ISSN 2799-8924
컨설팅융합연구 제 2권 제 1호 pp. 09-14, 2022 https://doi.org/10.55479/JCCR.2022.2.1.009

블록체인 기술의 DID 기반 백신 접종 검증 시스템에 대한 연구

문형진[1*]
[1]성결대학교 정보통신공학과 조교수

Research of DID-based Vaccine Verification System in the Blockchain Technology

Hyung-Jin Mun[1*]
[1]Professor, Dept. of Information & Communication Engineering, Sungkyul University

요 약 최근, 코로나 19로 인해 전염병에 대응하기 위해 전 국민의 백신 접종을 독려하고, 이로 인해 집단 면역을 구축하고자 노력하고 있다. 개인이 어려서부터 다양한 전염병에 대한 백신 예방 접종을 하고 있지만 백신 접종내역 및 접종일자를 기억하기 쉽지 않다. 특히, 여러 차례 접종하거나 주기적으로 접종해야 하는 경우, 효과적인 방역을 위한 경우 백신 접종 사실을 확인할 필요가 있다. 국내에서는 코로나 19의 백신접종 사실을 확인한 후에 출입을 허용하는 방역에서는 특히, 더 필요하다. 해외 여행시 백신접종 사실이 더욱 필요한 상태이지만 증명서의 위변조 가능성이 있어 이를 대응할 수 있는 연구가 필요하다. 블록체인 기술은 생성된 정보를 체인으로 연결되어 정보의 무결성을 보장하고, 신뢰기관에서 접종사실을 등록함으로써 정보의 신뢰성을 보장한다. 최근 DID 기술을 활용하여 개인의 신원을 블록체인에 분산 저장하고 검증한다. 백신접종 내역 정보를 저장하고, 정보의 제어권을 개인에게 부여할 수 있는 DID 기반 위에서 신뢰성있게 검증할 수 있는 기법을 설계하였다.

키워드 : 블록체인, 분산 ID, 백신 접종 이력, 코로나 19, 정보통신

Abstract Recently, in order to respond to the COVID-19 pandemic, efforts are being made to build collective immunity by encouraging the entire nation to get vaccinated. Individuals have been vaccinated against various infectious diseases since childhood, but it is difficult to recall the history and the date of vaccination. In particular, it is necessary to confirm the authenticity of vaccination in case of multiple vaccinations or periodic vaccinations, or for effective prevention. In Korea, quarantine is mandatory for all inbound travelers entering the country. After confirming the vaccination documents against COVID-19, individuals are then allowed to enter the country. The authenticity of vaccination documents is imperative when traveling abroad, but there is a possibility of fraud or forgery of the certificate, so research is needed to cope with it. Blockchain technology guarantees the integrity of information by connecting the generated information with a chain and guarantees the reliability of information by registering the records of an individual's vaccination certificate at a trusted institution. Recently, by using DID technology, individual identities are distributed and verified on the blockchain. We designed a technique that can be reliably verified on the basis of DID that can store vaccination history information and grant control of data to individuals.

Key Words : Blockchain, DID, Vaccine history, COVID-19, ICT

*Corresponding Author : Hyung-Jin Mun (mun.it@daum.net)
Received February 14, 2022 Revised March 18, 2022
Accepted March 24, 2022 Published March 28, 2022

1. 서론

WHO는 코로나 19로 인해 2020년 3월 11일에 세계적 대유행 팬더믹(pandemic)을 선언하였고, 코로나 19 확산을 막기 위해 사회적 거리두기 및 백신 접종을 독려하고 있다. 개인이 코로나 백신을 접종한 내역을 상점을 비롯한 기관에 출입 시 알림으로써 다양한 방역의 효과를 높일 수 있다. 자신의 백신 접종 내역을 확인하고, 기억하는 것이 어려움이 있기 때문에 내역 확인이 필요한 경우 다양한 증명서 등을 소지할 필요가 있다.

ICT 기술의 발달로 인해 다양한 서비스가 가능해짐에 따라 온라인상에서 신원확인은 필수적이다. 신분증으로 통해 인증하시는 시대에서 코로나 19로 인해 비대면으로 자신의 신원을 입증해야 시대로 전환이 되었다. COVID-19와 ICT 발달로 인해 다양한 분야에서 신원 인증 기술이 요구되고, 발전하고 있다[1]

최근 블록체인 기술을 통해 무결성이 보장됨에 따라 다양한 부각적인 서비스가 가능하다. 개인은 자신의 정보에 대한 제어권을 가능케 하는 신원인증의 필요성이 제기된다. 블록체인 기술을 활용하여 자기주권 신원인증이 가능하고, 또한 개인정보를 최소한으로 공개할 수 있는 연구가 진행되고 있다[2]. 블록체인 기술을 활용한 DID을 활용하여 원하는 곳에 원하는 정보만을 제공할 수 있는 기법을 제안하고자 한다. 정보를 저장된 블록에 체인을 연결하는 방식의 블록체인은 분산된 노드에 저장되어 분산된 신뢰구조를 제공한다. 블록에 짧은 시간에 따라 체인을 연결하는 방식으로 생성되어 위변조가 불가능한 시스템이 가능하여 무결성을 보장한다. 다양한 분야에서 블록체인 기술이 적용되고 있다. 블록체인의 블록 내에 저장된 트랜잭션을 암호화하여 저장하고 있다.

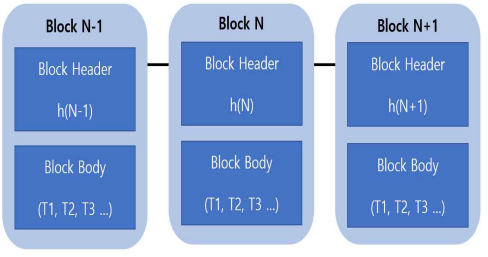

Fig. 1. Structure of blockchain

Fig. 1에서 보듯이 정보가 저장된 블록을 체인으로 연결되어 분산된 노드에 저장하여 짧은 시간마다 블록을 생성하기 때문에 공격자가 블록의 내용을 수정하고, 모든 노드에 배포할 수 있는 시간과 자원을 확보하기 어렵기 때문에 블록체인 기술의 안정성이 보장된다.

2. 관련연구

2.1 블록체인

블록체인 기술은 데이터를 하나의 서버에 저장관리하는 것이 아니라 분산 관리하는 신뢰구조를 가지며, 분산되어 있어 위변조시 바로 확인이 가능한 무결성을 제공하는 시스템의 구현이 가능하다. 블록체인 기술은 비트코인에서 암호화폐로 활용되다가 이더리움을 통해 스마트 컨트랙트(smart contract)가 가능해졌고, 무결성이라는 강력한 보안서비스가 지원되면서 차세대 인터넷 기술로 활용되고 있다[3, 4].

블록체인의 블록에 많은 트랜잭션이 담아 암호화한 후에 블록의 해시값으로 연결하여 분산 저장한다. 짧은 시간마다 블록을 생성하는 방식으로 공격자가 공격에 필요한 시간과 자원을 확보되지 않아 안전성을 보장 받는다. 일정 시간마다 블록이 생성되어 연결되어 무결성이 보장되고, 수 많은 노드에 블록이 분산 저장되어 위변조의 위험을 원천적으로 차단할 수 있다.

2.2 Decentralized IDentifiers

블록체인 기반 DID(Decentralized IDentifiers) 기술은 기존의 중앙화된 인증방식에서 탈중앙화 방식으로 신원을 증명하는 기술이다. 실생활에서 자신의 신원을 확인하기 위해 지갑에서 신분증을 보여줌으로 자신을 증명하는 것처럼 개인 블록체인 월렛(wallet)에 자신의 개인정보를 담고 신원을 확인이 필요할 때 DID 기술을 활용하여 자신을 증명한다. 서비스 관점에서 사용자가 서비스 제공 기관에서 요구된 필요한 정보만 선택적으로 제공할 수 있다. 예를 들어 술이나 담배 구입할 경우 성인여부를 확인하는 방법으로 DID를 활용하여 만19세 이상인지 여부만 확인하고, 다른 정보를 제공하지 않는 방식으로 활용된다.

인터넷이 시작되는 1990년부터 중앙 집중 형태의 온라인 신원 인증은 정보시스템의 사용자 식별 및 인

증의 주요 기법으로 사용되고 있다. 하지만 이 기법은 SPoF 과 성능 병목 현상으로 정보시스템의 사용자 인증에 한계가 노출되어 디지털 신원 식별 분야에서는 적합하지 않게 되어 다양한 인증 기법과 방법에 대한 연구가 진행되고 있다[5].

2.3 백신 여권

COVID-19는 2019년 12월에 중국 우한에서 처음으로 발견되어 급속하게 전세계로 확산되었다. 빠른 전파로 인해 2020년 3월에 전세계가 팬더믹에 빠졌다. 대부분의 국가에서 코로나 전염 확산을 차단하기 위해 국경을 차단하고, 마스크 착용과 건물 입장시 체온 체크 등을 실시하고 있다. 글로벌한 전세계 제약회사들의 코로나 백신 연구에 집중하여 2020년 부터 백신이 개발되어 3상이 끝나고 미국을 비롯한 국가에서부터 백신 접종을 시작하고 있다. 백신 접종을 통해 일부 전염 확산을 차단하는 나라들이 존재하면서 백신 접종을 통해 통제된 시민들에게 자유를 제공하고자 유럽에서 백신 여권에 대한 논의가 나오고 있다. Table 1는 OECD가 제시한 COVID-19 대응 정책으로 7가지를 제시하고 있다[6].

Table 1. OECD's COVID-19 Response Policy

▪ Restoring traveller confidence
▪ Supporting tourism businesses to adapt and survive
▪ Promoting domestic tourism and supporting safe return of international tourism
▪ Providing clear information to travellers and businesses, and limiting uncertainty (to the extent possible)
▪ Evolving response measures to maintain capacity in the sector and address gaps in supports
▪ Strengthening co-operation within and between countries
▪ Building more resilient, sustainable tourism

(Source : OECD(2020.12). Rebuilding tourism for the future: COVID-19 policy responses and recovery)

2021년 11월부터 국내는 위드 코로나를 실시하고 있다. "함께"라는 의미의 with와 코로나 19의 합성어 코로나 19와 일상을 함께 하는 것을 의미한다. 코로나 19의 완전한 종식이 아니라 코로나 19와의 공존을 의미한다. 국내에서는 위드 코로나를 실시하여 사적모임 인원을 늘리고, 영업 제한을 줄이거나 영업시간을 늘려주는 방식으로 운영하고 있다. 위드 코로나의 전제 조건으로 백신 접종률이 70%가 넘고, 중증환자 및 사망자가 축소되는 것이다.

전 세계적으로 COVID-19 백신 접종률이 높아지고 집단 면역이 생기면서 자유롭게 여행하거나 건물 출입 등 방역으로 인해 제한된 자유를 주자는 의미로 COVID-19 백신 여권(백신 접종 증명서) 도입 국가가 늘어나고 있다. 백신접종률 세계 1위인 이스라엘은 그린 패스(green passport)를 시행하고 있다[7]. 코로나 19 백신 접종이 완료되었다는 증명서를 정부가 발급하여 출입 중으로 활용되고 있다. 현재 국내에서는 질병관리청 전자예방접종증명 모바일 앱인 COOV을 도입하고 있다. COOV 기반이 되는 글로벌 백신 인증 솔루션(PASS INFRA)는 전 세계 국가 및 단체에 무료로 제공하고 있어 글로벌 호환성이 제공되고 있다. COOV 앱을 통해 백신 접종 여부를 확인할 수 있게 건물 출입시 접종여부를 확인하고 출입을 허용하고 있다.

유럽을 중심으로 백신 여권에 대한 논의와 도입 등 관련 계획이 활발하게 진행되고 있다[8].

독일은 면역 앱(Immunity App)을 출시하여 자신이 예방접종을 받았음을 쉽게 증명하고, 다른 지역이나 국가 여행을 목적으로 한다.

프랑스는 백신 여권 관련하여 French App를 시범사업으로 추진하여 코로나 바이러스 검사 결과와 백신 접종 기록을 증명하고 있다. Tous AntiCovid 접촉 추적 앱을 구축하여 코로나 19 백신 여권의 역할을 수행하고, EU의 디지털 녹색 증명서인 DGC(Digital Green Certificate)와의 연계가 가능할 것으로 전망하고 있다.

EU의 디지털 녹색 증명서는 2021년 3월 17일 EU 회원국가에 적용되어 자유롭게 이동을 할 수 있는 백신 여권을 만들자는 법을 제출하였고 5월 20일에 승인되었다. DGC는 디지털 또는 용지 형식으로 QR코드가 내장되며, 무상으로 제공되고, 자국어와 영어로 표현하여 모든 EU 국가에서 유효하다.

호주는 코로나 19 바이러스 확산을 차단하기 위해

봉쇄를 감행하고, 국민의 80%가 백신을 접종을 마치는 시점에서 자유롭게 해외여행을 재가하고자 하였다[9].

3. 블록체인 기반의 백신 접종 검증시스템

3.1 DID 기반의 백신 여권

개인이 자신의 개인정보에 대한 주권을 가지고, 자신의 신원인증을 가능하게 하는 블록체인 기반의 자기주권신원인증 기술로 개인정보를 최소한으로 공개할 수 있는 연구가 진행되고 있다[2]. 개인정보의 DID 기술은 기존의 중앙화된 인증방식에서 탈중앙화 방식으로 신원을 증명하는 기술이다. DID 기술은 실생활에서 신원확인을 위해 지갑에 신분증을 넣어 다니다가 필요할 때 꺼내서 보여주는 방식처럼, 개인의 블록체인 지갑(wallet)에 자신의 개인정보를 담고 필요할 때마다 자신을 증명하는 방식이다. DID 기술을 이용한 서비스 측면에서 보면 사용자가 서비스 제공하는 기업이나 기관에서 요구되는 필요한 정보만 선택적으로 제공할 수 있다. 편의점에서 술이나 담배 구입시 성인인증을 요구할 때 DID를 활용하여 만19세 이상인지 여부만 확인시켜주고, 얼굴이나 생년월일, 주소 등을 보여주지 않는 방식으로 활용될 수 있다. 즉, DID는 블록체인 기술을 활용하여 사용자 신원을 증명하기 때문에 서비스를 제공하는 기업이나 기관에 개인의 모든 정보를 제공할 필요가 없다.

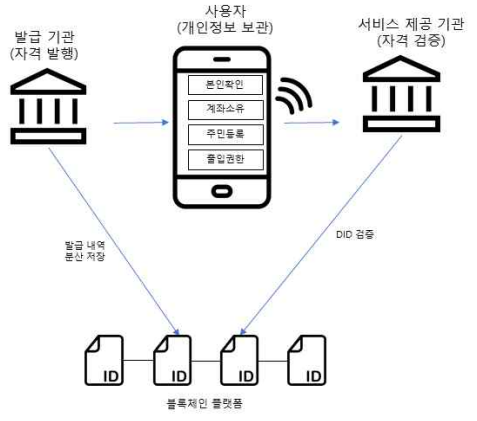

Fig. 2. Structure of DID

Fig. 2에서 보듯이 DID 구조로서 발급기관과 사용자, 서비스 제공기관으로 구성되어 있고, 정보는 블록체인 상에 저장되어 있다. 백신 접종 내역이나 주민등록등본과 같은 정부기관에서 발급하는 기관에서 DID를 발급하고, 관련 정보를 개인이 자신의 정보를 스마트폰과 같은 단말기에서 저장하고, 필요한 기관에서 정보를 요청시 DID를 제출하고, 제출받은 DID을 검증하는 과정을 보여주고 있다.

4. COVID-19 예방접종 증명 기법

4.1 증명 기법

질병관리청에서 백신을 접종한 후 증명서를 발급하는 방식으로 DID 기반의 예방접종증명을 하고 있다. 병원에서 백신을 접종하면 병원에서 질병관리청의 서버에 접종자의 정보 및 접종 일자, 백신명 등을 등록하여 블록체인에 저장한다. 블록체인에 저장된 정보를 DID 기술을 활용하여 조회할 수 있도록 COOV라는 앱을 통해 정보를 제공하고 있다. 해외에서도 사용할 수 있도록 백신접종자의 정보를 제공한다. Fig. 3는 DID 활용한 사례로 COOV앱에서 백신접종 관련 정보를 보여주고 있다. COOV앱에는 백신접종 이력 뿐만 아니라 성인인증 및 여권번호 등이 기록되어 있다.

Fig. 3. Examples of using DID

4.2 백신 접종 이력 기법

간염바이러스 면역이나 매년 접종하는 독감 예방접종을 받고 있다. 평생 자신이 접종한 백신의 내역을 기억하기 쉽지 않아 병원 진료 내역이나 개인 수첩에 기록하는 방식으로 확인하고 있다. 백신 부작용이나 오남용 등 다양한 문제를 해결하기 위해 무결성이 보

장된 블록체인 기반에서 다양한 바이러스 등에 대한 백신 접종내역을 확인하는 기법을 제안한다.

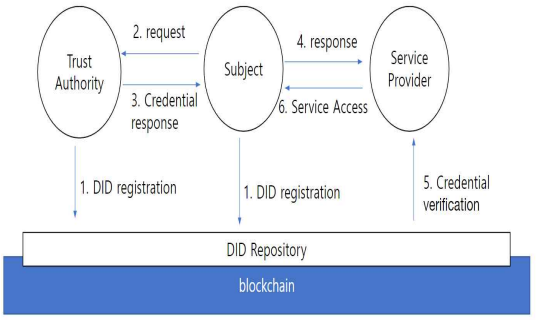

Fig. 4. Structure of DID for vaccination history

Fig. 4는 백신접종 이력을 위한 DID의 전체 구조이다. 신뢰기관과 개인인 정보주체는 블록체인에 DID를 등록하고, 개인이 신뢰기관으로부터 Credential를 요청하고, 그 정보를 서비스 제공자에게 전달한다. 서비스 제공자는 Credential를 검증하는 방식이다. 제안 기법은 크게 4개의 구성 요소를 가지고 있다. 일반적으로 개인은 다양한 병원에서 백신을 접종하고 있다. Fig. 5에서 A, B, C는 백신을 접종하는 병원이다. 기존 방식에서는 각 병원에 기록하고, 개인에게는 백신접종 수첩 등으로 기록하여 개인이 자신의 접종내역을 확인하기 어려워지만 제안 기법에서는 모든 접종 기록을 정부기관을 통해 블록체인에 기록한다.

- 정부기관 : 백신 접종 대상자 여부 확인 후 / 병원 : 백신 접종을 실시하고, 접종 병원, 일시, 백신 종류, 이상 반응 등을 임시 DB에 기록하고, 면역이 생기고 검증이 완료되면 정부기관에서 검증 후 백신 접종 정보를 서명하여 블록체인에 최종적으로 등록한다.
- Agent : 사용자와 검증자 사이에서 정보를 제고한다. 블록체인에 등록된 백신 접종관련 정보를 가지고 와서 서비스별 정보목록 등 제공에 관련된 정책으로 수립한다.
- User : 사용자는 스마트 폰을 통해 사용자 인증을 한 후에 백신접종내역을 요청하는 Verifier에서 요구하는 정보를 확인하고, Agent로 부터 받은 정보를 기관에 제공한다.
- Verifier : 검증자는 Service Provider이고, 서비스를 제공하기 전에 사용자에게 서비스에 필요한 정보를 요청한다. Agent 이 수립한 정책에 기반한 정보를 Agent로부터 받는다.

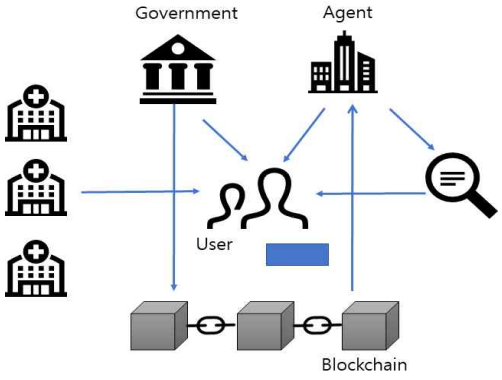

Fig. 5. DID-based vaccination history method

5. 결론

신원증명은 디지털을 기반으로 이루지고 있지만 쉽게 적용하기 어려운 이유는 디지털 정보의 특성 때문이다[10]. 디지털 정보는 생성, 흐름, 보관 등의 과정에서 위조나 변조의 가능성이 존재하기 때문에 이를 해결하지 않고는 적용하기 어렵다.

디지털 정보의 위조, 변조를 해결하는 방법으로 무결성이 보장되는 블록체인 기술이 대안이 될 수 있다. 즉, 블록체인 기술과 DID의 결합을 통해 SSI이 가능하다. 이를 통해 프라이버시 보호 및 효율성이 요구되는 다양한 기술에 적용이 가능하다[11].

제안 기법은 블록체인 기술인 DID를 활용하여 백신접종 내역을 블록체인에 기록하고, 이를 검증해 주는 Agent를 통해 사용자의 접종 사실을 기관에서 사용자의 동의하에 검증한다. 이 기법을 통해 코로나 19 뿐만 아니라 개인이 간염 예방접종이나 독감예방접종 등 다양한 정보를 등록하여 불의의 사고가 발생했을 때 처리할 수 있는 기회를 제공할 수 있다.

블록체인 상에 내역을 저장하고, 스마트 폰 기반의 생체인증과 원하는 정보만을 제공할 수 있는 권한을 개인에게 부여하므로 써 개인정보 노출을 줄일 수 있

다. COOV 앱을 통해 DID 기술을 적용한 사례가 있고, 이를 기반으로 확진자 접촉여부를 판단할 수 있는 시스템을 설계하였다.

ACKNOWLEDGMENTS

본 논문은 Research Institute of 4th Industrial Revolution Technology (RI4IRT) 지원을 받아 수행한 연구과제 “블록체인 기반의 탈중앙화 방식 신원 증명 기술 적용에 관한 연구”를 정리하여 작성한 것임

REFERENCES

[1] H.-Y. Kim, K.-H. Han & S.-S. Shin (2021). A Model for Self-Authentication Based on Decentralized Identifier. *Journal of Convergence for Information Technology*, 11(11), 66 - 74. DOI : 10.22156/CS4SMB.2021.11.11.066

[2]J.H. Lee, J.W. Kim, C.S. Kim & J. Yang (2020). A Study on Strengthening Personal Information Sovereignty through Analysis of Domestic Service Cases and Research Projects of Self-Sovereign Identity Technology. *The Journal of Korea Institute of Information, Electronics, and Communication Technology*, 13(6), 575 - 589. DOI : 10.17661/JKIIECT.2020.13.6.575

[3] H. J. Mun (2018). Biometric information and OTP based on Authentication Mechanism using Blockchain. *Journal of convergence for Information Technology*, 8(3), 85-90.

[4] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han & F.Y. Wang. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(11), 2266-2277.

[5] K.W. Cho, M.H. Jeon & S.U. Shin (2021). Secure De-identification and Data Sovereignty Management of Decentralized SSI using Restructured ZKP. *Journal of Digital Convergence*, 19(8), 205 - 217. DOI : 10.14400/JDC.2021.19.8.205

[6] OECD (2020). Mitigating the impact of COVID-19 on tourism and supporting recovery. *OECD Tourism Papers*, No. 2020/03, OECD Publishing, Paris. DOI : 10.1787/47045bae-en.

[7] BBC News (2021). COVID-19: Is it possible to issue a vaccine vaccination certificate from tomorrow..."Vaccine passport"?. Retrieved from https://www.bbc.com/korean/news-56745019

[8] J.H. Eom. (2021). Immunity Passport, A Double-Edged Sword in the Corona Era -A Public legal review and ethical implications-. *PHILOSOPHY·THOUGHT·CULTURE*, 36, 101-120. DOI : 10.33639/PTC.2021..36.005

[9] The JoongAng (2021). Australia to start 'with corona' includes south korea in 'vaccine passport', Retrieved from https://www.joongang.co.kr/article/25007108

[10] S. Kim, H.J. Mun & S. Hong (2022). Multi-Factor Authentication with Randomly Selected Authentication Methods with DID on a Random Terminal. *Applied Sciences*, 12(5), 2301. MDPI AG. DOI : 10.3390/app12052301

[11] D. Reed (2018). Self Sovereign Identity (SSI) Open standards with Drummond Reed, Retrieved from https://www.slideshare.net/SSIMeetup/self-sovereign-identity-ssi-open-standards-with-drummond-reed

문형진(Hyung-Jin Mun) **[정회원]**

- 2008년 2월 : 충북대학교 전자계산학과(이학박사)
- 2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수
- 관심분야 : 정보보안, 네트워크 보안, 빅데이터분석

- E-Mail : mun.it@daum.net