cloud transformation now 'start'. https://byline.network/2022/09/01-64/, September 2022.

[9] S. Park. Skt container cloud applies to hana card's mydata. https://zdnet.co.kr/view/?no=20220120103821, January 2022.

[10] H. Nam. Aia life supports customer health and happiness with digital transformation. https://zdnet.co.kr/view/?no=20211208163301, December 2021.

[11] M. Kim. Mirae asset life insurance catches incomplete sales with ai. https://www.etnews.com/20220303000048, March 2022.

[12] M. Jeon. Survival Strategies in the Non-face-to-face Era... Lina Life also wears "Cloud". https://www.moneys.co.kr/news/mwView.php?no=2021091710228048663, September 2021.

[13] D. Kim. [analysis] financial sector, how to calculate 'my data' usage...kookmin, woori, shinhan bank, lotte card comparison... different companies' capabilities and interests. http://www.bikorea.net/news/articleView.html?idxno=29609, February 2021.

[14] J. Park. [financial cloud 3] expecting the spread of the cloud with mydata. http://www.itdaily.kr/news/articleView.html?idxno=203914, August 2021.

[15] Penta Security Systems Inc. [easy to meet it] mydata platform, what cloud would fit in? https://blog.naver.com/pentamkt/222309506965, April 2021.

[16] M. Park. Woori bank expands 'ai customer counseling service'. https://www.boannews.com/media/view.asp?idx=105384, March 2022.

[17] H. Shim. Roh jin-ho, vice president of woori financial group from hancom, seeks to upgrade the group's cloud. https://www.dnews.co.kr/uhtml/view.jsp?idxno=202211102151198060462, November 2022.

[18] Y. Park. Kb savings bank completes cloud-based next-generation system. https://www.etnews.com/20221115000092, November 2022.

[19] J. Baek. SK C&C, builds KB Savings Bank's Next Generation Cloud-Based System. https://news.mt.co.kr/mtview.php?no=2021051709284339343, May 2021.

[20] H. Lee. Hyundai card innovates from finance to digital company with aws cloud. https://www.nextdaily.co.kr/news/articleView.html?idxno=50610, April 2018.

[21] Financial Services Commission. [press release] the financial services commission approves a revision to the electronic financial supervision regulations to rationalize cloud use procedures and ease network separation regulations - related to improvement plans for cloud and network separation regulations (april 2022) -. https://www.fsc.go.kr/no010101/78962?srchCtgry=&curPage=&srchKey=sj&srchText=%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C&srchBeginDt=&srchEndDt=, November 2022.

[22] Financial Services Commission. [press release] measures to improve cloud and network separation regulations in the financial sector. https://www.fsc.go.kr/no010101/77672?srchCtgry=&curPage=&srchKey=sj&srchText=%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C&srchBeginDt=&srchEndDt=, April 2022.

[23] Financial Services Commission. [easy to understand fintech 2] cloud and financial innovation. https://www.fsc.go.kr/no010101/73708?srchCtgry=&curPage=&srchKey=sj&srchText=%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C&srchBeginDt=&srchEndDt=, May 2019.

[24] Financial Services Commission. Cloud becomes more widely available in the financial sector. https://www.fsc.go.kr/no010101%20/73248?srchCtgry=&curPage=&srchKey=sj&srchText=%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C&srchBeginDt=&srchEndDt=, July 2018.

[25] Financial Services Commission. The financial sector can also utilize the cloud. https://blog.naver.com/blogfsc/220749020530, June 2016.

[26] Cloud Security Alliance. Cloud security alliance's top threats to cloud computing: pandemic 11 report finds traditional cloud security issues becoming less concerning. https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-se June 2022.

[27] S. Park. [security report] misconfiguration of the cloud platform is the most serious security threat. https://www.denews.co.kr/news/articleView.html?idxno=26819, July 2023.

[28] X.1601 security framework for cloud computing. Technical report, ITU-T, October 2015.

[29] X.1643 security requirements and guidelines for virtualization containers in cloud computing environments. Technical report, ITU-T, January 2022.

[30] Cloud Security Alliance. Security guidance for cretical areas of focus in cloud computing v4.0. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/, July 2017.

[31] US National Security Agency (NSA). Mitigating cloud vulnerabilities. https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF, January 2020.

[32] Cybersecurity & Infrastructure Security Agency (CISA). Cloud security technical reference architecture. https://www.cisa.gov/resources-tools/resources/cloud-security-technical-reference-architecture, January 2022.

[33] K. Park. 'shinhan bank's aws cloud in the u.s.' case... reasons for being cold on domestic flights. https://ddaily.co.kr/page/view/2017012002175046279, January 2017.

[34] S. Lee. How is 'samsung pay' overcoming difficult global service regulations? https://www.ddaily.co.kr/page/view/2018041916555029136, April 2018.

[35] J. Baek. Shinhan financial group, "it support for major global bases and conversion to cloud method by 2020". https://ddaily.co.kr/page/view/2018041815443397213, April 2018.

[36] S. Park. Shinhan financial group announces keynote at 'aws summit seoul 2018', "17 workloads will be converted to aws this year", evaluates over 5,000 servers within the group. http://www.bikorea.net/news/articleView.html?idxno=19974, April 2018.

[37] D. Kim. Kookmin bank's 'the k project', "just started to rise". http://www.bikorea.net/news/articleView.html?idxno=22700, February 2019.

[38] J. Shim. The story of how shinhan bank's it transformed into cloud native. https://byline.network/2019/10/17-66/, October 2019.

[39] N. Kim. Current status of cloud computing adoption in the financial sector. Technical report, Hana Financial Management Research Institute, August 2020.

[40] J. You. Toss bank's first shovel will float...rfp announcement of it system builders. https://it.chosun.com/site/data/html_dir/2020/02/18/2020021803199.html, February 2020.

[41] C. Shin. [it financial innovation] foreign business, main system...this is the 'cloud era'. https://www.mk.co.kr/news/it/9315246, April 2020.

[42] E. Lee. Shinhan financial will transform its it system into a cloud...launch of a '5-year plan'. https://www.thebell.co.kr/free/content/ArticleView.asp?key=20200529121053600108916&lcode=00, June 2020.

[43] J. Lee. Transition to post office financial systems cloud environment in 2023. https://www.newstomato.com/ReadNews.aspx?no=987618, August 2020.

[44] S. Lee. Kookmin bank seeks cloud transformation for 'core banking'...start 'post the k project'. https://ddaily.co.kr/page/view/2020081006470996331, August 2020.

[45] H. Hong. How insurers solved cloud worries. https://byline.network/2020/09/09109/, September 2020.

[46] J. Gil. [issue analysis] kb to build group joint cloud infrastructure in 2024. https://www.etnews.com/20201013000166, October 2020.

[47] J. Park. Nonghyup bank joins hands with naver cloud to introduce the industry's first "public cloud.". https://www.insightkorea.co.kr/news/articleView.html?idxno=84073, October 2020.

[48] J. Park. Nonghyup bank joins hands with naver cloud to introduce the industry's first "public cloud.". https://www.insightkorea.co.kr/news/articleView.html?idxno=84073, October 2020.

[49] M. Lim. Kakao bank completes aws financial security agency safety assessment... will channel and information cloud transition? https://www.ajunews.com/view/20201201110930514, December 2020.

[50] J. Song. "ai chatbot wrong answer rate 54%↓" hyundai card and google cloud met. https://it.chosun.com/site/data/html_dir/2020/12/09/2020120902054.html, December 2020.

[51] Samsung SDS. Hanwha life insurance builds hybrid cloud platform. https://www.samsungsds.com/kr/case-study/cloudsecurity-hanwha.html.

[52] J. Park. Cloud computing concepts and business cases of business. Technical report, KB Financial Group, Management Research Institute, February 2021.

[53] M. Lim. Sk telecom to build my data store of sc first bank... launching the 6 cloud businesses. https://www.ajunews.com/view/20210216103417242, February 2021.

[54] S. Lee. Mydata platform in the financial sector, what is your choice between private and public cloud? https://ddaily.co.kr/page/view/2021021807491415782, February 2021.

[55] S. Kim. [meeting financial ciso] park nam-gyu, managing director of bc card, "the completion of security is 'people'.". https://www.datanet.co.kr/news/articleView.html?idxno=156503, February 2021.

[56] H. Hong. [interview] why kookmin bank is working hard on mydata. https://byline.network/

2021/03/03-37/, March 2021.

[57] J. Kim. Kt is making efforts to target the 'hybrid cloud' market...management solution launch next month. https://www.etnews.com/20210304000192, March 2021.

[58] M. Kang. The financial sector initiates cloud adoption. https://www.polinews.co.kr/news/articleView.html?idxno=484910#0FV0, March 2021.

[59] S. Lee. Finger inc. wins order to build welcome savings bank's mydata. https://www.fnnews.com/news/202104261533349038, April 2021.

[60] Kakaopay. How infrastructure platform team uses public cloud for fast and secure service. https://blog.kakaopay.com/story/post/67-kakaopay-cloud/, June 2021.

[61] S. Lee. Kt and shinyoung securities will complete 100% cloud transformation for the first time in the financial sector. https://www.mk.co.kr/news/it/9922855, June 2021.

[62] M. Park. S. korean bourse operator seeks to create smart workplace. https://m.boannews.com/html/detail.html?idx=98784, July 2021.

[63] S. Kim. Kt wins order to build 'my data cloud' for bc card. https://www.itbiznews.com/news/articleView.html?idxno=41946, July 2021.

[64] J. Lee. Bank salad, a promising mydata player, dreams of real estate and health super-personalization services beyond finance. https://ddaily.co.kr/page/view/2021071904160841054, July 2021.

[65] H. Park. Financial cloud accelerates mydata platform readiness. https://newsroom.koscom.co.kr/27479, July 2021.

[66] J. Park. Promoting the introduction of cloud in the financial sector ahead of competition with big tech. https://www.comworld.co.kr/news/articleView.html?idxno=50341, July 2021.

[67] H. Na. Kakao pay dreaming of a new financial life. https://newsroom.koscom.co.kr/27479, August 2021.

[68] D. Kim. Nonghyup bank's next generation of information 'rfp' was released... https://newsroom.koscom.co.kr/27479, September 2021.

[69] E. Ryu. Why toss payments chose aws. https://it.chosun.com/site/data/html_dir/2021/10/22/2021102201579.html, October 2021.

[70] S. Nam. Kakao pay's development capabilities, reliability and stability come first. https://it.donga.com/101068/, November 2021.

[71] E. Ryu. Samsung financial networks turns to cloud for derivative analytics. https://it.chosun.com/site/data/html_dir/2021/11/12/2021111200931.html, November 2021.

[72] M. Gil. Initech builds sc first bank financial transaction system cloud. https://www.dailysecu.com/news/articleView.html?idxno=131966, November 2021.

[73] H. Hong. Nonghyup bank's unveiled 'all-one bank' next generation, core 'comprehensive finance and cloud'. https://byline.network/2022/02/07-69/, February 2022.

[74] O. Bae. Hana financial group's 'cloud integrated operation center' is newly established...increase efficiency. https://news.zum.com/articles/81284111?cm=news_rankingNews, February 2022.

[75] H. Yun. Ms korea helps establish a hybrid work environment for the national agricultural cooperative federation. https://www.cnet.co.kr/view/?no=20220324115333, March 2022.

[76] J. Seo. Kyobo life insurance partners with amazon web services..."apply cloud expansion to platforms". https://www.etoday.co.kr/news/view/2132033, May 2022.

[77] H. Hong. How to use the cloud of popular financial companies and fintech. https://byline.network/2022/05/12-169/, May 2022.

[78] H. Lee. Toss bank "difference from traditional banks, slim 'split service' structure". https://www.etnews.com/20220518000246, May 2022.

[79] S. Ko. 'introduction of cloud technology' that has emerged as a hot topic in the financial sector... why? https://www.sisaon.co.kr/news/articleView.html?idxno=139039, May 2022.

[80] Y. Park. Hana bank opens 'ai callbot' service. https://www.etnews.com/20220524000232, May 2022.

[81] H. Hong. How did toss bank and toss securities system work? https://byline.network/2022/06/10-234/, June 2022.

[82] S. Kim. Innovation for customer convenience over and over again. . . open data analysis system with cloud technology. https://www.joongang.co.kr/article/25082120#home, June 2022.

[83] H. Hong. How the financial sector uses public and private cloud. https://byline.network/2022/07/01-58/, July 2022.

[84] I. You. 'introduction of cloud' active financial sector, its scope of use will expand. https://www.kcloudnews.co.kr/news/articleView.html?idxno=11182, July 2022.

[85] K. Park. Evolving financial cloud expands horizon. https://ddaily.co.kr/page/view/2022072717471999475, July 2022.

[86] J. Park. The next generation in the financial sector, cloud-focused. https://www.comworld.co.kr/news/articleView.html?idxno=50649, July 2022.

[87] M. Kim. Ibk launches 'five-year plan' to build cloud system. https://www.etnews.com/20220803000130, August 2022.

[88] O. Bae. Hana bank to push for next-generation system in 13 years. https://www.etnews.com/20220805000185, August 2022.

[89] S. Lee. Will kakao bank's it expenses exceed 30 billion won this year?. . . increase cloud investment. https://ddaily.co.kr/page/view/2022080809242185770, August 2022.

[90] H. Hong. Kb kookmin bank's cloud transformation strategy. . . "private in a public way. https://byline.network/2022/08/23-216/, August 2022.

[91] H. Hong. There is also a 'generation' in the financial it system. https://byline.network/2022/08/24-201/, August 2022.

[92] H. Hong. Hana bank considers transition to private cloud for accounting operations. https://byline.network/2022/08/26-202/, August 2022.

[93] S. Choi. Shinhan financial investment stable online orders despite flood of orders. . . deploying mts on a public cloud. https://www.hankyung.com/finance/article/2022083199001, August 2022.

[94] S. Hong. Shinhan financial investment to build multi-cloud-based open platform. https://biz.newdaily.co.kr/site/data/html/2022/09/15/2022091500050.html, September 2022.

[95] W. Kim. Nhn cloud-shinhan financial investment signs mou on cloud transformation. https://zdnet.co.kr/view/?no=20220921140518, September 2022.

[96] I. You. Woori finance, accelerating the introduction of new technologies such as ai... group joint cloud platform advancement. https://www.kcloudnews.co.kr/news/articleView.html?idxno=11578, November 2022.

[97] J. Lee. Naver cloud establishes 'neuro cloud' system at ibk industrial bank of korea. https://news.mt.co.kr/mtview.php?no=2023020709200237954, February 2023.

[98] Cloud service incident case study analysis report. Technical report, Financial Security Institute, July 2022.

[99] US National Security Agency (NSA) and Cybersecurity & Infrastructure Security Agency (CISA). Kubernetes hardening guide. https://www.cisa.gov/news-events/alerts/2022/03/15/updated-kubernetes-hardening-guide, August 2022.

[100] LLOYD'S. Cloud down impacts on the us economy. https://assets.lloyds.com/assets/pdf-air-cyber-lloyds-public-2018-final/1/pdf-air-cyber-lloyds-public-2018-final.pdf, January 2018.

[101] T. Maurer and G. Hinck. Cloud security:a primer for policymakers. https://www.jstor.org/stable/pdf/resrep25787.1.pdf, August 2020.

[102] Y. Lee. 7 threats to the cloud. Technical report, AhnLab, Inc., April 2021.

[103] X-force cloud security threat landscape report. Technical report, IBM, September 2022.