논문 19-44-12-20 The Journal of Korean Institute of Communications and Information Sciences '19-12 Vol.44 No.12
https://doi.org/10.7840/kics.2019.44.12.2315

비공개 블록체인 기반 의료사물인터넷(IoMT)의 다중보안 인증기술 구성과 설계 Scheme

박 종 만◆

Design Scheme and Configuration of Private Blockchains Based Multiple Security Authentication Methods For Internet of Medical Things(IoMT) Application

Jong Man Park◆

요 약

사물인터넷(IoT) 기기 및 서비스 확대로 인한 불법 해킹 및 정보침해 증가를 원천적으로 차단할 효율적 대응방안이 시급하다. 특히 보안시스템의 고도화개발 여력이 부족한 중소기업들은 블록체인(BC) 기반 IoT 기기의 보안모듈, IoT 기기와 사용자 단말 간의 다중인증시스템, 사용자 앱에 대한 경량형태의 비 공개형 다중보안 인증체계의 개발과 보급이 필요하다. 이를 충족시키기 위해 이 논문은 선행연구 및 기술 동향분석, BC 기반의 다중보안 인증시스템의 신규 기술구성 및 디자인 구조, 이를 활용한 의료사물인터넷(IoMT) 보안 적용체계 및 실증 프레임에 대한 스킴 제시에 중점을 두고 있다.

키워드 : 블록체인, 사물인터넷 기기, 사용자 단말, 다중보안 인증, 의료사물인터넷 보안 스킴
Key Words : Blockchain, IoT device, User terminal, Multi security authentication, IoMT security scheme

ABSTRACT

It is urgent time on how efficiently to proceed to block at the source the multiplying of illegal hacking and information infringement due to the increasing numbers of internet of things(IoT) device and service. Particularly, small medium companies which lack in affordable resources to develop higher level security system require lightweight private multi-security authentication solutions such as blockchain(BC) based security modules of IoT device, multiple authentication system between IoT devices and user terminals, user web application. To meet these kinds of needs, this paper focuses to propose the previous study and trends, new technological configuration and design scheme for building of blockchain based multi-security authentication system, and practical instance of an integrated security frame on internet of medical things(IoMT) system.

Ⅰ. 서 론

IoT 시스템의 보안 위협요소는 센서 및 단말과 서버에 대한 비인가 접근을 통한 가용성 침해, 정보 조작 및 복제, 유출과 탈취를 통한 기밀성 및 무결성 공격과 인증방해, 서비스거부, 프라이버시 침해 등이 있다. 기존의 IoT 보안 상용화 제품들은 대부분 경량화 암호 모듈을 이용하며, 상호인증 및 구간암호 사용,

◆ First Author : ReSEAT Program (KOITA), jmp21c2012@reseat.or.kr/ jmp21c@paran.com, 정회원
논문번호 : 201908-156-D-RN, Received August 12, 2019; Revised October 1, 2019; Accepted October 8, 2019

키 관리지원이나 개별보안 인증방식으로 통합보안 형태로 볼 수 없다. 이와 관련 보안 수요공급자 모두에게 통합적 보안 위협요소가 상존한다. 특히 국내 경우 위협에 대응할 해결책이 시급하나 여력이 부족한 중소기업을 위한 적정가격대의 신뢰적 보안 모듈기술 및 솔루션이 부족한 환경이다. 현재 BC 기술 기반의 IoT 보안 인증 개발프로젝트를 추진하거나 도입 계획 중인 중소기업들이 늘고 있어도, 통합인증 보안에 대한 인식 부재나 구현비용 부담 여력이 부족한 경우, 준비가 부실하여 미해결과제로 남을 수밖에 없다.

연구는 이에 대한 해결책으로 BC 기반의 모바일 단말 및 IoT 기기 간 실질적인 경량형 다중보안 인증 시스템 및 방법을 제시하고 개발 및 실증을 통해 경량화 보안 통합모델을 구현 및 보급하려는 목적성과 계획을 공유하고 있다. 논문은 1장 서론, 2장 선행연구 및 기술 동향, 3장 실증을 위한 IoMT 시스템의 BC 기반 다중보안 인증기술 구성 및 설계 Scheme, 4장 결론으로 구성되어 있다.

Ⅱ. 선행연구 및 기술 동향

IoT 관점의 BC 관련 접근방법과 기술응용 분야, 기기와 데이터관리 분야, 기존 솔루션 등의 조사에서 IoT에 BC를 적용하려는 동기나 이유로, IoT 서비스 네트워크상의 분산 서비스거부, 중앙집중식 클라우드 서비스의 취약성, 데이터 인증과 기밀성의 고질적인 위협, 무결성과 실시간 가용성 확보, 데이터거래 참여 객체의 신뢰(trust) 문제[1] 등이 있다. BC 기술 기반의 응용시스템 설계에서 합의 프로토콜의 선택이나 운영을 위한 알고리즘이 다양하게 증식되고 있다. 작업증명(PoW:Proof of Work)[2], 지분증명(PoS:Proof of Stake)[3], 보안 취약증명(PoC:Proof of Concepts)[4], 경과 시간 증명(PoET:Proof of Elapsed Time)[5], 비잔틴 장애허용(BFT:Byzantine Fault Tolerance)[6], 연합 비잔틴 약정(FBA: Federated Byzantine Agreement)[7], 실용적 비잔틴 장애허용(PBFT: Practical Byzantine fault Tolerance)[8] 등의 합의 알고리즘들이 있다. 이외에도 앞서 언급된 알고리즘의 파생이나 중요도, 용량, 접속, 권위, 신뢰 기반의 다양한 알고리즘들이 있다. 이 알고리즘들과 BC 형태, 거래의 완결성과 속도, 토큰의 필요 여부, 참여비용, 네트워크의 확장성, 모델 신뢰 정도 등의 요소별 비교결과를 통해 통합보안을 위한 합의 알고리즘 선택이나 가이드로 활용할 수 있다. BC와 IoT의 융합을 BC 사물인터넷(BCoT: Block chain of Things)이라 명칭하고 통합구조 및 방향성을 제시한 연구[9]는 기존의 IoT와 BC의 융합 관련 연구들이 BC 융합기반 IoT의 일반화 구조 제시나 5G 상황에서의 IoT와 BC에 대한 고려, 스마트계약의 주기 등에 대한 검토가 부족하다고 지적하고 있다.

국내외에서 IoT와 BC 기술의 융합연구 및 추진에도 불구, 여전히 IoT의 기술적 해결과제로 이질적인 시스템, 네트워크 복잡성, 탈중앙화와 이질성에 의한 상호작용의 취약성, IoT 기기의 컴퓨팅과 스토리지, 배터리 등의 한계에 의한 자원 제약성, 프라이버시와 보안 취약성 등이 언급되고 있다. 통합관점에서의 BC 구현구조를 센서감지 데이터 감지와 수집 층, 네트워크층, 블록에 대한 분산 합의 층, 거래보상 및 보상 분배 층, 블록체인 서비스(BaaS: Blockchain as a Service) 층으로 구분 설명하기도 한다. IoT 기기는 자원제약 정도에 따라 데이터를 전부 저장하는 노드나 일부를 저장하는 경량형 노드로 설계할 수 있다. 실제 저장 노드에서는 클라우드나 엣지 서버의 복합적으로 사용이 대안이 되며, 엣지 서버는 IoT 게이트웨이, 광대역 기지국, 소규모 기지국이 될 수 있다. IoT 기기의 상호작용 형태는 엣지 게이트웨이나 기지국 엣지 서버의 BC 데이터에 직접 접속하는 방법, IoT 기기 간에 부분적으로 보유하는 BC 데이터의 교환 및 접속 방법, 상기 두 방법의 혼합에 의한 복합적 접속 방법 등이 사용될 수 있다. 5G 관련 IoT 융합 BC 기술적용 경우 첫째 통신주파수 경매 및 공유에 의한 혼잡도 및 비용 저감과 모바일 서비스 향상, 둘째 소프트웨어 정의기반 네트워킹(SDN: Software Defined Network)과 네트워크 기능 가상화(NFV: Network Functions Virtualization) 등 네트워크관리의 보안 효율 향상, 셋째 모바일 엣지 컴퓨팅에서의 보안 관리 효율 향상 등을 견인할 수 있는 장점이 있다.

건강관리 및 의료분야의 개인정보보호와 데이터보안을 위해 BC 기술을 활용하는 연구[10-14]에서 제시된 시스템, 솔루션, 기술구성, 관리 프레임 등은 후발 프로젝트의 가이드로 참조할 수 있다. 특히 비밀과 익명성을 보장하기 위한 IoT와 BC 기반의 MEC(Mobile Edge Computing) 통합, 홈에서의 치료관리 프레임[15] 등을 시스템설계에 참조할 수 있다. 실무적으로 IoT 플랫폼과 기기 관점에서 BC 기술을 연동하는 방법으로 IoT 플랫폼으로 수집된 데이터를 우회접속(proxy)을 통해 BC 형태로 변환하거나, 경량형 SW를 탑재한 분산형 기기를 통해 BC와 직접 연동하는 방법들이 있다. BC 관점에서 IoT와 연동을 위한 방법으로 다양한 플랫폼 및 시스템과 프레임, 합의 메커니즘 등이 가능

하나, 연구에서는 분산컴퓨팅 플랫폼인 Ethereum[16], 빅데이터 분산 DB와 분산제어 BC의 조합형 플랫폼인 Bigchain[17], 착탈형 합의 알고리즘 기반의 개방형 분산플랫폼인 Corda[18], 허가기반의 비 공개형 및 컨소시엄 형태로 BC 합의 알고리즘인 BFT를 이용하는 개방형 시스템인 Hydrachain[19], 건강관리 분야에 활용되는 비 공개형 BC 플랫폼 GemOS[20], 허가기반과 비체인 스토리지를 지원하는 플랫폼 Multichain[21], 다수 합의 알고리즘 설정과 다중 포맷 저장이 가능한 모듈구조 기반의 비즈니스플랫폼인 Hyperledger Fabric 및 신원 인증관리를 위한 플랫폼 Hyper ledger Indy[22] 등을 검토 및 참조할 수 있다.

IoT 기반의 탈 중앙집중식 프라이버시 유지를 위한 건강관리 BC 솔루션에서 고비용이 소요되는 BC 컴퓨팅은 자원 제약적인 대규모 IoT 기기에 적합하지 않다고 지적하고, 해결책으로 중첩 네트워크, 신규 해시 생성 체인 기반의 클라우드 스토리지, 지정 건강관리 제공자 노드, 스마트계약, 착용 형태의 IoT 기기 시스템을 제시[23]하는 연구는 경량화를 위해 참조할 수 있다. 엣지 컴퓨팅과 BC 기반의 산업인터넷(IIoT:Industrial IoT)에서 신원 관리와 접속제어를 위한 네트워크 객체들의 등록 및 인증에 자가인증 및 암호화 방식[24]도 참조할 수 있다. 이에 대한 설계 프레임은 우선 BC 기반의 신원 및 인증관리 메커니즘을 구축하고 생성되는 신원에 대한 절대 인증을 결합한 다음, Bloom 필터를 기반으로 설계된 접속제어 메커니즘과 신원 및 인증관리 메커니즘을 통합한다. 다음은 자원 여력이 부족한 IoT 엣지 기기의 보안통신을 위해 자가인증과 공공 키 기반의 경량화된 비밀키 약정 프로토콜을 구축하는 단계로 구성되어 있다.

이 같은 다양한 선행연구 이외에 IoT를 위한 BC 솔루션에 대한 분석[25]은 IoT 플랫폼에서 실제 BC를 실행하는 35개 사례를 분석하고 제시한 주요이슈는 시스템설계에 참조할 수 있다. 아래 설명에서 괄호 안의 숫자는 35개 사례 중 적용된 플랫폼과 알고리즘의 비중을 나타내 준다. 사례연구 영역은 일반적인 BC 기반 IoT 솔루션 분야가 다수(63%)이고 제조(9%) 및 자동차 인터넷(6%), 에너지 그리드(6%), 전기거래(6%), e-헬스(3%), 스마트홈(3%) 분야 등이다. 중심 이슈는 IoT 플랫폼의 키 관리 이슈의 해결을 위한 BC 활용이 다수(77%)이며, 플랫폼상의 사물 연산능력 부족(26%), 무결성(17%), 표준부족(11%) 등 소수의 중복 이슈가 있다. 전체 35개 조사사례 중 무응답 7개를 제외한 BC 플랫폼과 합의 알고리즘들의 활용 비중은 <그림 1>과 같다. 플랫폼 비중은 Ethereum(57%),

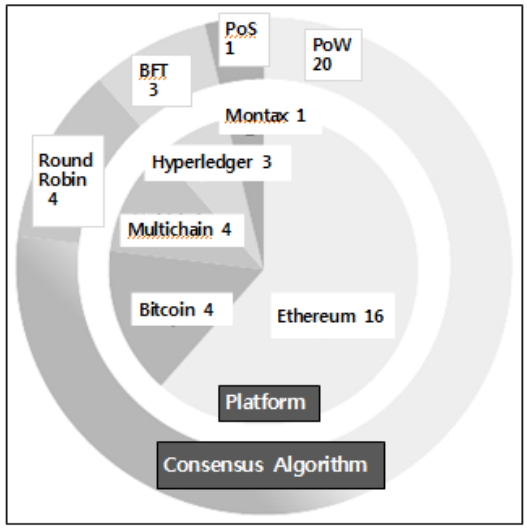

그림. 1. 블록체인 플랫폼과 합의 알고리즘 활용비율(N=35개)
Fig. 1. Usage Count of Blockchain Platform and Consensus Algorithm(N=35, Counts)

Multichain(14%), Bitcoin(14%), Hyper ledger(11%), Montax(4%) 순이며 합의 알고리즘은 POW(71%), Round Robin(14%), POS (4%), BFT(11%) 순이다. BC의 활용은 데이터 저장(53%), 접속제어(28%), 센서와 연산 노드 간 플랫폼 커넥터(17%), IoT 활용 보상 배분(2%) 순이다. IoT 적용에서, 데이터의 무결성이 기밀성을 상쇄시키지 않는 데이터 프라이버시 수준, 동적 접속제어의 적합을 위한 스마트계약의 확장성, 연산 보안과 코드 무결성을 위한 추가적 코드표현, 실시간 처리가 필요한 경우 속도가 빠른 허가 PBFT를 선호한다는 의견이 있다. BC 인프라 관련, IoT 적용에는 Multichain과 Hyperledger Fabric같이 인가기관 허가기반의 개별 BC이 적절하고, 허가가 필요 없는 공공 BC에는 앵커링 메커니즘인 다중 BC를 위한 확장플랫폼 구조가 적절하다는 의견이 있다. 특히 POW가 IoT에 적합하진 않아도 연산능력을 가진 IoT 게이트웨이의 활용이 가능하다. PoS 나 PBFT 가 IoT에 더 적절하다는 의견이 있다. BC와 다른 방식인 P2P 검증 기반의 IOTA Tangle의 방향성 비순환 그래프(DAG:Directed Acyclic Graph)는 확장성이 있으나 보안성은 낮다는 의견도 있다. 사물 측면에서, 스마트계약단계는 사물이 BC 계정을 보유하고 있으면 사물간 통신 및 거래가 자동으로 가능하나, 수동연결의 경우 사물과 BC 간 상호작용은 제약적이다. 신원 관리 단계에서는 공개키(PKI:Public Key Infra structure)가 중심적 역할을 하며 BC는 의사 익명 신원증명을 제공

한다. 특히 자기 주권적 신원증명(SSI:Self Sovereign Identity)은 신원 관리의 유연성을 제공하며 탈 중앙집중적 신원증명(DID:Decentralized Identity)은 네트워크 객체의 새로운 SSI 이므로 필수적 참조 사항이다. 신뢰 평가 단계에서는 시뮬레이션이 모든 엣지 경우를 감당할 수 없으므로 교차검토와 위험 및 책임 배분의 필요성도 있다.

IoT 데이터관리를 위해 다중 블록체인 통합에 대한 교차 체인 솔루션[26]에서 접속제어를 위한 컨소시엄 블록체인도 참조 대상이다. BC와 달리 코인이 없는 IOTA Tangle은 마스크 인증 메시지(MAM: Mask Authentication Message)를 통한 실시간 데이터 접속관리의 비용, 효율, 확장성, 유연성 측면에서의 이점으로, 엣지 기기의 로컬서버 대신 분산 헬스데이터 공유와 가속화가 가능한 IoT와 분산원장 기반의 솔루션[27] 연구도 참조가 필요하다. 모바일 플랫폼상에서 분산형 P2P 파일 연결시스템(IPFS:Inter Planetary File System)과 블록체인을 결합한 전자건강기록(EHR:Electronic Health Records) 공유 프레임의 접속제어 메커니즘[28]도 참조가 필요하다.

IBM은 공개형 BC에서 암호화폐 증가로 POW와 POS 알고리즘의 변경을 원하거나, 비 공개형 BC에서 소규모 노드나 네트워크에 적절한 PBFT의 확장을 원할 경우, 애플리케이션의 재구성과 BC 인프라의 재디자인 및 재준비, 검증 거래나 BC 이전(Migration) 등에 과도한 비용이 예상될 경우 요구 목적 달성이 어렵다는 점에 착안하여, 2019년 3월 기존 BC의 신뢰 설정 변경에 관련한 미국특허(US2019/0075022)를 출원하였다. 특허는 BC 설정 운영조건이 동적이며 특정 환경에서 자동으로 변경 가능한 로직을 갖고 있으며, 그 운영절차는 기존 BC 설정에 사용되는 기존 합의 절차 및 측정항목의 식별, 사전 정의된 규칙 대비 현재 측정항목의 비교, 비교를 통한 규칙이탈 측정과 이탈항목의 식별에 책임이 있는 기존의 BC이 다음 블록에서의 절차에 대한 합의를 위해 기존의 합의 절차를 변경하는 단계들로 구성된다. <그림 2>에서 의사결정 지원 모듈(120)은 기업 분산네트워크 서버 혹은 클라우드의 인터페이스(110)데이터를 처리하고 BC 데이터 처리를 위해 현재의 절차, 알고리즘, 전략 등을 동적으로 수정하는 모듈이다. 신뢰 모듈 속 보안 운영절차는 PBFT, RAFT (Reliable, Replicated, Redundant and Fault Tolerance), BFT 등의 합의 알고리즘, POW, POS 방식, 사용자 입력기반의 맞춤 방식 등을 포함하며, 이들은 임의 선택이나 사전에 결정된 운영조건 기준에 의해 선택된다. 이 같은 합의 절차의 변

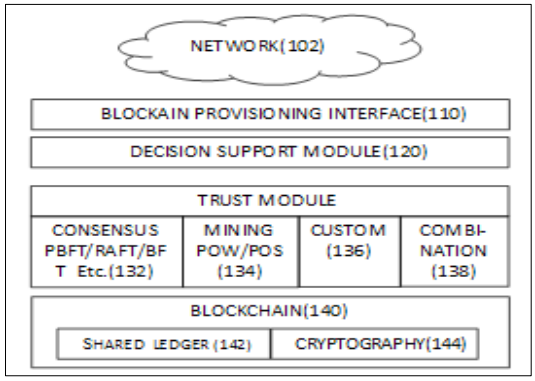

그림 2. 신뢰수준 변경 블록체인 설정 구조
Fig. 2. Blockchain Configuration for Changing of Trust Level

동성 반영 개념은 기술구성에 참조할 수 있다.

IoMT 표준동향 측면에서 애플리케이션 설계를 위해, ISO 27000-X, NIST CSF 2018, COBIT 같은 사이버보안 프레임 표준은 보안 프로토콜로 가능하나 미흡함이 있음을 지적하고, NIST 사이버보안 프레임 CSF V1.1을 확장하여 IoMT를 위한 복합적 사이버보안 프레임(HCSF:Hybrid Cyber Security Frame)에 사용하는 유용성을 언급하는 연구[29]를 참조할 수 있다. 거버넌스 관련, 정부의 효율 강화와 혁신 도구로서 BC의 역할과 필요성을 강조하는 연구[30]에서 언급한 미래지향적 보안 구현 과제인 보안 기반의 효율적 스마트계약 플랫폼 구축, BC 알고리즘 수정 및 보완을 위한 네트워크 참여자 전체의 신규 합의 메커니즘 개발, BC 프로세싱 성능향상을 위한 알고리즘 개발, 공공 BC에 비 공개형 데이터를 적절히 작동시키기 위한 영 지식(Zero Knowledge Proof), 다자간 연산(Multi-Party Computation), 동형암호(Homomorphic Encryption) 알고리즘 기반의 기술융합 검토, 자동인식기반의 BC 시스템 추진 등을 참조한다.

국내 기술 동향으로, IoT와 BC를 결합한 플랫폼 상용화가 가속화되고 있다. 국내 K 이통사가 발표(2019년 4월)한 BC 기반 IoT 보안솔루션은 신원이 검증된 송신자에게만 IoT 단말 IP 주소가 보이는 기술로 미검증된 익명의 송신자에겐 IoT 단말이 네트워크에서 보이지 않는 기술이다. BC에 사용자와 서버, IoT 단말 등 통신 관련 모든 요소의 고유 ID를 저장한다. 1회 용 상호인증 접속토큰을 발행해 IP가 아닌 ID 기반의 통신 보안을 보장한다. IoT 단말 해킹의 대부분이 인터넷을 통한 익명접속에 기인하므로, IoT 보안취약점 해결에 유용할 것으로 보인다. 다양한 온라인 신원인증 솔루션들의 제시에도 불구 더 우수한 신

뢰 기반 솔루션이 요구되면서, DID와 SSI 솔루션이 이슈화되고 있으나, 기존의 BC 및 비 BC 솔루션의 특성 평가 기준을 근거로 SSI에 BC 기술이 필수적은 아니라고 주장하는 연구[31]도 있어 검토 대상이다. 최근(2019년 6월)의 'FIDO(Fast Identity Online) 표준 기반 생체인증 기술 및 DID 블록체인 인증기술의 미래와 DID 표준 협력 네트워크 활성화 및 발전방안' 세미나에서 DID 관련 개인 보안위험에 대한 책임으로 개인과 서비스제공자(SP) 간의 책임 배분에 대한 이슈가 있었다. 개인인증 대상 자신이 본인임을 인증하는 신원정보(자격, 신용, 인증 등) 관리는 사용자와 기기 인증만으로 해결이 어려워 BC 기반 DID 협업과 인증기술 거버넌스의 활성화를 통한 해결 주장과 생태계 우선 생성, 보안성과 편의성을 향상한 비대면 실명확인, 인증 발행자 자격인증 이외 본인인증 방법의 결합 개발이 중요하다는 주장들이 있어 참조한다.

Ⅲ. 기술구성 및 설계 Scheme

보안 인증기술은 ID나 패스워드 같은 암기된 지식, 인증서나 OTP 같은 소유물, 신체의 구성요소 및 생리적 신호와 행동 특성 같은 생체특징과 같은 식별 및 인증요소와, 사용자, 공개 및 비공개 인증기관, 인증서비스 제공자 등의 기능 주체, 그리고 단말, 네트워크, 플랫폼, 앱 서비스 등의 인증시스템 요소로 구성된다. 다중인증에서 '다중'의 의미는 일반적 인증 구성요소와 다수(Multi/Multimodal/ Multi-factor)의 생체특징요소들을 결합 혹은 대체 활용하는 방법[32]이며, 생체특징의 융합 대상, 시점, 방법[33]에 따라 다양한 알고리즘 구성이 가능하다. 본 연구는 초기 과제 Scheme에 따라 다중보안 인증요소보다 BC 기반 다중보안 인증시스템에 대한 기술구성에 초점을 둔다.

BC 기반 IoMT 연동기술은 IoMT 플랫폼이나 기기를 직접 연동하는 방법이 있으며 플랫폼 연동을 디폴트로 고려하되 필요 경우 엣지 기기나 서버와의 연동도 고려할 수 있다. BC 인프라는 내부망을 우선으로 구성하되 부차적 연구에서 외부망과 BaaS 수준까지 단계별 확장 통합구성을 고려한다. 기존기술 대비 보안 인증 중계관리, 교차 보안 인증, 위험인증 차단 및 종료, 패킷 변조 및 탈취 체크, 추적성 보장, 비인가자 인증 자동차단 등의 차별성을 기본으로 한다. 스마트 기기와 IoMT 기기 간의 제삼자 보안 인증 구조에서 자체 및 외부 인증기관 사용자 자신의 본인 절대 인증 방법과 책임 배분 방법은 거버넌스에 의존적이므로 시범사업 기간엔 BC 기반 자체인증기능을 활용하는 구조로 제시 예정이다.

BC 기반 IoMT 기기 인증기술 구성은 IoMT 시스템 구성객체인 IoMT 기기와 기기를 원격제어하는 사용자 단말, IoMT 기기와 사용자 단말 인증 서버 간에 거래 발생 시 정보보호를 위해 사용자 단말과 IoMT 기기들에 대한 진위 및 변조 여부 식별과 서버를 통해 식별된 정보의 검증과 인증을 구현하는 기술이다. 핵심기술은 해킹의 원천적 차단이 가능한 BC 기술 기반의 다중보안 인증체계 구축기술이며, IoMT 기기의 보안 모듈 개발, IoMT 기기와 단말 간의 다중보안 BC 시스템과 사용자 앱 개발, 시험 및 검증의 3단계로 구성된다. 인증의 핵심단계는 <그림 3>과 같이, 첫째 IoMT 기기의 등록 해시값과 관련 정보를 BC에 기록하는 단계, 둘째 IoMT 제어기능 요청 시 사용자 단말이 수신한 해시값을 수신하고 첫째 단계 기능상의 해시값 관련 정보를 이용하여 인증 해시값의 진위 및 위조 여부를 판별하는 단계, 셋째 이전 단계에서의 인증 해시값이 정상 입증될 경우 IoMT 기기 제어를 승인하는 3단계 구조이다.

실증프로젝트는 IoMT시스템에 대한 BC 기반의 다중보안 인증기술과 설계 Scheme으로 구성된다. 보안 인증기술의 구성요소는 기기(노드) 등록 및 BC에 기록, 제어요청 및 인증과 제어승인 처리를 위한 플랫폼과 네트워크, 블록체인 정보저장 Ledger DB, 엣지 클라우드, 건강관리 통합 DB, 웹 관리자, IoMT 애플리케이션 및 IoMT 기기 사용자(의료진 및 건강관리 참여자, 환자, 관련 서비스제공자) 등이며, 주요 설계내용은 다수 식별정보를 BC를 통해 등록하고 상호접속 인증을 제어하는 통합적 보안모듈 및 플랫폼과 실증기술로 구성된다. 노드에서 BC 기반 다중보안 플랫폼

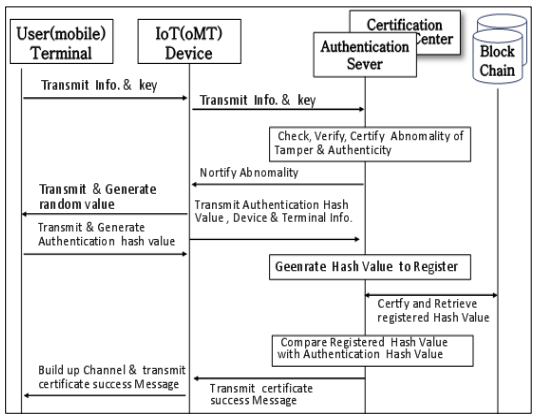

그림 3. 블록체인 기반 다중보안 인증 단계
Fig. 3. Blockchain based Multi Security Authentication Phases

개발을 위한 비 공개형 BC 기반 다중인증 프레임 구성은 <그림 4>와 같다.

핵심기술은 IoMT 서비스 객체 간 상호 비인가 접속을 방지하기 위한 BC 기반의 통합된 자동식별자 발행과 관리체계 설계 및 운영기술이다. 회원 서비스제공자(MSP)의 신원인증과 관련된 다중생체인식과 SIS 및 DID 등은 비공개 연구 대상이다. IoMT 기기에 BC 기술을 활용하여 통합인증하는 기술은 2019년 상반기 기준으로 국내의 실제 적용 및 검증사례가 없어 차별성 부여가 가능하다. ISO TC215 WG 기준에 의한 기술구성의 차별성은 사용자 식별정보관리, 인증방식, 보안 체크, 해킹 탐지조치, 비인가자 사용인증 불허, 국제표준 프로토콜 탑재, 별도 보안키 측면에서 우위적 성능을 보일 수 있다. 특히 IoMT 시스템의 해킹에 대비하는 3자 보안 인증 서버는 <그림 5>의 3자 보안 인증 서버 구성과 같이 별도의 사물인증센터를 통해 인증받는 형태를 활용한다.

시차를 두고 개발되는 기술은 첫째, IoMT 기기 보안 모듈 및 연동 플랫폼을 위한 기기와 모바일 단말 간 보안 인증 통신, 데이터 암호화, 해킹인지 및 알림 모듈, 기기 보안플랫폼 개발 및 설계기술, 둘째 다중보안 인증 시스템개발을 위한 데이터분할분산 저장 및 블록저장 데이터 개발 및 설계기술, BC 네트워크 저장 정보 조회 인증키 생성기술 개발 및 설계기술, 셋째 기기의 BC 및 서버연동 API 개발을 위한 API 설계기술, 앱 기획 및 디자인 기술, 넷째 기기 성능 고도화개발 및 설계기술, 다섯째 다중보안 BC 플랫폼 계발을 위한 네트워크, 접근제어, 스마트계약 API, 합의 알고리즘의 개발 및 설계기술, 여섯째 데이터사용자를 위한 UI/UX, 사용자 정보인증 다중보안시스템, BC 계약 API 및 연동 개발 및 설계, 일곱째 커뮤니티 모델과 시스템 검증기술 등으로 구성된다.

핵심기술은 모바일 단말 및 IoMT 기기 간의 다중보안 인증시스템 개발기술로, 모바일 단말 접속 시 BC와 데이터베이스를 이용한 사용자 신원인증기술, 데이터베이스 블록저장 데이터 설계기술, 인증키 생성기술이다. 사용자 신원인증기술은 사용자 자신의 본인 절대 인증과 IoMT 서비스제공자와 관리책임 범위에 대한 합리적 배분이 핵심이며 해결과제이기도 하다.

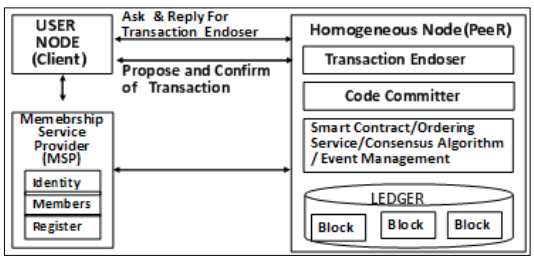

그림 4. 블록체인 기반 다중보안 인증의 기본 인증 프레임
Fig. 4. Basic Security Certification Frame by blockchain based multi security authentication

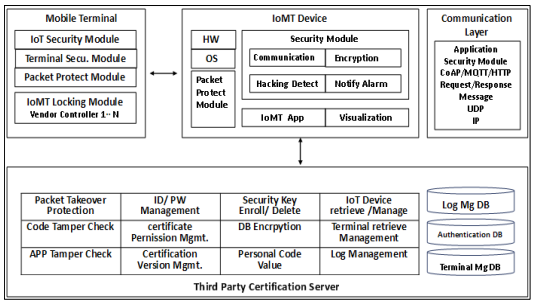

그림 5. 제삼자 보안 인증 서버플랫폼 구성
Fig. 5. Configuration of Third Party Security Certification Server Platform

Ⅳ. 결 론

BC 기반의 다중보안 인증시스템의 신규 기술구성 및 설계 Scheme의 제시와 의료사물인터넷(IoMT) 보안체계 구축 및 실증 프레임 제시를 통해 연구의 1차 자문목적이 달성되었다. 1차 선정된 과제의 단계별 추진을 통해 개발 및 실증과 검증, 사업화 등으로 연구의 최종목적이 달성될 것이며 기업의 사업화 과정에서 기술적용 범위와 법제화 수준에 따라 솔루션의 기술적 완성도 충족이 예상된다.

향후 IoT 분야별 보안 분야에서 BC 기반 혼합 알고리즘 기반 인증시스템과 상용화 사례가 증가하고, 엣지 컴퓨팅과 모바일 기기 등과의 결합이 가속화되면서 본 연구와 같은 경량화된 저가격 솔루션의 확산 전망이 있으나 연구 초기의 PBFT 기반 비 공개형 다중보안 메커니즘과 알고리즘도 솔루션의 복합적 기술변화 내용에 대응해야 할 점이 있다. 특히 신원 관리 부문에서 국내에서 지명도가 높고 접촉이 많은 해외 S사의 신원 관리 솔루션과 같이 단일특정의 제삼자에 의존하는 경우 중앙집중에 의한 신뢰 여부나 보안 취약성을 들어 부정적 의견이 있음을 주목해야 한다. 제3 자 인증 주관에 대한 뚜렷한 제약이 없어 누구나 비 공개형 보안 메커니즘의 주체가 될 수 있으나 전문성이나 신뢰의 정도, 책임과 권한의 공공성 인정문제는 해결과제이다. 다수국내업체와 개발자들도 유사개념의 솔루션을 개발 및 출시할 예정이어서 연구 주관 및 참여기업도 비 공개형 이외에 공개형 인증서비스 제

공을 계획하는 만큼 기술 추이와 회원 반응에 따른 알고리즘 변경과 경량화 경쟁요소에 대한 심층검토가 필요하다. 향후 연구에서 적용 알고리즘의 차별성 보완 및 적용 타당성 검토와 실무적 해결 이슈를 제시할 예정이다. 특히 모바일 부문의 BC 기반 통합보안, 엣지 컴퓨팅과 기존 클라우드 기반 복합알고리즘, 사용자본인 절대 인증을 위한 생체인증 알고리즘, SSI 및 DID 통합적용 가능성 연구를 계속할 예정이다.

References

[1] A. Panarello, et al., "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, Aug. 2018.

[2] R. Zhang and B. Preneel, "Lay down the common metrics: Evaluating proof-of-work consensus protocols' security," *40th IEEE Symp. Secur. and Privacy*, last revised, Jul. 2019.

[3] Cong T. Nguyen, et al., "Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities," *IEEE Access*, vol. 7, pp. 85727-85745, Jun. 2019.

[4] R. Angeles, "Blockchain-based healthcare: Three successful proof-of-concept pilots worth considering," *J. Int. Technol. and Inf. Management*, vol. 27, no. 3, Article 4, 2019. Available at: https://scholarworks.lib.csusb.edu/jitim/vol27/iss3/4, 2019.

[5] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *NIST, NISTIR 8202*, Oct. 2018.

[6] R. Schmid and R. Wattenhofer, "A permit-based optimistic byzantine ledger," *eprint arXiv:1906.10368*, Jun. 2019.

[7] A. Prabhakar and T. Anjali, "TCON - A lightweight trust-dependent consensus framework for blockchain," *IEEE: 11th Int. Conf. Commun. Syst. & Netw. (COMSNETS)*, Jan. 2019.

[8] W. Viriyasitavat, L. D. Xu, Z. Bi, and A. Sapsomboon, "New blockchain-based architecture for service inter operations in internet of things," *IEEE Trans. Computational Social Syst.*, vol. 6, no. 4, pp. 739-748, Aug. 2019.

[9] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: Survey," *IEEE Internet of Things J.*, Available at: https://arxiv.org/abs/1906.00245, Jun. 2019.

[10] K. Wang, Y. Shao, L. Shu, C. Zhu, and Y. Zhang, "Mobile big data fault-tolerant processing for e-health networks," *IEEE Network*, vol. 30, no. 1, pp. 36-42, Jan. 2016.

[11] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31-37, Jan. 2018.

[12] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, Available at:https://doi.org/10.1007/s10916-018-0982-x, 2018.

[13] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan, "Blockchain and big data to transform the healthcare," in *Proc. ICDPA ACM*, pp. 62-68, Guangdong, China, May 2018.

[14] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, "A decentralizing attribute-based signature for healthcare blockchain," in *27th ICCCN*, pp. 1-9, Hangzhou, China, 2018.

[15] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469-72478, 2018.

[16] M. Bez, G. Fornari, and T. Vardanega. "The scalability challenge of ethereum: An initial quantitative analysis," *2019 IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, San Francisco East Bay, CA, USA, May 2019.

[17] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto,

"*BigchainDB, A scalable blockchain database*," Available at: https://www.bigchaindb.com/ whitepaper/bigchaindb-whitepaper.pdf, Mar. 2018.

[18] R. G. Brown, "*The Corda Platform: An Introduction*," Available at https://www.corda.net/content/corda-platform-whitepaper.pdf, May 2018.

[19] T. K. Sharma, "*Top 10 blockchain platforms you need to know about*," Available at https://www.blockchain-council.org/blockchain/top-10-block chain-platforms-you-need-to-know-about/, 2019.

[20] GemOS, "*The blockchain operating system*," Available at https://enterprise.gem.co, Jun. 2019.

[21] G. Greenspan, "*Off-Chain(Alpha 3) Multichain 2.0*," Available at https://www.multichain.com /blog/2018/06/scaling-block chains-off-chain-data/, Jun. 2019.

[22] T. Fleming, "*Decentralized identity management for a maritime digital infrastructure: With focus on usability and data integrity*," Master Thesis, Linköping University, pp. 1-21, Available at http://www.diva-portal.org/smash/search.jsf?dswid=-8287, 2019.

[23] A. D. Dwivedi, et al., "*Decentralized privacy-preserving healthcare blockchain for iot*," Sensors, Available at http://www.mdpi.com/journal/sensors, 2019.

[24] Y. Ren and F. Zhu, et al., "Identity management and access control based on blockchain under edge computing for the industrial internet of thing," *Appl. Science,* Sep. 2019.

[25] S. K. Lo, et al., "Analysis of blockchain solutions for IoT: A systematic literature review," *IEEE Access*, vol. 7, May 2019.

[26] Y. Jiang, et al., "A cross-chain solution to integrating multiple blockchain for IoT data management," *Sensors,* May 2019.

[27] X. Zheng, et al., "Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies," *J. Med. Internet Res*. 2019, vol. 21, Jun. 2019.

[28] Dinh C. Nguyen, "Blockchain for secure EHRs sharing of mobile cloud based e-health system," *IEEE Access*, vol. 7, May 2019.

[29] D. Nkomo and R. Brown, "Hybrid cyber security technology for the internet of medical things, blockchain and clinical trial," *Springer Chem.*, pp. 211-229, Apr. 2019.

[30] M. Jun, "Blockchain government- A next form of infrastructure for the twenty-first century," *J. Open Innovation: Technol., Market, and Complexity*, vol. 4, no. 7, 2018.

[31] D. van Bokken, et al., "*Self-sovereign identity solutions: The necessity of blockchain technology*," Available at.: https://www.researchgate.net/publication/332750774, Jun. 2019.

[32] B. Cho and J. M. Park, "Technology review on multimodal biometric authentication," *J. KICS*, vol. 40A, no. 01, pp. 132-141, Jan. 2015.

[33] J. M. Park, "Authentication technology and tasks based on fusion of multimodal biometric information," *KOSEN Report 2019(KISTI),* Sep. 2019, (http://www.kosen21.org)

박 종 만 (Jong-Man Park)

1978년 2월 : 인하대학교 산업공학 학사

1983년 8월 : 연세대학원 경영석사

1987년 2월 : Lehigh Univ. IE 정보과학 석사(박사 수학)

1997년 2월 : 인하대학교 산업공학 박사

1998~2014년 : 유한대학교 초빙 및 겸임 교수

2008~2017년 : KISTI ReSEAT 전문 연구위원

2018~2019년: Koita ReSEAT 전문위원(현)

<관심분야> IIoT, IoMT, 엣지 컴퓨팅, 스마트 제조, AI, 보안

[ORCID: 0000-0002-3603-3037]