

차량 인터넷에서 블록체인 기반 인증 프로토콜*

아흐메드 사비르(가천대학교), 압바스 수해일(University of Sharjah)
김도현(제주대학교)

목 차

1. 서 론
2. 차량 인터넷과 블록체인 개념
3. 차량 인터넷에서 블록체인 기반 인증 프로토콜
4. 결 론

1. 서 론

차량 인터넷(IoV : Internet of Vehicles)은 도로에서 지능형 서비스를 제공하고 운전자와 승객을 위해 다양한 애플리케이션을 지원하며 보다 효율적으로 지능형 교통 시스템을 달성하는 전통적인 차량 애드혹 네트워크(VANET : Vehicular Ad-hoc Networks)의 발전으로 부상했다. 차량 인터넷 및 차량 애드혹 네트워크 환경은 유익한 도로 서비스를 제공할 수 있도록 개방형 채널을 통해 무선으로 차량 네트워크의 서로 다른 통신 주체 간에 막대한 양의 데이터가 생성되고 교환할 수 있게 한다. 하지만 이는 공격자들을 유인하는 루트가 되거나 여러 유형의 보안 침입을 통해 네트워크를 위협할 수 있다. 본 논문에서는 보안 시

스템의 인증 부분을 대상으로 하는 동시에 사물인터넷(IoT : Internet of Things) 및 차량 애드혹 네트워크 환경에서의 블록체인의 효율성을 강조한다. 우선 사물인터넷 및 블록체인에 대한 자세한 배경 및 광범위한 보안 요구 사항, 차량 네트워크 공격 가능성을 소개한다. 다음으로, 사용된 기법, 네트워크 모델, 평가 도구 및 공격 대응 측면을 살펴보고, 사물인터넷 및 차량 애드혹 네트워크의 최근 블록체인 기반 인증 체계에 대해 집중적으로 비교하여 소개한다.

2. 차량 인터넷과 블록체인 개념

2.1 차량 인터넷 개념

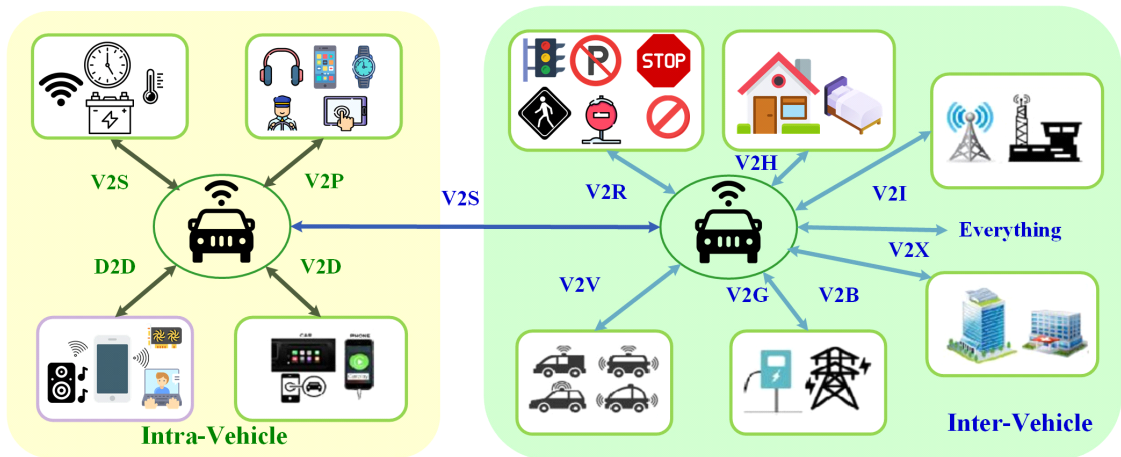
차량 인터넷은 차량 정보 서비스, 첨단 무선 통신 기술, 클라우드 컴퓨팅, 에지 컴퓨팅 및 자동차 전자 장치 등 광범위한 기술 및 응용 프로그램을 포함하며, 주로 ITS와 사물인터넷 기술을 통합하는 신흥 분야이다. 이 기술을 통해 도로 위에서의

* 본 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (2021-0-00188, AI 기능 지원 프레임워크 기반의 이기종 IoT 플랫폼 연동 오픈소스 및 국제 표준 개발)

네트워크 품질을 향상시킨다. 지능형 차내 센서 장치를 인터넷 기술로 차량 및 차량 간 무선 통신 기술과 통합하여 추후 도로 관련 조치 및 의사결정을 개선하는 데 사용할 수 있는 차량 및 교통 관련 데이터를 수집하고 교환할 수 있다. 차량 인터넷은 차량 내 네트워크, 차량 간 네트워크 및 차량 모바일 인터넷 [5]의 세 가지 기본 구성요소로 구성된다. 여기에는 각각 동일한 차량 네트워크에 있는 차량 간의 통신, 서로 다른 차량 네트워크 간의 통신, 차량과 모바일 간의 연결이 포함된다. 차량 인터넷의 기능은 차량에 전자 제어 장치, OBU(OnBoard Unit), 센서, 이벤트 데이터 기록, 카메라, GPS 모듈, 다양한 수의 유선(Controller Area Network and Local Interconnect Network) 및 무선(예: Bluetooth) 통신 기술을 포함한 여러 스마트 장치를 장착하며 활성화된다.

최근 사물인터넷 프레임워크에 대한 다양한 계층 구조가 제안되어 있는데, 제안된 계층의 수 및 명칭에는 서로 차이가 있다. 이러한 아키텍처들은 계층들의 수를 최적화하고 다른 계층들 간의 구별성을 강화하기 위해 경쟁한다 [6]. 가장 일반적인 사물인터넷 아키텍처는 6개 계층, 즉 물리, 통신,

처리, 서비스, 비즈니스 및 보안을 가리키며, 그리고 물리계층의 주된 책임은 차량에 설치된 감지 장치, 액추에이터, GPS 모듈, 액세스 포인트 등을 통해 차량의 속도, 위치, 주행 방향, 노상 차량 밀도, 기상 상태 등 차량과 주변 환경에 대한 정보를 수집하는 것이다. RSU 및 기타 개인 장치도 사용할 수 있다. 수집된 데이터는 통신 계층을 통해 처리 계층에 안전한 방식으로 전송되며, 통신 계층은 다양한 무선 통신 표준과 네트워크 모듈을 사용하여 WAVE, WiFi, RFID, 블루투스, 4G/LTE, UW 및 위성과 같은 서로 다른 이기종 네트워크 엔티티 간의 상호 운용성을 보장한다. 처리 계층은 하위 계층에서 받은 데이터의 저장, 처리 및 변환을 나타내며 의사 결정에 사용할 수 있는 유용한 정보로 사용된다. 여기에는 다양한 빅데이터 분석 툴과 클라우드 컴퓨팅 플랫폼의 채택이 포함된다. 그런 다음 서비스 계층에서 처리 계층에서 처리한 정보와 결정을 취하여 최종 사용자에게 지능형 사물인터넷 서비스와 애플리케이션을 제공하여 도로 안전과 교통 효율에 기여할 수 있는 역할을 한다. 비즈니스 계층에는 경제 투자, 예산 추정 및 규제, 가격 책정 및 운영 관리에



(그림 1) 차량 인터넷 유형

관한 결정이 포함된다. 마지막으로 보안 계층에서는 여러 노드 간의 안전하고 안정적인 데이터 수집 및 통신에 중점을 두어 사물인터넷 환경에서 발생할 수 있는 다양한 보안 공격 및 위협을 방지한다.

2.2 블록체인 개념

블록체인은 DLT(Distributed Ledger Technology)라고도 불리며 트랜잭션의 기록이나 이벤트를 저장하는 데 사용되는 연결된 블록의 그룹으로 정의할 수 있으며 네트워크를 통해 분산된 모든 참여 사용자가 이를 관리한다. 블록체인 기술은 모든 사용자가 P2P(Peer to Peer) 네트워크에서 직접 거래를 생성하고 유효기간 동안 거래할 수 있게 해 중개자와 관련된 금융 및 시간 관련 비용을 크게 절감하는 데 도움이 되기 때문에 중앙 당국에 대한 의존도를 없앤다. 블록체인의 블록 구축은 암호화와 합의 메커니즘 [6]이라는 두 가지 핵심 기술에 의존한다.

암호화 해시 함수와 디지털 서명을 사용하여 데이터의 보안과 개인 정보 보호, 참여자의 익명성을 보장하기 위해 블록체인에 암호화가 채택된다 [7]. 암호화 해시함수의 도입은 블록체인에 매우 인기가 있는데, 각 블록은 이전 블록의 해시값을 자신의 헤더에 유지함으로써 체인의 첫 번째 블록에 연결된다. 첫 번째 블록은 상위 블록이 없으므로 이전 블록의 해시 값이 0으로 설정된다. 이러한 해시 기반 연결 구조는 사용되는 해시 값의 고유성으로 인해 블록체인을 상호 호환 불가능하게 만든다. 반면에 디지털 서명은 비대칭 암호법의 일종으로 각 사용자가 공개 키와 개인 키를 소유한다. 대부분의 블록체인 애플리케이션에서 사용되는 대표적인 디지털 서명 알고리즘은 타원 곡선 디지털 서명 알고리즘(ECDSA)이다.

2.3 사물인터넷에서 블록체인

차량 인터넷은 클라우드와 에지 컴퓨팅 플랫폼을 통합한 경우, 다수의 커넥티드 차량과 도로변 인프라, 모바일 개인용 기기, 중앙 및 분산 스토리지 및 컴퓨팅 서버를 결합하는 대규모 이기종 네트워크가 된다. 이 경우 오픈 채널 무선 통신 모델 및 대부분의 통신을 지배하는 공용 인터넷 연결과 함께 사물인터넷 네트워크내비게이션, 사고 감지 및 알림, 동적 대체 라우팅, 경로 최적화 등 차량 인터넷 애플리케이션을 위협할 수 있는 다양한 보안 공격에 취약하다. 또한 도로 위의 운전자와 승객에게 위협이 되는 교통체증 관리 체계 및 사물인터넷 시나리오에는 실시간 서비스와 의사 결정이 필요할 뿐만 아니라 높은 이동성과 대량의 데이터 교환이 포함되기 때문에 기존 기술보다 더 효율적이고 강력하며 신뢰할 수 있는 기술을 차량 인터넷 프레임워크로 채택해야 한다.

이에 반해 블록체인 기술은 최근 분산형 스토리지 측면뿐만 아니라 보안, 개인정보 보호, 성능, 자동화, 전산비용 절감 등 다양한 산업 응용 분야에서 탈중앙화 스토리지 메커니즘으로 부상하고 있다. 최근에는 데이터 보호 및 관리, 리소스 트레이딩, 자원 공유, 승차 공유, 교통 통제 및 관리, 법의학 응용 등 다양한 목적으로 블록체인 기술을 차량 인터넷 패러다임에 도입하고 있다.

블록체인이 제공할 수 있는 다양한 기능들은 관련 업계의 연구자들이 블록체인 기술을 사물인터넷에 접목하도록 동기를 부여한다. 이러한 속성을 포함한다.

1. 분산: 블록체인 기술은 데이터 저장과 관리를 중앙집중식 노드로 처리하는 중앙집중식 스토리지 플랫폼과 달리 데이터 기록을 모든 참여 주체가 보관하고 관리하는 탈중앙화 성격을 보인다. 이를 통해 중앙 집중식 서버 배열과 관련

된 리소스 병목 현상 및 유지보수 비용을 줄이고 차량 인터넷 환경에 이로운 단일 장애 지점 방식을 할 수 있다.

2. 불변성: 블록체인에 추가되기 전에 서로 다른 합의 메커니즘을 통해 새로운 트랜잭션 블록 생성 및 검증에 관해 피어 전체 또는 대부분의 동의를 얻어야 하기 때문에 블록체인은 변조나 수정이 거의 불가능하다.
3. 보안 및 개인 정보: 암호화 그래픽 해시함수와 디지털 서명이 모두 채택된 블록체인의 암호화 특성은 사물인터넷에서 트랜잭션 데이터의 보안과 참여 사용자의 프라이버시를 보장할 수 있다.
4. 투명성: 모든 참가자가 공개 대장 복제본을 보관하기 때문에 타임스탬프가 찍힌 모든 블록체인 트랜잭션을 처리할 수 있다. 따라서 피어는 문서 없이도 언제든지 투명한 방식으로 트랜잭션을 관리 및 조회할 수 있다. 이러한 자체 감사 가능성과 투명성은 자신의 거래를 관리함으로써 동종업자의 구제를 촉진할 뿐만 아니라 중간 당사자와 관련된 시간과 금융 비용을 경감시킨다.

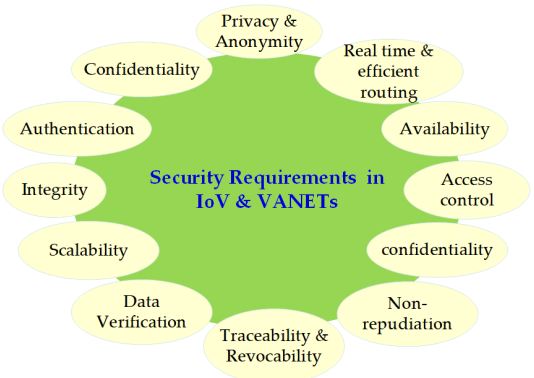
3. 차량 인터넷에서 블록체인 기반 인증 프로토콜

3.1 차량 인터넷에서 보안 문제

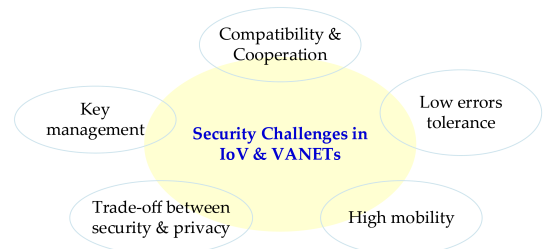
사물인터넷 네트워크는 서로 다른 표준과 규정을 가진 다양한 기술(예: 인터넷 연결, 서로 다른 무선 기술, 센서, 클라우드 서비스)이 융합된 것으로, 다양한 유형의 보안 공격에 취약하게 만든다. 공격자의 목표에 따라 공격 시작은 수동적이거나 능동적일 수 있으며 내부에서 생성되거나 외부에서 생성될 수 있다. 그러나 공격의 소스 또는 활동

유형에 관계없이 이러한 보안 위협은 일반적으로 손상된 네트워크의 보안 측면에 따라 다른 범주로 분류된다. 예를 들어 공격은 사용자의 신뢰성, 차량 인터넷 데이터의 무결성 또는 제공된 서비스의 가용성에 영향을 미칠 수 있다.

사물인터넷 시스템이 겪을 수 있는 다양한 보안 위협에 따른 보안 측면이 문헌에 정의되어 있다. 이러한 보안 측면은 1) 효율적인 차량 인터넷 시스템을 위해 유지해야 하는 보안 요구 사항과 2) 차량 인터넷 환경의 보안 서브시스템에 직면한 보안 문제로 분류할 수 있다. 그림 2와 3에서는 이러한 차량 인터넷 및 차량 애드혹 네트워크 플랫폼의 보안 요구사항 및 주요 과제를 보여주고 있다 [8]-[11].



(그림 2) 차량 인터넷 및 차량 애드혹 네트워크 플랫폼의 보안 요구 사항



(그림 3) 차량 인터넷 및 차량 애드혹 네트워크 플랫폼의 주요 과제

3.2 퍼블릭 블록체인 기반 인증 프로토콜

퍼블릭 블록체인은 모든 사람이 블록의 서로 다른 거래에 접근하고, 보내고, 받고, 확인할 수 있는 개방형 액세스 블록체인이다. 완전히 개방된 블록체인이기 때문에 대상 인증 파라미터에 대한 대장을 조회하면 차량 역시 인증 과정에 참여할 수 있다. 인증 프로세스를 몇 개의 신뢰할 수 있는 노드로 제한하는 것에 비해 사물인터넷 환경에서 사용 가능한 컴퓨팅 리소스를 더 잘 활용할 수 있으므로 보다 분산적이고 시간 효율적인 인증 프로세스가 달성된다. 퍼블릭 블록체인의 이러한 특성 때문에 많은 연구자들이 사물인터넷 인증을 위해 퍼블릭 블록체인을 채택하고 있다.

[16]의 저자들은 차량 인터넷 네트워크의 인증 지연 문제와 시간 복잡성을 해결하는 데 기여한다. 제안된 작업은 퍼블릭 블록체인 채택을 통해 실시간 인증 및 적수 탐지 기능을 제공한다. MICAz mote(하드웨어 무선 센서 모듈)는 V2V 배열에서 무선 통신 인터페이스 역할을 하기 위해 두 대의 차량에 설치된다. 측정은 실시간으로 실내 및 실외에 기록되며 MATLAB R2020a의 도움으로 보고된다. Pearson 상관 계수[17]는 네트워크의 값이 0.9보다 작거나 같을 때 네트워크에서 적수를 탐지하도록 계산된다. 이 방식은 자사 블록체인에 사용되는 단순하고 가벼운 해시함수로 인해 $O(1)$ 만큼 낮은 것으로 밝혀진 시간 복잡도 측면에서도 평가된다. [18]의 저자들은 인증이 개별적이고 일괄적으로 수행되는 인공지능(AI) 기반의 차량 인터넷 지원 스마트 시티 "BBAS-차량 인터넷"을 위한 새로운 블록체인 지원 인증 체계를 설계한다.

3.3 프라이빗 블록체인 기반 인증 프로토콜

프라이빗 블록체인은 특정 작업을 수행하기 위

해 특정 그룹의 신뢰할 수 있는 개체(네트워크 관리자 결정)에게만 블록체인 트랜잭션에 대한 액세스 권한을 부여하는 제한된 액세스 블록체인이다. 프라이빗 블록체인의 특성상 블록체인에 저장된 차량의 인증 매개 변수에 액세스할 수 있는 신뢰 노드는 소그룹에 불과해 인증 시 높은 수준의 신뢰도 구축이 가능하다. 또한 단일 조직에 의해 제어되므로 원장에 보관된 인증 데이터를 보다 쉽고 효율적으로 관리 및 감독할 수 있다. 따라서 많은 연구자들이 차량 인터넷 플랫폼에서 인증 목적을 제공하기 위해 프라이빗 블록체인을 구현한다.

사물인터넷 네트워크에 합류하는 새로운 노드 문제를 해결하기 위해 프라이빗 블록체인 기술을 지능형 계약과 통합한다. 저자들은 인증 효율성을 높이기 위해 암호 축전지 기반의 공개키인프라(PKI) 기술을 도입해 등록된 차량의 인증을 다루었다[12]. 높은 이동성 동안 제한된 시간 내에 많은 수의 동시 차량 요청을 인증하지 못할 수 있는 중앙 집중식 인증 프로토콜 및 단일 신뢰 가능 기관(TA)? 체계가 직면한 컴퓨팅 및 통신 병목 현안에 대해서도 논의했다. [13] 스마트 계약은 인증 프로세스의 일부를 자동화하기 위해 사용되며, 위임된 스택 증명[14]은 보다 효율적인 자원 활용과 전력 소비를 위한 합의 메커니즘으로 채택된다. 프라이빗 블록체인의 프레임워크를 도입해 인증 기관(CA)에 대한 의존도가 낮은 안전한 상호 인증 체계를 제안한다. 차량 이외에, 해당 모델과 관련한 물리적 실체는 모두 블록체인에 대한 완전한 통제권을 가지고 있는 CA와 해지권한(RA)이다. 반면 RSU는 블록체인에 대한 읽기 허가만 가지고 있다[15].

3.4 컨소시엄 블록체인 기반 인증 프로토콜

컨소시엄 블록체인은 일명 하이브리드 블록체

인으로 불리는 프라이빗 블록체인과 퍼블릭 블록체인의 결합으로 읽기 접근이 개방되거나 제한될 수 있으며, 서로 다른 조직에 속한 소수의 노드 그룹만이 컨센서스를 담당한다. [19]의 저자들은 차량 인터넷 정보를 컨소시엄 블록체인에 추가하기 전에 정확성을 검증하기 위해 시간 순서와 가십 프로토콜[20]을 채택하여 비잔틴 합의 알고리

즘을 최적화한다. [21]의 저자들은 블록체인 기반의 경량 익명 인증 체계인 BLA를 제안함으로써 차량 포그 컴퓨팅 (VFC) 환경에서 교차 데이터 센터 인증 문제를 다루었다. [22]의 저자들은 상호 인증 및 키 교환 매커니즘의 채택을 통해 [21]에서 제안된 인증 체계의 신뢰성을 향상시켰다. 의사 ID, 블록체인 및 해지 태그를 사용하여 차량 애드

〈표 1〉 차량인터넷 및 차량 애드혹 네트워크 인증 기술 비교

논문	차량 애드혹 네트워크에서 사물인터넷으로 전환	보안 공격	블록체인 기반 인증	특징
차량 애드혹 네트워크 2017[1]	×	√	×	<ul style="list-style-type: none"> 차량 애드혹 네트워크의 인증, 개인 정보 보호 및 보안 메시지 배포 문제를 해결함. 조사된 논문에 사용된 도구와 기술을 기반으로 한 다중 분류를 제안함.
차량 인터넷 2019[2]	×	√	×	<ul style="list-style-type: none"> 차량 인터넷의 다양한 보안 프로토콜에 대한 분류법을 제공함. 차량 인터넷의 인증 프로토콜을 조사함. 통신 및 계산 overhead 측면에서 성능 비교를 제공함.
차량 인터넷[3]	√	×	√	<ul style="list-style-type: none"> 차량 네트워크에서 블록체인 기반 응용 프로그램을 포괄적으로 비교. 차량 네트워크에서 블록체인 기반 애플리케이션의 요구 사항을 분석. 차량 네트워크 내 블록체인의 통합과 관련된 다양한 과제에 대해 논의함.
차량 인터넷[4]	√	×	×	<ul style="list-style-type: none"> 블록체인 기술을 사물인터넷과 결합할 수 있는 7 가지 측면을 간략하게 제공함. 이러한 각 측면에 대한 몇 가지 계획을 조사함. 블록체인 지원 사물인터넷 분야의 몇 가지 연구 방향을 개괄적으로 설명함.
차량 애드혹 네트워크 및 차량 인터넷 [5]	√	√	√	<ul style="list-style-type: none"> 차량 애드혹 네트워크 및 사물인터넷의 특정 영역을 다루어 사물인터넷 분야의 연구자들에게 보다 집중적인 참조를 제공하는 동시에 차량 기술과 ITS에 대한 보다 포괄적인 참조를 제공함. 블록체인 기반 인증 방식에 대해 논의하여 사물인터넷에서 블록체인의 효율성을 강조함. 인증에 사용되는 블록체인 유형 측면에서 명확한 분류법을 제공함. 사용된 기술, 대응된 공격, 네트워크 모델 및 평가 도구 측면에서 조사된 논문 간의 자세한 비교를 진행함.

혹 네트워크에서 차량의 익명 인증과 효율적인 해지 모두를 다루기 위한 접근방식을 제안한다. 이 체계는 세 가지 유형의 노드, 즉 교통부(TD)인 감독 노드, 복수의 TA로 대표되는 회계 및 해지 노드, 도로 측면 장치인 검증 노드를 정의한다.

표 1에서는 차량인터넷 및 차량 애드혹 네트워크 인증 기술을 보안공격, 블록체인 기반 인증 등을 통해 특징을 분석하고 상호 비교한다.

4. 결 론

지능형 교통시스템에서 진화를 이룬 차량 신형 기술인 차량 인터넷과 앞선 차량 애드혹 네트워크의 보안 측면에 대해 논의했다. 다양한 보안 요건, 과제 및 차량 네트워크에 대한 잠재적인 보안 공격과 위협이 제시되고 있는데, 대응책으로 사물인터넷과 차량 애드혹 네트워크 환경에서의 최신 블록체인 기반 인증 기법에 관한 광범위한 논의에 집중했으며, 두 기술을 종합적으로 비교 고찰했다. 전반적으로 사물인터넷에 등장한 블록체인 기술의 힘이 부각됐다. 또한 사물인터넷과 차량 애드혹 네트워크의 보안 과제에 대한 향후 연구 방향을 제시했다. 본 논문에서는 조사된 블록체인 기반 사물인터넷 인증 체계 간의 개념적 비교, 즉 사용되는 다양한 기술, 네트워크 아키텍처 및 평가 도구, 특징 및 제한 사항에 초점을 맞췄는데, 추후 양적 측정을 비교 대상에 더 많이 포함할 필요가 있어 보인다.

참 고 문 헌

[1] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: a comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017.

- [2] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: a comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017.
- [3] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (차량 애드혹 네트워크)," *Vehicular Communications*, vol. 25, p. 100247, 2020, doi: 10.1016/j.vehcom.2020.100247 [4] ATSC T3/S17, ATSC DASE(Digital TV Application Software Environment) Standard, Feb 2001.
- [4] S. Kumar, S. Velliangiri, P. Karthikeyan, S. Kumari, S. Kumar, and M. K. Khan, "A survey on the blockchain techniques for the Internet of Vehicles security," *Transactions on Emerging Telecommunications Technologies*, pp. 1-23, 2021, doi: 10.1002/ett.4317.
- [5] L. Mendiboure, M. A. Chalouf, and F. Krief, "Survey on blockchain-based applications in internet of vehicles," *Computers and Electrical Engineering*, vol. 84, p. 106646, 2020, doi: 10.1016/j.compeleceng.2020.106646.
- [6] S. Zhang and J. H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93-97, 2020, doi: 10.1016/j.ict.2019.08.001.
- [7] M. B. Mollah et al., "Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4157-4185, 2021, doi: 10.1109/J사물인터넷.2020.3028368.
- [8] H. Hasrouny, A. E. Samhat, C. Bassil, and

- A. Laouiti, "차량 애드혹 네트워크 security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017, doi: 10.1016/j.vehcom.2017.01.002.
- [9] K. N. Qureshi, S. Din, G. Jeon, and F. Piccialli, "Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges with Future Aspects," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1777–1786, 2021, doi: 10.1109/TITS.2020.2994972.
- [10] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, p. 100182, 2019, doi: 10.1016/j.vehcom.2019.100182.
- [11] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, "A survey on security and privacy issues in 차량 인터넷," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 5409–5419, 2020, doi: 10.11591/IJECE.V10I5.PP5409-5419.
- [12] Wang, X.; Zeng, P.; Patterson, N.; Jiang, F.; Doss, R. An improved authentication scheme for internet of vehicles based on blockchain technology. *IEEE Access* 2019, 7, 45061–45072.
- [13] Xu, Z.; Liang, W.; Li, K.C.; Xu, J.; Jin, H. A blockchain-based Roadside Unit-assisted authentication and key agreement protocol for Internet of Vehicles. *J. Parallel Distrib. Comput.* 2021, 149, 29–39.
- [14] Yang, F.; Zhou, W.; Wu, Q.; Long, R.; Xiong, N.N.; Zhou, M. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access* 2019, 7, 118541–118555
- [15] Malik, N.; Nanda, P.; Arora, A.; He, X.; Puthal, D. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE*, New York, NY, USA, 1–3 August 2018; pp. 674–679.
- [16] Kamal, M.; Srivastava, G.; Tariq, M. Blockchain-based lightweight and secured V2V communication in the internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* 2020, 22, 3997–4004.
- [17] Benesty, J.; Chen, J.; Huang, Y.; Cohen, I. Pearson correlation coefficient. In *Noise Reduction in Speech Processing*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1–4.
- [18] Bagga, P.; Sutrala, A.K.; Das, A.K.; Vijayakumar, P. Blockchain-based batch authentication protocol for Internet of Vehicles. *J. Syst. Archit.* 2021, 113, 101877.
- [19] Hu, W.; Hu, Y.; Yao, W.; Li, H. A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles. *IEEE Access* 2019, 7, 139703–139711.
- [20] Cooper, M.C.; Herzig, A.; Maffre, F.; Maris, F.; Régnier, P. The epistemic gossip problem. *Discrete Math.* 2019, 342, 654–663.
- [21] Yao, Y.; Chang, X.; Mistic, J.; Mistic, V.B.; Li, L. BLA: Blockchain-assisted lightweight anonymous authentication for dis-

- tributed vehicular fog services. *IEEE Internet Things J.* 2019, 6, 3775–3784.
- [22] Kaur, K.; Garg, S.; Kaddoum, G.; Gagnon, F.; Ahmed, S.H. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. *arXiv* 2019, arXiv:1904.01168v1, 2019, 1–6, 1–6.
- [23] Rathore, H.; Mohamed, A.; Guizani, M. A survey of blockchain enabled cyber-physical systems. *Sensors* 2020, 20, 282.
- [24] Lee, J.; Azamfar, M.; Singh, J. A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems. *Manuf. Lett.* 2019, 20, 34–39.
- [25] Xu, Q.; Su, Z.; Yang, Q. Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system. *IEEE Internet Things J.* 2019, 7, 1098–1110.
- [26] Du, Y.; Cao, J.; Yin, J.; Song, S. An overview of blockchain-based swarm robotics system. *Artif. Intell. China* 2020, 572, 353–360.
- [27] Ferrer, E.C. The blockchain: A new framework for robotic swarm systems. In *Proceedings of the Future Technologies Conference, Vancouver, BC, Canada, 13–14 November 2018*; pp. 1037–1058.
- [28] Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.-H. Convergence of blockchain and artificial intelligence in 사물인터넷 network for the sustainable smart city. *Sustain. Cities Soc.* 2020, 63, 102364.
- [29] Chen, X.; Ji, J.; Luo, C.; Liao, W.; Li, P. When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018*; pp. 1178–1187.
- [30] Wang, R.; Liu, H.; Wang, H.; Yang, Q.; Wu, D. Distributed security architecture based on blockchain for connected health: Architecture, challenges, and approaches. *IEEE Wirel. Commun.* 2019, 26, 30–36.
- [31] Ramani, V.; Kumar, T.; Bracken, A.; Liyanage, M.; Ylianttila, M. Secure and efficient data accessibility in blockchain based healthcare systems. In *Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018*; pp. 206–212.
- [32] Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.-Y. Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Trans. Comput. Soc. Syst.* 2018, 5, 942–950.
- [33] Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet Things J.* 2018, 6, 4660–4670.
- [34] Shi, K.; Zhu, L.; Zhang, C.; Xu, L.; Gao, F. Blockchain-based multimedia sharing in vehicular social networks with privacy protection. *Multimed. Tools Appl.* 2020, 79, 8085–8105.
- [35] Li, Z.; Yang, Z.; Xie, S. Computing resource trading for edge-cloud-assisted Internet of Things. *IEEE Trans. Ind. Inform.* 2019, 15, 3661–3669.
- [36] Qiao, G.; Leng, S.; Chai, H.; Asadi, A.; Zhang, Y. Blockchain empowered resource trading in mobile edge computing and networks. In *Proceedings of the ICC 2019—2019 IEEE International Confe-*

rence on Communications (ICC), Shanghai, China, 20-24 May 2019; pp. 1-6.

- [37] Chai, H.; Leng, S.; Zhang, K.; Mao, S. Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles. *IEEE Access* 2019, 7, 175744-175757.
- [38] Wang, S.; Huang, X.; Yu, R.; Zhang, Y.; Hossain, E. Permissioned blockchain for efficient and secure resource sharing in vehicular edge computing. *arXiv* 2019, arXiv:1906.06319.
- [39] Al Amiri, W.; Baza, M.; Banawan, K.; Mahmoud, M.; Alasmay, W.; Akkaya, K. Privacy-preserving smart parking system using blockchain and private information retrieval. In *Proceedings of the 2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*, Sharm El Sheikh, Egypt, 17-19 December 2019; pp. 1-6.
- [40] Chen, C.; Xiao, T.; Qiu, T.; Lv, N.; Pei, Q. Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles. *IEEE Trans. Ind. Inform.* 2019, 16, 4122-4133.
- [41] Li, M.; Zhu, L.; Lin, X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet Things J.* 2018, 6, 4573-4584.
- [42] Li, M.; Zhu, L.; Lin, X. CoRide: A privacy-preserving collaborative-ride hailing service using blockchain-assisted vehicular fog computing. In *Proceedings of the International Conference on Security and Privacy in Communication Systems*, Orlando, VA, USA, 23-25 October 2019; pp. 408-422.

저 자 약 령

아흐메드 샤비르

이메일 : shabir@gachon.ac.kr

- 2009년 UET Peshawar, Pakistan (학사)
- 2013년 NUST, Pakistan (석사)
- 2020년 제주대학교(박사)
- 2011년~2016년 프로그래머/개발자
- 2016년~2017년 UET Peshawar, Pakistan/ 강사
- 2020년~현재 가천대학교 문화콘텐츠기술연구소/ 연구교수
- 관심분야: 사물 인터넷, 인공 지능, 기계 학습, 빅데이터

압바스 수해일

이메일 : sababs@sharjah.ac.ae

- 2003년 University of Peshawar, Pakistan (학사)
- 2011년 Liverpool John Moores University, Liverpool, UK (박사)
- 2012년~2016년 University of Malakand / 주교수
- 2016년~현재 University of Sharjah / 주교수
- 관심분야: Network Security, Adhoc Networks, IoT

김도현

이메일 : kimdh@jeju.ac.kr

- 2004년 제주대학교 컴퓨터공학 정교수
- 2019년 제주대학교 빅데이터 연구센터 센터장
- 관심분야: 사물인터넷, 빅데이터, 최적화 및 예측