정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

디지털운행기록 장치 데이터 보안 원칙과 디지털 포렌식을 위한 데이터 식별 방안

김 태 근*

요 약

디지털운행기록장치(DTG)는 차량의 운행정보를 기록하고 저장하는 장치로, 여객 및 화물자동차에 의무적으로 장착되어 여러 실시간 운행기록을 수집하고 관리할 수 있도록 하고 있다. 대부분 버스, 택시, 화물차 등에 사용되며, 상용 자동차의 운전자를 인증하고 과도한 운행으로 인한 사고를 줄이는 데 중요한 역할을 한다. 본 연구에서는 기존의 국내 디지털운행기록장치 관련 지침 및 표준 사양의 보안 기술 관련한 내용을 살펴보고 더 나아가 문헌조사를 통해 발견된 디지털운행기록장치 데이터 보호 관련 기본적 보안원칙을 소개한다. 더불어, 디지털 포렌식을 위한 데이터 식별 방법에 대한 실험적인 시도 사례의 결과를 함께 소개한다.

Ⅰ. 서 론

디지털운행기록장치(DTG, Digital Tachograph)는 차량의 운행정보를 디지털로 기록하고 저장하는 장치로서 여객자동차 운수사업법에 따른 여객자동차 운송사업자와 화물자동차 운수사업법에 따른 화물자동차 운송사업자(가맹사업자)를 대상으로 디지털운행기록장치의 장착을 의무화하고 있다. 이에 따라 디지털운행기록장치는 버스, 택시, 화물차 등에 이미 장착되어 운행 데이터를 기록 및 관리하는 데 사용되고 있다. 디지털운행기록장치를 통해 상용 자동차의 운전자를 인증하고, 인증된 운전자의 운행정보를 실시간으로 기록하고 외부 기관으로 보고하도록 관리함으로써 과도한 운행으로 인한 차량 사고 발생을 줄이고 더 나아가 올바른 운전문화를 정착시키는 데 많은 이바지를 하고 있다.

국토교통부에서 고시한 자동차 운행기록 및 장치에 관한 관리지침에는 디지털운행기록장치와 관련한 세부지침이 정리되어있다. 이중 제 17조가 보안관리에 관한 지침을 담고 있다. 총 5개의 지침에 나타나있으며, 4개 지침은 디지털운행기록장치를 통해 얻은 정보를 한국교통안전공단에서 분석하는 동안에 발생가능한 보안 문제를 해결하기 위한 지침이라 할 수 있고 나머지 한개의 지침에 디지털운행기록장치와 관련한 보안 준수 사항이 나와있다.

“표준화된 운행기록장치를 제조하는 자는 운행기록정보를 보호하기 위하여 운행기록장치에 암호화프로그램을 탑재하여야 한다.”라는 지침이 있으며, 암호화프로그램 탑재를 명하고 있다. 이외에도 세부지침으로 기록된 정보가 암호화되어야 한다는 내용이 있으나, 원래의 지침과 크게 다르지 않은 수준으로 의무 권고사항이 정리되어있다. 지침은 다양한 사례에 포괄적으로 적용될 수 있도록 만들어져야 하므로 다소 추상적이고, 넓은 의미로 해석될 수 있는 형태로 문구가 작성된 것을 알 수 있다. 지침의 자체적 한계를 극복하기 위해서는 적절한 가이드와 관련 표준이 마련되어야 할 필요가 있다.

한국교통안전공단은 다양한 상용차 그리고 DTG 장치들이 표준화된 형태로 운영서비스에서 요구하는 사항을 준수할 수 있도록 전자식 운행기록장치 표준사양[1]을 제정하고 업데이트하고 있다. 해당 사양에는 전자식 운행기록장치 구조, 전자식 운행기록장치 성능/기능, 운행기록 데이터 정의 등이 포함되어 있다. 개발에 필요한 여러 사항을 구체적으로 설명하고 있으나, 보안과 관련한 사항이 정리되어있지 않아 디지털운행기록장치 데이터가 적절하게 보호될 수 있다는 보장이

본 연구는 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2022-0-01022, 이벤트 기반 실험시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발)
* 순천향대학교 정보보호학과 (교수, tg.kim@.sch.kr)

어렵다고 할 수 있다. 이에 따라 우리는 해외 관련 가이드를 조사하고 정리하여 필요한 여러 보안 요구사항을 정리한다. 관련한 내용을 3장에서 설명한다.

이와 더불어, DTG 보안 요구사항 분석을 통한 연구 결과, 대부분 가이드에서는 디지털 포렌식과 관련된 보안 요구사항이 제대로 정립되어 있지 않았음을 확인하였다. 특히 현장에서의 차 사고 등의 상황에서 휘발성 메모리의 일부가 손상될 수 있는데, 이 경우에는 남아있는 운행 데이터의 정확한 추출이 중요하다. 디지털 포렌식의 부재는 DTG 데이터의 정확한 분석과 복구를 어렵게 만들며, 법적 증거로서의 가치를 저하할 수 있다. 이러한 문제를 해결하기 위해, 보다 체계적이고 표준화된 디지털 포렌식 절차와 관련 보안 요구사항의 마련이 시급하다. 또한, 차 사고로 인한 휘발성 메모리의 일부 손상 시, 메모리 내의 DTG 데이터를 유추하는 방안의 연구와 개발도 필요하다. 일부 남아있는 운행 데이터를 통해 전체 데이터의 누락 없이 정확한 복원과 분석을 할 수 있도록 하는 기술이 요구된다. 이는 사고 재구성, 책임 소명, 보험 처리 등 다양한 분야에서 중요한 역할을 할 수 있으며, 차량의 안전 운행을 더욱 강화하는 데에도 이바지할 것으로 기대된다. 간단하게 암호화되지 않은 메모리 내 잔여 차량운행데이터가 남아있다고 가정하고 데이터 종류를 유추해보는 실험을 통해 데이터 포렌식을 위한 데이터 종류 판별 방법에 대해 4장에서 알아본다.

임베디스시스템 메모리 복원 혹은 스와핑 기법 등과 같은 자체 복원 기술에 관한 사항은 논외로 하며, 데이터 유추 가능성만을 시사하도록 한다.

Ⅱ. DTG 운행기록정보

국내 한국교통안전공단에서는 안전한 사용차 운행을 위하여 운행기록 분석 시스템을 구축하여 운영중에 있다. 2011년도 12월부터 처음 시험운영을 시작한 이래로 지금까지 계속하여 운행기록 관리를 위한 활동을 지속하고 있다. 이와 더불어, 한국교통안전공단은 다양한 상용차 그리고 DTG 장치들이 표준화된 형태로 운영서비스에서 요구하는 사항을 준수할 수 있도록 전자식 운행기록장치 표준사양 제정 및 업데이트하고 있다. 이에 따라 국내 DTG 제공 업체는 해당 표준사양의 최소 요구사항을 만족하기 위해 노력하고 있다.

상용차 운전자는 차대번호, 자동차 관리 코드, 운송사업자 관리 코드, 기기 및 통신상태 코드 등의 데이터를 필수적으로 기록하도록 권고하고 있으며, 정해진 순서와 포맷에 맞춰 기록 정보를 가공하여 교통안전공를 DTG로 로깅하고 이를 일정한 형식으로 변환하여 운행기록분석시스템(eTAS)에 제출하도록 하고 있다. 여기서 운행기록분석시스템(eTAS)이란 운행기록장치를 통해 수집된 데이터를 전달 받아 운전자의 운전습관을 파악, 분석하여 실증적인 운전자의 안전관리를 수행하기 위해 마련된 별도의 시스템이라 할 수 있다.

2.1. DTG 운행기록정보

운행기록정보의 배열 및 포맷은 [표 1]와 같다. 주요 운행기록 정보는 아래와 같이 정리된다.

- **차대번호:** 차량의 동일성 확인을 목적으로 규칙 제14조에 규정된 방법에 따라 차대 또는 차체가 일체 구조인 경우에는 차체(이하 "차대"라 한다)에 표기한 아라비아숫자 및 알파벳 글자를 의미한다.
- **자동차 관리 코드:** 자동차 관리 코드는 자동차 유형과 자동차 등록번호 정보로 구성되는 코드이며 주체적으로 자동차 유형(2자리)와 자동차 등록번호(12자리)로 정의된다. 차대번호를 통해 차량을 식별하고 생산 국가, 제조사, 공장 등의 구분이 가능함에도 불구하고 DTG는 상용차의 운행 목적을 명확하게 구분하기 위하여 자동차 관리코드를 기록하도록 권고하고 있다.
- **운송사업자 관리 코드:** 운행되는 상용차를 관리하는 운송사업자를 구분하기 위한 용도로 만든 코드를 의미한다. 운송사업자 관리 코드를 차량마다 DTG 데이터로 기록하도록 하고 있다. 여객자동차운수사업법상 여객자동차운송사업 면허가 있는 자나 화물자동차운수사업법상 화물자동차운송사업의 허가를 받은 자의 사업자등록번호(구분자 포함 총 10자리)를 사용한다.
- **운전자 코드:** 운전자 식별을 위한 코드를 의미한다. 한 차량에 여러 운전자가 운전할 때를 가정하여 운전자별 운행기록 관리를 위한 운전자 코드를 DTG 시스템이 기록한다. 운전자가 직접 운전자 코드를 입력하거나, 생체인식 장치를 기반으로 운전자 인증을 수행하고 자동으로 코드가 입력되도록 할 수 있다.
- **기기 및 통신상태 코드:** 예외 상황 혹은 상태를 나타내는 코드를 의미한다. DTG 장치에 일시적인 에

〔표 1〕 운행기록정보 배열

항 목		자릿수	표기방법	표기시기
운행기록장치 모델명		20	오른쪽 정렬하고 빈칸은 #으로 표기	최초 사용 시 등록
차대번호		17	영문(대문자) 및 아라비아 숫자로 전부 표기	최초 사용 시 등록
자동차 유형		2	유형 별 두자리 코드 표기	최초 사용 시 등록
자동차 등록번호		12	자동차등록번호 전부 표기 (한글 하나에 두 자리 차지, 빈칸은 #으로 표기)	최초 사용 시 등록
운송사업자 등록번호		10	사업자등록번호 전부 표기	자동차 운송사업자 설정
운전자코드		18	운전자 자격증번호 전부 표기(빈칸은 #으로 표기하고 중간자 '-'는 생략)	실시간 기록
주행거리	일일	4	0000~9999 사이 주행거리 표기	실시간 기록
	누적	7	0000000~9999999 사이 주행거리 표기	실시간 기록
정보발생 일시		14	YYMMDDhhmmssss (연/월/일/시/분/0.001초)	실시간 기록
차량속도		3	000~255 사이 속도 표기	실시간 기록
분당 엔진회전수		4	0000~9999 사이 RPM 표기	실시간 기록
브레이크 신호		1	0(off) 또는 1(on) 표기	실시간 기록
GPS	X좌표	9	10진수로 표기	실시간 기록
	Y좌표	9		실시간 기록
위성항법장치 방위각		3	0~360 사이 각도 표기	실시간 기록
가속도	X 축	6	-100~+100 사이 가속도 표기	실시간 기록
	Y 축	6		실시간 기록
기기 및 통신 상태		2	사전 정의된 에러 코드 표기	실시간 기록

러가 발생하거나 통신 컴포넌트에 문제가 발생하였을 때 이를 파악하기 위하여 DTG 장치는 자신의 현 상태를 모니터링하여 기기 및 통신 상태코드로 정보를 기록한다.

- **주행 거리:** 운행되는 상용차가 하루 주행한 거리와 DTG 탑재 이후 운행한 총 누적거리를 의미한다. 해당 정보는 DTG 시스템의 디스플레이 장치에 표출될 수 있도록 구현된다.
- **정보발생일시:** 정보발생일시는 특정한 DTG 기록정보가 발생된 일시를 년/월/일/시/분/초/밀리초/(YYMMDDhhmmssfff) 형태의 14자리 수로 표현한 데이터를 의미한다.
- **차량속도:** 차량속도는 상용차가 운행되는 동안 측정되는 차량의 속도를 의미한다. 자세히, 자동차의 속도 센서로부터 순간 속도가 검출된 시간 당 진행거리를 의미한다고 볼 수 있음
- **분당 엔진 회전수:** 분당 엔진 회전수는 회전속도계의 RPM(Revolution Per Minute)을 의미한다. 자동차의 출력과 속도에 영향을 주는 지표 수치로서 이용되는 데이터를 의미한다.
- **브레이크 신호:** 브레이크 신호는 상용차를 운행하는 운전자가 브레이크를 밟았는지를 나타내기 위환 데이터를 의미한다.
- **차량 위치:** 차량 위치는 위치추적장치(GPS)에서 측정한 상용차의 위치를 의미한다. X, Y 좌표 값으로 데이터를 표현된다.
- **GPS 방위각:** 방위각이란 방향을 각도로 표현한 것으로 정해진 기준 벡터에서 목적(측정) 벡터까지의 시계 방향으로 측정한 각도를 의미한다.
- **가속도:** DTG 시스템 내에 가속도 센서가 존재하고, 가속도 정보를 실시간으로 측정할 수 있을 경우, 매초마다 X, Y 축 가속도를 기록하도록 선택적으로 권고하고 있다.
- **연료소모량 및 연비:** 연료소모량은 하루동안 소모된 연료의 양 혹은 DTG 시스템이 탑재된 이후 운행이 시작된 시점부터 소모된 연료의 누적 양으로 구분되어 정의된다. 리터 단위(소수점 둘째 자리까지 측정)로 측정/기록하게 되어있다.

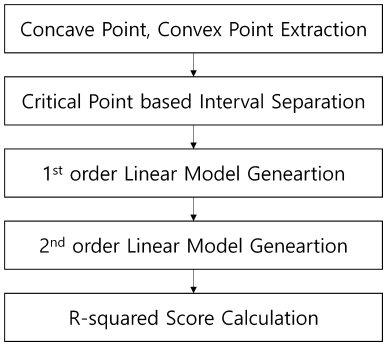
Ⅲ. DTG 데이터 보안 요구사항 분석

"Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles"[2], "UNECE Regulation No.155 - Cybersecurity Regulation" [3], NIST의 보안 관련 표준 문서[4]를 바탕으로 DTG 데이터 관련 보안 요구사항을 정리하여 설명한다.

- 외부 서버와의 이동무선통신을 통해 운행기록정보를 실시간으로 보고하는 DTG의 경우에 TLS (Transport Layer Security) 등의 통신 보안 메커니즘을 활용하도록 해야 한다.
- 블루투스를 사용하여 모바일 기기에 운행기록정보를 전송하는 DTG는 비정상 접근에 대비한 기기 인증 및 접근제어 메커니즘을 제공해야 한다. 블루투스 버전마다 사용가능한 여러 보안 모드가 존재하고 특정 모드에도 서비스 레벨을 지정하여 다른 방식으로 보안을 적용할 수 있다. 자세히, 블루투스 4.1 기기의 경우, 보안모드 4(레벨 4) 사용이 권장되고, 블루투스 2.1 기기의 경우, 보안모드4(레벨 3) 사용이 권장된다. 마지막으로 블루투스 2.0 이전 기기의 경우, 보안모드3 사용이 권장된다.
- DTG에 디버그 포트, JTAG 포트 등의 디버깅 인터페이스가 존재하는 경우, 인증된 외부기기만이 해당 인터페이스에 접근할 수 있도록 제어되어야 한다. 예를 들어, USB, UART, JTAG 등 입출력포트의 콘솔 접속 시, 비인가된 접속을 방지하기 위한 아이디/패스워드 기반 인증 기능을 구현하도록 한다.
- DTG가 기록하는 운행기록정보들과 그 외 개인정보 등의 민감한 정보들은 중요도에 따라 암호화 처리되어야 한다. 이때 암호화 처리에 걸리는 시간이 DTG 기록 성능 최소 요구조건을 만족하는 데 영향을 주어서는 안 된다.
- DTG 데이터의 암호화를 적용한 경우, 외부기기로의 반출 시에도 암호화가 적용된 채로 데이터가 전달되어야 함. 외부기기에 복호화 키가 있어 암호화된 데이터를 복호화할 수 있어야 하며, 암/복호화 키는 정품 기기 혹은 DTG 및 외부 반출용 외부기기 제작사 등에 권한이 있는 관련자에게만 배포/관리되어야 한다.
- DTG는 검증된 알고리즘과 안전한 크기의 보안 키를 활용하여 암호화를 수행해야 한다. NIST SP 800-175B [4]에 소개된 검증 암호화 알고리즘과 안전한 키 사이즈 목록이 나타나 있으며 해당 알고리즘에서 선택하여 사용한다.
- 이미 기록된 DTG의 운행기록정보가 허가되지 않은 방법에 의해 수정/변경되었을 때 이를 확인할 수 있도록 무결성 검증 기능을 갖추고 있어야 하며, 무결성 검증 처리(MAC 토큰 생성 등)에 걸리는 시간으로 DTG 기록 성능 최소 요구조건이 만족하지 않는 상황에 발생해서는 안 된다.
- DTG는 검증된 알고리즘을 활용하여 무결성 검증을 수행해야 하고, HMAC (Hash Message Authentication Code)중 FIPS 180-4 [5]에서 권고하고 있는 알고리즘은 SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256이며, FIPS 202에서는 SHA3-224, SHA3-256, SHA3-384, SHA3-512와 SHAKE128, SHAKE256의 사용을 허용하고 있다. 안전성이 검증된 해시 알고리즘을 기반으로 하는 HMAC 알고리즘을 사용하여 무결성 검증을 수행해야 한다.
- DTG 기록 데이터의 무결성 검증을 위한 MAC 등의 토큰을 생성한 경우, 외부기기로 데이터를 반출 할 때 무결성 검증용 토큰도 함께 전달되어야 하며,외부기기에 무결성 검증 키가 있어 전달받은 데이터와 무결성 검증 토큰을 이용하여 데이터 훼손 여부 파악을 할 수 있어야 한다. 보안 키는 정품 기기 혹은 DTG 및 외부 반출용 외부기기 제작사 등에 권한이 있는 관련자에게만 배포/관리되어야한다.

Ⅳ. DTG 데이터 디지털 포렌식을 위한 데이터 유추 방안

다양한 DTG 기록 정보들 중 차량속도, 누적거리량 등과 같이 시간 순으로 연속된 데이터가 선형적으로 증감하는 데이터를 식별하기 위한 방법을 소개한다. 선형 모델 기반 데이터 의미 분석 방법론의 세부 과정이 [그림 1]에 정리되어있다. 주어진 일련의 시계열 데이터가 존재할 때 전체 시퀀스를 세부 구간으로 나눈다. 시퀀스 데이터를 단위구간으로 나누는 과정이라 할 수 있다. 페달을 밟아 속도를 증가시키거나, 감소시키는 시간에 맞추어 구간을 나누고자 시퀀스 데이터를 시간 순의 그래프로 나타내고 표현된 그래프의 Convex 혹은 Concave 포인트를 찾아 각 구간의 시작



〔그림 1〕 선형모델 기반 데이터 의미 분석 흐름도

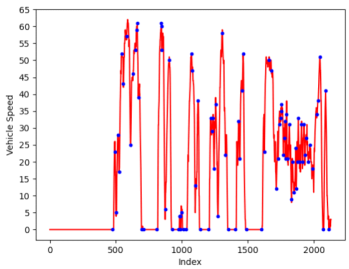
과 끝으로 지정한다. 구간이 나뉘면 구간별로 별도의 선형 모델을 생성한다. 1차, 2차 모델을 각각 생성하고 학습 R-sqaured 스코어를 계산[6]하여 추후 임계값과의 비교에 이용한다.

만약, 임계치 이상의 구간이 연속적으로 다수 (전체 구간 대비 90% 이상) 나올 시 해당 분석 데이터를 차량 속도 혹은 누적거리량 등의 데이터로 분류한다.

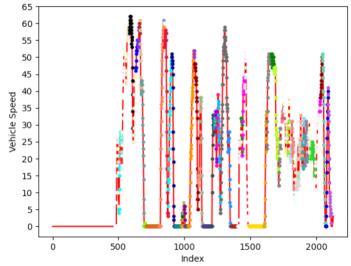
이부 세부절에서는 실험데이터 35분가량 운행된 상용차의 디지털운행기록장치의 운행 데이터를 이용하여 식별 흐름에 맞추어 실험한 내용을 차례로 다음 세 부절에서 설명한다.

4.1. 선형 모델 분석 대상 데이터 구간 분할

전체 차량 속도 시계열 데이터를 선형 모델 생성 대상이 되는 단위 구간으로 분할 하기 위해 가장 먼저 그래프로 표현된 시계열 데이터로부터 Critical 포인트 (Concave 포인트, Convex 포인트)를 찾아내는 일을 수행해야 한다. 확인된 Critical 포인트가 분할된 구간의 시작/끝 지점이 된다. 차량 속도 실험에서 찾아낸 Critical 포인트와 구간 분할 결과는 [그림 2]과 [그림 3]에 각각 나타나 있다. [그림 2]의 그래프의 청색으로



〔그림 2〕 Critical 포인트 식별 결과



〔그림 3〕 구간 분할 결과(다른 색은 다른 구간 의미)

표현된 점이 Critical Point를 의미하고, [그림 3]에서는 분할된 구간별로 색을 달리하여 각 이벤트 데이터(차량 속도 데이터)를 점으로 나타내고 있다. 총 91개의 Critical Point가 확인되었으며 이를 이용하여 전체 시계열 데이터를 나눈 구간의 개수는 90개이다. 시각화된 각 그림의 그래프를 보면 적절하게 구간이 나뉜 것을 확인할 수 있다.

4.2. 1,2차 선형모델 생성

시계열 데이터의 구간이 식별되면, 선형회귀 분석을 통해 직선을 따르는 형태의 데이터 포인트을 나타내기 위한 1차 선형 모델, 2차 곡선을 따르는 데이터 포인트를 나타내기 위한 2차 선형 모델을 각각 생성한다. 구간 별 모델 생성 결과 예시는 아래 [표 2]와 같다.

〔표 2〕 선형모델 예시 (x: 시간, y: 차량 속도)

구간	1차 선형모델	2차 선형모델
1	y=2.05*x^1	y=- 0.3*x^1 + 0.16*x^2
2	y=- 2.47*x^1	y=- 0.12*x^1 - 0.26*x^2
…	…	…

4.3. 구간 별 정합성 계산 결과

구간 별 1차/2차 모델이 실 데이터를 얼마나 잘 나타내는 지를 확인하기 위하여 모델 별 정합성 정도를 나타내는 R-squared 스코어 값을 계산한다. 해당 지표는 0-1 사이 값을 갖으며 데이터와 모델의 정합성이 높을수록 1에 가까운 R-squared 값을 갖는다. [표 3]에 나타나 있듯이 1차 선형 모델의 R-squared 값의 최소/최대/평균/분산/중앙값은 각각 0.006, 1.0, 0.81, 0.04, 0.86이며, 2차 선형 모델의 경우 최소/최대/평균/분산/중앙값은 0.097, 1.0, 0.91, 0.019, 0.95로 계산되었다.

〔표 3〕 R-squared 스코어 통계

	최소	최대	평균	분산	중앙값
1차	0.006	1.0	0.81	0.04	0.86
2차	0.097	1.0	0.91	0.019	0.95

평균값이 1에 매우 가깝고 특히 2차 선형모델의 경우 0.91로 매우 정합도가 높은 결과가 도출되었음을 알 수 있다.

운전자가 차량 속도를 정확히 일정하게 증가시키기 위해서는 액셀러레이터 페달에 가하는 압력을 정확하게(Consistently) 일정하게 가해야 하지만 그렇지 못한 경우가 대부분이기 때문에 가속도의 변화가 생기기 마련이며 이에 따라 2차 선형모델이 더 좋은 성능을 보이게 된 것으로 예상한다.

R-squared 스코어 값이 모두 계산 되면 추후 분류(데이터 식별)가 가능하도록 데이터 종류 별로 임계치를 설정하는 작업을 수행하면 식별 알고리즘이 완성된다. 우리 실험에서는 0.5를 임계치로 설정할 때 1차 선형 모델은 91%의 구간이 임계값을 초과하였고, 2차 선형 모델은 97%의 구간이 임계값을 초과하였다. 비휘발성 메모리의 특정 데이터 영역의 구간 별 선형 모델을 만들었을 때 대략 90% 이상 구간이 0.5 이상의 R-squared 값을 갖는다면 대상 정보로 판단하는 것이 가능하다는 것을 의미한다.

Ⅴ. 결 론

본 연구에서는 기존 문헌들을 조사하여 디지털운행기록 장치 데이터 보안 요구사항들을 확인하였다. IoT 기기 등의 일반적인 임베디드 시스템 내 데이터 보안의 요구사항과 크게 다르지 않음을 알 수 있다. 기본적인 보안에 대한 배경 지식과 기술적 지원이 있으면, 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보장할 수 있을 것으로 보인다. 더불어, 운행 데이터 종류 식별을 위한 간단한 실험적 사례 분석 결과 1/2차 선형식을 활용하여 비교적 간단하게 차량 속도를 확인해 낼 수 있음을 알 수 있고 더 나아가 그 외의 비슷한 성격을 갖는 주행거리, 누적 거리, 가속도 등의 데이터에도 적용해 볼 수 있을 것으로 기대한다.

참 고 문 헌

[1] eTAS 운행기록분석센터 디지털 운행기록장치 표준 사양 개정(안), https://etas.kotsa.or.kr/etas/frtf0100/goDetail.do

[2] Klinedinst, D. (2020). Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles.

[3] UNECE Regulation No.155 - Cybersecurity Regulation, https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[4] Barker, E. (2016). Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms. NIST special publication, 800-175B.

[5] Dang, Q. H. (2015). Secure hash standard.

[6] Miles, J. (2005). R squared, adjusted R-squared. Encyclopedia of statistics in behavioral science.

〈저 자 소 개〉

김 태 근 (TaeGuen Kim)

종신회원

2011년 2월 : 한양대학교 컴퓨터전공 졸업

2013년 2월 : 한양대학교 컴퓨터소프트웨어학 석사

2018년 8월 : 한양대학교 컴퓨터소프트웨어학 박사

2018년 8월~2021년 2월 : 현대자동차 책임연구원

2021년 3월~현재 : 순천향대학교 정보보호학과 조교수

<관심분야> 인공지능 보안, 차량보안, 악성코드 탐지