사물인터넷융복합논문지 Vol. 11, No. 5, pp. 217-222, 2025 https://doi.org/10.20465/KIOTS.2025.11.5.217

ARVIS: 클라우드 환경을 위한 자동화된 복원력 검증 및 개선 시스템

이찬휘[1], 이근호[2*]
[1]백석대학교 컴퓨터공학부 학생, [2]백석대학교 컴퓨터공학부 교수

ARVIS: An Automated Resilience Verification and Improvement System for Cloud Environments

Chan-Hwi Lee[1], Keun-Ho Lee[2*]
[1]Student, Division of Computer Engineering, Baek-Seok University
[2]Professor, Division of Computer Engineering, Baek-Seok University

요 약 최근 다양한 분야에서 클라우드 서비스 도입이 가속화되면서, 클라우드 장애는 곧 비즈니스 장애를 뜻한다. 그러나 기존 복원력 관리 방식은 파편화된 환경, 복구 신뢰성 검증 부족, 정량적 평가의 한계와 같은 문제를 안고 있으며, 이는 장애나 공격 발생 시 복구 지연과 실패를 유발해 서비스 연속성과 신뢰성 확보에 큰 위협이 된다. 본 논문은 이러한 한계를 극복하기 위해 카오스 엔지니어링, 불변형 백업, 클라우드 네이티브 오케스트레이션, AI/ML 기반 복원력 분석을 통합한 ARVIS(Automated Resilience Verification and Improvement System)를 제안한다. ARVIS는 장애를 능동적으로 검증하고, 클린 복구 지점을 보장하며, 복구 프로세스를 자동화하고, 복원력을 정량화·예측함으로써 검증–측정–개선의 자동화된 폐쇄 루프를 구현한다. 이를 통해 클라우드 환경의 복원력 관리에서 신뢰성, 가시성, 효율성을 동시에 향상시킬 수 있다.

주제어 : 클라우드 복원력, 카오스 엔지니어링, 불변형 백업, 오케스트레이션, 인공지능

Abstract With the recent acceleration of cloud service adoption across various sectors, cloud failures have become synonymous with business disruption. However, existing resilience management approaches suffer from fragmented environments, insufficient verification of recovery reliability, and limitations in quantitative assessment. These challenges lead to delayed and failed recovery in the event of failures or attacks, posing a significant threat to service continuity and reliability. To overcome these limitations, this paper proposes the Automated Resilience Verification and Improvement System (ARVIS), which integrates chaos engineering, immutable backup, cloud-native orchestration, and AI/ML-based resilience analytics. ARVIS actively verifies failures, ensures clean recovery points, automates recovery processes, and quantifies and predicts resilience, thereby implementing an automated, closed loop of verification, measurement, and improvement. This system simultaneously enhances reliability, visibility, and efficiency in resilience management in cloud environments.

Key Words : Cloud Resilience, Chaos Engineering, Immutable Backup, Orchestration, Artificial Intelligence

이 논문은 2025학년도 백석대학교 학술연구비 지원을 받아 작성되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2025년 10월 10일 수정일 2025년 10월 20일 심사완료일 2025년 10월 22일

1. 서론

클라우드 서비스가 다양한 분야에서 도입이 가속화되면서, 클라우드 장애는 곧 비즈니스 장애를 의미하게 되었다. 그러나 하이브리드 및 멀티 클라우드 환경은 복잡성을 증가시켜 서비스 연속성과 데이터 보호에 새로운 위험을 초래한다. 특히 랜섬웨어 공격, 대규모 네트워크 장애 등 사례는 클라우드 복원력(resilience)이 기업 생존의 핵심 요소임을 보여준다.

기존 복원력 관리 방식은 백업과 재해 복구(Disaster Recovery, DR)를 중심으로 발전해 왔으나, 환경의 파편화, 복구 신뢰성 검증 부족, 정량적 평가의 한계라는 문제가 남아 있다[1]. 이로 인해 실제 장애 상황에서 복구가 지연되거나 실패하는 사례가 발생하며, 기업 신뢰성에도 부정적 영향을 준다.

본 논문에서는 이러한 문제를 해결하기 위해 ARVIS (Automated Resilience Verification and Improvement System)를 제안한다. ARVIS는 카오스 엔지니어링, 불변형 백업, 클라우드 네이티브 오케스트레이션, AI/ML 기반 복원력 분석을 통합하여 복원력을 검증–측정–개선하는 자동화된 폐쇄 루프 체계를 구축한다. 이를 통해 클라우드 환경에서 신뢰성과 효율성을 동시에 향상시키는 복원력 관리 방안을 제시한다.

2. 관련연구

2.1 카오스 엔지니어링

카오스 엔지니어링은 분산·클라우드 환경에서 의도적으로 장애를 주입해 시스템의 복원력을 검증하는 기법으로, Netflix의 Chaos Monkey가 대표적이다[2]. 이는 정상 상태를 정의하고, 장애를 주입한 뒤 시스템의 반응을 관찰·분석하는 흐름으로 수행된다. 이를 통해 숨은 취약점을 발견하고 복구 절차의 신뢰성을 강화할 수 있으며, 클라우드 환경 전반의 안정성과 가용성을 높이는 효과가 있다. 또한, 이러한 방법은 사전적·능동적 복원력 관리 방안을 가능하게 한다.

2.2 불변형 백업

불변형 백업(Immutable Backup)은 생성된 데이터를 일정 기간 동안 수정이나 삭제가 불가능하도록 설정하여, 랜섬웨어 공격 상황에서도 클린 복구 지점을 확보할 수 있는 기법이다. 기존의 백업 방식은 공격자가 침투할 경우 데이터가 훼손될 수 있다는 한계가 있으나, 불변형 백업은 이러한 위협을 근본적으로 차단한다. 최근에는 블록체인 기반 로그 관리 기법이 제안되어, 대규모 클라우드 시스템에서 로그의 무결성과 추적 가능성을 강화할 수 있음을 보여주었다[3].

2.3 클라우드 네이티브 오케스트레이션

클라우드 네이티브 오케스트레이션은 인프라와 복구 절차를 코드로 정의해 자동화하는 기술로, 컨테이너 관리 도구인 Kubernetes, 인프라 정의도구인 Terraform과 같은 도구가 대표적으로 사용된다. 관리자는 복구 플레이북을 코드 형태로 작성하고, 이를 통해 복구 과정이 수동 스크립트가 아닌 자동화된 워크플로로 실행된다. 이러한 방식은 장애 발생 시 복구 절차의 일관성을 확보하고 실행 속도를 높이며, 사람의 개입으로 인한 오류를 줄일 수 있다. 또한 멀티 클라우드 및 하이브리드 환경에서 자원을 통합적으로 관리할 수 있어 이식성과 확장성을 높일 수 있다[4-8].

2.4 AI/ML 기반 복원력 분석

AI/ML 기반 복원력 분석은 로그, 성능 지표, 네트워크 트래픽 등 다양한 운영 데이터를 학습하여 장애 발생 가능성을 예측하거나 복구 시간(*RTO*)과 데이터 손실(*RPO*)을 정량화하는 기법이다. 머신러닝 모델은 과거 장애 패턴을 기반으로 복구 실패 가능성을 탐지하고, 사전에 병목 지점을 식별할 수 있다. 이를 통해 관리자는 복구 과정에서의 위험 요소를 미리 파악하고, 대응 전략을 최적화할 수 있다. 또한, 복원력 지표를 자동 산출·예측함으로써 기존 수동적인 사후 분석 방식보다 빠르고 정확한 의사결정을 지원한다[9-11].

3. 제안 방법

3.1 선정 배경

클라우드 서비스는 다양한 산업 분야에서 핵심 인프라로 자리 잡고 있으며, 장애 발생은 곧 비즈니스 중단으로 직결된다. 그러나 기존의 재해 복구(Disaster Recovery, DR) 방식은 수동 절차와 정적 시나리오에 의존하기 때문에 실제 환경의 복잡성과 다양한 위협을 충분히 반영하지 못한다. 특히 파편화된 관리 체계, 복구 절차의 불확실성, 복원력의 정량적 평가 부족은 복구 지연과 신뢰성

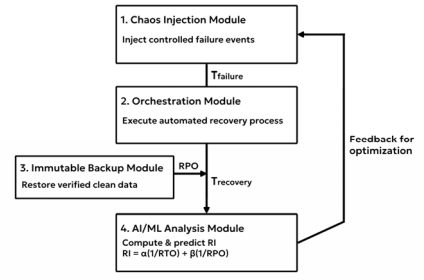
저하로 이어지고 있다[1][15].

이러한 한계를 극복하기 위해서는 장애를 능동적으로 검증하고, 신뢰할 수 있는 복구 지점을 확보하며, 복구 과정을 자동화하고, 복원력을 정량적으로 분석할 수 있는 통합적 관리 체계가 필요하다. 본 논문에서는 이러한 요구를 충족하기 위해 카오스 엔지니어링, 불변형 백업, 클라우드 네이티브 오케스트레이션, AI/ML 기반 분석을 결합한 ARVIS 시스템을 제안한다[12-14].

3.2 ARVIS 시스템 개요

제안하는 시스템은 Fig. 1과 같다. Chaos Engineering, Immutable Backup, Orchestration, AI/ML Analysis 네 가지 핵심 모듈이 통합되어 복원력 검증–측정–개선을 자동화하는 지속적인 폐쇄 루프 (closed-loop) 시스템 흐름을 갖는다. ARVIS의 통합은 기존 수동적 재해 복구 방식의 한계를 극복하고, 능동적 검증을 통해 복구 신뢰성과 데이터 무결성을 확보하는 데 중점을 둔다.

시스템 성능은 장애 발생 시각($T_{failure}$)과 정상 복귀 시각($T_{recovery}$)을 기준으로 산출되는 RTO 및 RPO와 같은 정량 지표로 평가되며, 이는 3.3절에서 정의된다.



[Fig. 1] ARVIS system workflow

Step 1. Orchestration 모듈의 명령에 따라 Chaos Injection이 Kubernetes API를 통해 장애 시나리오를 주입한다. 장애 발생 시각 정보($T_{failure}$)를 Orchestration에 전달하여 복구 시간(RTO) 측정 및 자동 복구의 시작점을 설정한다.

Step 2. 장애 발생 시각 정보($T_{failure}$)를 받은 Orchestration이 복구 절차를 자동으로 실행하며 시스템 정상 복귀 시각($T_{recovery}$)을 측정한다. 이 모듈은 복구 과정의 일관성을 확보하고 지표 산출을 위한 데이터를 준비한다.

Step 3. 복구 절차 중 Orchestration의 호출에 따라 Immutable Backup 모듈이 S3 Object Lock 검증을 통해 무결성이 확보된 클린 백업 이미지로 복원을 수행한다. 이는 랜섬웨어 공격에도 안전한 복구 지점을 보장하여 복구 시점(RPO) 확보에 기여하는 핵심 통합 기능이다.

Step 4. Orchestration으로부터 장애 발생 시각, 정상 복귀 시간 등의 정량 데이터를 전송받은 AI/ML 분석 모듈이 복원력 지수(RI)를 산출하고 취약점을 분석한다. 도출된 개선 권고사항은 Chaos Injection 모듈로 피드백되어 다음 실험의 파라미터를 자동으로 최적화하며 루프를 완성한다.

3.3 복원력 지표

ARVIS는 복구 성능을 평가하기 위해 복구 시간(Recovery Time Objective, RTO), 복구 시점(Recovery Point Objective, RPO), 복원력 지수(Resilience Index, RI)를 산출한다[14][15].

복구 시간 RTO는 다음과 같이 정의된다.

$$RTO = T_{recovery} - T_{failure} \quad (1)$$

여기서 $T_{failure}$는 장애 발생 시각, $T_{recovery}$는 시스템이 정상 상태로 복귀한 시점을 의미한다. 본 연구에서는 HTTP 200 응답 및 200 ms 미만의 지연 조건이 연속 10회 충족되는 최초 시점을 복구 완료 시점으로 간주하였다. 복구 시간 $T_{recovery}$는 장애 발생 $T_{failure}$후 서비스 응답 상태가 정상으로 전환되어 일정 시간(10초 이상) 안정적으로 유지되는 최초 시점으로 정의하였다.

복구 시점 RPO는 데이터 손실 시간을 나타내며 다음과 같이 정의된다.

$$RPO = T_{last} - T_{failure} \quad (2)$$

이는 장애 발생 직전 커밋 타임스탬프와 복구 후 최신 커밋 타임스탬프의 차이로 측정되며, 상태저장 시나리오에서는 MySQL 트랜잭션 단위로 비교하여 산출하였다. 데이터 손실 한계 T_{last}는 장애 발생 직전의 최신 정상 백업 또는 커밋 타임스탬프를 의미하며, 이는 복구 시점에서 허용 가능한 최대 데이터 손실 범위를 나타낸다.

복원력 지수 RI는 복구 속도와 데이터 손실을 동시에 고려하여 다음 식으로 계산된다[15].

$$RI = \alpha \cdot \frac{1}{RTO} + \beta \cdot \frac{1}{RPO} \quad (3)$$

본 연구에서는 α=0.6, β=0.4로 설정하였다. 여기서 α, β는 복구 속도(RTO)와 데이터 손실(RPO)의 상대적 중요도를 반영하는 가중치이다. RTO와 RPO가 작을수록 RI가 커지며, 높은 RI는 우수한 복원력을 의미한다.

단위 불일치를 방지하기 위해 RTO와 RPO는 각각 기준값(RTO_{base}, RPO_{base})으로 정규화하여 무차원화하였다. 이에 따라 실제 계산식은 다음과 같이 표현된다.

$$RI = \alpha \cdot \frac{RTO_{base}}{RTO} + \beta \cdot \frac{RPO_{base}}{RPO} \quad (4)$$

여기서 RTO_{base}와 RPO_{base}는 실험에서 측정된 최댓값을 사용하였다. 이를 통해 두 항목의 단위 차이를 제거하고, 복원력 지표가 0~1 범위 내에서 비교 가능하도록 하였다.

또한, 장애 복구의 성공률(Success Rate, SR)은 다음과 같이 정의된다.

$$SR = \frac{N_{success}}{N_{total}} \times 100(\%) \quad (5)$$

여기서 $N_{success}$는 정상 복구에 성공한 횟수, N_{total}은 전체 실험 횟수를 의미한다.

복원력 지수(RI)의 가중치 α, β는 복구 속도(RTO)와 데이터 손실(RPO)의 상대적 중요도를 반영한다. 본 연구에서는 서비스 연속성 관점에서 RTO를 상대적으로 더 중시하는 운영 가정을 반영하여 $\alpha > \beta$로 설정하였다. α를 0.1~0.9 범위에서 변화시키며($\beta = 1 - \alpha$), 각 조합에 대해 3.4절의 실험 데이터를 이용한 민감도 분석을 수행하였다. 그 결과, α = 0.6에서 조건 간 분리도(Cliff's δ)와 RI-SR 스피어만 상관이 최대값에 근접하였으며, α = 0.5와 0.7일 때 RI 평균값의 변동은 ±4% 이내로 나타났다.

3.4 실험 환경

실험은 3노드 Kubernetes 1.28 클러스터 환경(각 노드 4 vCPU, 8 GB RAM)에서 수행하였다. 워크로드는 비상태 애플리케이션(podinfo)과 상태저장 데이터베이스(MySQL PV)로 구성하였다.

〈Table 1〉 은 본 연구에서 수행한 주요 카오스 시나리오를 나타낸다.

〈Table 1〉 Chaos experiment scenarios

Scenario	Failure Type	Duration	Measurement Target
S1	Pod Kill (podinfo)	30 s	RTO_app
S2	Network Delay/Loss	Delay 1000 ms, Loss 5%	RTO_app
S3	MySQL Process Kill	20 s	RTO_db, RPO_db
S4	I/O Chaos (MySQL)	I/O delay 150 ms	RTO_db, RPO_db

각 실험은 세 가지 조건에서 수행되었다. 조건 A는 기존 수동 복구 방식(Manual), 조건 B는 Chaos + Backup 모듈만 적용한 환경, 조건 C는 ARVIS 전체 모듈을 적용한 환경이다. 각 시나리오는 동일한 초기 상태에서 10회 반복 실행되었으며, 모든 측정값은 중앙 수집 시스템을 통해 취합하였다.

3.5 실험 설계 및 분석 절차

복구 성공 여부는 애플리케이션 레벨에서의 정상 응답을 기준으로 판정하였다. 복구가 실패하거나 TIMEOUT(300초) 내 복귀하지 못한 경우 실패로 간주하였다. 성공한 시나리오에 대해 RTO, RPO, RI를 계산하였으며, 평균, 표준편차, 중앙값을 이용하여 통계적으로 요약하였다. 또한, 데이터베이스 시나리오의 경우, 애플리케이션 복구 외에도 DB 트랜잭션 복귀 여부를 별도로 측정하여 RTO_{db}, RPO_{db}로 병행 분석하였다.

ARVIS의 효과를 검증하기 위해 각 조건별 복구 성능을 비교하였다. 〈Table 2〉는 ARVIS 적용 전후의 복구 결과이다.

〈Table 2〉 Comparison of recovery performance before and after applying ARVIS

Condition	SR(%)	RTO(s)	RPO(s)	RI
A (Manual)	81.2	68.3 ± 12.1	142.5 ± 30.4	0.017
B (Chaos + Backup)	91.4	48.7 ± 9.8	93.2 ± 27.1	0.026
C (ARVIS)	98.6	29.4 ± 5.1	58.7 ± 18.5	0.041

ARVIS 적용 시 평균 RTO는 약 57 % 감소하였으며, RPO는 약 59 % 감소하였다. 복구 성공률은 18 %p 증가하였고, RI는 약 2.4배 향상되었다. 이는 카오스 주입과 자동 오케스트레이션, 불변형 백업의 결합이 복원력 개선에 실질적인 효과를 가짐을 의미한다[2][8][14][15].

조건 간 차이 검정은 성공률에 대해 피셔의 정확 검정을, RTO·RPO·RI와 같은 연속 지표에 대해 Mann–Whitney U 검정을 적용하였다. 효과크기는 Cliff's δ로 산출하였으며, 모든 검정은 유의수준 α = 0.05에서 수행하였다.

AI/ML 분석 모듈은 수집된 데이터를 기반으로 Random Forest 회귀모델을 학습하였다[9][13]. 모델은 장애 유형, 지속시간, 복구 지표(RTO, RPO, RI 등)를 입력 변수로 사용하였다. 예측 결과의 평균 절대 백분율 오차(MAPE)는 6.8%로 나타났으며, 예측된 복원력 지수와 실측 복원력 지수 간의 피어슨 상관계수(Pearson's r)는 0.93으로 계산되었다. 이는 두 변수 간의 선형 상관 정도를 나타내는 지표로, 1에 가까울수록 예측값과 실제값의 일치도가 높음을 의미한다. 따라서 ARVIS의 AI/ML 분석 모듈이 복구 성능을 높은 정확도로 예측함을 확인하였다.

Random Forest 모델의 주요 하이퍼파라미터는 n_estimators = 200, max_depth = 10, min_samples_split = 4, min_samples_leaf = 2, max_features = "sqrt", random_state = 42로 설정하였다. 학습 과정은 10-fold 교차검증과 OOB(out-of-bag) 평가를 통해 과적합을 방지하였으며, 평균 R^2 = 0.86, MAPE = 6.8%, MAE = 0.017, RMSE = 0.025로 측정되었다. Feature importance 분석 결과, 복원력 지수(RI)에 가장 큰 영향을 미치는 요인은 RTO(0.31), Error Rate(0.24), Recovery Time(0.19), Latency(0.13) 순으로 나타났다. 이는 복구 시간 관련 지표가 복원력 예측의 핵심 변수임을 보여주며, 앞서 설정한 α = 0.6의 가중치 선택과도 일관된다. 이를 통해 ARVIS가 단순한 복구 도구를 넘어 지속적인 학습과 성능 향상이 가능한 복원력 개선 프레임워크임을 확인하였다.

4. 결론

본 논문은 클라우드 환경에서 기존 복원력 관리가 수동적 절차, 신뢰성 검증 부족, 정량적 평가의 한계로 인해 효과적 대응이 어렵다는 문제를 지적하였다. 이를 해결하기 위해 카오스 엔지니어링, 불변형 백업, 오케스트레이션, AI/ML 분석을 통합한 ARVIS(Automated Resilience Verification and Improvement System)를 제안하였다.

ARVIS는 장애 주입을 통한 능동적 검증, 클린 복구 지점 확보, 코드 기반 복구 절차 자동화, 복원력 지표의 정량화·예측을 통합한 폐쇄 루프를 구현한다. 이를 통해 복원력을 단순한 사후적 대응이 아닌 관리 가능한 자산으로 전환하고, 클라우드 환경에서 신뢰성과 효율성을 동시에 향상시킬 수 있음을 보였다.

향후 연구에서는 ARVIS의 프로토타입을 구축하여 실제 클라우드 환경에서 다양한 장애 시나리오를 검증하고, 비용 대비 성능 효과를 분석할 필요가 있다. 또한 카오스 실험의 안전한 적용, AI/ML 모델의 학습 데이터 품질 관리, 규제 준수 기능 강화 등을 통해 ARVIS를 실무적으로 확장 가능한 복원력 관리 프레임워크로 발전시키고자 한다.

REFERENCES

[1] B. Liu, Y. Xin and C. Zhang, "A Solution for A Disaster Recovery Service System in Multi-cloud Environment," 2022 International Applied Computational Electromagnetics Society Symposium (ACES-China), pp.1-4, 2022.

[2] K. A. Torkura, M. I. H. Sukmana, F. Cheng and C. Meinel, "Security Chaos Engineering for Cloud Services: Work In Progress," 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), pp.1-3, 2019.

[3] T. Kwon, M. Kim, Y. Jung, J. Kim and B. Kim, "Traceable Blockchain Logging System for Cloud-Based Systems," 2024 15th International Conference on Information and Communication Technology Convergence (ICTC), pp.1720-1724, 2024.

[4] J.-B. Kim, J.-B. Choi and E.-S. Jung, "Design and Implementation of an Automated Disaster-recovery System for a Kubernetes Cluster Using LSTM," arXiv:2402.02938, 2024.

[5] Y. Doyomade and V. Ogunrinde, "Disaster Recovery Strategies in Kubernetes-Based Cloud Orchestration," (Unpublished Work), 2022

[6] N. niemi, E.salo, A. Vainio, and A. James, "Stateful Application Management in Kubernetes Environments," 2021.

[7] S. Malhotra, F. Yashu, M. Saqib and F. Divyani, "A Multi-Cloud Orchestration Model Using Kubernetes For Microservices," SSRN: 5194262, 2020.

[8] J.-B. Kim, J.-B. Choi and E.-S. Jung, "Design and Implementation of an Automated Disaster-recovery System for a Kubernetes Cluster Using LSTM," arXiv:2402.02938, 2024.

[9] M. Züfle, F. Erhard and S. Kounev, "Machine Learning Model Update Strategies for Hard Disk Drive Failure Prediction," 2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA), pp.1379-1386, 2021.

[10] E. Zeydan and S. S. Arslan, "Cloud2HDD: Large-Scale HDD Data Analysis on Cloud for Cloud Datacenters," 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), pp.243-249, 2020.

[11] C. Koh, J. Kang, T. Kim and S. W. Han, "Temporal-Contextual Attention Network for Solid-State Drive Failure Prediction in Data Centers," IEEE Access, Vol.12, pp.154455-154466, 2024.

[12] T. Welsh and E. Benkhelifa, "On Resilience in Cloud Computing: A Survey of Techniques across the Cloud Domain," ACM Comput. Surv., Vol.53(3), pp.59:1-59:36, 2021.

[13] F. Wang, J. Tian, C. Shi, J. Ling, Z. Chen and Z. Xu, "A multi-stage quantitative resilience analysis and optimization framework considering dynamic decisions for urban infrastructure systems," Reliability Engineering & System Safety, Vol.243, p.109851, 2024.

[14] H. Cho, J.-H. Sung, H.-J. Kang, J. Jang and D. Shin, "Quantifying Cyber Resilience: A Framework Based on Availability Metrics and AUC-Based Normalization," Electronics, Vol.14(12), p.2465, 2025.

[15] A. De Marco, D. Berardi, M. Galuppi and M. Lombardi, "Quantitative resilience assessment on critical infrastructures – A systematic literature review of the last decade (2014-2024)," Journal of Safety Science and Resilience, Vol.6(3), p.100201, 2025.

이 찬 휘(Chan-Hwi Lee) [준회원]

■ 2020년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉

클라우드, 네트워크, 개인정보보호, 보안 엔지니어링

이 근 호(Keun-Ho Lee) [종신회원]

■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)

■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 기술전략팀 과장

■ 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉

융합보안, 블록체인, 개인정보보호, 이동통신 보안