데이터 무결성 제공을 위한 클라우드 기반의 차량용 블랙박스 시스템 설계

, 김보경*, 조수빈*, 백혜란*, 정선제*, 최영준*, 오석윤**, 이경현*
*부경대학교 IT융합응용공학과
**부경대학교 대학원 정보보호학과
e-mail:{sakdqt, shfo2020, adslgo4, tnqls1044, cyj0104, laol1, khrhee}@pknu.ac.kr

System design for vehicle black box data integrity provision of cloud computing base

Bo-Kyung Kim*, Hye-Ran Baek*, Su-Bin Jo*, Sun-Jae Jung*, Young-jun Choi*, Seok-Youn OH**, Kyung-Hyune Rhee*
*Dept of IT Convergence and Application Engineering, Pukyong National University, Korea
**Dept of Information Security, Pukyong National University, Korea

요 약

차량용 블랙박스는 영상, 음성 및 자동차의 주행정보를 저장하는 매체로서 저장되는 데이터를 통해 차량 접촉사고 시 운전자의 과실여부를 판단할 수 있는 중요한 장치로 최근 자동차 시장에서 많은 주목을 받고 있다. 그러나 현재 차량용 블랙박스는 단순히 주행 데이터를 저장만 하고 있어 법적인 근거 자료로 활용되기 위해서는 데이터에 대한 무결성 보장을 제공하는 기능이 없는 상황이다. 블랙박스에 저장된 데이터는 공격자에 의해 위, 변조될 위험이 존재함으로 본 논문에서는 보다 안전한 환경에서의 무결성 보장을 위해 클라우드 컴퓨팅 환경에서의 무결성을 제공하는 시스템을 설계 한다.

1. 서론

일반적으로 Event Data Recorder (EDR)로 알려져 있는 블랙박스 장치는 비행기에 장착되어 항공기의 추락이나 대형 참사 등으로 동체가 거의 소멸되었을 때, 사고의 원인 규명에 결정적인 역할을 하는 장치로 사용되어 왔다. 이러한 개념을 차량에 적용한 것이 차량용 블랙박스 이다. 최근 차량용 블랙박스는 사고 시점 전, 후 일정시간 동안의 상황을 기록하여 원인 규명이 어려웠던 교통사고를 보다 정확히 파악할 수 있게 해준다는 장점으로 각광을 받고 있다. 하지만 현대의 차량용 블랙박스는 데이터를 기록만 할 뿐이며 의도직인 데이터 위·변조를 확인하기 위한 무결성 보장이 되고 있지 않으므로 법적 증거 자료로서의 증거능력을 확실히 신뢰 할 수 없다. 따라서 본 논문에서는 차량용 블랙박스에서 수집되어 저장된 데이터가 법적인 근거 자료로써 증거능력을 충분히 가지도록 데이터의 무결성 증명을 위한 기법을 제안하고자 한다.

2. 차량용 블랙박스 작동

제안에 들어가기에 앞서 차량용 블랙박스는 어떠한 방식으로 작동하는지 알아보도록 하겠다.

2.1 사고 감지

대표적인 방법은 블랙박스의 가속도 감지기를 통해 얻을 수 있는 충돌 감지에 적합한 물리량을 선정하고 기준인 임계값을 두어 임계값 이상의 수치가 감지되면 사고로 인식 한다. 이때, 충돌과 충돌이 아닌 유사상황을 신뢰성 있게 판별하는 기술은 기준 물리량 선정과 임계값 결정 또는 시간에 따른 변동 임계값을 이용할 경우 기울기를 정하는 것이 관건이 된다. 이외에 운전자의 수동 조작에 의해서도 충돌 감지를 할 수 있다.

2.2 데이터 저장

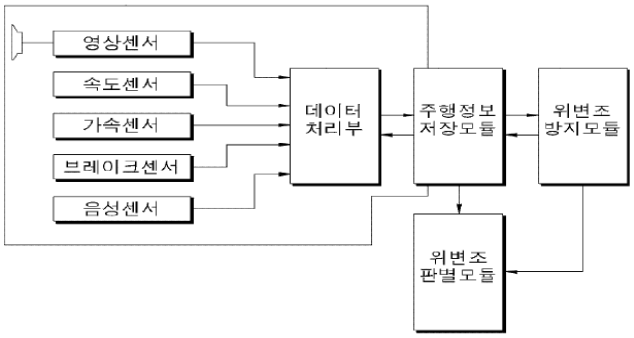
주기억장치인 SD메모리에 데이터(동영상, 음성, 주행속도 등)녹화가 시작되어 최대 기록 가능한 용량이 초과되면, 메모리의 처음으로 돌아가 순차적으로 덮어쓰는 방식으로 저장된다. 이 방식이 사용되는 이유는 일반적인 주행 중의 상시영상은 크게 중요하지 않기 때문이다. 따라서 평소에는 위의 방식으로 데이터를 저장하다가, 외부의 충격(사고)에 의하여 블랙박스에 내장되어 있는 G감지기가 자신이 기울어져 있는 상태 및 지면 방향을 감지하여 초기화되어 있는 G-감지기의 기준점보다 임계치 이상의 중력이 감지될 경우 이벤트 처리를 하고 그 시점을 기준으로 전, 후 약 10 ~ 20초를 추출하여 별도의 파일로 저장한다. 이외에도 운행기록, 음성, 속도, 궤도, 페달사용, 엔진 RPM, 전조등 작동 여부 등의 데이터를 저장할 수 있는 추가적인 기능도 존재한다.

3. 관련 기술 및 기존 연구

이번 장에서는 본 논문의 제안에 앞서 현재까지 차량용 블랙박스의 무결성 보장과 관련된 기술들에 대해서 알아보고, 또한 현재까지 관련된 무결성 특허들에는 어떤 것들이 있는지 알아본다.

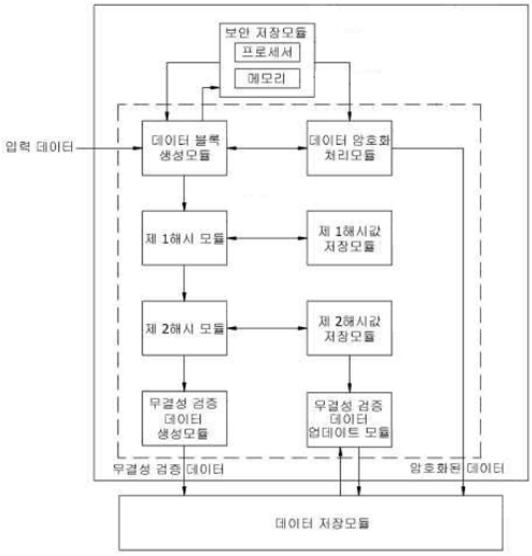
3.1.1 특허

차량용 블랙박스 데이터의 무결성 보장과 관련된 특허는 현재 국내에서 크게 2가지가 출시되었다. 첫째로 한국전자통신연구원에서 출원한 블랙박스 데이터의 위·변조 방지 장치 및 방법[2](이하 방안1)이 있다. 수집된 데이터를 저장하는 주행정보 저장모듈 및 설정된 암호화 체제로 수집된 데이터를 암호화하여 위·변조 판별 데이터를 생성하고, 생성된 데이터를 저장하는 위변조 방지모듈을 포함한다. 위·변조 방지 모듈은 설정된 암호화 체제를 제공하는 키 관리부와 블랙박스에 의해 수집된 데이터를 상기 암호화 체제로 암호화하여 위·변조 판별 데이터로 변환하는 암호처리부 및 상기 위·변조 판별 데이터를 저장하는 판별데이터 저장 부를 포함하는 것을 특징으로 한다.



(그림 1) 방안 1의 블록도

둘째로 ㈜아나스타시스에서 출원한 실시간 데이터의 무결성과 기밀성을 보장하기 위한 데이터 처리방법과 장치 및 이를 이용한 블랙박스 시스템[3](이하 방안2)이 있다. 입력 데이터 스트림을 미리 정의된 크기의 블록으로 분할하는 블록 생성 모듈, 사용자로부터 입력된 패스워드를 기초로 시드 값을 생성하고, 최초 데이터 블록값, 최초 데이터 블록에 관한 타임 스탬프값 및 인덱스값을 결합한 것에 대해 서명키에 의한 서명을 수행하여 초기 인증 데이터를 생성하는 보안 저장 모듈, 생성된 시드 값을 이용하여 데이터 블록을 암호화하는 암호화 처리 모듈이 있다. 처리된 데이터는 현재 데이터 블록에 관한 타임 스탬프값 및 현재 데이터 블록에 관한 인덱스값을 결합하고 해싱 함으로써 현재 데이터 블록에 관한 제1 해시 값을 생성하는 제1 해시모듈, 제1 해시 값을 결합하여 해싱하고 제2 해시 값을 생성하는 제2 해시모듈을 거친다. 생성된 제2 해시 값에 현재 데이터 블록 에 관한 타임 스탬프 값을 결합하여 데이터 블록에 관한 무결성 검증데이터 모듈을 통해 무결성 검증 데이터를 생성 후에 데이터 블록의 제1 해시 값과 직전 데이터 블록의 제2 해시 값을 결합하여 해싱하고, 직전 데이터 블록에 부가한 타임 스탬프 값을 직전 데이터 블록의 무결성 검증 데이터의 업데이트 값으로 하는 무결성 검증 데이터 업데이트 모듈을 포함하는 것을 특징으로 한다.



(그림 2) 방안 2의 블록도

3.1.2 기존 연구

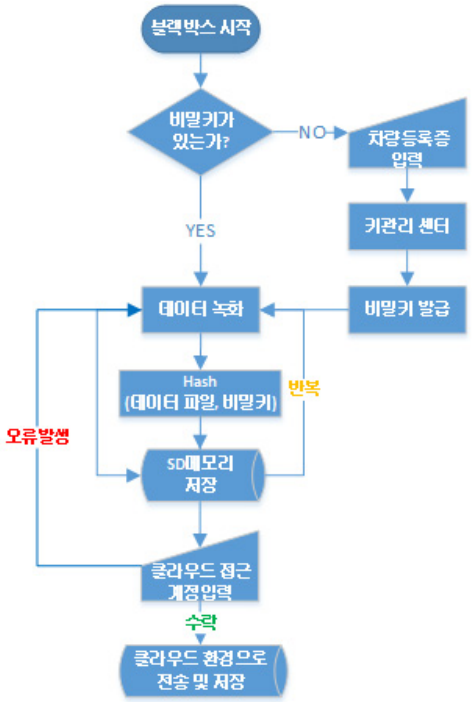
먼저 박대우, 서정만이 제안한 자동차의 블랙박스를 이용한 실시간 포렌식 자료생성 연구[4] 이 기법은 유비쿼터스 네트워크의 텔레매틱스 기술을 기반으로 자동차에 장착된 블랙박스에 IPv6에 의한 고유 주소를 부여하도록 설계하였다. 자동차 시동시에 블랙박스는 인증을 받아 작동하며 기록된 자료는 Wibro를 통해 끊임없는 위치 추적과 이동성 자료를 생성하고 암호화 되어 실시간으로 전송되며, 교통사고나 범죄에 사용된 경우 블랙박스에서 회수된 코드와 IP주소, 데이터베이스에 저장된 교통기록등의 자료를 비교하여 검증 및 인증을 통해 무결성을 확보 하도록 제안되어 있다.

다음으로는 김윤규, 김범한, 이동훈이 제안한 차량용 블랙박스 시스템을 위한 실시간 무결성 보장기법[5]은 데이터를 미리 정의된 크기의 블록으로 분할하여 데이터를 암호화하고, 최초 데이터 블록의 값과 타임 스탬프값, 인덱스값을 결합한 것에 대해 서명키에 의한 서명을 수행하여 초기 인증데이터(Initial Authentication Data;IAD)를 생성하고, 분할된 각 블록에 대해 무결성 검증 데이터를 생성 후 무결성 검증 데이터를 업데이트함으로써, 블랙박스 시스템에 저장되는 데이터의 무결성과 기밀성을 모두 보장할 수 있는 효과를 갖는다고 제안되어 있다.

4. 제안하는 무결성 보장기법

본 논문에서 제안하는 블랙박스에서 수집되고 저장된 데이터의 무결성 보장 기법은 이벤트가 발생하였을 때 생성되는 데이터 파일을 1차적으로 로컬 환경(블랙박스)에서 해싱 및 저장을 하고, 무선 네트워크 환경을 이용하여 클

라우드 컴퓨팅 환경으로 데이터를 전달하여 블랙박스의 물리적인 도난, 분실, 손상에 따른 데이터 위·변조 및 손실을 방지 하도록 시스템을 설계 하였다. 동작 순서는 아래(그림3)와 같다.



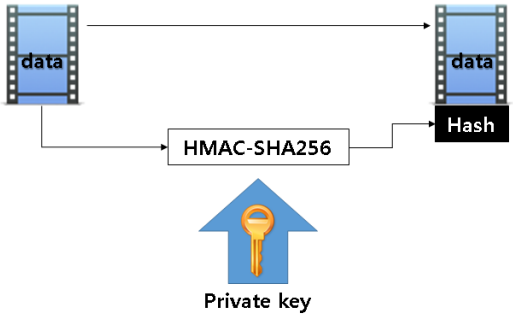
(그림 4) 블랙박스 동작 순서

4.1 비밀키 발급

블랙박스가 구동될 때 가장 먼저 무결성 보장을 위한 데이터 해시 과정에 사용될 기법인 HMAC(hash-based message authentication code)을 위한 비밀키가 존재 하는지 확인한다. 없다면, 클라우드 컴퓨팅 환경에 있는 키관리서버(KMS)에게 차량등록증을 제출하여 비밀키를 발급받는다. 이때 비밀키 발급을 위하여 차량등록증을 사용하는 이유는 사용자가 소속된 국가에서 합법적으로 운전을 하려면 반드시 등록 절차를 걸쳐야 하는데, 이 등록 절차는 국가기관이 직접 자동차 및 소유주의 신분과 정보를 확인하여, 문제가 없을 때 고유한 값의 등록증을 발급하기 때문에 개인키를 생성하기 위한 값으로 사용하기에 신뢰할 수 있다. 비밀키 발급이 완료되면 다음으로 데이터 녹화를 시작하고, 이미 비밀키를 블랙박스가 소유하고 있다면 즉시 데이터 녹화를 시작한다.

4.2 데이터 해시

이벤트 발생으로 저장된 데이터 파일과 발급받은 비밀키 값을 함께 사용해서 해시 알고리즘인 SHA-256으로 해시를 함으로 HMAC(hash-based message authentication code)을 구현한다. 이때 사용되는 비밀키는 사용자 자신과 키관리서버만이 알고 있음으로 공격자가 블랙박스의 기존 데이터들(데이터, 해시값)을 위·변조한다면 비밀키를 이용하여 무결성에 문제가 있음을 발견 할 수 있을 것이다. SHA-256은 256 bit 크기의 내부 상태를 가지며 256 bit의 결과 값을 가짐으로 현재까지 충돌을 발생 시킬 수 있는 알려진 공격 기법이 없기 때문에 데이터 무결성 제공 및 확인을 위하여 적합하다. 최종적으로 생성된 이벤트 데이터와 해시 결과 값은 같은 파일 이름을(날짜/시간) 가지고, 데이터와 해시값 구분을 위해 서로 다른 확장자로 저장된다. 설계된 해시 구상도는 다음과 같다.



(그림 5) 해시 구성도

4.3 데이터 전송

블랙박스에 저장된 데이터들은 사용자의 클라우드 컴퓨팅 환경으로 전송하기 위한 방법으로 TCP/IP 프로토콜을 사용한 소켓통신을 사용한다.[10] TCP를 사용하는 이유는 흐름제어, 혼잡 제어의 기능으로 전송되는 데이터의 손상을 막아주는 연결 지향적인 프로토콜로써 손상이 빈번하게 발생하는 가변적인 무선 네트워크 환경에서 데이터를 손상으로부터 안전하게 전달하기에 적당하다. 전송에 앞서 사용자가 클라우드 환경으로 접속하기 위한 계정정보(ID/Password)를 입력하고 확인받아 문제가 없다면 이벤트 데이터와 해시 결과 값을 따로 2회에 걸쳐 전송한다. 계정정보 확인은 각 클라우드 컴퓨팅 서비스에서 제공하는 API(application program interface)를 이용 하는 것이 시스템 개발과 사용자가 사용하기에 용이함으로 API를 사용 하도록 한다. API를 이용한 구현 방법은 각 서비스 제공사 마다 다르고 개발사 취향에 따라 얼마든지 다르게 구현 할 수 있음으로 본 논문에서는 다루지 않는다.

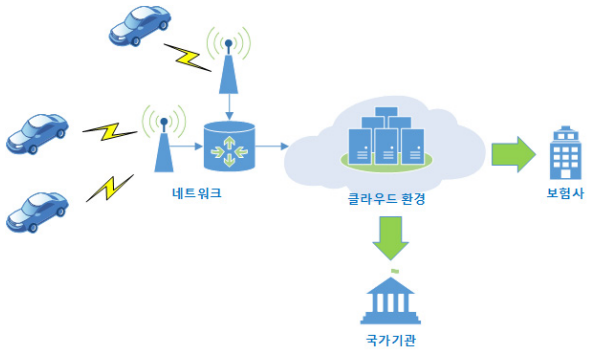
4.3 데이터 저장

사용자의 클라우드에서 받은 데이터와 해시 값은 생성된 날짜를 이름으로 가지는 폴더를 생성한 후에 하위에 읽기(Read)전용 속성으로 파일을 저장한다. 읽기전용으로 만드는 이유는 혹시 모를 사용자의 실수나 시스템의 오류로 데이터와 해시 값이 변경 되는 것을 방지하기 위해서다.

4.4 서비스

사용자는 다양한 무선 네트워크(3G, LTE, Wi-Fi, Wibro, etc)가 허용되는 범위 내에서 데이터를 클라우드 시스템으로 자동적 또는 수동적으로 전송할 수 있으며 반대로, 사용자는 무선 또는 유선 네트워크가 허용되는 범위 내에서

클라우드 시스템에 저장되어 있는 데이터와 해시 값에 접근하고 가져올 수 있다. 또한 필요에 따라 국가기관이나 보험 회사와 같은 곳에 근거 자료로 제출 할 수도 있을 것이다.



(그림 6)서비스 구성도 설계

5. 클라우드 보안

본 논문에서 설계한 클라우드는 IaaS(Infrastructure as Service)형식을 사용한다. 스토리지의 경우 사용자 인증 및 접근제어, 데이터 암호화를 통해 적절하게 방어 할 수 있으며 한국 인터넷 진흥원에서 만든 클라우드 서비스 정보보호 안내서[9]의 가이드 라인의 해당 부분을 요약하면 다음과 같다.

5.1 이용자 데이터 보호를 위한 정보보호 고려사항

(1)표준 암호화 알고리즘을 사용해야 하며, (2)데이터 암호화는 안전한 키 분배, 관리 메커니즘을 적용해야 하고, (3)암호 키는 기밀수준이 높은 데이터로 관리하고, (4)원거리 데이터 전송, 암호화 속도, 저장 용량 등 시스템 환경을 고려하여 적합한 알고리즘을 적용해야 한다.

5.2 이용자 데이터 보호를 위한 정보보호 고려사항

(1)서비스 연결을 승인하기 전에 모든 단말의 무선 접속은 규정된 절차에 따라 인증하고, 접속로그를 관리해야 하고, (2)무선 접속을 인증과 통신 세션의 기밀성·무결성을 보장하기 위해 암호 기술을 적용해야 하며, (3)모바일 단말의 통제 가 필요하다. 추가로 계정 분할 및 권한 최소화, 사용자 세션 관리등을 적용해야 한다.

6 결론 및 향후과제

현제 한국의 차량용 블랙박스는 최근 들어 언론이나 각종 매체들을 통해 많이 보편화 되었다고 보도되고 2000년도 초기와 달리 차량 구입 시 선택 옵션으로 반드시 들어가 있는 만큼 시장이 활성화 되어 있다고 볼 수 있다. 하지만 단순히 규정에만 맞춘 기술들로 제조되었고 데이터의 보안이나 무결성에 대한 연구 및 개발은 아직까지 미흡하거나 부족한 점이 많다. 저장되는 데이터의 무결성이 보장되지 않는다면, 데이터의 위·변조를 통해 피해자와 가해자가 바뀌거나 범죄에 악용될 소지가 있다. 따라서 본 논문에서는 현제 시중의 차량용 블랙박스들을 분석한 결과 현제의 블랙박스 시스템을 이용하여 저장되는 단일 데이터만으로는 무결성을 제공할 수 없다고 판단하여 데이터의 무결성 제공을 위한 시스템을 설계하였다. 추후 좀 더 구체적인 설계와 시뮬레이션을 통해 보다 개선된 방안을 제안할 것이며 또한 실질적인 구현을 통해 smart 사회구현에 도움이 되는 시스템을 개발할 예정이다.

참고문헌

[1] 김무섭, 최수길, 정치윤, 한종욱, “차량용 블랙박스 보안이슈 동향,” 한국전자통신연구원, 전자통신동향분석 제 27권 4호, pp.123-129, 2012.

[2] 공개특허,“블랙박스 데이터의 위변조 방지 장치 및 방법”, 10-2011-0040556, 특허청 2011.

[3] 등록특허, “실시간 데이터의 무결성 과 기밀성을 보장하기 위한 데이터 처리 방법과 장치 및 이를 이용한 블랙박스 시스템”, 10-1105205, 특허청.

[4] 박대우, 서정만, “자동차의 블랙박스 를 이용한 실시간 포렌식 자료 생성 연구,” 한국컴퓨터정보학회논문지,제 13권 1호, pp.254-260, 2008.

[5] 고윤규, 김범한, 이동훈, “차량용 블랙박스 시스템을 위한 실시간 무결성 보장기법,” 한국컴퓨터정보학회논문지, 제 19권 6호, pp.50-61, 2009.

[6] Datasheet 'LIS331DL', "MEMS motion sensor 3-axis - ±2g/±8g smart digital output “nano” accelero meter", 2.5, p.15.

[7] 박현식, “휴대전자 기기의 가속도 센서 기술,” 주간기술동향 통권 1288호, pp.3-4, 2007.

[8] James F.Kurose, Keith W.Rose 저 “컴퓨터 네트워킹 -하향식 접근”, 교보문고, Part 3, Chapter 5,pp. 111-125, 2007.

[9] KISA 안내·해설 제 2011-8호. “클라우드 서비스 정보보호 안내서 2011. 10