

블록체인을 적용한 軍 전자적 비밀관리 개선방안*

(전장관리정보체계 중심으로)

윤 홍*, 차 영 균**, 박 종 범***

요 약

현재 군의 작전은 다양한 정보·분석·무기·작전체계 등을 이용하여 효과적으로 적을 제압하는데 목적을 두고 있다. 이러한 여러 체계들은 통합적인 구성과 해당 자료를 분석·공유하는 기능들로 이루어져야 한다. 이에 우리 군에서 운용하고 있는 전장관리정보체계는 다양한 데이터를 수집·분석하여 비밀을 생산·공유하여 효과적인 작전을 수행한다. 하지만 전장관리정보체계에서는 비밀의 생산부터 폐기·이관까지 전자적인 형태로 운용하지 못하고 있으며, 출력물 기반으로 관리함에 따라 관리의 어려움과 분실 및 유출 등의 다양한 문제가 남아있다. 따라서 본 논문에서는 모든 비밀을 전자문서형식으로 관리하고 무결성과 부인방지를 제공하기 위해 블록체인 기술을 적용한 ESDMB(Electronic Secret Document Management with Blockchain)방안을 제시한다. 특히, 이 제안방식에서는 비밀 생산부터 파기까지 조작 및 유출 등에 대한 보호 대책으로 적합할 것으로 생각된다.

Blockchain applied Military Electronic Secret Document Management Scheme (focused on C4i)

Hong Yoon*, Yeong Gyun Cha**, Jong Beom Park***

ABSTRACT

Recently, military operations have been aimed at winning using various information, analysis, weapons, and operation systems. These systems should consist of integrated composition and the function of analyzing and sharing data. Accordingly, military C4I collects and analyzes a lot of data and produces and shares secrets to perform effective operations. However, C4I cannot operate in electronic form from secret production to disposal. And as it is managed based on the output, problems such as difficulty in management and loss/leakage arise. Therefore, in this paper, we propose an ESDMB(Electronic Secret Document Management whit Blockchain) plan based on blockchain technology to manage all secrets in electronic document format and provide integrity and denial prevention. In particular, the blockchain-based proposal method will be suitable as a protection measure against manipulation and leakage, from secret production to destruction.

Key words : BlockChain, C4I Document Management , Security Management

접수일(2023년 11월 17일), 수정일(2023년 12월 11일),

게재확정일(2023년 12월 15일)

★ 본 논문은 한양여자대학교 교내연구비 지원(2023년)으로
수행하였습니다.

* 국군방첩사령부 국방보안연구소 연구원

** 국군방첩사령부 국방보안연구소장

*** 한양여자대학교 스마트 IT과 교수(교신저자)

1. 서 론

전장관리정보체계는 현대의 네트워크중심전(NCW)에서 C4ISR·PGM(지휘통제·통신·감시정찰·정밀타격 통합체계)의 통합 전투능력을 보장하기 위한 진술통신체계이다. 또한, 우리군의 작전수행을 위한 전시 및 평시 전략/전술 지휘통제·통신을 지원한다. 그리고 현재의 전장관리정보체계에서는 미래 전장 환경에 적합하도록 통합성 및 지능화를 발휘할 수 있도록 운용하기 위해 네트워크 중심의 체계를 구축하는 한편, 컴퓨터 기술과 전장감시체계(ISR)와 정밀타격체계를 지휘통제체계에 직접연결하고 실시간 종합상황을 볼 수 있도록 구성하여 운용하고 있다.

미래의 전쟁은 전장을 가시화하기 위해 다양한 형태의 정보를 제대간, 지역간을 통합하여 보다 빠르고 정확하게 데이터를 전파 공유하기 위한 속도전에 돌입하고 있다. 특히, 신뢰할 수 있는 정보의 생산, 신속한 공유를 통해 정확한 의사 결정하고 통합적인 전투력을 발휘하여 전투 시너지 낼수 있는 전장관리정보체계 구축에 최선을 다하고 있다.

이를 위해서 국방부에서는 해당 체계를 전력화하고 각 전장체계의 범주와 기능을 개발하였다. 하지만, 이러한 전장관리정보체계가 시기별, 기능별로 각각 구성되어서 앞서 언급했던 사항과 같이 종합적인 자료 공유 등에 대해서는 한계점을 나타내고 있다. 그리고, 해당 체계에서 운용하고 있는 비밀자료에 대한 관리는 기존의 출력물 기반으로 운용하고 있다. 이에 본 논문에서는 전자적인 방식을 통해 비밀자료의 관리방안을 제시하고 필요한 사항을 분석하도록 한다.[1][2][3][4]

전장관리정보체계 내 비밀자료는 로그기록을 통해서 추적관리하고 있으며 원본 비밀은 일부를 제외하고 출력물을 기반하여 관리하고 있다. 따라서 원본 기록물에 대한 이관시에는 많은 문서들이 이송되며 관리 소요도 많다. 이에 본 논문에서는 비밀의 생산부터 이관까지 전자적으로 관리할 수 있는 방안을 제시한다. 1장 서론에 이어 2장에서는 우리 군에서 운용하고 있는 전장관리정보체계에 대한 소개 및 전자적 비밀관리를 위해 생산에서부터

이관까지 필요한 구성과 무결성·부인방지·블록체인을 이용한 이력 관리 방안을 분석하고 3장에서는 블록체인 기반 전장관리정보체계 비밀관리를 위한 모델 제시한다. 그리고 마지막 4장에서는 결론을 맺는다.

2. 전장관리정보체계 內 비밀자료 관리방식 분석

2.1 전장관리정보체계 구성

전장관리정보체계로는 합참에서 운용하고 있는 합동지휘통제체계(KJCCS¹⁾)와 육군 전술지휘정보체계(ATCIS²⁾), 해군 지휘통제체계(KNCCS³⁾), 공군 지휘통제체계(AFCCS⁴⁾)가 있다. 전장관리정보(C4I)체계는 첨단 정보체계를 기반으로 지휘통제를 지원하는 정보가 상호 결합되어 모든 군사활동을 계획, 지시, 협조 및 통제할 수 있도록 융합된 정보를 모든 제대들이 상호 제공할 수 있는 통합된 정보관리체계이다.

우리 군(軍)에서 C4I체계는 특성상 군에서 요구되는 기능의 구현을 위한 소프트웨어개발 및 특정 임무를 수행하기 위한 하드웨어개발을 수반한다. C4I체계를 사람의 몸에 비유하면 눈·귀와 같은 센서역할의 감시·탐지체계, 팔·다리로 비유할 수 있는 기동·타격체계를 이어주는 역할로써 사람의 뇌에 비유할 수 있다. 다양한 통신기반이 구축되고 통신기반의 전송용량이 확대되며 전술데이터링크를 적용하여 접속되는 무기체계가 급속히 증가함에 따라, 우리 군의 NCW가 구축되고 있으며, 그 중심인 C4I체계의 지휘 통제 능력향상은 더욱 중요해지고 있다. 우리 군(軍)에서 구축하는 C4I체계는 연합지휘통제체계(AKJCCS, MIMS-C), 합동지휘통제체계(KJCCS, MIMS), 육·해·공군지휘통제체계(ATCIS, KNCCS, AFCCS)로 구성되어 제대별, 군별, 기능별로 별도의 C4I체계를 구축하여 운용하며, 고도의 상호운용성을 갖추고 서로 연동되어 있다. 과거에는

1) KJCCS : Korean Joint Command & Control System
2) ATCIS : Army Tactical Command Information System
3) KNCCS : Korea Naval Command Control System
4) AFCCS : Air Force Command and Control Systems

정보처리능력, 네트워크 및 통신능력, 체계 운용간 기동성 여부 등을 고려하여 필요한 체계를 분리하여 구축하는 개념으로 소요 결정되었으며, 이에 따라 전략·전술·전투부대, 육·해·공군, 지휘통제·화력·정보기능에 따라 C4I체계를 구축하였다. IT기술의 발전에 따라 앞으로는 통합된 C4I체계를 구축하는 요구가 높아지고 있으며, 4차 산업혁명 기반의 체계 융합을 통해 운용자가 하나의 단말기로 필요한 기능을 활용하고 있다.[2][3][4][5]



그림 1 KJCCS 체계 운용 및 구성

2.1.1 한국군 합동지휘통제체계(KJCCS)

그림 15)에서와 같이 KJCCS체계는 합참을 중심으로 각 군의 작전사급 부대와 수방사, 특전사, 미사일 사령부 등에 설치하고 있으며, 전·평시 합동작전 수행을 위한 지휘·통제 수단으로 운용하고 있다. 또한, 해당 체계에서는 타 체계 연동 및 체계 내 웹을 기반한 통합 관리를 위해 통합 데이터 서버와 타 체계와의 연동을 수행하는 연동 서버를 구축하였다. 이 연동망을 이용해 군사정보통합처리체계(Military Intelligence Management System :MIMS), 각 군 전술C4I 체계와 연동하여 필요한 정보를 수신할 수 있다.[2]

5) <http://www.seminartoday.net/news/articleView.html?idxno=3534>

2.1.2 육군 지휘통제체계(ATCIS)

전장에서 아군과 적국의 상황을 가시화하고, 실시간 탐지·타격 전력을 통합하며, 지휘 결함에 필요한 정보를 실시간으로 제공할 목적으로 육군 전술지휘 정보체계(ATCIS)를 구축하여 운용하고 있다. 현재 2차 체계 개선 사업 중에 있다. ATCIS 체계의 주요 기능으로는 정보·작전·화력·전투근무지원 및 공통 분야 구성되어 있다. <그림 26>에서와 같이 지상작전을 위해 차량에 탑재되어 전장상황에 따라 수시로 이동하는 지휘소와 같이 이동하면서 시스템을 운영하고 필요한 전장정보를 지휘관 및 참모에게 제공한다. 이러한 전장 상황에 대한 정보를 이용하여 지휘관은 신속한 작전 결심을 내려 전장의 주도권을 장악하기 위해 올바른 판단과 결심을 하게 된다[4]. 이를 위해서 이동이 가능한 차량등을 이용하여 ATCIS 지휘소를 신속하게 이동하여 업무 연속성을 지원한다.[2][4]

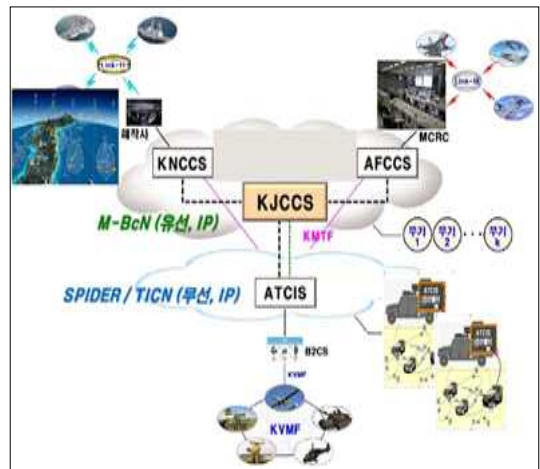


그림 2 각군 C4I 체계 운용 및 구성

2.1.3 공군 지휘통제체계(AFCCS)

공군지휘통제체계(Air Force Command& Control System : AFCCS)는 공작사를 중심으로 전술 부대의 지휘관이 전·평시 작전 임무 수행을 위한

6) 아주대학교 장위국방연구소, 합동정보통신 직 무역량 모델 연구

계획, 지시, 조정 및 통제하는 수단으로 운용하고 있으며, 공작사, 비행단, 전술항공통제 부대에 구축되어 있다. 전술 제대의 작전 임무 지원을 위해 전 항공권역에 대한 감시·식별 및 방공작전을 지휘·통제하는 중앙방공통제소(MCRC)를 기반으로 전장 기능(정보, 작전 등)과 통합하여 작전 임무 수행이 가능한 지휘·통제수단으로 운용하고 있으며 체계 구성은 <그림 2>와 같다.[1][2][5]

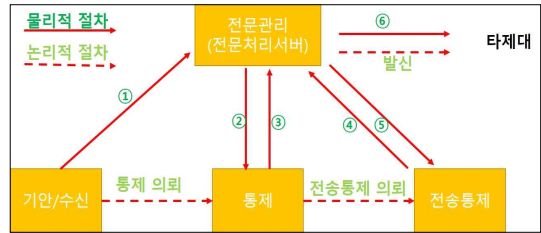


그림 3 각군 C4I 체계 운용 및 구성

2.2 전장관리정보체계 내 비밀자료 관리방식

앞서 언급했던 KJCCS 체계를 중심으로 <그림 4>에서와 같이 연동망을 중심으로 각군 C4I체계와 자료를 소통할 수 있는 방식을 취하고 있다. 기존에는 전문송수신체계를 이용하여 합참과 각 군이 전자 비밀문서를 송수신하고 있으나, 자료의 활용도 측면에서 호환성이 떨어진다. 이는 문서를 전달해주는 역할만을 수행하는 체계로 운용하고 있는 한편, 자료의 활용도를 높이기 위해서 KJCCS 체계 내 웹 페이지 통해 각 군 전장관리정보체계 단말에서도 자료실의 열람이 가능하도록 연동망을 구성하여 운영하고 있다.[2]

2.2.2 전장관리정보체계 內 비밀자료 공유 (발송·열람) 방식

KJCCS 체계를 중심으로 <그림 4>에서와 같이 각 C4I체계 전용단말에서 KJCCS 연동 웹 페이지로 접속하여 비밀자료를 열람할 수 있도록 자료실 기반의 공유 개념을 도입하여 설치 운용하고 있다. 이러한 자료 열람은 앞서서 설명했던 전문송수신체계에서와 같이 수신자가 자료를 수신할 수 있다는 개념에서 기존의 전문송수신체계와 마찬가지로 자료를 전달할 수 있는 의미로 볼 수 있다. 물론 모든 사용자에게 접근을 허용하는 것이 아니고 업무상 필요한 인원으로 한정하여 관리하고 있다.[2]

2.2.1 전문송수신체계 구조 및 운용방식

전문처리는 전문을 타 부대 및 부서에 전송하기 위해 전문기안·결재·통제·발신·착신 등의 주요 기능과 전문원본 및 사본의 관리 그리고, 부가적인 기능으로 구성되어 있다.

전문처리체계는 <그림 3>에서와 같이 전문관리, 기안 /수신, 통제, 전송통제 체계로 구성된다. 각 부속체계는 전문관리체계를 통해 전문처리를 위한 제반 기능을 수행한다. 전문처리체계는 전문관리체계와 기안/수신체계로 구성된다. 기안/수신 영역에서는 전문을 생성하고 비밀문서에 대한 결재와 발송을 수신하기 위해 결재를 위해서 비밀지정권자를 지정하고 결재 절차를 수립한다. 이 절차는 통제체계 내에서 비밀지정권자에 의해 비밀이 생성된다. 그리고 전송통제 체계를 사용하여 타 부대로 전송 한다.



그림 4 비밀자료 게시·공유

2.2. 전장관리정보체계 통합 및 효과적인 모델

비밀의 생성부터 이관까지 전장관리정보체계 내에서는 상이한 방식을 사용하고 있으며 이로 인하

여 이력 관리 문서를 사용하고 있다. KJCCS에서는 원본비밀을 생산 운용하고 이관까지 체계 내에서 관리하고 있다. 하지만, 체계 내에서는 원본 파일임을 증빙할 방법과 이관시 부인방지에 대한 대책은 미흡한 실정이다. 한편, 각군 C4I에서는 원본을 문서로 생성한 후 사본을 체계 내 탑재 운용하고 이관시 문서형식의 원본을 이관하고 있다. 따라서, 문서형식의 원본 비밀에 대한 열람·대출을 수행할 때 모든 기록을 관리해야 한다.

앞서 언급한 사항을 다음의 3가지 형태로 정리할 수 있다. 첫 번째, 비밀의 생산을 전장관리정보체계 내에서 수행해야 한다. 하지만 현재 비밀의 원본을 생산하는 체계는 KJCCS에서 생산하고 있으나, 원본에 대한 진본성을 제공하는 기능이 제한되고 있다. 두 번째 비밀에 대한 이력 관리를 수행해야 한다. 현 체계에서는 로그 기록을 기반으로 관리하고 있으나, 일부 제한되는 기능 또는 로그 자체를 변경하는 경우에는 정확하게 알 수 없다. 세 번째는 첫 번째 비밀의 생산 과정에서 원본임을 증빙하기 위한 무결성·부인방지 기능을 확인하는 과정이 필요하다. 이 세 가지 취약요소를 해소하는 방안을 기반으로 비밀관리 모델을 제시하도록 한다. 또한, 전문송수신체계 대신 비밀자료 공유체계를 기본으로 구성한다.

3. 블록체인 기반 전장관리정보체계 비밀관리 모델 제시

3.1 블록체인 기반 전장관리정보체계 자료 유통 모델

앞서 언급했던 KJCCS 체계를 중심으로 기능을 확인해 보면 <그림 5>에서와 같이 연동망을 중심으로 각군 C4I체계와 자료를 소통할 수 있는 방식을 취하고 있다. 기존에는 전문송수신체계를 이용하여 합참과 각군이 전자 비밀문서를 송수신하고 있으나, 전송되는 자료는 문서 출력형식으로 전달받을 수 있기 때문에 문서를 전달해주는 역할만을 수행하는 체계로 운용하고 있다.

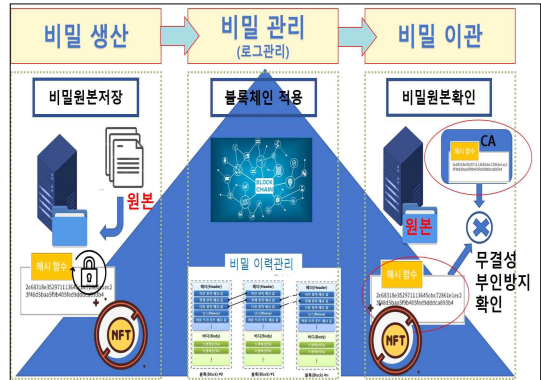


그림 5 전자적 비밀관리 제안모델

3.2 무결성·부인방지 기술을 적용한 비밀 자료 원본 생산

전자적 비밀관리를 위해서는 필요한 무결성·부인방지 기능이 필요하며 <그림 5>에서와 같이 비밀을 저장할 때 사용한다. 그림에서는 이관 관련 사항에 있어서 원본 비밀만 표시를 두었으며 원본임을 나타내며 기존의 로그를 대신할 수 있는 기능을 제공하는 기술로 블록체인을 적용하였다. 따라서 비밀의 생산과 이관을 위해서 사용되는 해시함수와 비밀자료에 대한 이력 관리와 실제 파일의 변경이 생기는 부분까지 포함하도록 해야한다.

비밀의 자료를 전자문서형식으로 해시값 기반이 토큰을 주입하여 현재 암호화 작업을 수행할 때 해당 정보를 포함하도록 한다. 이러한 해시값을 기준으로 이관시 변동 여부를 확인한다.[6][7][8]

3.3 파일 변경 및 이력 관리 수행을 위한 블록체인 적용모델

전자문서형식의 비밀을 전장관리정보체계 내에서 관리하기 위해서는 MSP(Membership Service Provider) 적용할 수 있는 구조를 사용하도록 한다. CA의 정보들을 모아서 MSP를 구성하는 하이퍼레저에서는 MSP를 통해서 채널의 관리 권한이나 접근 권한을 관리할 수 있기 때문에 <그림 6>과 같이 구성하도록 한다. 전자문서 하나에 해당 블록체인을 작성하여 관리하도록 한다.

사용자가 비밀을 등록하거나 수정문을 대체한 경우 수정사항을 각 단말은 MSP 또는 local MSP에 알려 그림과 같이 관리정보의 해시값을 업데이트하고 파일의 등록 또는 변경사항을 FM(File Modification)이벤트를 활성화하여 블록을 생성하도록 한다. 이때 부가적인 검증과정을 수행한다.[9][12][13]

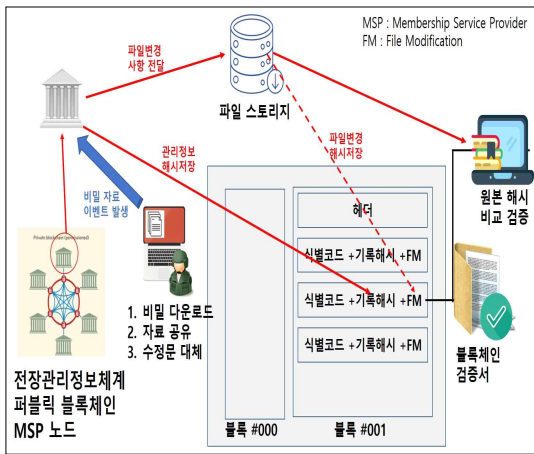


그림 6 전자적 비밀관리 적용을 위한 블록체인 시스템 개발

앞서 알아본 바와 같이 무결성은 진본인증을 통해서 이루어진다. 만일, 기록관리의 신뢰성을 확보하기 위해서 식별자와 기록을 구성하는 본문 그리고 첨부파일 등의 컴포넌트, 메타데이터를 블록의 페이로드에 탑재하는 경우에는 하나의 블록 용량이 너무 커진다. 지속적으로 다양한 형태의 매체에 기록되는 데이터는 많아지고 이 모든 데이터를 블록체인 네트워크로 공유하는 것은 불가능하다. 따라서 이러한 모델의 경우에는 제한적으로 대상 기록을 수행해야 하며, 시스템 내 제한적으로만 이용해야 한다. 따라서 전장관리정보체계의 블록체인 모델로 <그림 6>과 같이 기록 정보 블록 생성 모델을 제안한다.

각 노드의 블록은 블록헤더와 기록관리 데이터가 포함되는 페이로드로 구성되며, 블록의 헤더에는 앞 블록의 해시와 페이로드 해시를 포함한다. 블록에는 기록의 식별정보와 함께 기록의 생산 시점부터 기록관리 과정의 단계별 기록이 해시값으로 생성

되어 저장되며, 전자문서에 대한 변경 이벤트가 발생하여 해시를 생성하게 되면, 해시 생성 시점과 컴포넌트의 식별정보가 해시와 함께 탑재되고, 기록관리 이벤트의 내용과 해당 파일의 변경 저장을 수행한다.

전장관리정보체계 내 MSP에 공유된 기록관리 분산원장은 기록의 진본인증 요청이 발생하면 블록 체인에 탑재된 해시와 인증 대상 기록의 해시를 비교하여 무결성·부인방지를 제공한다. 이 정보는 등록에 저장된 해당 컴포넌트의 최종 해시를 검증하여 블록체인 검증서로 활용한다.

앞서 언급한 바와 같이 블록체인의 진본(무결성·부인방지)성을 제공하는 방식으로 블록체인 검증서를 사용하는 한편 이관용을 사용했던 해시 정보의 경우에는 원본 비밀의 파일에 대해서 저장 정보를 <그림 5>에서와 같이 확인할 수 있다.

따라서, 제안한 ESDMB(Electronic Secret Document Management with Blockchain)방안을 이용하여 구축하고 운용한다면, 비밀관리에 대해서 불필요한 행정 소요 제거, 비밀관리에 대한 부담감 감소, 효과적인 유출 등에 대한 문제점 해소 등의 장점이 있다. 무엇보다도 신속한 자료 공유 및 관리가 이루어질 것으로 판단된다.[10][11][12][13]

4. 결론

전장관리정보체계에서의 정보에 해당하는 비밀 자료는 생산부터 이관까지 전자적인 관리를 위한 방식을 제시하였다. 이를 통해 전장관리정보 체계에서 문서로 관리되었던 원본비밀, 이력관리 대장 등을 제거하여 비밀의 분실 유출·오인파기 등의 문제를 차단할 수 있어 보안성을 강화하고 불필요한 행정 소요를 감소시킬 수 있는 장점을 기대할 수 있다.

비밀생산부터 이관까지 전자적 비밀관리를 위한 3단계 유통구조에서는 해시함수를 이용한 비밀 원본 생산, 파일 이력 관리 및 추적관리, 이관 자료에 대한 부인방지 기능을 제공한다.

이러한 체계적인 구조를 완성하는 것보다 중요한 것은 사용자의 인식변화라고 할 수 있다. 출력물

중심의 보고 결재를 없애고 체계 내에서 지휘관의 결재 등을 수행하는 문화를 만들고 비밀은 안전한 시스템 내에서 관리하는 것이 올바른 생각으로 자리매김해야 할 것이다.

참고문헌

- [1] 한광택, 이수연, 박창섭. “PKI 인증기반 전장 관리체계 웹 연동에 관한 연구”, 융합보안 논문지, 14권, 6호, pp.147-155, 2014.
- [2] 김영성, 이윤호, 이수진. “국방진산통신망을 위한 국방인증체계(MPKI) 개선 방안에 관한 연구”, 한국국방경영분석학회, 36권, 1호, pp.123-140, 2010.
- [3] 박호, “미래 합동전장 지휘통제를 위한 한국군 C4I 발전방안”, 한국방위산업진흥회, 국방과 기술, pp.34-43, 2020.11.
- [4] 김의순, “한국군 C4I체계 진단과 발전방향”, 한국국방연구원 국방획득연구센터, 주간 국방논단, 제1416호, 2012.6.
- [5] 김경희, 강석중, “NCW환경에서 지휘통제체계(C4I) 상호운용성 시험평가체계 개선방안 연구”, 한국군사과학기술학회, 제15권 6호, pp.786-801, 2012.1.
- [6] 김태환, 조창희, 최형광, “오픈소스 블록체인을 활용한 전자문서 위·변조 방지 시스템 설계 및 구현 연구 -하이퍼레저를 중심으로”, 한국IT정책경영학회 논문지, 제13권(1), pp.2,271-2,279, 2021.1.
- [7] 김태환, “블록체인 기반의 전자문서 위·변조 방지 시스템 설계 및 구현 : 하이퍼레저를 중심으로”, 숭실대학교 대학원, 2020.
- [8] 지정은, “블록체인 기반 신뢰적 디지털기록 문서 관리 기법”, 숭실대학교 대학원, 2020.
- [9] 서예령, 박성환, 최동준, “블록체인 보안 이슈와 보안에 견고한 최신 블록체인 기술”, 한국정보과학회, 정보과학회지, 제 38권(7), pp.14-18, 2020.7.
- [10] 원중운, 김도훈, 김희상, “최신 블록체인 동향과 응용 기술” 한국정보기술학회지, 제 19권(1), pp.1-6, 2021.12.
- [11] 김성환, 김영곤, “블록체인 기반 시스템 인증 방법에 대한 연구” 한국인터넷방송통신학회 논문지, 제 20권(1), pp.211-218, 2020.1.
- [12] 김성진, 옥현, 김태학, “블록체인 기반의

BIM 라이브러리 공유를 위한 개념적 설계.” 한국통신학회 학술대회논문집, p.831, 2021.2.

- [13] 서중원, 고덕윤, 박수용; “분산 네트워크 환경에서 BIM 파일들을 저장하기 위한 블록체인 시스템 설계 및 구현. ”, 한국컴퓨터정보학회논문지, 제 26권 12호, pp. 159-168, 2021.12.

【저자소개】



윤 홍 (Hong Yoon)
2001년 2월 한국항공대학교 학사
2003년 2월 한국항공대학교 석사
2007년 8월 한국항공대학교 박사
2008년 12월 PR 프로모션 연구소장
2009년 1월 ~ 현재 국군방첩사령부 제직
email : yhlove00@naver.com



차영균 (Young-kyun Cha)
1989년 2월: 고려대학교 학사
1992년 6월: 고려대학교 석사
2012년 8월: 고려대학교 박사
2023년 2월: 고려대 정보보호대학원 교수
現. 국군방첩사령부 국방보안연구 소장
email: ykCha@dcc.mil.kr



박종범 (Jong Beom Park)
1992년 2월 광운대학교 학사
1994년 8월 광운대학교 석사
2001년 8월 광운대학교 박사
현한양여자대학교 스마트 IT과 교수
email : jbpark@hywom.ac.kr