블록체인 기반 제조데이터 거래의 데이터 암호화 및 키 전달 방법에 관한 연구

김용길[1], 박부곤[1], 배경훈[1], 최민성[1], 윤태현[2]

[1]비피앤솔루션, [2]한국전자통신연구원

[1]{ykkim, bgpark, khbae, mschoi}@bpnsolution.com, [2]thyoon0820@etri.re.kr

A Study on the Data Encryption and Key Transfer Methods in Blockchain-Based Manufacturing Data Transactions

Youngkil Kim[1], Bugon Park[1], Kyunghoon Bae[1], Minsung Choi[1], Tae Hyun Yoon[2]

[1]BP&Solution Co.,Ltd., [2]Electronics and Telecommunications Research Institute

요 약

본 논문은 전년도 수행한 블록체인 기반 제조 기업 데이터 거래방법에 관한 고도화 연구를 구현하며 데이터의 암호화가 필요하며, 암호화 키를 전달하는 방식에 관해 연구하였다. 제조데이터의 특징은 데이터가 다양하고, 대용량으로 보관되어 있으며, 각 기업의 노하우가 포함되어 있어 기업들이 거래를 꺼리고 있다는 점이다. 이를 보완하기 위해 데이터 거래 시 암호화가 필요하였다. 본 연구에서는 블록체인을 활용한 데이터의 암호화 방식과 암호화된 키의 전달 방식에 대한 방법을 제시하고자 한다.

Ⅰ. 서론

4차 산업 혁명 시대는 정보통신기술(ICT)의 눈부신 발전과 함께 데이터의 양이 기하급수적으로 증가하는 전환기를 맞이하고 있다. 이러한 데이터의 폭발적 증가는 다양한 산업 분야에서 혁신을 촉발하는 핵심 원동력이 되고 있으며, 특히 빅데이터와 인공지능(AI) 기술의 발전은 그 잠재력을 더욱 확장하고 있다. 국내에서도 정부는 지능화 기반 구축을 위해 빅데이터[1]와 AI 기술을 적극적으로 지원하는 다양한 사업들을 추진하고 있으며, 이는 산업 경쟁력 제고와 사회적 난제 해결에 실질적으로 기여하고 있다.

하지만 데이터의 안전한 거래와 활용은 여전히 해결해야 할 중요한 과제로 남아있다. 데이터 거래의 활성화를 위해서는 거래 당사자 간 신뢰 구축이 필수적이며, 이를 위해 데이터의 안전한 암호화가 필요하다. 데이터가 암호화되면 외부의 위협으로부터 보호될 뿐만 아니라, 거래 당사자만이 해당 데이터에 접근할 수 있게 된다. 이러한 암호화 기술은 데이터의 무단 접근을 차단하고, 데이터 거래의 투명성을 높이며, 개인정보 보호를 강화하는 데 결정적인 역할을 수행할 수 있다.

따라서 본 논문에서는 4차 산업 혁명 시대의 데이터 중요성을 부각시키고, 국내 정부의 빅데이터 및 AI 기술 지원사업의 필요성을 심도있게 논의하며, 안전한 데이터 거래를 위한 암호화 방법의 필요성과 적용 가능성을 자세히 살펴보고자 한다. 이를 통해 데이터 기반의 혁신적인 서비스와 솔루션 창출을 위한 명확한 방향성을 제시하고, 안전하고 신뢰할 수 있는 데이터 거래 생태계 조성[2]에 기여할 수 있을 것으로 기대된다.

본 논문에서는 데이터 거래소를 위한 블록체인의 SmartContract 기술과 분산신원 증명 및 분산 데이터 관리 기술을 적용한 안전한 데이터 거래방법을 제시하고자 한다.

Ⅱ. 본론

1) 대칭키 암호화 방식과 비대칭 키 암호화 방식 특징

암호화 방식은 크게 대칭키 암호화 방식과 비대칭키 암호화 방식으로 구분할 수 있다[3]. 이 두 가지 방식은 암호화와 복호화의 암호키가 같은지를 가지고 구분을 할 수 있다. 두 가지 방식의 특징을 정리하면 아래의 표와 같이 정리할 수 있다. 대칭키의 특징은 암호화키와 복호화 키가 동일하므로 키 길이가 짧아도 사용할 수 있으며, 암복호화 속도가 빠르므로 경제성이 높다고 볼 수 있다. 비대칭키는 암호화 키와 복호화 키가 다르므로 키 길이가 길고 암복호화 속도가 대칭키에 비해 느린 특징을 가지고 있다. 대칭키 암호화 방법은 일반적인 데이터의 암호화에 많이 사용되며, 비대칭키의 경우 인증과 전자서명 등에 많이 활용된다.

표 1 대칭키 비대칭키 특징 비교[3]

	대칭키	비대칭키
키 관계	암호화 키 = 복호화키	암호화 키 ≠ 복호화 키
암호화 키	비밀키	공개키
복호화 키	비밀키	개인키
비밀키 전송	필요	불필요
키 길이	짧다	길다
인증	곤란	용이
암복화 속도	빠르다	느리다
경제성	높다	낮다
전자서명	복잡	간단
주 용도	고용량 데이터 암호화(기밀성)	키 교환 및 분배, 인증, 부인방지
장점	- 암·복호화 키 길이가 짧다 - 구현이 용이하고 암·복호화가 빠르다 - 암호화 강도 전환이 용이 - 암호화 기능이 우수 - 각종 암호 시스템의 기본으로 활용	- 사용자가 증가하더라도 관리해야 할 키의 개수가 상대적으로 적다 - Key 전달이나 교환에 적합하다 - 인증과 전자 서명에 이용 - 대칭키 보다 확장성이 좋다 - 여러가지 분야에서 응용이 가능 - 키 변화의 빈도가 적음
단점	- 키 교환 절차가 명시되지 않음 → 키 분배가 어렵다 - 관리할 암·복호화 키가 많다 N명 → N(N-1)/2 - 확장성이 낮다 - 전자서명(디지털서명)이 불가능 - 부인방지 기능이 없다	- 키 길이가 길다 - 복잡한 수학적 연산을 이용함으로 암호화·복호화 속도가 느리다 - 중간에 인증과정이 없으므로 중간자 공격에 취약하다 (전자서명,인증서 등으로 해결)

2) 비대칭 키 암호화 방식을 통한 대용량 데이터 암호화 확인

데이터 거래는 주로 대용량 데이터를 기반으로 이루어지며, 이 과정에서 암호화 및 복호화 시간과 암호화 후 파일 크기의 변화가 중요한 요소이다. 이를 확인하기 위해 AES-256-CBC와 AES-256-GCM(대칭키 암호

화 방식), 그리고 RSA-2048과 RSA-4096(비대칭키 암호화 방식)을 사용하여 각각 10MB(용량이 작은 경우 비교) 및 100MB(용량이 커진 경우 비교) 파일을 10번씩 암호화 및 복호화하였다. 그 결과 파일 크기의 변화와 암호화 및 복호화 시간을 측정할 수 있었다. 각 암호화 방식을 적용한 코드 내용은 다음과 같다.

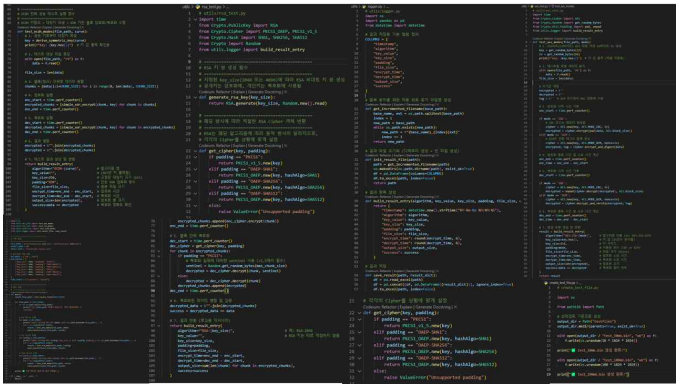

그림 1 암호화 테스트 코드 구성

3) 대칭키와 비대칭 키를 활용한 암호화 방식 결과 확인

대칭키 암호화 방식에서는 암호화 전후의 파일 크기 변화가 거의 없으며, 암호화 및 복호화 시간도 큰 차이가 나타나지 않았습니다. 또한, 원본 파일의 크기가 증가할 경우 암호화 및 복호화 시간도 비례하여 증가하였다. 반면, 비대칭키 암호화 방식에서는 암호화 이후 파일 크기가 최대 2배까지 증가했으며, 복호화 시간은 암호화 시간보다 최소 6배에서 최대 10배까지 더 소요되었습니다. 또한, 파일 크기가 증가함에 따라 암호화 및 복호화 시간도 비례적으로 증가하는 것을 확인할 수 있다. 이러한 결과를 바탕으로, 데이터 암호화에는 대칭키 방식이 효과적인 방법으로 확인되었으나, 대칭키 방식에서는 암호키를 안전하게 전달해야 하는 문제가 발생한다. 이를 해결하기 위해 비대칭키 암호화 방식을 활용하여 암호키를 안전하게 전달한다면, 암호화된 파일이 잘못 전달되더라도 개인키를 가지고 있는 당사자가 아니라면 해당 암호 파일을 복호화할 수 없어 보안성이 유지될 수 있다.

표 2 암호화 방식에 따른 암복호화 테스트 결과

방식	알고리즘	키 크기 (bits)	패딩 방식	평균 암호화 시간 (초)	평균 복호화 시간 (초)	암호화 전후 크기 비율 평균
대칭키	AES-256-CBC	256	CBC	0.037	0.035	1.00001
	AES-256-GCM	256	GCM	0.017	0.019	1.000001
비대칭키	RSA-2048	2048	PKCS1	28.3	197.5	1
	RSA-2048	2048	OAEP-SHA256	42.1	259.6	1.34
	RSA-2048	2048	OAEP-SHA512	58.2	385.6	2.03
	RSA-4096	4096	PKCS1	51.6	530.8	1.04
	RSA-4096	4096	OAEP-SHA256	61.9	600.3	1.34
	RSA-4096	4096	OAEP-SHA512	69.6	698.1	2.03
	ECDH-secp256r1	256	XOR	1.35	1.35	1.02
	ECDH-X25519	256	XOR	1.35	1.36	1.3

4) 블록체인 hyperledger INDY를 이용한 키 전달 방식 구현

대칭키를 이용한 파일데이터의 암호화 후 해당 대칭키를 블록체인에 공개되어있는 거래 대상자의 public key로 암호화하여 전달한다. 데이터 구매자는 자신이 보유하고 있는 private key로 데이터를 복호화할 수 있다. 블록체인의 활용은 부산 저장소와 영지식 증명을 통한 사용자 인증의 통해 데이터의 공유를 더 편리하게 진행할 수 있다. 제조데이터 보호 거래 플랫폼에서 사용하고 있는 분산신원증명(DID)에서 사용하는 암호화 방식은 ECDH-X25519 방식[5]이다. 이를 사용하여 사용자의 인증, 데이터의 전송, 메시지 전송 등으로 활용하고 있다. 이에 해당 기능을 통해 데이터의 암호화 키 전달을 한다면 암복호화 속도와 데이터 키의 안전한 전달이 가능한 구조로 적용할 수 있다.

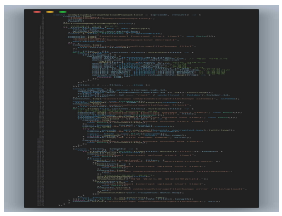

그림 2 파일 암호화 후 저장(대칭키)

그림 3 파일 위치 및 암호키 암호화 후 전송(비대칭키)

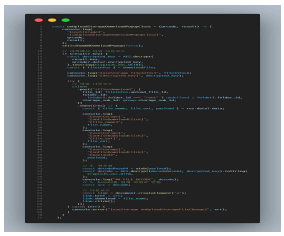

그림 4 파일다운로드 후 복호화(대칭키)

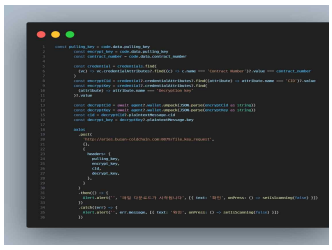

그림 5 파일 위치 및 암호키 확인을 위한 복호화(비대칭키)

Ⅲ. 결론

본 논문에서는 제조 기업들이 보유하고 있는 데이터의 부가 가치 창출 및 새로운 자원으로 조명되고 있는 데이터의 활용을 위한 거래 방식에서 데이터의 암호화와 암호화키 전달 방식에 블록체인 기술의 적용을 통한 시스템을 제안하였으며, 울산에서 연구개발 후 실증을 진행하고 있다. 추후 제조 기업의 데이터뿐만 아니라 유통기업, 농작물 생산기업 등 다양한 기업들이 데이터를 활용하고 유용하게 사용할 수 있는 시스템으로 전국으로 확대 적용할 계획이다.

ACKNOWLEDGMENT

본 논문은 한국전자통신연구원 기본사업과 울산광역시-ETRI 공동협력사업의 지원을 받아 수행되었음. [25ZS1210, 산업현장에서의 사람-이동체-공간 자율협업지능 기술 개발, 25AB1600, 제조 혁신을 위한 주력산업 지능화 기술 개발 및 산업현장에서의 사람-이동체-공간 자율협업지능 기술 개발]

참 고 문 헌

[1] 관계부처 합동, 혁신성장동력 추진계획 2017.12.22.

[2] 민대홍, 오정숙 (2018) “ICT 기반 신산업 발전을 위한 데이터 거래 활성화 방안”

[3] Mohammad Shohel Rana(2023) “Comparative Analysis Of Selected Symmetric And Assymetric Key Encryption Algorithms: A Review“

[4]https://techblogs.42gears.com/encrypt-and-decrypt-a-message-using-des-algorithm-in-python/

[5] https://www.lfdecentralizedtrust.org/learn/white-papers