

Accident Information Based Reliability Estimation Model for Car Insurance Smart Contract

Soojin Lee[†] · Aeyoung Kim^{††} · Seung-Hyun Seo^{†††}

ABSTRACT

In order to reduce the time and cost used in insurance processing, studies have been actively carried out to apply blockchain smart contract technology to car insurance. However, by using traffic data that is insufficient to prove accidents, existing studies are being exposed to the risk of insurance fraud, such as forgery and overstated damage by malicious insurers. To solve this problem, we propose an accident data-based reliability estimation model by using both various types of data through sensors, RSUs, and IoT devices embedded in automobiles and smart contracts. In particular, the regression model was applied in consideration of the weight estimation according to the type of traffic accident data and the reliability estimation model trained according to various accident situations. The proposed model is expected to effectively reduce fraud and insurance litigation while providing transparency in the insurance process and streamlining it well.

Keywords : Blockchain, Reliability Estimation, Regression Analysis, Car Insurance, Smart Contract

자동차보험용 스마트 컨트랙트를 위한 사고정보 기반 신뢰도 산정 모델

이 수 진[†] · 김 애 영^{††} · 서 승 현^{†††}

요 약

최근 보험 처리과정에서 소요되는 시간과 비용을 절감하고자, 자동차 보험에 블록체인 스마트 컨트랙트 기술을 도입하는 연구들이 활발하다. 그러나 기존의 연구들은 사고를 입증하기에 미흡한 수준의 교통 사고관련 데이터의 활용으로 악의적인 보험자의 사고 위조, 손상 확대 등의 보험사기 위험에 노출되어 있다. 이를 해결하고자, 본 논문에서는 자동차에 탑재된 센서, RSU, IoT 기기 등을 통한 다양한 종류의 데이터와 차량용 스마트 컨트랙트를 이용하여 사고데이터 기반 신뢰도 산정 모델을 제안한다. 특히 교통사고 데이터의 종류 및 상태에 따라 가중치를 달리하고, 다양한 사고 상황에 따라 학습되는 신뢰도 산정 모델을 고려하여 회귀모델을 적용했다. 제안 모델은 보험 처리과정의 투명성, 보험 처리 과정의 간소화와 같은 기존 장점을 유지하며 효과적인 보험사기 차단, 보험 소송의 감소의 효과를 보일 것으로 기대된다.

키워드 : 블록체인, 신뢰도 산정, 회귀분석, 자동차 보험, 스마트 컨트랙트

1. 서 론

스마트 컨트랙트 기능을 제공하는 블록체인의 등장으로 기존 보험 산업의 과도한 유통마진, 정보의 비대칭성 등의 문제

를 해소할 수 있는 혁신적인 디지털 변화가 시작되었다[1]. 스마트 컨트랙트는 중개자 없이 사용자가 필요한 때에 적합한 상품을 계약하게 함으로써 유통마진을 해소하고 합리적인 보험요율을 책정함으로써 보험료를 감소시킬 수 있다. 또한 데이터 무결성 및 정보 공유를 기반으로 한 블록체인 기술을 통해 사용자에게 적합한 상품이 추천되도록 함으로써 정보의 비대칭성을 해소할 수 있다.

현재까지, 교통사고 처리를 위한 자동차 보험료 산정방식은 보험회사 직원이 직접 현장에 나와 사고가 난 자동차의 블랙박스 및 자동차의 손상 정도를 확인하는 것이었다. 그러나 이러한 방식은 블랙박스 영상 삭제 및 변조 등 악의적인 보험자로 인한 사고 위조, 손상 확대 등이 가능하다. 보험 처리과정의 맹점을 이용한 자동차 보험 사기는 보험 처리 과정에 따

* This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2020-2018-0-01417) supervised by the IITP (Institute for Information & Communications Technology Promotion).

** 이 성과는 2018년도 미래창조과학부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A2B6006903).

† 준 회 원 : 한양대학교 전자공학과 석사과정

†† 정 회 원 : 한양대학교 ERICA 공학기술연구소 연구교수

††† 종신회원 : 한양대학교 ERICA 캠퍼스 전자공학부 부교수

Manuscript Received : October 1, 2019

First Revision : December 2, 2019

Accepted : December 26, 2019

* Corresponding Author : Seung-Hyun Seo(seosh77@hanyang.ac.kr)

른 시간 및 인적 비용의 낭비, 과대 보험료 청구 등을 초래하여, 보험요율의 상향, 불필요한 보험료 지급 등으로 보험업체의 피해규모를 키우고 선량한 보험 가입자들의 보험료를 높인다. 실제로 금융감독원에서 제공하는 보험사기 통계를 보면 전체 보험사기 적발 인원들 중에서 자동차 보험에 해당하는 인원은 62%로 가장 높은 비율을 차지한다[2]. 블록체인의 특징 중 하나인 데이터의 무결성은 이러한 보험사기 가능성을 줄일 것으로 기대된다.

이에, 자동차 보험에 블록체인 기반 스마트 컨트랙트를 적용하고자하는 시도가 증가하고 있다. 대표적인 사례로 KasKo2go의 Go2solution[3]이 있다. Go2solution은 운전자의 자동차 사진 데이터를 근거로 자동차 손상 여부를 판단하고 스마트 컨트랙트를 통해 보험료를 지급한다. 그 결과, 기존 보험 처리 과정을 간소화하고 보험 처리 비용을 줄이고 효율적으로 보험료 책정을 하게 되었다. 그러나 여전히 사진 데이터가 보여주는 사고관련 사실을 입증할 수 있는 정보양이 부족하고 사고 입증에 대한 위조 가능성이 존재하여 교통사고와 자동차 손상 여부를 증빙하기 위한 추가적인 데이터가 요구된다.

최근 IoT 통신 기술 및 지능형 교통시스템(ITS: Intelligent Transport System)의 발달로, 차량-포그 컴퓨팅(Vehicular-Fog-Computing)[4] 환경이 현실화되면서 교통사고에 대한 객관적 판단을 위해 자동차에 탑재된 센서, RSU(Road Side Unit), 운전자 및 탑승자가 소지한 스마트폰 또는 IoT 기기 등이 수집한 데이터 활용이 블록체인 기반 차량용 스마트 컨트랙트에서 가능하게 되었다. 차량-포그 컴퓨팅 환경에서 수집된 데이터들은 사고 당시 상황을 객관적으로 담은 영상, 이미지 등을 포함하고 보험회사 서버로 실시간으로 전송되기 때문에, 보험료 산정을 위한 데이터 위변조 등의 사기 대응이 가능하다.

본 논문에서는 사고정보의 신뢰성을 제공하는 스마트 컨트랙트 기반 보험사고처리 모델을 고려하여, 각종 센서로부터 사고관련 데이터를 수집하고 사고정보에 대한 신뢰도를 신뢰 점수 및 신뢰등급으로 정량화할 수 있는 모델을 제안한다. 이를 위해, 스마트 컨트랙트 기반 자동차 보험료 산정 모델에 적용할 수 있는 교통사고 데이터의 종류를 분류하고, 체계화하였다. 보험사기용 허위 데이터 수집 예방을 위하여, 데이터의 수집 시간과 사고 발생 시점 간, 데이터의 수집 위치와 사고 발생 위치간의 차이 정도에 따라 해당 데이터가 미치는 교통사고 정보의 영향력을 수치화하였다. 이를 기반으로 다변량 학습 모델의 기본인 회귀모델[5]을 이용하여, 교통사고 관련 데이터의 종류 및 상태에 따라 데이터의 가중치를 달리하고 신뢰도와 신뢰 등급을 산정할 수 있는 신뢰도 산정 모델을 설계하였다. 교통사고 발생 시나리오를 구성하고 서울시 교통관련 공공 데이터와 공공데이터 포털의 데이터 셋을 이용하여 신뢰도 계산 모델의 효과성을 실험을 통해 분석한다. 마지막으로, 블랙박스 영상, 사진 등을 수집하는 과정에서 사고 주변에 위치했던 차량 운전자, 목격자의 적극적인 정보 제공을 유도하기 위해 블록체인 상에서 정보 제공에 대한 인센티

브 시스템을 적용했다. 인센티브 지급 내역, 잔고는 블록체인과 스마트 컨트랙트를 통해 투명하게 공개되어 중계자 없이 이해관계자와의 원활한 협의가 가능하게 된다. 운전자로부터의 영상, 사진 데이터 수집과 인센티브 지급, 보험금 산출 및 지급 과정을 자동차 보험용 스마트 컨트랙트 프로토타입을 이더리움 블록체인 플랫폼 상에서 스마트 컨트랙트로 구현하여 실현성을 보였다.

본 논문의 구성으로 2장에서 블록체인 기반의 자동차 보험 시스템 관련 연구를 소개하고 3장에서는 차량용 스마트 컨트랙트를 위한 사고정보 기반 신뢰도 산정 모델을 소개하고 이때 필요한 수집가능 사고 정보와 신뢰도 산정 방식에 대해 기술한다. 4장은 스마트 컨트랙트 구현 예시를 보인다. 마지막으로 5장은 제안 모델에 대해 결론을 짓는다.

2. 관련 연구

KasKo2go의 Go2solution은 모바일 어플리케이션과 스마트 컨트랙트의 활용으로 사용자가 보험 청구와 보험금 지불 과정을 빠르고 간편하게 진행하도록 한다. 사용자는 사고 후 생긴 자동차 손상 부분을 회사와 연결된 모바일 어플리케이션으로 찍어서 회사에 전송하면 보험회사는 이를 토대로 사기 여부를 결정한다. Go2solution은 보험 처리 과정 시간을 15분으로 단축했으나 운전자의 사진 데이터 위조, 사고 손상 확대와 같은 보험사기 범죄에 취약하다. 특히 사진 데이터는 사진의 각도, 조명 등 외부 환경에 따라 사고 정보가 누락되거나 확대된다. 운전자는 이미 보상을 받은 손상을 다른 외부 조건으로 촬영하여 이중보상을 받거나 작은 손상을 확대하여 촬영할 가능성이 있다. 따라서 사진 데이터만으로는 사고 내용에 대한 보험회사의 객관적인 판단이 어렵다.

Lambertu[6]은 자동차에 설치한 전자 장비들과 스마트 컨트랙트를 적용하여 on_demand형 보험서비스를 제시했다. 운전자는 모바일 어플리케이션을 통해 낮은 비용으로 보험 상품을 실행하거나 내용을 변경하도록 했다. 차량 내부 전자 장치들을 이용하여 탑승 인원 수, 안전 벨트 장착여부, 차량 위치 등을 감지하여 상황에 따라 지동으로 특정 보험을 실행한다. [5]는 운전자가 사고와 관련 없는 손상을 추가하지 못하도록 운전자가 운전을 시작하기 전에 자동차의 상태를 사진으로 찍도록 한다. 이는 일부 보험사기를 방지할 수 있더라도 운전자에게 물리적으로 번거롭고 비효율적인 추가 과정을 요구하여 비실용적인 서비스이다.

Bader[7]은 보험 처리 비용 절감을 위한 이더리움 기반 자동차 보험 정책 프레임워크(Car insurance Policy Framework : CAIPY)를 제안했다. 차량에 부착된 센서들의 데이터는 이상 행위 발생 시 스마트 컨트랙트를 통해 기록되고 보험회사는 이를 기반으로 보험 처리를 진행한다. 이 경우, 보험회사는 센서 데이터를 바탕으로 사고 발생의 진위여부 판단은 가능하지만 데이터의 신뢰도를 평가할 수 있는 방법이 없고, 피

해 손상 내용을 명확히 알 수 없어 보험금 산정을 구체적으로 하는 부분에 어려움이 있다.

자동차 사고 및 보험 모델에서 신뢰도 산정 방안은 차량 충돌 사고 재구성[11], 보험 고객 신뢰도를 기반으로 한 적정 보험료 산출[12] 등에 적용되고 있다. 특히 [12]에서는 고객의 보험금 청구 건수를 토대로 유효대수 법칙, 제곱근 법칙 등을 사용하여 신뢰도를 계산하였다. 그러나 이와 같은 이전 논문들에서 사고 데이터를 이용하여 사고 발생에 대한 신뢰도 측정 모델이 제안된 사례를 찾을 수 없다. 따라서 본 논문에서는 사고 정보를 통해 보험 청구에 대한 신뢰도를 산정하는 모델을 새롭게 제안하고자 한다.

기존 연구들의 문제점을 해결하기 위해, 본 논문에서는 차량-포그 컴퓨팅을 통해 RSU, 목격자의 웨어러블 IoT 기기, 자동차 센서 등에서 수집된 사고정보 데이터를 활용하여 보험 청구에 대한 신뢰도를 산정한다. 보험회사는 사고정보 기반 신뢰도를 바탕으로 다각도의 합리적인 판단을 할 수 있고 보험사기로 인한 피해를 줄인다. 또한 신뢰도에 따라 보험금이 산정되므로 보험회사와 소비자 간의 합의 과정이 원활하게 진행될 것으로 기대된다.

3. 차량용 스마트 컨트랙트를 위한 사고정보 기반 신뢰도 산정 모델

3.1 전체시스템 흐름

제안하는 사고정보기반 신뢰도 산정 모델이 적용될 수 있는 시스템의 전체 흐름도는 Fig. 1과 같다. 해당 시스템은 교통사고 발생 전후의 다양한 데이터들을 실시간으로 수집 및 분석하고, 스마트 컨트랙트를 통해 보험료를 실시간으로

지급하는 시스템이다. 본 시스템의 참여자는 보험계약자인 운전자, 목격자, 보험관계자, 교통경찰, 자동차정비사이며, 스마트 컨트랙트를 운용하는 앱, 교통제어용 IoT 기기 및 센서, 자동차 탑재 IoT 기기 및 센서, 드라이버 또는 목격자의 웨어러블 기기 및 센서를 포함한다. 해당 시스템은 프라이빗 블록체인 플랫폼에서 운용된다고 가정한다. 보험 회사 서버는 안전한 블록 배포, 채굴과 원장의 동기화를 위한 충분한 계산 능력과 메모리를 가지고 있으며 항상 블록체인 노드와 연결되어 있다. 서버의 오작동, 해킹으로 인한 블록체인 서버 운영의 지연을 방지하기 위해 여러 대의 보험 회사 서버를 사용할 필요가 있다. 또한 운전자, 목격자들은 어플리케이션에 연동된 블록체인 클라이언트 앱을 사용하여 자신의 계정과 개인키를 관리하고 스마트 컨트랙트를 실행할 수 있다.

이 시스템은 Go2solution과 마찬가지로 교통사고 발생 시 운전자가 스마트 컨트랙트를 운용하는 앱을 실행하여 교통사고 발생을 알림과 동시에 데이터 수집을 시작하고, 수집된 데이터를 근거로 스마트 컨트랙트에 의한 보험청구가 신청되어 수분 내에 보험료가 지급된다.

그러나 운전자가 스마트폰으로 촬영한 사진에만 의존하여 보험청구가 진행되는 Go2solution과는 달리, 본 논문에서 제안하는 시스템은 차량-포그 컴퓨팅 환경 내에서 RSU, 자동차 센서, 운전자 및 탑승자의 스마트폰, 목격자의 스마트폰 등 사고당시 수집된 사고관련 여러 데이터를 확보한다. 또한 수집된 데이터를 기반으로 신뢰점수를 계산하여 신뢰등급을 결정하고, 보험료 산정에 반영한다. 보험료 산정과정에서 유용하게 사용된 데이터를 제공한 목격자에게 보험 회사가 스마트 컨트랙트를 통해 인센티브를 지급한다. 받은 인센티브는 보험료 할인, 주유료 할인 등에 사용할 수 있다. 제안하는 시스템은 사고차량정비 관련 데이터도 수집하고, 이를 기반

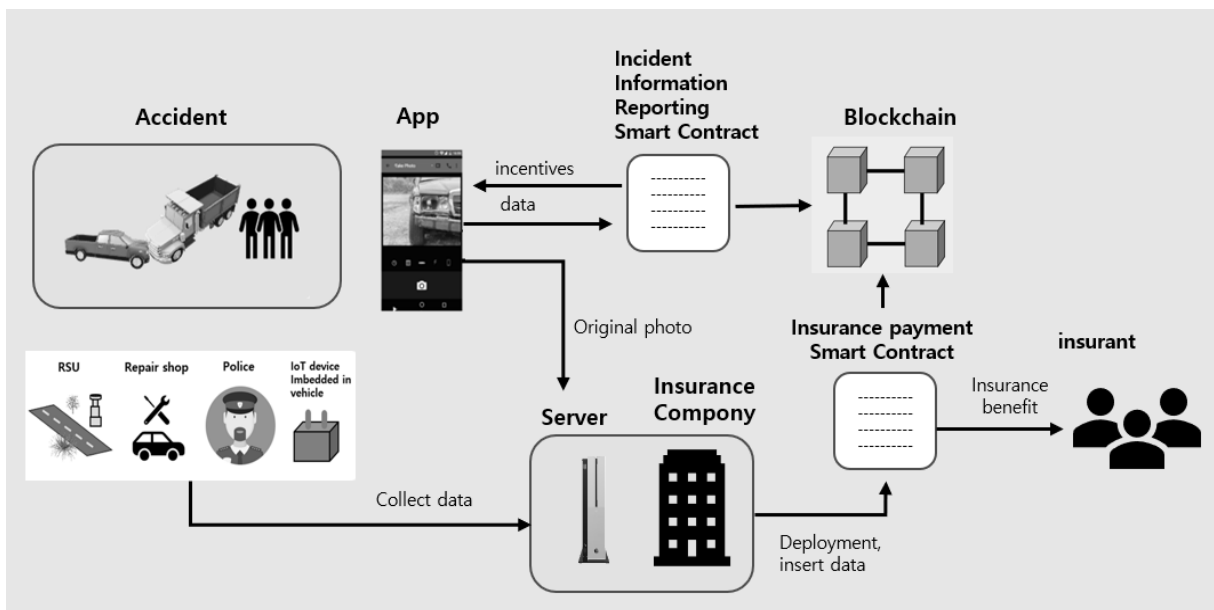


Fig. 1. Overall Model

으로 신뢰점수를 계산하고 지속적으로 운전자의 신뢰등급을 업데이트시킨다. Go2solution과 제안 모델을 비교분석한 Table 1을 통해 제안 모델은 Go2solution보다 다양한 객체들이 사고 증명에 참여하고 사진을 포함한 여러 경로의 데이터를 수집하고 이에 따른 보험금 산정 방법을 제시하는 것을 볼 수 있다.

3.2 수집 가능한 사고정보의 분류

오늘날의 IoT 추세는 모든 기기들이 인터넷으로 연결가능하며 고사양의 하드웨어를 탑재하는 등의 하이-엔드 IoT 기기로의 진화를 보이며 A-IoT (Advance IoT)로 불린다[8]. 이 A-IoT는 고사양 웨어러블기기 (Hi-End Wearables), 드론, 스마트 차량 등을 포함하며 Table 1과 같은 다양한 센서들을 탑재하고 있어 다양한 정보 수집이 가능하다[9, 10]. 교통사고와 같이 사고발생 위치 및 시간, 상황, 운전자 또는 차량 행위, 주변 환경 등의 복합적인 정보가 필요한 이벤트에서 이러한 Table 1의 센서들의 융합은 매우 중요하다. 교통사고 발생 시 이러한 센서들을 탑재한 A-IoT를 통해 보험계약자, 목격자/목격차량, RSU 등으로부터 수집 가능한 데이터는 Table 2와 같다. Table 2와 같은 사고정보는 사고수습, 보험료청구 등에 사용된다.

Table 1. Comparison between go2solution and Proposed Model

Categories	Go2solution	Proposed Model
Participant	driver, an insurance company	driver, witness, a group of insurance company, police, repair shop
Payment method	smart Contract	
Claim method	smart phone	
Proof of accident	picture	picture, video, Riot sensor data,
benefit evaluation	not mentioned	calculation using reliability regression equation

본 논문에서는 교통사고 E에 대한 사고정보의 신뢰성은 목격자, 시간, 거리 등의 영향을 받는다고 보고 이 요소들 간의 관계를 다음과 같이 정의한다.

$$\frac{\text{목적성 } W \times \text{관공성 } G}{E \text{ 대비 시간차 } T \times A \text{ 대비 거리차 } D} \propto \text{신뢰 점수 } CS \quad (1)$$

수집된 교통사고 정보를 정보사용 목적에 따라 보험료 청구를 위한 사고정보 I01, I01의 신뢰도 판별을 위한 사고정보 I02, 그리고 사후분석 및 판별모델의 지속적 학습을 위한 나머지 사고정보 I03로 분리한다. 분리한 사고정보 중에서 I02는 Table 2의 수집 가능한 사고정보에 대해 위 관계를 고려하여 I01 정보에 대한 신뢰점수를 계산하고 신뢰등급을 결

Table 2. Sensors for A-IoT

Categories	Sensors	Purpose		
		Action	Location	Environment
High-End Wearables	Infrared			○
	Magnetometer	○		
	Radar			○
	RFID	○		
	GPS		○	
	Accelerometer	○		
	Linear Acceleration	○		
	Gyroscope	○		
	Ultrasound			○
	UWB			○
	Bluetooth		○	
	Wi-Fi		○	
	Capacitive sensor			○
	GSR	○		
	Humidity sensor			○
	Light sensor			○
	Magnetometer			○
	Noise sensor			○
	Pressure Sensor			○
	Temperature Sensor			○
Thermistor			○	
Camera	○	○	○	
Consumer Drones	GPS		○	
	RGB-D sensor			○
	Ultrasonic sensor			○
	infrared			○
	Bluetooth	○	○	○
Smart Vehicles	Ultrasonic Ranging Devices			○
	Millimeter Wave Radar	○		○
	Infrared Ranging			○
	LiDAR			○
	GPS			○
	Vibration Sensor		○	
Camera	○	○	○	

정하는데 사용가능한 정보이다. Table 3은 I01로써 사용될 수 있는 데이터 목록들이다. Table 4와 Table 5에서 분류한 사고정보 I02를 기반으로 Equation (1)을 고려하여 전체 I01 정보에 대한 신뢰점수 CS를 계산하고 신뢰등급을 결정할 수 있다. 즉, I02는 I01의 내용이 얼마나 믿을만한 정보인지를 판별하는데 사용되는 정보이다.

Table 3. A-IoT Based Collectable Accident Information

	Type	Sensors or Devices
picture	I	Camera, RGB-D
video	A	Camera
message	M	Recorder
GPS	N	GPS
acceleration	N	Acceleration
heat	N	Temperature Sensor
vibration	N	Vibration Sensor

Table 4와 Table 5에서는 수집 가능한 정보들의 W, T, D, G을 나타내었다. Table 4는 운전자, 목격자/차량, 비공인 정비소에 의한 사고정보이며, 이 정보들은 사고시점 대비 시간차인 T와 사고지점 대비 거리차인 D에 크게 영향을 미치는 정보이다. 이 T와 D는 보험 청구를 위한 사고정보에 허위, 과장, 부정확한 내용이 포함될 정도를 반영한다. Table 5는 경찰서, 보험사, 공인정비소에 의한 사고정보이며, 이 정보들은 주로 교통사고 발생 후 사고수습 및 사고차량정비에서 수집되는 정보이다. 이 정보는 일정 시간 및 위치의 변동이 발생하지만 정보처리의 주체가 국공립 또는 인증기관을 통해 수집되는 공신력 있는 정보이다. 각 정보들은 이들이 갖는 중요도와 신뢰 요소 값의 따라 Equation (1)의 각 파라미터의 값에 비례되어 결정되고 그에 따라 신뢰점수 CS가 결정된다. 여기서 목격성 W은 목격자의 사진, 비디오 등 사고 당사자는 아니지만 사고를 목격한 객체로 부터의 데이터의 양, 범위에 따라 다르게 관공성 G는 해당 데이터가 제공된 객체의 관공성에 따라 차등적으로 결정된다.

Table 4. Accident Information by Driver, Witness, and Unauthorized Repair Shop (D-Document, N-Number, I-Image, B-Boolean, A-AV, M-Message)

	Type	W	T	D	G
driver's picture	I	++		+	-
driver's video	A	+++	+	+	+
driver's message	M	+	+		
accident vehicle's picture	I	++		+	
accident vehicle's video	A	+++	+	+	
accident vehicle's GPS	N			+	
accident vehicle's Acceleration value	N				+
The existence of accident vehicle's blackbox	B	+++			+
The existence of witness	B	++			+++
The number of witness vehicles which has imbedded blackbox	N	++	+	+	++
wtness vehicle's picture	I	++		+	+
witness vehicle's video	A	+++	+	+	
witness vehicle's GPS	N			+	
witness vehicle's message	M		+		
The existence of witness	B				+++
The number of witness	N				++
witness's picture	I	++		+	
witness's video	A	+++	+	+	
witness's message	M	+	+		
unauthorized repair shop's repair estimate	D		-	-	-
unauthorized repair shop's authority level	N				-

Table 5. Accident Information by Police, Insurance Company, and Authorized Repair Shop (D-Document, N-Number)

	Type	W	T	D	G
The number of RSU	N	++		++	++
The distance to RSU	N			+	
The number of data types which is provided by RSU	N	++	+	+	++
authorized repair shop's repair estimate	D			-	+
authorized repair shop's authority level	N				+
police's document	D	-			+++
investigator from insurance Company	D				+

보험계약자가 보험 청구를 위해 보험사에 제공하는 정보에 대한 신뢰점수는 이러한 Table 3과 Table 4의 각 사고정보를 신뢰점수계산식의 독립변수 $x_i (i = 1, \dots, n)$ 로 적용하여 계산한다.

3.3 사고정보 기반의 신뢰도 산정 방식

교통사고에 대한 즉각적인 보험료 지급 시스템의 효과적인 운용을 위해 제안하는 사고정보 기반 자동차 보험용 스마트 컨트랙트 운영 흐름은 Fig. 2로 나타낼 수 있다. 사고발생 직후 수집되는 데이터는 사고관련 정보의 신뢰성을 판단해줄 수 있으며, 사고수습 및 사고차량 정비 과정에서 수집되는 데이터는 보험 청구자의 사고처리 관련 행위의 신뢰성을 판단하는데 사용될 수 있는 정보이다. 제안하는 사고정보 기반 신뢰도 산정 방식의 구성단계는 크게 사고정보수집 단계, 신뢰점수계산 단계, 신뢰등급결정 단계이다.

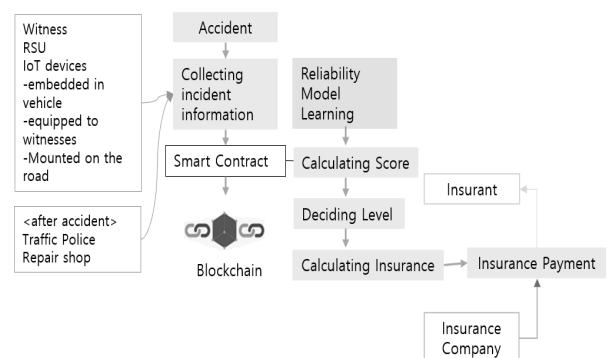


Fig. 2. Main Process

1) 사고정보수집 단계

사고정보는 사고즉시 수집되는 정보와 사후수습 및 정비 과정에서 발생하는 정보로 나누며, Table 2와 같이 다양한 센서, 기기, 주체자로부터 여러 종류의 정보로 수집되며, 이 정보를

사고 시점 및 지점 대비 변동정도를 고려하여 신뢰점수계산에 사용 가능한 정보를 Table 3 및 Table 4와 같이 추출한다.

2) 사고정보 기반 신뢰점수계산 단계

교통사고 E에 대한 신뢰점수의 계산을 위해 제안하는 방식은 사고정보에 대한 신뢰도를 신뢰의 영향력을 나타내는 계수 $a_i (i=1, \dots, n)$ 를 갖는 사고정보들 $X_A = [x_1, \dots, x_n]$ 의 선형결합으로 해석하자하는 것이며, 이를 식으로 나타내면 Equation (2)와 같다. 신뢰점수 계산을 위한 입력 값은 X_A 이며, 계산된 결과 값 y_A 는 교통사고 E의 사고정보에 대한 신뢰 점수이다.

$$y_A = a_1x_1 + a_2x_2 + \dots + a_nx_n \quad (2)$$

사고정보의 종류가 다양할수록 신뢰도 y_A 를 설명하는 변수가 많아지고, 그만큼 정보수집비용과 계산비용이 높아진다. 이에 신뢰점수 계산에 적용할 정보의 수 k 를 결정할 필요가 있다. 제안 모델에서는 k 개의 신뢰요소를 적용한 최적화된 신뢰점수계산식을 적용한다.

$$y_A = a_1x_1 + a_2x_2 + \dots + a_kx_k (k < n) \quad (3)$$

본 논문에서는 최적화된 신뢰점수계산식을 얻기 위해 사고정보를 다중회귀모델로 학습시킨다. 다중회귀모델을 통해 각 신뢰요소의 중요도에 따른 가중치를 계산할 수 있으며 후에 새로운 사고 데이터가 추가로 발생했을 때, 해당 데이터를 반영하여 회귀모델을 재학습함으로써 회귀식을 업데이트할 수 있다. 학습을 통해 산출된 회귀식은 각 신뢰요소들이 주어지면 간단한 연산으로 사고 신뢰도를 계산할 수 있어서 스마트 컨트랙트 내에서 구동가능하다. 다양한 교통사고 관련 정보를 독립변수로 설정하고 보험료 청구에 필요한 사고관련 정보의 신뢰점수를 종속변수로 설정한다. 신뢰점수를 잘 나타낼 수 있는 교통사고 관련 데이터와 각 데이터들의 가중치인 회귀계수로 회귀식을 구성하여 신뢰도를 산정한다.

회귀식의 최적화를 위해, 보험 청구를 위해 수집된 수많은 사고관련 정보 중에서 사고정보의 신뢰도를 파악할 수 있는 정보를 선별하고, 선별된 사고정보에서도 중복성이 높은 정보를 제외함으로써 효율적인 신뢰점수계산식을 구성한다. 본 논문에서 제안한 최적 신뢰점수계산식 구성 단계는 Algorithm (1)과 같다.

3) 신뢰등급결정 단계

신뢰등급표를 이용하여 전 단계에서 계산된 신뢰점수가 포함된 구간에 해당하는 신뢰등급을 사고정보의 신뢰지표로 사용한다. 이 신뢰등급을 스마트 컨트랙트의 보험료 산정에 반영하여 교통사고 상황에 최적화된 보험료가 지급되도록 한다.

Algorithm 1

Input: n 개의 샘플 $(X_1, Y_1), \dots, (X_n, Y_n)$

이때 $X_i = \{x_{i1}, \dots, x_{ik}\}, Y_i \in \{1, 2, 3\}$

x 는 각 신뢰요인 값, k 는 신뢰요인의 개수

Output: 계수 $B = \{\beta_1, \dots, \beta_k\}$. 상수항 ϵ , 회귀식 y

$$y = XB^T + \epsilon$$

$$y_n = \beta_0 + \beta_1x_{n1} + \dots + \beta_kx_{nk} + \epsilon$$

이때 k' 는 선택된 신뢰요인의 개수

1. 각 x_1, \dots, x_k 에 대하여 Y 에 대한 선형성을 검토한다.
2. x_1, \dots, x_k 에 대한 다중공선성을 검토하고 회귀식을 추정하여 후보 회귀식들을 선별한다.
3. 추정 회귀식들에 대해서 R-square, Adjusted R-square, C(p), MSE의 값을 검토하여 최소의 독립변수 k 개로 종속변수를 가장 잘 설명하는 최적 회귀식을 선택한다.
4. 선택한 회귀모델의 잔차의 산점도를 그려 검토하고 등분산성, 독립성, 정규성을 만족하는지 확인한다. 만약 만족하지 않으면 2번으로 돌아간다.
5. 선택한 최적의 회귀식을 최종 회귀 모델로 선택하여 신뢰점수 계산식으로 사용한다.

Table 6. The Criterion of Reliability Level

Level	Score	Meaning
1	30-39	The information is very reliable. very unlikely to include exaggeration / false
2	20-29	The information is reliable. low likelihood of exaggeration / false
3	10-19	The information is hard to believe. high probability of including exaggeration / false
4	0-9	The information is very incredible. very high likelihood of exaggeration / false

4. 신뢰평판모델을 적용한 스마트 컨트랙트 구현 예

4.1 사고 정보 데이터 수집 및 처리

제안 시스템은 회귀모델을 위한 변수 생성을 위해 한국 도로공단, 서울 열린 데이터 광장과 공공데이터 포털을 활용했고 데이터 셋을 구성했다. 실제 사고 관련 데이터와 가상의 허위 신고 시나리오 데이터를 적절히 혼용하여 65개의 샘플들을 생성했다. 회귀모델 분석을 위한 변수 설정은 다음과 같다. 최적화를 위한 실험 환경 및 적용 틀은 CPU Intel core i5, RAM #GB, R Studio이다.

- 종속변수 y : 시간 및 거리를 고려한 교통사고 정보들로 보험 청구에 사용되는 정보에 대한 신뢰점수
- 독립변수 $x_j (j=1, \dots, 4, k=4)$: 교통사고 정보 중에서 선별한 4가지의 신뢰요인

Table 7. Examples of Traffic Accident Dataset

Year	Date, time	minute	day/night	Day	Death toll	City	Location	Type	longitude	Latitude
2018	2018031708	0	day	Sat	1	Seoul	Gangnam	V2V	127.0486	37.52936
2018	2018071903	20	night	Thur	1	Seoul	Gangnam	V2V	127.0358	37.52871
2018	2018092023	50	night	Thur	1	Seoul	Gangnam	V2P	127.0298	37.49359
2018	2018010813	8	day	Mon	1	Seoul	Gangnam	V2P	127.055	37.48932

$$X = [x_1, x_2, x_3, x_4] \quad (4)$$

- x_1 = 목격자의 사진 수
= Witness_n
- x_2 = 사고지점에서 RSU와의 거리(최소거리)
= RSU_d
- x_3 = 사고지점에서 100m 이내 위치한 RSU 수
= RSU_n
- x_4 = 사고시점 대비 운전자 사진 촬영 경과시간
= Picture_m

실험 데이터는 2018년 1월 기준이며 강남구, 강동구, 강북구 지역을 대상으로 수집했다. 실제 사고 발생 시간과 위치를 파악하기 위해 한국 도로교통공단의 사망교통사고 데이터를 사용했으며 원본 데이터에서는 Table 7에서 볼 수 있다. 제공하는 목격자의 사진 수 x_1 는 사고가 발생했던 지역과 시간대에 해당하는 생활 인구수에 비례하여 최대 수가 50명이 되도록 목격자 수를 설정했다. 이때 심야시간(0시~6시)에는 사람들의 외부활동이 적을 것으로 가정하여 30%가량으로 줄여서 변수를 정했다. RSU에 대한 신뢰요인 x_2, x_3 은 실제 CCTV 설치 위치 데이터셋을 토대로 구성했다. x_2 의 경우, 사고 발생 위치와 가장 가까운 RSU와의 거리를 계산하여 변수 값을 정했고 x_3 는 사고 장소에서부터 100m 반경 이내에 위치한 RSU의 개수로 적용했다. 운전자 사진 촬영 경과시간 x_4 는 랜덤 샘플링하여 가상의 데이터를 생성했다. 이때 운전자의 사고 손상 위조를 방지하기 위해 30분으로 제한했다. 20개의 일부 샘플 데이터는 허위 신고 시나리오를 세워 위 방법론을 따르되 목격자 수는 5명 이하로 랜덤 샘플링하여 생성했다. Table 8은 설정한 변수의 정의이다. 이러한 독립변수를 갖는 회귀식 $Y = [y_1, \dots, y_{5i}]$ 은 다음과 같은 식으로 나타낸다.

$$y_1 = \beta_1 x_1 \quad (5)$$

$$y_{5i} = \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 \quad (6)$$

이때, 학습을 위한 종속변수 $y (= score)$ 의 샘플 데이터는 x_i 들의 65여개의 데이터를 육안으로 확인하여 Equation (1)에서 제안한 파라미터를 고려해서 신뢰점수를 부여하였고, 그 값의 범위는 {0, ..., 39}이다. 이러한 변수들에 대한 데이터 셋의 예는 Fig. 3과 같다.

Table 8. Variables Definition

variable	name	Type	Range	meaning
x_1	Witness_n	Range	[0, 50]	witness number
x_2	RSU_d	Range	[3.01, 329.21]	distance to RSU
x_3	RSU_n	Range	[0, 49]	RSU number
x_4	Picture_m	Range	[1, 30]	driver's photo time

```
> head(DF)
  witness_n RSU_d RSU_n Picture_m Score
1         12 12.83   37          7    39
2         49 96.25    3         10    39
3         10 24.95   32         12    38
4         17 21.36   15          5    38
5         26 82.60   11          3    37
6         17 31.00   22         17    37
```

Fig. 3. Examples of Dataset

4.2 사고 정보 기반 신뢰 모델 선정

먼저 교통사고 정보의 여러 요인 중에서 선별한 x_1, \dots, x_4 로 y 를 설명할 수 있는지 대략적인 선형성을 확인하기 위하여 y 에 대한 x_1, \dots, x_4 의 산점도를 확인한다.

Fig. 4의 산점도를 확인하면 y 에 대하여 변수 x_1, x_3 는 양의 상관관계를 갖고 나머지 변수들은 음의 상관관계를 갖는 것을 알 수 있다. 육안으로 보았을 때 변수 x_4 의 상관관계가 가장 약하다.

선형성을 확인한 후, 변수들 간의 다중공선성 문제를 검토하기 위해 각 변수의 분산팽창계수를 확인한다. Table 8를 보면 모든 변수들의 분산팽창계수는 4 이하로 다중공선성의 문제가 없다. 따라서 선택한 변수들을 그대로 사용하여 회귀식을 추정한다. 추정된 회귀식들 중에서 최적의 회귀식을 선택하기 위해서 각 회귀식에 대한 Adjusted R-Square, MSE, Cp를 비교한다. Adjusted R-Square는 독립변수가 하나씩 증가할 때마다 높아지는 정도를 보는데, 일정 수준으로 높아져 그 차이 값이 미미한 회귀식들을 대상으로 MSE와 Cp를 비교한다. Table 10과 같이 Adjusted R-Square 값이 0.9084인 변수 세 개인 회귀식부터 변수가 하나씩 증가해도 그 증가폭이 감소했다. 이는 최적 회귀식으로는 최소 변수의 개수가 세 개($k \geq 3$)임을 의미한다. 검토 대상 회귀식에 대해서 MSE 및 Cp는 가장 최소인 회귀식을 찾는다.

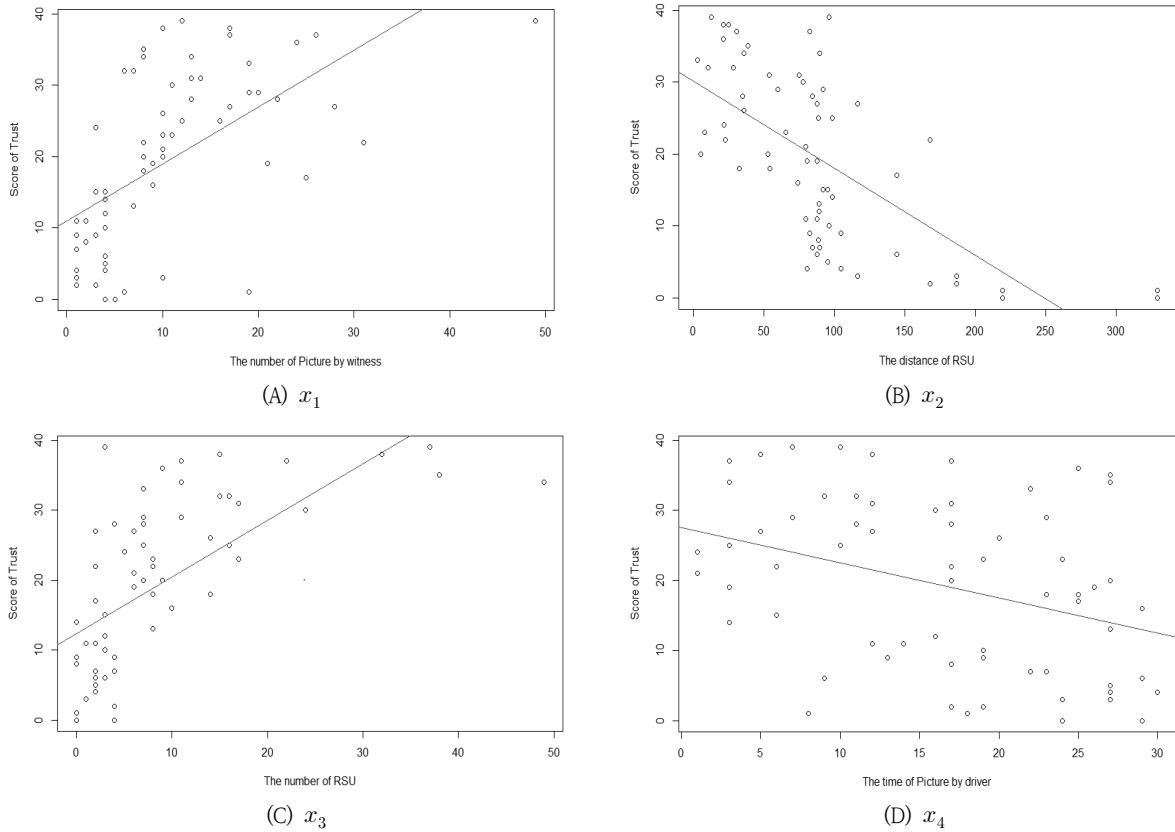


Fig. 4. Scatter Plots of x_1, \dots, x_4 for y

Table 9. Multicollinearity Review of x_1, \dots, x_4

Variation Inflation Factor			
x1	x2	x3	x4
1.052864	1.217278	1.216883	1.059473
<4	<4	<4	<4

Table 10. Adjusted R-squared Precedence Regression Model($k \geq 3$)

N	Multiple R-squared	Adjusted R-squared	MSE	C(p)	P-value	variables
1	0.8146	0.8053	2.15	259.62	< 2.2e-16	x_1, x_2, x_4
2	0.9128	0.9084	1.54	92.47	< 2.2e-16	x_1, x_2, x_3
3	0.9653	0.963	1.49	5.00	< 2.2e-16	x_1, x_2, x_3, x_4

그 결과 선택된 최적 회귀식은 Table 10의 모델 3으로 네 개의 변수 x_1, x_2, x_3, x_4 이고 추정 회귀계수는 0.674171, -0.091670, 0.519007, -0.321806이고 추정 회귀상수는 20.957399인 다음과 같다.

$$y = 0.674171x_1 - 0.091670x_2 + 0.519007x_3 - 0.321806x_4 + 20.957399 \quad (7)$$

제안 시스템에 좀 더 가벼운 즉 계산비용이 좀 더 저렴한

식을 적용하고 싶다면 Table 10의 모델 2와 같이 MSE 및 Cp가 최소와 별 차이가 없고 다중공선성 문제도 없으면서 변수의 수가 하나라도 더 적은 회귀식을 선택해도 좋다. 따라서 최적 회귀식은 두 번에 걸친 분석에 의해 변수 세 개만을 포함하는 모델로 다음과 같이 설정한다.

$$y = 0.737085x_1 - 0.095627x_2 + 0.496055x_3 + 15.620327 \quad (8)$$

이렇게 선택된 추정 회귀식이 최적 회귀식으로 결정되기 위한 마지막 단계는 선택된 회귀식에 대하여 회귀모델의 기본 가정(잔차의 등분산성, 정규성, 독립성)을 만족하는지 확인하는 단계로 잔차의 산점도를 이용하여 잔차 및 극단점에 대해 검토한다. Fig. 5는 위 선택된 추정 회귀식에 대한 잔차 및 극단점을 살펴볼 수 있는 차트이다, Fig. 5A는 잔차가 0을 중심으로 골고루 분포가 되어있으며 Fig. 5B의 경우에도 데이터들이 골고루 분산되어 위치한다. 또한 Fig. 5C는 샘플 데이터가 선을 따라 위치하고 있음을 보여주고 있으며 Fig. 6D의 차트에서도 잔차가 0을 중심으로 분산되어 분포되어 있다. 이는 선택된 회귀 모델이 선형성, 등분산성, 정규성을 만족하고 있음을 보인다. 따라서 이 차트는 몇 개의 이상치가 발견되지만 선택한 추정 회귀식이 회귀모델의 기본 가정을 충족하고 있다.

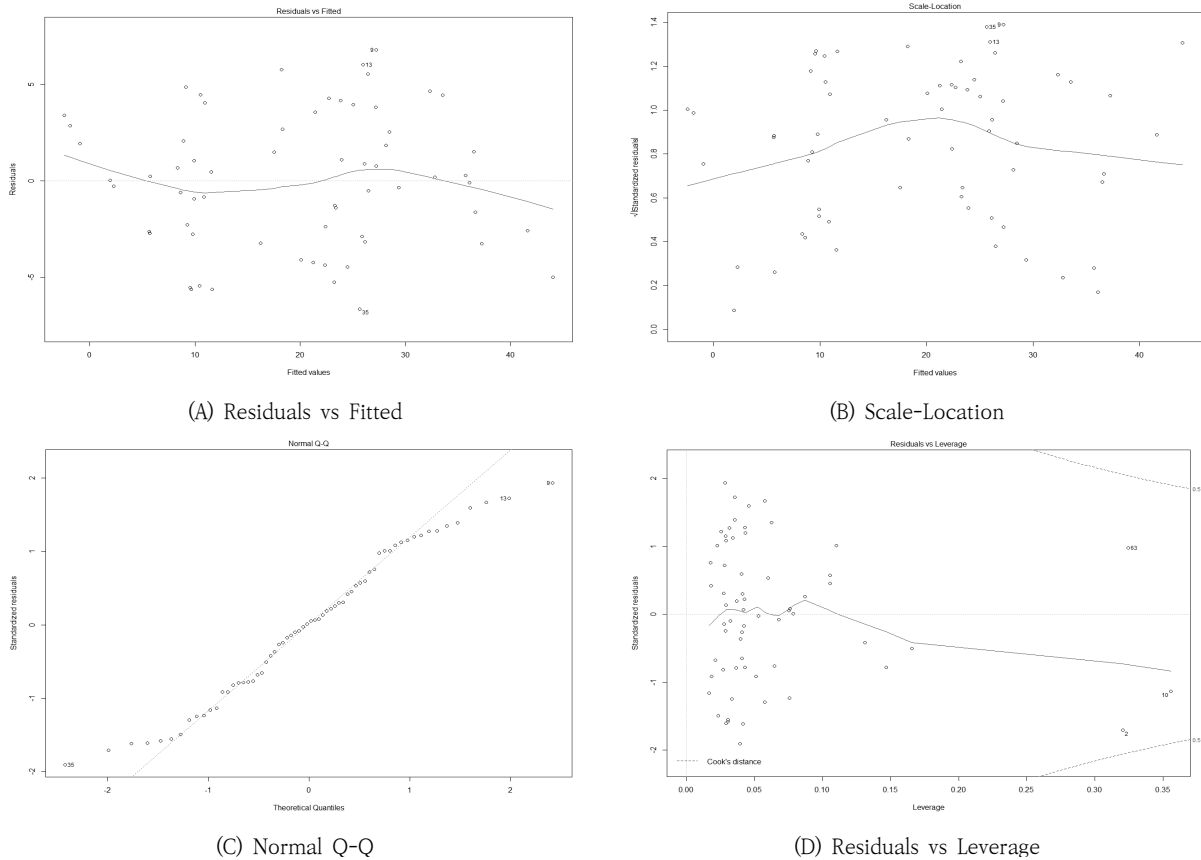


Fig. 5. Selected Optimal Regression Model

Table 11. Incident information based Insurance Claim Example

Scenarios	Reliability Score	Reliability Level	Insurance Payment Range(%)
There are RSUs at a distance of 13m from the accident location and there are 10 RSUs nearby, 15 witnesses provided photographic information.	30.39	4	100
There are RSUs at a distance of 30m from the accident location and there are 7 RSUs nearby, 10 witnesses provided photographic information.	23.59	3	75
Four witnesses provided photographic information when there was no RSU within 100m of the accident site and the nearest RSU was 103m.	8.71	1	25

마지막 검토까지 진행된 최적 회귀식은 제안 시스템의 스마트 컨트랙트에 적용되는 신뢰점수계산식이며, 이 식은 보험 계약자의 사고 발생 시 보험요청에 신뢰성을 부여해주며, 사고이후 업데이트된 사고 정보를 추가하여 위와 같은 과정을 재수행해 지속적인 학습이 가능하다.

4.3 스마트 컨트랙트 구현 예

스마트 컨트랙트 기반의 보험 계약자에게 발생한 사고 및 보험 청구 예는 Table 11과 같다. Table 11의 시나리오와 같이 사고가 발생할 때 보험계약자가 사용할 스마트 컨트랙트

앱은 이더리움 기반으로 구현하였다. 구현한 스마트 컨트랙트 앱은 사진 제보용 모듈, 보험금 지불용 모듈로 구성한다.

사고정보 제보 모듈은 Fig. 6과 같이 운전자 또는 목격자가 사고 현황의 촬영 정보를 보험사에 제공하는 모듈이다. 운전자는 일정 시간 내에 정보를 제공하여 정보의 조작 또는 누락을 방지하여 제공 정보의 신뢰성을 높이고, 목격자는 목격한 사고에 대한 정보 제공으로 해당 교통사고에 대한 신뢰성을 높여 주는 역할을 한다. 목격자의 참여를 유도하기 위해 보험회사는 사고정보를 검토한 후, 정보 제공에 대한 적극적인 활동에 대한 보상을 준다. 이 모듈의 주요 함수원형은 Table 12에서

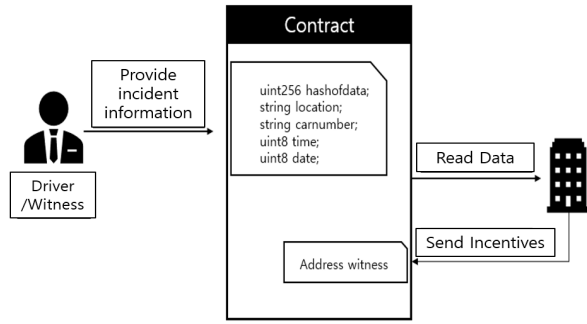


Fig. 6. Incident Information Reporting Process

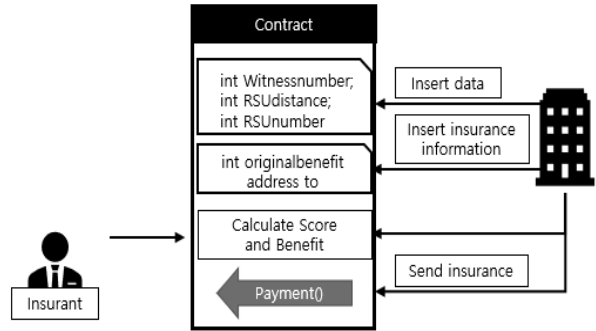


Fig. 7. Insurance Payment Process

Table 12. Accident Information Reporting Module

function	input	output	explanation
getPicture /getVideo	string witnessorDriver, uint256 _picture, string _gps, uint8 _time, uint8 _date, string _carnumber		Driver or witness inserts the information of the video
checkPicture /checkVideo		True/False	Insurance company reads photo or video information
TransferIncentive	address _to	True/False	Insurer pays Ether for witnesses
check Balance		this. balance	Insurance company views current contract balance

Table 13. Insurance Payment Module

function	input	output	explanation
assign Value	int _RSUlevel, int _witnesspicture, int _witnesscar, int _repairquote, int _min_driver		Insurer inserts each data value
initial benefit	int _originalbenefit, address _to		Insurer inserts original benefit and driver's address
Calculate benefit		int _Score, int _Trust level, int _benefit	Calculate reliability score, level and insurance according to regression stored in smart contract
Payment		True/False	Send ether to driver and self-destruction

설명한다. 사진, 동영상 정보는 블록에 저장하기에는 용량이 크므로 원본 정보는 모바일 어플리케이션이나 보험 회사 사이트에 올리고 스마트 컨트랙트를 이용할 때는 원본의 해쉬 값이나 URL을 이용한다.

보험금 지급 요청 모듈은 전송받은 사고 정보에 대해 신뢰 점수계산식을 이용하여 신뢰점수 및 신뢰등급을 결정하고, 산정된 신뢰등급을 고려한 사고 정보 기반 보험금을 산정하여 즉각적인 보험금 지급을 수행한다. 이 때 설계된 컨트랙트는 특정 사고 당사자들만이 사용하며 보험금이 지급되면 소멸된다. 보험금 내역이 투명하게 공개되는 블록체인의 특성으로 인한 사고 당사자들의 프라이버시 보호 문제를 위해 보험금 지급을 위한 사용자 계정은 일회성으로 사용한다. 컨트랙트 안에 저장된 신뢰점수계산식은 추가적인 사고 데이터에 따라 학습되어 새로 배포된 컨트랙트에 반영된다. 보험회사에서 산정한 신뢰요인 값들이 스마트 컨트랙트를 통해 블록에 저장되면 보험계약자는 그 값을 확인할 수 있다. 모듈을 통한 서비스의 구성은 Fig. 7과 같고, 이 모듈의 주요 함수원

형은 Table 13과 같다. 사고정보 제보용 스마트 컨트랙트와 신뢰점수 계산식 기반 스마트 컨트랙트의 운영 예시는 각각 Fig. 8과 Fig. 9에서 보인다.

본 논문에서는 이더리움 플랫폼을 예시로써 활용하여 스마트 컨트랙트를 수행하였으나 실제 보험 프로세스에 적용 시 보험 계약 조건과 블록체인 운영 방침에 따라 이더리움이 아닌 다른 플랫폼에서도 적용가능하다. 또한 이더 가치의 잦은 변동성을 고려하여 이더를 바로 보험금으로 사고 당사자에게 지급하는 것이 아니라 스마트 컨트랙트를 통해 보험금을 받을 수 있는 토큰을 발급하는 등의 방식으로 변형하여 본 제안 모델에 적용할 수 있다.

(A) The Accident Witness Sends a Original Picture to the Mobile App and Enters the Picture Information Via the GetPicture

(B) The Contents are Written to the Block in Log Form

```

{
  "from": "0x9dd1e8169e76a9225b07ab9185cc20a5e1ed44dd",
  "topic": "0x124b2a063195a71936a21b635cba1c6b3c329918721c6d644639b1cbd6f5a4e1",
  "event": "RecordPicture",
  "args": {
    "0": "0xCA35b7d915458EF540aDe6068d1Fe2F44E81a733c",
    "1": "witness",
    "2": "2453402134",
    "3": "127.0486,37.52936",
    "4": 1620,
    "5": 20190901,
    "6": "서울가H1324",
    "_provider": "0xCA35b7d915458EF540aDe6068d1Fe2F44E81a733c",
    "_identity": "witness",
    "_HashofPicture": "2453402134",
    "_gps": "127.0486,37.52936",
    "_time": 1620,
    "_date": 20190901,
    "_carnumber": "서울가H1324",
    "length": 7
  }
}
    
```

(C) The Insurance Company Checks the Picture and Sends Ether to the Witness

Fig. 8. Operation Example Using Accident Information Reporting Smart Contract

(A) The Insurance Company Enters the Trust Factor Values Into the Smart contract Based on the Collected Data

(B) The Insurer Enters the Account of the Accident Party and the Contractual Insurance Benefit

benefit	0: int256: 15
Score	0: int256: 23
Trustlevel	0: int256: 3

(C) The Insurance Company and Accident Parties Calculate the Reliability Scores, Trust Level, and Benefit and The Company Transfers the Ether to Accident Parties

Fig. 9. Operation Example Using Reliability Evaluating Smart Contract

5. 결 론

제안하는 사고정보 기반 신뢰산정모델은 교통사고 발생에 대한 즉각적인 보험처리를 위한 차량보험용 스마트 컨트랙트를 위한 신뢰평판모델이다. 다양한 데이터의 활용으로 보험 사기 방지에 큰 효과가 있으며 보험회사는 기존의 중계자가 수집하는 데이터보다 더 많은 데이터를 이용하여 사고의 신뢰도를 정밀하게 측정할 수 있게 되었다. 소비자 역시 자신의 보험 청구 내용을 증명할 수 있어 보험회사가 실제 책정해야 할 금액보다 보험금을 낮게 책정하는 경우를 막을 수 있다. 스마트 컨트랙트를 이용한 사고 신뢰도 선정모델은 한국 도로 교통공단, 경찰서 등의 공공기관들도 참여한다면 사고에 대한 빠른 대응과 효율적인 실시간 교통 서비스를 제공하는 데 도움이 될 것으로 기대된다.

References

- [1] H. Kim and H. Kwon, "Blockchain Adoption in the Korean Insurantee Industry: Review and Response," Korea Insurance Research Institute, 2018.
- [2] Financial Supervisory Service [Internet], <http://m.fss.or.kr:8000/insucop/>
- [3] kasko2go AG, "go2solution ICO White paper," 2018.
- [4] Flavio Bonomi, "Fog Computing and Its Role in the Internet of Things," 2012.
- [5] C. H. Mason and W. D. Perreault Jr., "Collinearity, Power, and Interpretation of Multiple Regression Analysis," *Journal of Marketing Research*, Vol.28, No.3, pp.268-280, 1991.
- [6] F. Lambertu, V. Gattescgu, C. Demartini, M. Pelissier, A. Gomez, and V. Santamaria, "Blockchains Can Work for Car Insurance: Using Smart Contracts and Sensors to Provide On-demand Coverage," *IEEE Consumer Electronics Magazine*, Vol.7, No.4, pp.72-81, 2018.
- [7] L. Bader, J. C. Burger, R. Matzutt, and K. Wehrle, "Smart Contract-Based Car Insurance Policies," *IEEE Globecom Workshops*, 2018.
- [8] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT (A-IoT) Applications," *IEEE Network*, 2019.
- [9] G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless Vehicle Security: Challenges and Future Research Opportunities," *Future Gener. Comput. Syst.*, 2018.
- [10] I. olusi, E. Marks, and M. Hallowell, "Wearable Technology for Personalized Construction Dafety Monitoring and Trending: Review of Applicable Devices," *Autom. Constr.* 2018.
- [11] Wach, W., M. Gidlewski, and L. Prochowski, "Modelling Reliability of Vehicle Collision Reconstruction Based on the Law of Conservation of Momentum and Burg Equations,"

20th International Scientific Conference TRANSPORT MEANS, 2016.

- [12] Y. Kim and H. Lee, "A Comparison Study for the Pricing of Automobile Insurance Premium Based on Credibility," *Communications for Statistical Applications and Methods*, Vol.17, pp.713-724, 2010.



이 수 진

<https://orcid.org/0000-0003-1690-8577>

e-mail : tssn195@hanyang.ac.kr

2019년 한양대학교 ERICA 전자공학부(학사)

2019년 ~ 현 재 한양대학교 전자공학과

석사과정

관심분야 : Blockchain Security, IoT Security



김 애 영

<https://orcid.org/0000-0002-9731-5011>

e-mail : aeyoung@hanyang.ac.kr

2000년 한신대학교 정보처리학과(학사)

2003년 이화여자대학교 컴퓨터학과(석사)

2012년 이화여자대학교 컴퓨터공학과

(박사)

2012년 ~ 2015년 이화여자대학교 컴퓨터공학과 연구교수

2016년 ~ 2016년 아주대학교 소프트웨어공학과 연구교수

2016년 ~ 2018년 국가수리과학연구소 암호기술연구팀

박사후연구원

2018년 ~ 현 재 한양대학교 ERICA 공학기술연구소 연구교수

관심분야 : IoT Security, Cryptographic algorithm and

application, Biometric-based Security, Post-

quantum cryptography



서 승 현

<https://orcid.org/0000-0002-1150-7080>

e-mail : seosh77@hanyang.ac.kr

2000년 이화여자대학교 수학과(학사)

2002년 이화여자대학교 컴퓨터학과(석사)

2006년 이화여자대학교 컴퓨터학과(박사)

2006년 ~ 2010년 금융보안연구원

주임연구원

2010년 ~ 2012년 한국인터넷진흥원 선임연구원

2012년 ~ 2014년 미국 퍼듀대학교 컴퓨터학과 박사후연구원

2014년 ~ 2015년 고려대학교 정보보호대학원 BK21+ 사업단

연구교수

2015년 ~ 2017년 고려대학교 세종캠퍼스 수학과 조교수

2017년 ~ 현 재 한양대학교 ERICA 캠퍼스 전자공학부 부교수

관심분야 : IoT Security, Blockchain Security, Cryptographic

Protocol Design and Application