고가용성 보장형 국방 클라우드 시스템 도입 전략

Deployment Strategies of Cloud Computing System for Defense Infrastructure Enhanced with High Availability

강기완*, 박준규*, 이상훈**, 박기웅[1)]
Ki-Wan Kang, Jun-Gyu Park, Sang-Hoon Lee, Ki-Woong Park

(05006) 서울특별시 광진구 능동로 209 세종대학교 정보보호학과 시스템보안 연구실*,
국방과학연구소**, 세종대학교 정보보호학과[1)]
{kkwan0226, wnsrb3001}@gmail.com, shlee@add.re.kr, woongbak@sejong.ac.kr

요 약

세계적으로 ICT(Information & Communication Technology)를 통한 비용절감 및 업무혁신이 이루어지면서 클라우드 컴퓨팅(이하 클라우드) 시장이 급성장하고 있다. 이러한 패러다임에 맞춰 우리나라는 다양한 연구를 통해 공공부문, 국방 분야 등 다양한 분야에 클라우드를 도입시키기 위해 노력하고 있다. 특히 국방 분야에서는 2015년 육·해·공·군 전산소를 통합하여 국방통합데이터센터(DIDC, Defense Integrated Data Center)를 설립하였으며, 센터 내 일부 시스템을 대상으로 IaaS(Infrastructure as a Service) 형태의 클라우드 서비스를 제공하고 있다. 국방통합데이터센터 및 추후 도입될 국방 분야의 다양한 클라우드 시스템에서 네트워크 지연, 시스템 자원 고장 등과 같은 시스템 장애가 발생하게 되면 전장의 결과와 직결되기 때문에 국방 부문의 클라우드 시스템에 가용성을 보장하는 것은 중요한 이슈라 할 수 있다. 그러나 국방 클라우드의 모든 시스템을 대상으로 최고 수준의 가용성을 확보하는 것은 비효율적일 수 있으며, 클라우드 시스템 구축으로 얻을 수 있었던 효율성이 감소할 수 있다. 본 논문에서는 국방 클라우드 시스템의 가용성 확보 수준을 단계별로 분류 및 정의하고, 각 가용성 확보 수준에 따른 Erasure Coding 및 장애 허용 시스템, 재난 복구 시스템 기술 도입 전략을 제안한다.

Abstract

Cloud computing markets are rapidly growing as cost savings and business innovation are being carried out through ICT worldwide. In line with this paradigm, the nation is striving to introduce cloud computing in various areas, including the public sector and defense sector, through various research. In the defense sector, DIDC was established in 2015 by integrating military, naval, air and military computing centers, and it provides cloud services in the form of IaaS to some systems in the center. In DIDC and various future cloud defense systems, It is an important issue to ensure

※ 본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원(No.2018-0-00420, No.2019-0-00273), 한국연구재단 연구과제(NRF-2017R1C1B2003957) 및 국방과학연구소의 국방 지휘통제 통합·연동 기반기술 특화연구실 과제의 지원(UD180012ED)의 지원을 받아 수행된 연구임.

1) 교신저자

논문투고일자 : 2019. 06. 07 심사일자 : 2019. 06. 07 게재확정일자 : 2019. 06. 21

availability in cloud defense systems in the defense sector because system failures such as network delays and system resource failures are directly linked to the results of battlefields. However, ensuring the highest levels of availability for all systems in the defense cloud can be inefficient, and the efficiency that can be gained from deploying a cloud system can be reduced. In this paper, we classify and define the level of availability of defense cloud systems step by step, and propose the strategy of introducing Erasure coding and failure acceptance systems, and disaster recovery system technology according to each level of availability acquisition.

키워드: 클라우드 컴퓨팅, 국방 인프라, 고가용성
Keyword: Cloud Computing, Defense Infrastructure, High Availability

1. 서론

제 4차 산업 혁명 흐름에 맞춰 ICT를 통해 기업 및 국가적으로 비용절감 및 업무 혁신이 이루어지면서 클라우드 시장이 급성장하고 있다. 최근에는 개인에서부터 기업 · 정부에 이르기까지 다양한 분야 및 사용자가 클라우드 서비스를 활용하고 있으며 기존 컴퓨터 시스템에 비해 서버 유지 · 보수 · 관리 비용 절감과 자료 저장의 안정성 및 신속한 접근성의 편리함을 통해 차세대 ICT 패러다임으로 부각되고 있다[1].

이러한 차세대 ICT 패러다임에 맞춰 우리나라는 행정자치부에서 발행한 “행정 · 공공기관 민간 클라우드 이용 가이드라인[2]” 과 안보경영 연구원에서 발행한 “국방 클라우드 컴퓨팅 운영환경 구축 방안 연구[3]” 를 통해 공공부문, 국방 분야 등 다양한 분야에서 정책 마련, 기반환경 조성 등 클라우드 도입을 위해 노력하고 있는 것을 알 수 있다. 특히 국방 분야에서 육 · 해 · 공군 전산소를 통합한 국방통합데이터센터를 설립하였으며, 현재 전군을 대상으로 일부 IaaS 형태의 클라우드 서비스를 제공하고 있다[4] [5].

국방기술품질원에서 발간한 “국가별 국방과학기술 수준조사서[6]”에 따르면 우리나라는 국방과학기술에 있어 최고 선진국인 미국을 100%로 두고 이와 비교해 평균 80%의 기술력을 확보하고 있으며, 우리나라 국방과학기술 수준은 세계 주요 16개국 중 이탈리아와 공동 9위를 차지하고 있다고 한다. 국방과학기술에 있어 최고 수준을 자랑하는 미 국방부는 2018년 ‘프로젝트 제다이(JEDI)’를 실시하였다. 해당 프로젝트는 세계 각국에서 미국이 수집한 영상 등 각종 군사 정보들을 분류하고 통합할 클라우드 인프라 구축을 위한 것으로, 10년 간 약 100억달러(약 11조 4000억 원)가 투입될 예정이다[4]. 아직까지 우리 군은 클라우드 운영환경 및 구축방안에 대해서 연구 및 시범적으로 사업을 추진하고 있다. 하지만 국방통합데이터센터 개관 등과 같이 기반환경 조성과 다양한 정책 등을 통해 단계적으로 국방 클라우드가 구축될 것이라고 전망하고 있다[6].

국방 분야의 경우 지휘체계, 전투체계, 무기체계 등 군과 관련된 다양한 정보체계들로 구성된다. 국방이라는 특성 상 전시상황을 준비 및 분석하고, 각 상황에 맞는 최선의 결정을 내리게 된다. 이러한 국방 분야의 클라우드 시스템에서 네트워크 지연, 시스템 자원 고장 등과 같은 시스템 장애가 발생하게 되면 전장의 결과와 직결되기 때문에 국방 부문의 클라우드 시스템에 가용성을 보장하는 것은 중요한 이슈라 할 수 있다. 그러나 국방 클라우드의 모든 시스템을 대상으로 최고 수준의 가용성을 확보하는 것은 비효율적일 수 있으며, 클라우드 시스템 구축으로 얻을 수 있었던 효율성이 감소할 수 있다. 따라서 본 논문에서는 국방 클라우드 시스템의 가용성 확보 수준을 단계별로 분류 및 정의하고, 각 가용성 확보

수준에 따른 Erasure Coding 및 장애 허용 시스템, 재난 복구 시스템 등 가용성 보장을 위한 기술 도입 전략을 제안한다. 첫 번째는 데이터 수준에서의 가용성 확보를 위한 방안으로 Erasure Coding 도입을 제안한다. Erasure Code를 통해 손실 데이터의 규모 및 범위를 파악하고 손실된 부분에 대해 복구한다. Erasure Coding과 유사한 개념인 RAID(Redundant Array of Independent Disks)는 장애가 발생하였을 때 장애가 발생한 디스크의 개수에 제한이 있지만 Erasure Coding은 관리자가 원하는 만큼 인코딩 데이터를 생성하여 장애에 대비 가능하다. 이를 통해 국방 클라우드 시스템에 저장되는 데이터의 안정성을 확보한다. 두 번째는 시스템 자원 수준에서의 가용성 확보를 위한 방안으로 장애 허용 시스템 도입을 제안한다. 국방 클라우드 시스템을 구성하는 구성요소(프로세서, 디스크, 메모리, 파워 서플라이, 팬, 메인보드, 확장 슬롯, 백본 등)에서 장애 또는 고장이 발생해도 부분적으로 혹은 전체적으로 본래의 기능을 수행할 수 있어야 한다. 세 번째는 인프라 수준에서의 가용성 확보를 위한 방안으로 재난 복구 시스템 도입을 제안한다. 재난 및 전쟁으로 인해 시스템이 파괴되었을 때를 대비하여 국내 타 지역 및 해외에 백업 시스템을 구축하는 것이다. 일반적으로는 장애 허용 시스템 도입을 통해 대부분의 Single Point of Failure를 해결 가능하지만 국방이라는 특수한 상황을 고려해 매우 높은 가용성을 요구하는 국방 시스템을 대상으로 재난 복구 시스템 도입을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 시스템에서 데이터의 가용성을 확보하는 연구에 대해 설명하고 각 연구들의 한계점을 도출한다. 3장에서는 가용성 확보 수준을 단계별로 분류 및 정의하고, 4장에서는 분류한 가용성 확보 수준에 따라 효율적인 국방 클라우드 시스템 도입 방안을 제안한다. 5장에서는 과거 발생했던 클라우드 가용성 침해 사례에 대해 분류한 국방 클라우드의 가용성 확보 수준 별 대응 여부를 제시한다. 마지막으로 6장에서는 본 논문의 결론 및 향후 연구방향에 대해 기술한다.

2. 관련 연구

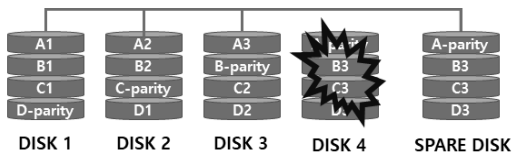
본 장에서는 기존 시스템 환경에서 데이터의 가용성을 확보하기 위해 도입한 기술들에 대해 물리 계층, 파일 시스템, 정보 이론 차원으로 분류 및 설명하고, 각 기술의 한계점을 제시한다.

2.1 물리 계층 차원의 데이터 가용성 확보 관련 연구

본 절에서는 기존 시스템 환경에서 물리 계층 차원의 가용성 확보를 위해 일반적으로 사용되는 RAID에 대해 다룬다.

소모품으로 분리가 되는 하드디스크는 고가용성 시스템 운영 중 고장 확률이 가장 높은 구성 요소이다. 하지만 서버에 저장되는 데이터의 경우 손실 또는 유출되었을 때는 치명적인 결과를 초래할 수 있다. 상황에 따라 백업이 절대적으로 필요한 경우가 존재하며, 하드디스크 추가를 통해 부족한 데이터 용량을 확보하는데 데이터의 손실 없이 증설해야하는 경우가 존재한다. 따라서 기존의 많은 서버 관리자들은 RAID 구성을 통해 서버의 성능 및 하드디스크 가용성, 데이터의 안정성을 확보하였다. RAID는 주로 중요한 데이터를 보관하거나 높은 성능을 요구할 때 사용되며, 여러 대의 하드디스크가 존재할 때 데이터를 중복 및 분할하여 저장하는 방법이다[7]. 하드디스크가 많으면 많을수록 MTBF(Mean Time Between Failure)를 증가시키며, 중복해서 저장할 시 하드디스크의 고장에도 대비할 수 있다. 기존에는 RAID 0~6까지 존재했지만 최근 RAID 10, RAID 01과 같이 RAID 레벨을 동시에 2개 이상을 사용하는 사례도 존재한다. (그림 1)은 RAID 5의 parity 영역이 전체 디스크에 로테이션 되는 것을 도식화 한 것이다. 오류가 발생한 디스크는 스페어 디스크에 복구 가능하다.

RAID의 경우 데이터 단위가 아닌 디스크 단위로 복구를 진행하게 된다. 디스크 용량이 증가함에 따라 복구에 소요되는 시간도 증가하며, 복구 중 추가적인 장애 발생으로 인해 데이터가 손실 될 수 있는 가능성이 존재한다.



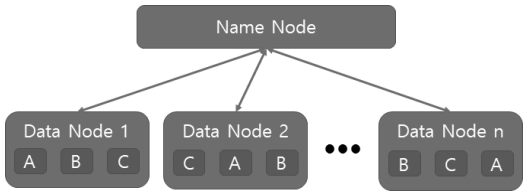
(그림 1) RAID 5를 통한 디스크 장애 해결

2.2 파일 시스템 차원의 데이터 가용성 확보 관련 연구

본 절에서는 기존 시스템 환경에서 파일 시스템 차원의 가용성 확보를 위해 사용되는 NFS(Network File System), CIFS(Common Internet File System) 등 다양한 분산 파일시스템 중 구글의 GFS(Google File System)의 영향을 받아 만들어진 오픈 소스 파일 시스템인 HDFS(Hadoop Distributed File System)에 대해 다룬다.

HDFS는 대용량의 데이터 처리 및 데이터 저장에 특화된 파일 시스템이다. HDFS는 (그림 2)와 같이 하나의 네임노드와 다수의 데이터 노드로 구성된다. 네임노드는 HDFS의 네임 스페이스를 관리하며 클라이언트의 파일 접근 요청을 처리한다[8]. 데이터 노드는 클라이언트의 데이터 입출력 요청을 128MB(Hadoop v2.0 이상) 블록 단위로 저장한다. 컴퓨터 클러스터에서 데이터 복제본을 생성하여 복구하는 기능을 제공한다. 복구 기능은 사용자가 설정한 만큼 복제본을 생성하여 동작하는데 일반적으로 3개의 복제본을 생성하여 데이터 손실이 발생했을 때 데이터 복구를 진행한다[9].

일반적으로 3개의 복제본을 생성하여, 낮은 스토리지 효율을 가지고 있으며, 다른 스토리지 기술에 비해 많은 비용이 든다. 또한 HDFS는 파일 생성, 삭제, 이동, 수정 등이 가능하지만, 사용자의 직접적인 접근 권한과 링크는 지원하지 않고 있다. 데이터 노드에 장애가 발생하면 해당 블록과 동일한 블록을 가지고 있는 데이터 노드는 다른 데이터 노드에게 전송하여 항상 3개의 블록을 유지하도록 한다. 블록의 복구를 위한 복사 과정은 블록의 가용성을 높이는 장점이 있지만, 데이터의 수정으로 인해 업데이트가 발생할 경우에 원본 데이터의 블록인지 확인할 방법이 없다.



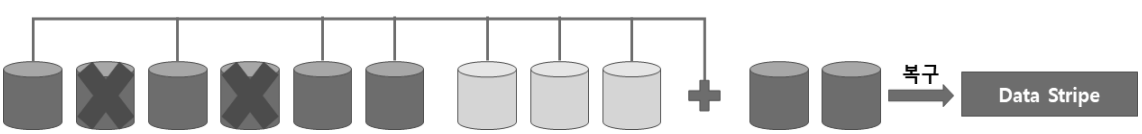
(그림 2) HDFS의 데이터 저장 구조

2.3 정보 이론 차원의 데이터 가용성 확보 관련 연구

본 절에서는 기존 시스템 환경에서 정보 이론 차원의 가용성 확보를 위해 2.2절에서 다룬 HDFS의 스토리지 및 네트워크 오버헤드를 줄이기 위해 고안된 Erasure Coding에 대해 다룬다.

Erasure Coding은 데이터 저장 공간의 효율성 및 안정성을 높이기 위해 설계되었다. (그림 3)과 같이 데이터를 사전에 정의한 개수로 분할 및 오류정정코드를 생성한다. 데이터의 손실이 발생했을 시 (그림 4)와 같이 손실되지 않은 데이터와 오류

(그림 3) Erasure Coding Encoding Process



(그림 4) Erasure Coding Decoding Process

정정코드를 통해 데이터를 복구한다. 생성한 오류 정정 코드의 개수가 k개라면 최대 k개의 데이터가 손실 되어도 n개의 손실 되지 않은 데이터를 통해 원본 데이터를 복구할 수 있다. 유사한 개념인 RAID는 parity를 통해 최대 2개의 동시 오류를 지원하지만 Erasure Coding은 관리자의 설정에 따라 원하는 만큼 인코딩 데이터를 생성하여 3개 이상의 동시 오류를 지원한다[10].

Erasure Coding은 손실 데이터를 복구하는 기법이며, 데이터 백업을 대체할 수 없다.

3. 국방 클라우드 시스템의 가용성 확보 수준 분류

고가용성의 척도는 숫자 9의 조합으로 평가된다. 99% 가용성을 유지하는 것과 99.99%의 가용성을 유지하는 것은 엄청난 비용과 기술의 차이가 존재한다. 따라서 국방 클라우드의 모든 시스템을 대상으로 최고 수준의 가용성을 확보하는 것은 비효율적일 수 있으며, 클라우드 시스템 구축으로 얻을 수 있었던 효율성이 감소할 수 있다. 본 장에서는 효율적인 국방 클라우드 시스템의 가용성 확보를 위해 가용성 확보 수준을 데이터, 시스템 자원, 인프라 수준으로 분류하고, 각 단계에 대해 정의한다[11].

• Level 1 : None

본 논문에서 국방 클라우드 시스템의 가용성 확보를 위해 분류한 데이터, 시스템 자원, 인프라 수준의 가용성을 확보하지 않는다. 국방 클라우드 시스템 운영 중 데이터, 시스템 자원, 인프라의 장애 발생 시 관리자가 별도의 백업을 하지 않은 이상 모든 데이터에 대한 손실 가능성 존재 및 국방 클라우드 시스템의 운영이 불가능할 수 있다.

• Level 2: Data Level

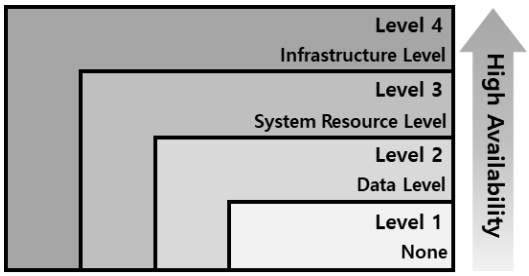
국방 클라우드 시스템 운영 중 필요 데이터에 대해 장애가 발생했을 경우 정상적으로 데이터를 사용할 수 있게 복구해야 한다. 국방이라는 특수한 환경을 고려했을 때 전장과 관련된 데이터를 적시에 열람하지 못하는 것은 군사작전에 있어 매우 큰 영향을 끼칠 수 있다. 따라서 신속하고 신뢰할 수 있는 데이터 복구를 통해 데이터 가용성을 확보해야 한다.

• Level 3: System Resource Level

시스템을 구성하는 자원(프로세서, 디스크, 메모리, 파워 서플라이, 팬, 메인보드, 확장 슬롯, 백본 등)에서 장애 또는 고장이 발생해도 부분적으로 혹은 전체적으로 본래의 기능을 수행할 수 있어야 한다. 같은 기능을 수행할 수 있는 두 대의 시스템을 대해 구축하고, 한 쪽 시스템에 장애가 발생했을 경우 다른 시스템이 대체 작동하여 가용성을 확보한다. 추가적으로 네트워크 수준까지 고려하면 대부분의 Single Point of Failure를 제거 가능하다.

• Level 4: Infrastructure Level

재난 및 재해에 대한 자동 복구 시스템을 구축하는 것은 시스템 보호 단계 중 가장 비용이 많이 소요되며, 높은 수준의 IT 기술력이 결집되어야만 가능하다. 천재지변에 대비하여 시스템은 원격지에 서로 이중화되어야 하며, 백업 시스템은 언제든지 자동으로 메인 시스템을 대체할 준비가 되어 있어야 한다. 국방 클라우드 시스템과 같이 매우 높은 가용성을 요구하는 시스템에 대해서는 이중화된 시스템 내부에 동일한 시스템을 병렬로 배치하여 시스템의 다운타임을 극소화시킬 수 있다.



(그림 5) 국방 클라우드 시스템의 가용성 확보 수준

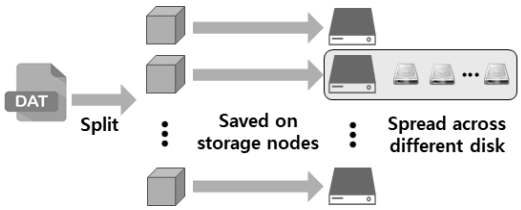
4. 가용성 확보 수준을 고려한 국방 클라우드 시스템 도입 방안

본 장에서는 3장에서 분류한 가용성 확보 수준에 따라 Erasure Coding 및 장애 허용 시스템, 재난 복구 시스템 기술 도입 방안을 제안한다.

4.1 Erasure Coding 적용을 통한 국방 클라우드의 데이터 가용성 확보 방안

Erasure Coding은 데이터 저장 공간의 효율성 및 안정성을 높이기 위해 설계되었으며 최대 k개의 데이터가 손실 되어도 n개의 데이터만 존재한다면 원본 데이터를 복구할 수 있다. 군사기밀은 국가안전보장에 명백한 위험을 초래할 우려가 있는 군(軍) 관련 문서, 도화(圖畵), 전자기록 등 특수매체기록 또는 물건을 뜻한다[12]. 군사 기밀의 유출은 국방에 있어서 큰 문제이지만 군사 기밀을 적시에 열람하지 못하는 것 또한 군사작전에 있어 큰 영향을 끼칠 수 있다.

(그림 6)과 같이 Erasure Coding은 관리자가 사전에 설정한 만큼 데이터를 분할하여 각 스토리지 노드에 저장하고, 각 스토리지 노드에 저장된 데이터는 연결된 디스크들에 분산시켜 저장한다.

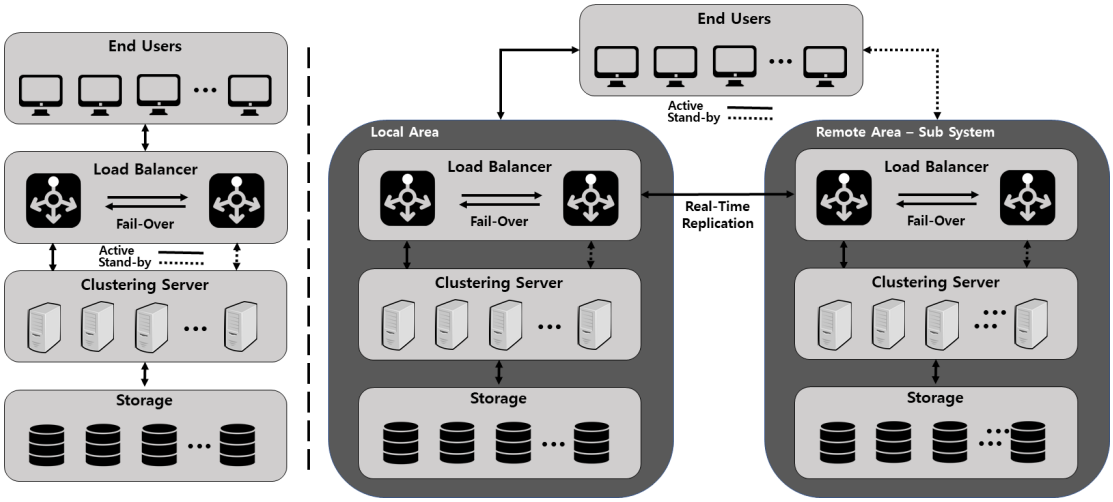


(그림 6) Erasure Coding을 통한 데이터 저장

4.2 장애 허용 시스템을 통한 국방 클라우드의 시스템 가용성 확보

장애 허용 시스템은 시스템을 구성하는 자원(프로세서, 디스크, 메모리, 파워 서플라이, 팬, 메인보드, 확장 슬롯, 백본 등)에서 장애 또는 고장이 발생해도 부분적으로 혹은 전체적으로 본래의 기능을 수행할 수 있는 시스템이다. 중앙 집중화된 자원의 장애뿐만 아니라 DDoS(Distributed Denial of Service) 공격 등의 네트워크 보안 위협이 발생해도 온라인 상태에서 사용자 모르게 자원을 교체 가능하며, 장애가 발생해도 데이터 손실 없이 시스템의 정상동작을 제공할 수 있다.

(그림 7)과 같이 다수의 서버들을 하나로 묶어 하나의 시스템처럼 동작하게 하는 클러스터링 기술과 서버에서 수행해야 할 작업들을 분산시켜주는 로드 밸런서를 통한 국방 클라우드의 장애 허용 시



(그림 7) (좌)장애 허용 시스템, (우)재난 복구 시스템을 통한 시스템 가용성 확보

스템을 제안한다[13]. 그러나 단일로 로드 밸런서를 배치할 경우 Single Point of Failure 문제가 발생할 수 있다. 따라서 여분의 로드 밸런서를 배치하여 분산 작업을 수행하는 Active 로드 밸런서의 장애 발생 시 대기 중이던 여분의 Stand-by 로드 밸런서가 Active 상태로 전환하여 작업 부하 분산 기능을 수행하도록 하는 장애 극복 기능을 제공할 수 있게 구축해야 한다.

4.3 재난 복구 시스템을 통한 국방 클라우드의 시스템 가용성 확보

재난 복구 시스템은 예기치 못한 화재, 정전, 홍수, 해킹 등과 같은 각종 자연적 또는 인위적 재해 발생 및 전쟁으로 인해 시스템이 파괴되었을 때를 대비하여 국내 타 지역 및 해외에 백업 시스템을 구축하는 것이다[14]. (그림 8)과 같이 국방 클라우드 시스템은 원격지에 서로 이중화되어야 하며, 백업 시스템은 언제든지 자동으로 메인 시스템을 대체할 준비가 되어 있어야 한다. 가장 높은 가용성을 확보하는 단계인 만큼 가장 많은 비용이 요구되며, 최고의 IT 기술들의 적용을 통해 고가용성을 확보할 수 있다.

일반적인 시스템의 경우 장애 허용 시스템을 통해서 충분한 가용성을 확보할 수 있지만 국방의 경우 전쟁 발생 시 적의 우선순위 목표가 될 수 있기 때문에 추가적으로 국내 타 지역 및 해외에 백업 시스템 구축은 필수적이다. 국방 클라우드 시스템과 같이 매우 높은 가용성을 요구하는 시스템은 원격지에 이중화되어 있는 백업 시스템에도 장애 허용 시스템을 도입하여 다운타임을 극소화시킨다.

5. 국방 클라우드 시스템의 가용성 확보 수준에 따른 클라우드 가용성 침해 대응

본 장에서는 앞서 분류한 국방 클라우드의 가용성 확보 수준을 바탕으로 클라우드 가용성 침해 사례에 유형에 대해 대응 가능 여부를 판단한다.

클라우드 가용성 침해 사례 유형으로 데이터 유실, 시스템 마비, 인프라 파괴로 분류하였으며, 본 논문에서 제시한 가용성 확보 수준에 따라 분류한 침해 사례의 대응 여부를 <표 1>로 나타내었다.

- **Case 1: 국방 클라우드 내 데이터 유실**
  - 파일 시스템의 오류 또는 관리자 및 사용자의 부주의로 인한 데이터 유실
- **Case 2: 국방 클라우드 시스템 마비**
  - 과도한 트래픽 양으로 인한 과부하, 예기치 않은 장애 등의 사고 발생으로 인한 시스템 마비
- **Case 3: 국방 클라우드 인프라 파괴**
  - 예기치 못한 화재, 정전, 홍수, 해킹 등과 같은 각종 자연적 또는 인위적 재해 발생 및 전쟁으로 인한 인프라 파괴

〈표 1〉 가용성 확보 수준에 따른 클라우드 가용성 침해 사례 대응

침해 사례 유형	가용성 확보 수준			
	Level 1	Level 2	Level 3	Level 4
Case 1		√	√	√
Case 2			√	√
Case 3				√

6. 결론 및 향후 연구방향

현재 우리나라는 국방 분야의 클라우드 도입을 위해 기반 환경 조성 및 다양한 정책, 연구를 진행하고 있다. 국방 분야의 경우 지휘체계, 전투체계, 무기체계 등 군과 관련된 다양한 정보체계들을 운영한다. 국방이라는 특성 상 전시상황을 준비하고, 분석하여 결과에 따라 행동하게 된다. 국방 시스템에 장애가 발생 하는 등 군 체계에서의 네트워크 지연, 시스템 자원 고장 등과 같은 시스템 장애가 발생하게 되면 전장의 결과와 직결되기 때문에 국방 부문의 클라우드 시스템에 가용성을 보장하는 것은 중요한 이슈라 할 수 있다. 그러나 국방 클라우드의 모든 시

스템을 대상으로 최고 수준의 가용성을 확보하는 것은 비효율적일 수 있으며, 클라우드 시스템 구축으로 얻을 수 있었던 효율성이 감소할 수 있다.

따라서 본 논문에서는 국방 클라우드 시스템의 가용성 확보 수준을 1 ~ 4 단계로 분류하였으며 각 단계 별로 도입 방안을 제안하였다. Level 1은 본 논문에서 국방 클라우드 시스템의 가용성 확보를 위해 분류한 데이터, 시스템 자원, 인프라 수준의 가용성을 확보하지 않으며, Level 2는 국방 클라우드 시스템 운영 중 필요 데이터에 대해 장애가 발생했을 경우 Erasure Coding을 통한 복구를 제안하였다. Level 3는 국방 클라우드 시스템의 자원에 부하가 걸리지 않게 로드 밸런서를 통한 작업 분산과 최소 2개의 로드 밸런서 도입을 통해 Single Point of Failure 문제를 해결하고 이를 통해 국방 클라우드의 고가용성을 확보하는 방안을 제안한다. Level 4는 가장 높은 가용성을 제공하며 예기치 못한 화재, 정전, 홍수, 해킹 등과 같은 각종 자연적 또는 인위적 재해 발생 및 전쟁이 발생하여 인프라가 파괴되어도 원격지에 이중화되어 있는 백업 시스템이 자동으로 메인 시스템을 대체한다. 본 논문에서 제안한 국방 클라우드 가용성 확보 수준을 토대로 효율적인 국방 클라우드 시스템의 가용성 확보에 활용될 것으로 기대된다.

▌참고문헌

〔1〕 박천출 외 4명, "제4차 산업혁명 속 클라우드 컴퓨팅의 현재와 국방분야 적용방안",월간 궁방과 기술, 2017.11

〔2〕 편집부, "2019년 전세계 퍼블릭 클라우드 시장 17.3% 성장 전망", ITWorld, 2018.09

〔3〕 정구돈 외 4명, "국방 클라우드 컴퓨팅 운영환경 구축방안 연구", 안보경영연구원(SMI), 2016. 10.

〔4〕 이선목, "아마존·MS, 11조원짜리 美 국방부 IT 사업 놓고 격돌", 조선뉴스, 2019.04

〔5〕 강맹수, "클라우드 컴퓨팅 시장 동향 및 향후 전망", 산업기술리서치센터, 2019. 1.

〔6〕 신민희, "클라우드 컴퓨팅 산업현황 및 발전 전망", 한국차세대컴퓨팅학회 논문지, 2011.12

〔7〕 박미유,"국가별 국방과학기술 수준조사서", 국방기술품질원, 2019.04

〔8〕 D. A. Patterson, G. A. Gibson, and R. H. Katz, "Introduction to Redundant Arrays of Inexpensive Disks (RAID)", Proceedings of ACM Special Interest Group on Management of Data, pp. 109-116, 1988

〔9〕 Hadoop, "HDFS Architecture Guide," Apache Software Foundation, https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html#Introduction

〔10〕 이준우, 나연묵, "클라우드 컴퓨팅 기반의 대용량 이동객체 분산 처리 시스템", 한국차세대컴퓨팅학회 논문지, 2012.02

〔11〕 Alexandros G Dimakis, P Brighten Godfrey, Yunnan Wu, Martin J Wainwright, and Kannan Ramchandran, "Network coding for distributed storage systems", IEEE Transactions on Information Theory, vol.56, pp.4539 - 4551, 2010

〔12〕 최정열, "클라우드 데이터 센터의 에너지 효율성 평가", 한국차세대컴퓨팅학회 논문지, 2014.08

〔13〕 허아라, 류연승, "국방과학기술 정보의 분류체계 고찰", 한국정보보호학회 정보보호학회지, pp. 25-32, 2018.12

〔14〕 박준규 외 2명, "국방 지휘통제체계의 클라우드 도입 방안", 디지털문화아카이브지, 2019.04

〔15〕 에버밸류컨설팅, "서비스 지향적 차세대 데이터센터 통합 운영모델 연구용역", 안전행정부, 2013.11

저자소개

◆ 강기완

- 2019년 순천향대학교 정보보호학과 학사
- 2018년 세종대학교 정보보호학과 석사 과정
- 관심분야: 클라우드 컴퓨팅, 임베디드 시스템, 시스템 보안 등

◆ 박준규

- 2018년 대전대학교 정보보안학과 학사
- 2018년 세종대학교 정보보호학과 석사 과정
- 관심분야: 클라우드 컴퓨팅, CTF(Capture The Flag), 시스템 보안 등

◆ 이상훈

- 1978년 한양대학교 전자공학과 학사
- 1989년 경북대학교 전자공학과 석사
- 2002년 충북대학교 정보통신공학과 박사
- 78년~ 현재 국방과학연구소
- 관심분야: C4I 체계, 보안구조 연구

◆ 박기웅

- 2005년 연세대학교 Computer Science 학사
- 2007년 KAIST Electrical Engineering 석사
- 2012년 KAIST Electrical Engineering 박사
- 2008년 Microsoft Research Asia, Wireless and Networking Grourp, Research Intern
- 2009년 Microsoft Research, Network Research Group, Graduate Research Fellow
- 2012년 국가보안기술연구소 연구원
- 2012년~2016년 대전대학교 정보보안학과 교수
- 2016년~현재 세종대학교 정보보호학과 교수
- 관심분야: 시스템 보안, 모바일-클라우드 컴퓨팅, 보안 프로토콜, 디지털 포렌식 등