The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 23, No. 1, pp.209-214, Feb. 28, 2023. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2023.23.1.209
JIIBC 2023-1-30

블록체인을 이용한 자율주행 차량의 포렌식 연구

Forensic study of autonomous vehicle using blockchain

강장묵*

Jang-Mook Kang*

요 약 장래 국내외 자율주행 차량이 보급되면, 자율주행 차량의 사고 역시 발생 빈도가 늘어날 전망이다. 특히, 완전자율주행 자동차가 운행할 경우, 자동차의 사고 자체뿐만 아니라 운행 중 승객 간의 성폭력, 폭행, 사기 등 여러 가지 형사/민사상 문제가 발생할 수 있다. 이 경우, 자율주행차량의 운행 사고와 차량 내 승객의 사고에 대한 포렌식 역시 변화할 전망이다. 이 글은 자율주행차량의 보안 위협에 대한 유형, 블록체인 기술을 이용한 증거 데이터의 무결성 유지 방안, 디지털 포렌식의 연구를 고찰하였다. 이를 통해 블록체인 기술을 활용한 자율주행 차량에서 발생할 위협과 다양한 사고 유형 별 포렌식 기법 등을 시나리오식으로 기술할 수 있었다. 본 연구를 통해 자율 주행 차량 대상 취약점, 공격에 대응하기 위한 국내외 웹사이트의 포렌식 보안 기술 조사 및 연구기관, 정보보안기업의 블록체인 보안 연구를 조사하여 사고 전/후 자율주행 차량의 포렌식을 돕는 블록체인 기법을 제안하였다.

Abstract In the future, as autonomous vehicles become popular at home and abroad, the frequency of accidents involving autonomous vehicles is also expected to increase. In particular, when a fully autonomous vehicle is operated, various criminal/civil problems such as sexual violence, assault, and fraud between passengers may occur as well as the vehicle accident itself. In this case, forensics for accidents involving autonomous vehicles and accidents involving passengers in the vehicles are also about to change. This paper reviewed the types of security threats of autonomous vehicles, methods for maintaining the integrity of evidence data using blockchain technology, and research on digital forensics. Through this, it was possible to describe threats that would occur in autonomous vehicles using blockchain technology and forensic techniques for each type of accident in a scenario-type manner. Through this study, a block that helps forensics of self-driving vehicles before and after accidents by investigating forensic security technology of domestic and foreign websites to respond to vulnerabilities and attacks of autonomous vehicles, and research on block chain security of research institutes and information security companies. A chain method was proposed.

Key Words : AI, autonomous vehicles, blockchain technology, forensic, vulnerabilities

*정회원, 극동대학교 해킹보안학과
접수일자 2022년 12월 31일, 수정완료 2023년 1월 30일
게재확정일자 2023년 2월 3일

Received: 31 December, 2022 / Revised: 30 January, 2023 / Accepted: 3 February, 2023
**Corresponding Author: honukang@gmail.com
Dept of Hacking & Security, Far East University, Korea

Ⅰ. 서 론

1. 교통사고 현황과 안전기술의 이해

경찰청 통계를 기준으로 대한민국에서 일어나고 있는 교통 관련 사고의 현황은 다음과 같다. 2018년에는 3,781명의 사망자와 323,036명의 부상자가 발생하였다. 2019년에 3,349명의 사망자와 341,712명의 부상자가 있었다. 2020년은 3,081명의 사망자와 306,194명의 부상자가 발생하였다. 2021년은 2,916명의 사망자와 291,608명의 부상자가 발생하였다.[1]

특히, 2021년 교통사고는 사고 203,130건, 사망 2,916명, 부상 291,608명으로 2020년대비 사고건수 -3.1%(-6,524건), 사망자 -5.4%(-165명), 부상자 -4.8%(-14,586명)로 모든 영역에서 감소하였다.

이와 같은 원인은 세계적으로도 '안전기술도입에 따른 전세계 교통사고 사망자 수' 자료를 분석해 다음과 같은 원인을 추정할 수 있다. 세계적으로 교통사고와 안전기술의 관계를 살펴보면, 1965년 100만 마일당 550명의 사망자가 발생하던 것이 안전기술도입에 따라 2010년에는 200명 이하로 감소하였다.[2]

2. 연구목적과 내용

이 글은 국내외 자율주행 차량의 보안 위협 유형, 디지털 포렌식의 연구 동향을 통해 블록체인 기술을 활용한 자율주행 차량에서 발생하고 있는 위협과 포렌식을 전반적으로 조사하고자 하는 목적을 갖는다.

특히 연구내용으로는 자율주행차량 사고 현장에 가해자와 피해자인 이해관계자 사이에서 발생하는 데이터 기록 및 처리 (보험, 민/형사 처벌 유무)를 블록체인 기술로 검증가능하도록 돕는 기술과 서비스 모델을 다루었다.

이를 위해 인공지능의 대표적인 기술이 탑재될 자율주행차량의 사고 기록을 블록체인 기술로 봉인하고 이를 바탕으로 검증가능하고 영구적인 방식으로 분산 처리하는 프로세스를 제안하였다.

Ⅱ. AI기반 자율주행차량과 블록체인 기반 포렌식 관련 연구

1. 포렌식을 위한 무결성 보장형 블록체인 연구

블록체인(Blockchain)이란 정보데이터에 대한 '보안성'과 '무결성'을 이끌어낼 수 있는 정보보안 플랫폼을 말하며, 각종 정보가 기록된 데이터를 해쉬(Hash)와 비대칭 암호체계 방식으로 블록(Blocks)에 저장하여 노드별로 분산・보관하는 기술을 의미한다. 블록체인은 크게 퍼블릭, 프라이빗, 콘소시엄 등 형태로 온체인/오프체인에서 작업증명, 지분증명 등의 방식으로 작동하는 보안기술이다.

예를 들어, 비트코인에서 블록체인은 주기적으로 발행하는 화폐인 비트코인의 이동 이력을 저장하는 일종의 분산된 디지털 장부라고 할 수 있다.[3] 이 장부는 위변조할 수 없는 암호학적 기술로 만들어지며 비트코인의 소유권 이동을 위해 비트코인의 거래(Transaction) 과정과, 발생한 거래를 모아 시간이 매우 오래 걸리는 특정 조건의 해시 값을 갖게 하는 난수(Nonce) 찾기 문제로 거래 내용의 위변조를 방지한다.[4]

이러한 블록체인 기술은 "유효성이 검증된 데이터의 연결"이라는 정의와 "새로운 분산 트랜잭션의 혁신적 키(Key)" 와 "인터넷 등장만큼의 디지털혁명"이라고 논평도 하고도 있다.[5]

따라서, 분산된 원장을 활용할 수 있는 구체적인 방법을 체계적으로 구성한다면, 현존하는 기술 중 포렌식의 증거 자료의 처리에 최적의 기술로 사료된다.

2. 자율주행차량에 적용가능한 블록체인 연구

블록체인 기반의 자율주행차량은 V2V(Vehicle-to-vehicle) 소통 기술이 적용된다. 구체적인 적용 사례로는 여러 차량이 군집해서 자율주행을 하는 도로상황을 고려할 수 있다. 뿐만 아니라, 여러 자율주행차량의 운행기록 등을 블록으로 저장하면 사고 발생 시 무결성이 보장된 포렌식을 수행할 수 있다. 즉 공격자 입장에서 자율주행의 여러 데이터를 분산 원장에 기록되고 나면, 해당 블록에 속한 데이터를 변경하기가 어려워진다. 이는 아래 그림 1과 같이 이어지는 모든 블록을 변경해야 하기 때문이다.

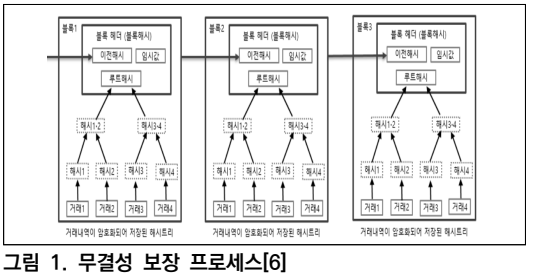

그림 1. 무결성 보장 프로세스[6]
Fig. 1. Integrity assurance process

자율주행 차량은 기존의 내연기관과는 비교할 수 없는 비정형데이터를 갖는다. 자율주행차량에 탑재된 레이더, 라이더, GPS, 카메라 등 여러 센싱에서 수집된 데이터가 실시간으로 저장되고 분석된다. 또한 분석 결과나 로그 파일 등도 기존의 내연기관과는 비교할 수 없는 종류와 크기를 갖는 특징을 보인다. 여러 자율주행차량이 도로에서 이동하면서 소통한 정보, 개별 자율주행차량이 수집한 센싱 정보 그리고 사고 발생 전후 데이터 등이 모두 위 그림 1과 같이 개별 처리가 이전 해쉬로 묶여 무결성을 보장하는 프로세스를 갖기 때문이다.

그러나 이와 같은 이종의 여러 데이터를 실제 모두 온체인에 실시간으로 분산 저장하는 것은 현재 컴퓨팅 자원으로는 불가능하다. 따라서 3장에서 이를 구체적인 시나리오 상황에서 해결하는 방법을 제안하고자 한다.

Ⅲ. 3장 자율주행차량의 시나리오 별 블록체인 적용

1. 자율주행차량의 보안 취약점

국·내외 IBM 보안연구소, 파수닷컴 등을 통해 자율주행차량에서 발생하는 주요 취약이 보고되었다. 해외 OWASP, FIRST CERT 등의 국제보안기관도 자율주행차량의 보안 취약성을 보고하였다. 구체적인 보안위협은 차량, 통신채널 그리고 백엔드 인프라로 구분할 수 있다. 좀 더 세부적으로는 공격자는 도청 및 데이터 변조를 수행, 백엔드 인프라에 대하여 도스(DoS)공격, 차량 제어기의 인터페이스를 통해 송수신되는 데이터 또는 저장된 데이터를 도청, 변조, 업데이트 패키지를 위변조하여 공격 등 다양한 사이버공격이 있다. 해당 공격은 아래 그림 2의 자율주행차량의 시나리오 별로 구체적으로 적용할 수 있다.

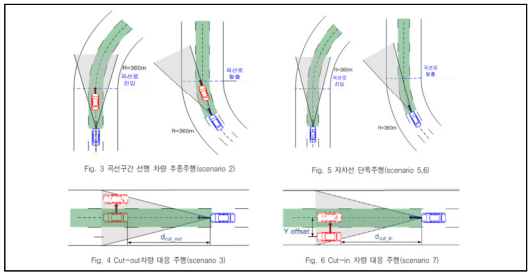

그림 2. 시나리오 별 안정성 평가[7]
Fig. 2. Stability evaluation by scenario

그림 2와 같은 시나리오 별 안정성 평가의 대상 범위는 확장되고 있는데 상세하게는 사물인터넷, 자율주행차량 자체 센싱 데이터 그리고 승객의 SNS 데이터등 비정형 데이터에 대한 보안이 요구된다. 데이터 품질 측면에서는 비정형데이터를 전처리 및 후처리하는 방법을 통해 열화를 줄인다. 포렌식 대상 데이터의 품질을 높이는 방법으로 블록체인 기술을 다음 절과 같이 적용할 수 있다.

2. 자율주행차량 사건 별 블록체인 적용

자율주행차량의 사고 전/후에는 차대번호(VIN), 보증 식별자, 마일리지 기록, 수리점 식별자, OEM 식별자, 수리 부품 SKU 비용, 공임, 지불 정보 등이 요구된다.

만약, 자율주행차량 내에서 동승자 간의 물리적 폭력, 언어적 성추행, 사기행각, 수면 및 마취, 불법의료행위, 불법성행위 등 불법행위가 의심될 경우에는 차량 내 다양한 센싱값을 추론하여 범죄를 재구성할 수 있어야 할 것이다.

이처럼 자율주행차량의 사고 원인을 밝히거나 차량 내 사고 증거를 법원에 제출할 때는 무결성 즉 증거데이터의 수집과 처리 그리고 전송 전 과정에서 안전성을 보증할 수 있어야 한다.

지금과 같이 신뢰할 수 있는 공무를 수행하는 경찰관 등이 직접 USB 등을 제출하는 방식에서 하이퍼레저 기반의 프라이빗 블록체인 기술을 적용한 '현장 증거의 법원 증거물 채택'까지 전과정을 무결하게 유지하는 기술이 요구된다.

만약 위에서 언급한 차량 관련 여러 정보를 하나로 묶어 분산 원장에 기록하면, 차량 소유자, 수리점, 차량 제조사, 수리 부품 제조사가 해당 거래 기록을 조회할 수 있다. 또는 이를 바탕으로 차량 내 센싱데이터를 블록체인에 저장하여 무결성을 보장하는 방안을 디지털 증거로 활용할 수 있다.

이는 전자적 증거, 전파기록, 전파적 기록, 컴퓨터 관련 증거, 컴퓨터 전자기록 등의 용어로 부르며 디지털 증거가 포함된 매체는 컴퓨터, 휴대폰, 디지털 카메라 등과 같은 전통적인 디지털매체와 자동응답기, 게임기, 손목밴드 등 쉽게 인지하거나 접근할 수 없는 새로운 형태의 디지털 매체로 변화가 있어 법원이 증거로 채택하는데 신중한 입장을 가지게 한다.

이외에도 자율주행차량은 승객의 디지털 워치, 승객의 스마트폰 외에도 라이더, 레이더, 위성측위값, 카메라 등 다양한 센싱값 등이 디지털 포렌식의 대상이 된다. 이 모든 데이터는 빅데이터이면서 비정형성을 갖고 있어 사건 유형별로 이를 정형화하는 것이 어렵다.

Ⅳ. 무결성 보장 시나리오 적용 및 결과

1. 해쉬함수를 이용한 무결성 보장

OWASP, FIRST CERT 등 국제보안기관이 발표하는 자율 주행 차량의 보안 취약점에 대한 유형, 위협에 대한 심각성이 보고되었다.[8] 이를 해결하기 위해서는 해쉬함수를 이용하여 무결성을 보장하는 것을 아래 [그림 3]을 통해 제안할 수 있다.

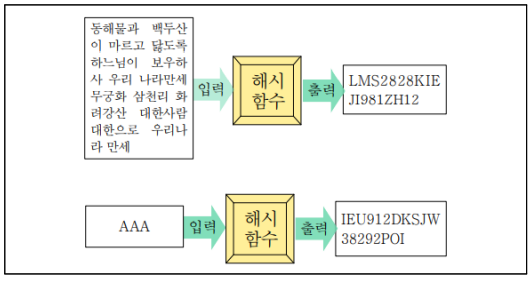

그림 3. 자율주행 차량에 적용 가능한 임베딩된 숫자 및 임의문자에 대한 해시 함수

Fig. 3. Hash function for embedded numbers and random characters applicable to autonomous vehicles

블록체인은 두 이해관계자(사고 현장에 가해자와 피해자) 및 자율주행차량 내 승객간의 피해자-피의자 사이에서 발생하는 트랜젝션(보험, 민/형사 처벌 유무)을 효과적이며 검증가능하고 영구적인 방식으로 기록하는 공개되고 분산된 원장을 활용하기 위해 위 [그림 3]와같은 구체적인 일방향 해쉬 함수 이용을 제안한다.

해쉬함수의 특징은 임의의 길이에 값이 입력되더라고 일정한 길이(크기)의 출력을 보장해줌으로 자율주행차량의 여러 센싱 데이터와 승객의 행동 추정 데이터에 적합하다고 판단된다.

자율주행차량은 블렉박스 외에도 사고 시점 차량 주변의 IoT 데이터, 사고 추정 발생 시간 전후의 차량 내 부착된 CCTV, 라이더, 레이더, 탑승기록, 차량 속도계 그리고 환경값으로 사고지역의 당일 기상정보 마지막으로 페이스북, 인스타그램, 틱톡 등을 통해 유추한 승객정보 등 여러 비정형 데이터를 수집, 전처리, 후처리, 분석을 수행한다.

이 경우 위 [그림 3]과 같이 이종의 비정형 데이터를 입력하고도 정해진 출력양을 만들어냄에 따라 데이터 처리의 효율성을 기대할 수 있다. 뿐만 아니라, 이를 블록의 체인으로 연결할 경우, 자율주행차량의 사고데이터에 대한 무결성을 보장할 수 있어 법원의 증거로 채택할 수 있다. 이 경우 비정형의 큰 크기의 데이터에 대한 메타값을 해쉬함수로 처리하는 방법을 병행하면 큰 크기의 데이터에 대한 처리 효율성을 높일 수 있다.

2. 블록체인의 자율주행차량 적용 사례와 포렌식 시나리오 제안

앞 절에서 다양한 이기종의 비정형 데이터가 수집되어도 이를 일방향 해쉬 함수로 처리하여 무결성을 보장하는 방안을 제안하였다. 자율주행차량에서 데이터 자체의 무결성은 해쉬함수를 통해 수집한 증거가 다음 해쉬 함수에 포함됨으로 체인을 형성하게 된다. 앞 블록을 해쉬함수한 값이 포함된 현재 블록의 해쉬함수 값은 다음 블록의 생성에 포함되는 값이 된다. 즉 해쉬 값이 체인으로 포함되는 블록 간의 관계를 만들어 전체 네트워크는 견고성을 갖는다.

그림 4. 비트코인 노드에서 트랜젝션 추적 원리를 이용한 포렌식 사례

Fig. 4. Forensic case using the transaction tracing principle in Bitcoin node

만약 블록체인의 무결성과 견고성 원리를 바탕으로 포렌식 수사 증거로 활용한다면 위 [그림 4]와 같은 트랜젝션 추적이 대표적 사례가 될 전망이다.

블록체인은 다양한 분산 원장 개념을 정립하기 위해, 새로운 블록을 검증하고 합의하는 프로토콜에 의존한다. 사고 차량의 포렌식 대상 데이터에 대한 무결성을 보장받기 위해서는 데이터의 전송 기록, 새로운 노드 생성 기록 등 블록 간의 트렌젝션을 추적할 수 있어야 한다. 즉 트렌젝션을 블록에 저장하고 이를 체인으로 연결하는 합의 프로토콜이 일종의 포렌식 블록체인이 될 수 있다.

다음 [그림 5]는 입력된 해쉬값으로 생성된 블록과 출력될 해쉬값으로 새로 봉인될 블록을 포렌식에서 비교 및 추적할 대상 데이터를 자동차 오너라는 가정하에서 정리한 것이다.

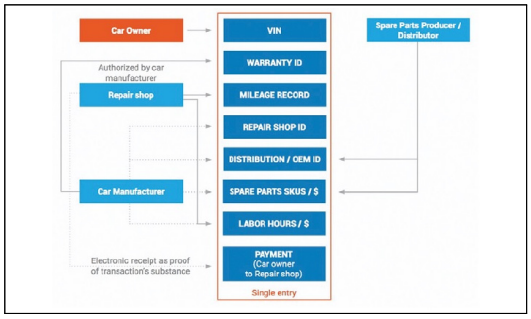

그림 5. 포렌식 대상 자율주행차량의 수리 관련 레코드 시나리오[9]
Fig. 5. Record scenarios related to repair of autonomous vehicles for forensics

만약 사고 난 자율주행차량이 '실제 누구의 것인지', '사고 전 인공지능의 모델 등을 제조사 초기 버전과 달라진 것은 없는지' 등을 포렌식할 때, 위 [그림 4]와 같은 방법으로 추적할 수 있다. 그리고 추적할 대상 데이터가 [그림 5]에서 구체적으로 도식화하였는데 인공지능의 이상탐지 기술을 응복할 수 있다. 이상탐지란, 예상된 행동에 부합하지 않는 특이한 패턴을 식별하기 위해 사용하는 방법이며 일반적으로 Novelty Detection, Outlier Detection이라고 불리기도 한다.[10]

실제 자율주행차량에서 사고 즉 포렌식 대상이 되는 주요 데이터에 대해서는 [그림 5]와 같이 제조사와 차량 수립 업체로 나누어 추적 및 관리한다.

여기서 차량의 마일리지, 수리점 식별 번호, 배포자 식별 번호, 수리 부품, 수리 시간, 비용 등의 데이터는 사고 전/후의 무결성이 보장된다. 여기서, '무결성이 보장된다'는 의미는 법원 또는 법관의 입장에서 증거에 대한 신뢰 문제로 무척 중요한 잣대이다. 뿐만 아니라, 보험금을 지불하는 보험사 입장이나 가해자와 피해자가 혼재되거나 모호한 상황에서 불신과 의혹을 해결하는데 드는 사회적 비용을 줄일 수 있다.

이 글에서는 그림 4를 사례로 하여 자율주행차량의 사고 발생 시, 블록 간의 트랜젝션을 추적할 수 있는 시나리오의 주요 값(입력해쉬, 출력해쉬, 새로봉인된 블록 정보, 보낸 주소, 받은 주소 등)을 제안하고 포렌식 영역에서 이를 활용하는 시나리오 방안을 위 설명을 통해 도출하였다.

두 번째는 좀 더 구체적으로 포렌식 대상의 자율주행차량에 관한 수리 관련 데이터 레코드를 제출하는 시나리오를 제안한다.

자율주행차량의 사고 전/후를 비교/분석하면 포렌식의 실제 적용 현장에서 도움을 주는 경우가 다수 발생한다. 예를 들면, 차대번호(VIN), 보증 식별자, 마일리지 기록, 수리점 식별자, OEM 식별자, 수리 부품 SKU 비용, 공임, 지불 정보를 하나로 묶어 분산 원장에 기록하면, 차량 소유자, 수리점, 차량 제조사, 수리 부품 제조사가 해당 거래 기록을 조회하고 이를 바탕으로 차량내 센싱데이터를 블록체인에 저장하여 처리할 수 있다.

V. 결 론

최근 레벨4 이상의 완전자율주행차에 대한 시범 사업이 활발하게 이루어지고 있다. 가까운 장래 완전자율주행차가 운행되기 위해 차량자체의 센싱기술, 이를 분석하는 인공지능기술 뿐만 아니라 자율차량을 지원하는 인프라와의 통신, HD급 이상의 지도 그리고 법 및 제도 완비 역시 필수적이다.

이 글은 디지털 포렌식의 주요 대상인 자율주행차량의 사고 전/후, 증거조작을 방지하고 정확한 사고원인을 파악할 수 있는 프로세스 기법에 대한 연구를 수행하였다. 그 결과 포렌식 대상인 자율주행차량의 수리 관련 레코드를 예로 들어 사고 발생 후 포렌식을 수행하는 시나리오를 제안하였다. 뿐만 아니라, 암호자산의 불법거래를 추적하고자 트랜젝션을 트레킹하는 비트코인의 실제 입출금 주소 추적 시스템을 활용한 포렌식 프로세스를 시나리오로 설명하였다.

이상의 시나리오는 향후 도래한 자율주행차량의 포렌식에 절차 또는 세부 규칙을 정립하는데 도움을 줄 것으로 여겨진다.

이 글은 도래하고 있는 자율주행차량의 변화하는 기술환경 특히 비정형 데이터인 센싱값과 이를 처리하는 인공지능 기술의 발전 변화 뿐만 아니라, 신기술에 대응하는 포렌식에 있어서 블록체인 기술 도입을 통한 무결성 강화 방안을 도출하였다. 이 글은 기술변화에 뒤따르는 제도 또는 사고가 발생한 후에서야 포렌식 기법을 개발하는 기존의 사고 후 대처에 따른 한계를 극복하는데 기여할 것으로 사료된다.

References

[1] S. H. Park and S. G. Lee, "Review on the Documentability of Electronic Documents in Criminal Procedure of Minor Traffic Offenses", The Journal of Police Science, Vol. 19, No. 1, pp. 33-58, Mar. 2019.

http://doi.org/10.22816/ polsci.2019.19.1.002.

[2] https://www.yna.co.kr/view/AKR20171022052800033. [accessed: Nov. 11, 2022]

[3] Sunghwan Kim, Younggon Kim, 'A Study on the Blockchain-based System Authentication Method,' The Journal of The Institute of Internet, Broadcasting and Communication (IIBC) Vol. 20, No. 1, pp.212-213, Feb. 29, 2020. https://doi.org/10.7236/JIIBC.2020.20.1.211

[4] Satoshi Nakamoto, "Bitcoin: A Peer to Peer Electronic Cash System", Oct 2008.

[5] Ackner/Kühl, §267 Rn. 16; SK/Samson, §267 Rn. 9;Schönke/Schröder/Cramer, §267 Rn. 42;Tronder/ Fischer, §267 Rn. 12.

[6] Hyungjoong Yun, Economy · Culture Cryptocurrency and Korean society. consonants and vowels, 37, 2018. pp. 357-370, https://bitcoin.org/ bitcoin.pdf [accessed: Dec. 11, 2022]

[7] Hyeongho Lim, Heungseok Chae, Myungsu Lee, Kyongsu Lee, 'Development and Validation of Safety Performance Evaluation Scenarios of Autonomous Vehicle based on Driving Data', Journal of Auto-Vehicle Safety Association v.9 no.4 , 2017, pp.9 - 10

[8] owaso, Application Security Verification Standard 4.0.3, October 2021, https://owasp.org/www-project-application-security-verification-standard/migrated_content# [accessed: OCT. 20, 2022]

[9] Cheol Hee Yoon, A Study on the Implementation of a Blockchain based Autonomous Vehicle Accident Data Convergence Platform, A Dissertation Submitted to the Department of Technology Policy and the Graduate School of Yonsei University in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Science and Technology Policy, December 2022

[10] Songhee Kim, Sunhye Kim, Byungun Yoon, "Deep Learning-Based Vehicle Anomaly Detection by CombiningVehicle Sensor Data", Journal of the Korea Academia-Industrialcooperation SocietyVol. 22, No. 3 p. 22, 2021, http://dx.doi.org/10.5762/KAIS.2021.22.3.20

저 자 소 개

강 장 묵(정회원)

- 1999년 2월 : 고려대학교 일반대학원 석사
- 2005년 8월 : 고려대학교 정보보호대학원 (공학박사)
- 2020년 8월 ~ 현재 : 동국대학교 국제정보보호대학원 AI융합 보안 교수
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수
- 관심분야 : 인공지능, 블록체인, 융합보안, 산업보안

※ "이 연구는 2021년도 극동대학교 교내연구비 지원에 의해 수행된 것 임(FEU2021R24)"
"This work was supported by the 2021 Far East University Research Grant(FEU2021R24)"