프라이빗 블록체인 기반의 시험평가서 위변조 방지 기술 설계 및 구현

김형진[1], 차중혁[2], 이재민[3], 김동성*
주식회사 엔에스랩 기술연구소[1,2,*], 금오공과대학교 {IT융복합공학과[3,*]}
{haengg[1], jh.cha[2]}@nslab.tech, {ljmpaul[3], dskim*}@kumoh.ac.kr

Design and Implementation of Private Blockchain-based Forgery Prevention Technique

Hyeong-Jin Kim[1], Joong-Hyuck Cha[2], Jae-Min Lee[3] and Dong-Seong Kim*
NSLab Co., Ltd. Technology Research Institute[1,2,*],
Kumoh National Institute of Technology Dept. of IT Convergence Eng.[3,*]

요 약

본 논문은 스마트 제조환경에서 사용되는 장비의 시험평가서에 대한 신뢰성 및 보안성 향상을 위해 프라이빗 블록체인을 이용하여 시험평가서 위변조 방지 시스템을 제안한다. 스마트 제조환경에서 사용하는 장비에 대한 시험평가서는 성능평가 및 신뢰성 검증 테스트로부터 발행되어 운용되고 있다. 하지만 현재 운용되고 있는 시험평가서는 서류 저장 및 관리 방식에 따라 위변조 문제에 노출되어 품질 및 성능평가와 관련한 위험이 있다. 이러한 문제를 해결하기 위해 본 논문에서는 프라이빗 블록체인 기술을 활용하여 시험평가서 위변조 방지가 가능한 기술을 제안한다. 제안하는 기술은 시험평가서가 발행됨과 동시에 시험평가서 원본을 3가지의 암호화 알고리즘을 복합적으로 적용하여 무결성 검증 기능을 지원한다. 시험평가서 정보를 블록체인에 저장함과 동시에 스마트 컨트랙트를 활용하여 각 데이터의 무결성을 강화하여 스마트 제조환경에서 시험평가서에 대한 신뢰성과 보안성을 높이는 데에 기여할 것으로 기대된다.

Ⅰ. 서 론

스마트 제조환경은 현대 제조산업에서 혁신적인 기술과 정보통신 기술을 통합하여 생산 프로세스를 최적화하고 효율적으로 관리하는 환경이다. 현대 스마트 제조환경에서 사용되는 다양한 장비들은 제조 공정에서의 성능과 효율성을 결정짓는 핵심 요소로 작용한다. 이러한 장비들의 성능 시험평가서는 각종 제조 장비의 성능, 안정성, 정확성 등을 측정하고 문서화한 보고서로 생산 프로세스의 효율성을 최적화하고 제품 품질을 보장하기 위해 중요한 문서이기에 신뢰성과 무결성이 보장되어야 한다[1]. 하지만 기존의 중앙 집중식 서버 기반의 시험평가서는 성능평가 결과물 및 평가 정보를 중앙 서버에 집중적으로 저장하고 관리하는 시스템으로 중앙화된 데이터베이스를 사용하기 때문에 평가 결과 데이터의 위변조 가능성과 보안 문제에 취약하다. 한편 블록체인 기술은 분산 원장을 통해 모든 거래와 데이터 변경 이력을 체인 형태로 기록함으로써 모든 데이터가 추적이 가능하며 블록체인에 저장된 데이터는 변경이 어려워 데이터의 무결성 측면에서 장점을 갖고 있다[2]. 이러한 특성으로 신뢰성과 보안성이 요구되는 시스템에서 다양하게 활용되고 있고 특히 디지털 문서의 위변조 방지를 위한 시스템에서 활발히 연구되고 있다. 하지만 기존 연구들은 스마트 제조환경과 같은 고신뢰성이 요구되는 시스템에 대한 고려가 부족하다.

따라서 본 논문에서는 프라이빗 블록체인을 활용하여 스마트 제조환경을 위한 시험평가서 위변조 방지가 가능한 기술을 제안한다. 제안하는 기술은 발행된 시험평가서 파일을 3가지 암호 알고리즘에 적용하여 위변조 방지 기법을 설계한다. 시험평가서 발행부터 저장까지 일련의 모든 과정은 프라이빗 블록체인에 저장되며 기존 시스템과 독립적으로 작동하기 때문에 기존 시스템에 적용이 쉽게 가능하다. 또한 무결성 검증을 통해 위변조 방지 시스템을 제공함으로써 신뢰성 높고 데이터가 무결한 시스템을 구축할 수 있다.

Ⅱ. 스마트 제조환경을 위한 블록체인 기술 적용 분석

블록체인은 데이터 교환 시 기존 중앙 집중 서버가 아닌 분산형 구조로 데이터를 기록하고 관리하는 기술이다. 블록체인은 중앙 집중 서버의 단일 지점 장애에 대한 취약성을 줄이고, 네트워크 참여자들 간의 권한과 책임을 분산시킨다. 또한 한번 기록된 데이터는 수정이 어렵기 때문에 데이터의 신뢰성과 무결성을 확보할 수 있다.

현대 제조업에서는 빅데이터, 사물인터넷(IoT), 클라우드 컴퓨팅과 같은 첨단 기술의 적용으로 스마트 제조환경이 등장하고 있다[3]. 이는 생산 프로세스의 최적화와 효율성 향상을 목표로 하며, 자동화, 데이터 활용, 분석 등이 주요 특성으로 부각되고 있다. 이러한 특성들은 제조 프로세스의 실시간 모니터링, 데이터 기반 의사 결정, 자율화된 생산 과정 등을 가능하게 한다. 스마트 제조환경에서 블록체인은 데이터의 불변성과 신뢰성을 제공하여 제조환경에서 발생하는 다양한 데이터의 정확성을 보장한다. 특히 장비에 대한 성능 시험평가서는 평가 대상 장비, 시험 방법 및 절차, 평가 대상 속성, 평가 결과와 같은 많은 데이터가 발생하고 이러한 데이터에 대해 신뢰성 및 무결성을 확보해야 한다.

Ⅲ. 제안하는 프라이빗 블록체인 기반 시험평가서 위변조 방지 시스템

그림1은 제안하는 프라이빗 블록체인 기반의 시험평가서 위변조 방지 시스템 구조이다. 스마트 제조환경에서 사용하는 장비의 시험평가서가 발급되면 DAPP(Decentralized Application)은 특정 디렉터리에 새로운 시험평가서가 발행되는 것을 감지하고 암호화 처리를 진행한다. 암호화 처리는 필요시 복호화를 위해 양방향 암호화 알고리즘인 AES(Advanced Encryption Standard)를 적용한다. 암호화 처리와 동시에 원본 시험평가서 데이터를 단방향 암호화 알고리즘인 SHA-256을 사용하여 해시값을

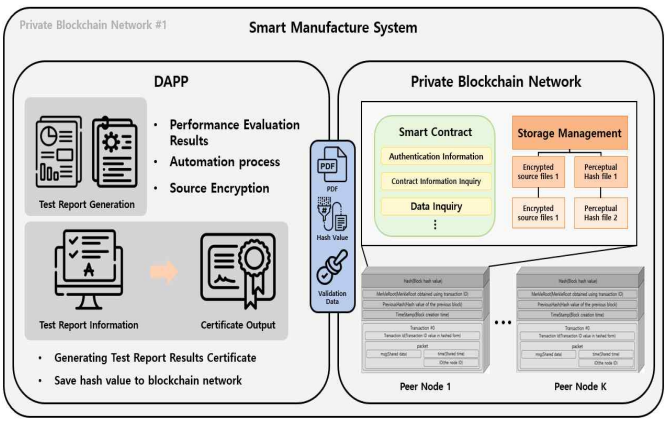

그림 1 제안하는 프라이빗 블록체인 기반의 시험평가서 위변조 방지 시스템 구조

생성하고 Smart Contract를 통해 블록체인에 저장한다. 블록체인에 저장된 원본 데이터는 영구히 보존되며 추후 무결성 검증 알고리즘에 의해 사용된다.

시험평가서의 위변조 유무를 판단하기 위해 본 논문에서는 지각 해시(Perceptual hash) 알고리즘을 적용하였다. 지각 해시 알고리즘은 입력 데이터의 특징을 추출하여 고정된 크기의 해시값으로 변환하는 알고리즘이다. 해시 알고리즘의 특성상 동일한 데이터를 해시값으로 출력하면 동일한 해시값이 출력된다. 따라서 PDF 데이터를 기반으로 해시값과 일치하지 않는 경우, 위변조되었다고 판단할 수 있다. 그림2는 시험평가서 일치도 대조를 위한 지각 해시 파일 예시이다. 제안하는 위변조 방지 기술에서는 시험평가서 원본 PDF 파일 데이터를 추출하고 정규화하여 16진수 문자열인 해시값으로 출력한다. 이러한 지각 해시값은 블록체인 노드 내에서 최초의 시험평가서가 발행되었을 때, AES 암호화 알고리즘 적용과 병렬적으로 생성되고 데이터베이스에 저장된다.

그림3은 제안하는 블록체인 기반의 시험평가서 위변조 기술의 순서도이다. 위변조검증 DAPP을 실행하면 검증하려고 하는 파일의 데이터를 추출한 뒤 지각 해시값으로 변환한다. 지각 해시값은 스마트 제조환경에서 사용되는 장비의 특성상 고신뢰성을 만족해야 하므로 다양한 환경에 적용할 수 있도록 변환할 수 있다. 변환된 지각 해시값은 사전에 저장된 원본 시험평가서 지각 해시값과 비교되어 일치도를 추출한다. 일치도는 시험평가서 PDF파일을 사전에 정의된 데이터 크기로 나누어 해시값으로 변환한 뒤 원본 해시값과 대조하여 계산한다. 대조한 일치도 결과가 100%일 경우 원본 시험평가서의 해시값과 비교하여 최종적으로 검증하려는 파일의 위변조검증 결과를 도출한다. 제안하는 위변조검증 과정은 원본 데이터의 단방향 암호화 알고리즘을 적용한 해시값과 일치도 추출을 위한 지각 해

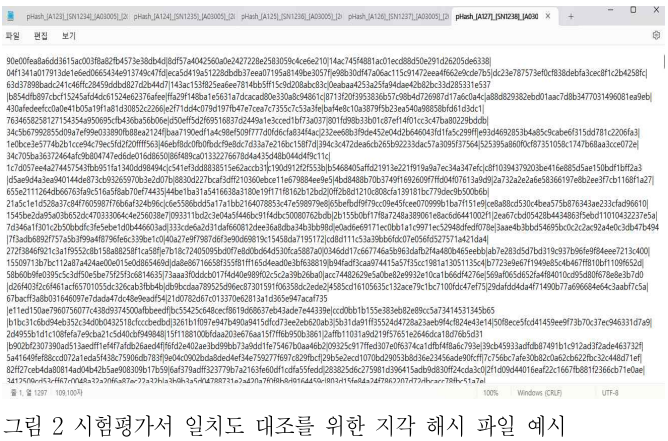

그림 2 시험평가서 일치도 대조를 위한 지각 해시 파일 예시

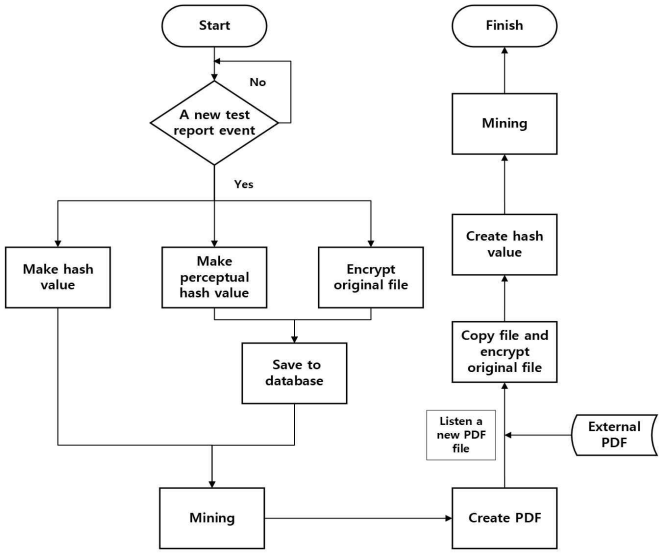

그림 3 시험평가서 위변조 검증 과정 순서도

시값의 교차검증을 통해 신뢰성 및 데이터에 대한 무결성을 확보하였다. 스마트 제조환경에서 장비 시험평가서를 운용하는 환경은 자동/수동 시험관리 시스템을 중심으로 운용되나, 기존에 발급된 성적서, 외부 평가 기관을 통해 발급받은 성적서 등 다양한 사용환경을 고려해야 한다. 따라서 지각 해시값과 암호화된 원본 데이터는 특정 디렉토리 내에 저장되는데, 이는 다양한 사용환경을 운용해야하는 스마트 제조환경을 지원하기 위함이다.

Ⅳ. 결론

본 논문에서는 스마트 제조환경을 위한 프라이빗 블록체인 기반 시험평가서 위변조 방지 기술을 제안하였다. 제안하는 기술은 AES 알고리즘, 지각 해시 알고리즘, SHA-256 암호화 알고리즘과 같은 3가지 암호화 알고리즘을 복합적으로 적용하여 시험평가서에 대한 무결성 검증 기능을 지원한다. 각각의 데이터는 블록체인 Smart Contract를 통해 관리되어 시험평가서에 대한 신뢰성과 보안성을 높이는 데에 기여할 것으로 기대된다.

향후 연구로는 제안하는 시스템의 성능평가 및 마이닝에 필요한 리소스 감소를 위한 최적화 연구를 수행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2023년도 과학기술정보통신부의 재원을 지원받아 수행된 연구임(1711202170/2023-IT-RD-0083-01).

참 고 문 헌

[1] M. A. P. Putra, A. P. Hermawan, D.-S Kim and J.-M. Lee, "Data Prediction-Based Energy-Efficient Architecture in Industrial IoT", IEEE Sensors Journal, vol. 23, no. 14, pp. 15856-15866, 2023.

[2] I. S. Igboanusi, A. Allwinnaldo, R. N. Alief, M. R. R. Ansori, J.-M. Lee and D.-S. Kim, "Smart auto mining(SAM) for industrial IoT blockchain network", IET Commun., vol. 16, no. 18, pp. 2123-2132, 2022.

[3] A. Corallo, A. M. Crespino, M. Lazoi and M. Lezzi, "Model-based Big Data Analytics-as-a-Service framework in smart manufacturing: A case study", Robotics and Computer-Integrated Manufacturing, vol. 76, no. 102331, pp. 1-15, 2022.