블록체인을 활용한 위·변조가 불가능한 로그관리시스템

김진주*, 한영근**, 변재영***
*숙명여자대학교 컴퓨터과학전공
**전북대학교 소프트웨어공학과
***LG CNS 정보기술연구소(블록체인 기술팀)
e-mail:jjinju222@gmail.com

Blockchain Based Log Management Service for Non-Modifiable

Jin-Ju Kim*, Young-Geun Han**, Jae-Young Byun***
*Dept of Computer Science, Sook-Myung Women's University
**Dept of Software Engineering, Chonbuk National University
***Blockchain Technology Team, LG CNS Information Technology Research Center

요 약

시스템을 안정적으로 운용하기 위해서는 신뢰성 기반의 로그관리시스템이 필요하다. 모든 이력이 기록되는 로그의 위·변조를 방지하기 위해 로그 정보를 블록체인 기술로 관리하여 어떠한 상황에서도 시스템 이력을 신뢰할 수 있는 서비스를 제안한다. Hyplerledger Fabric을 사용하여 인증 관리 시스템에 의해 허가된 사용자만이 접근할 수 있다. 또한 분산원장에 한 번 기록된 로그 파일은 더 이상 수정하거나 삭제될 수 없다. 이 시스템을 활용하면 로그 파일의 위·변조 여부를 판단하는데 발생하는 시간, 비용, 불확실성을 크게 줄일 수 있을 것으로 기대된다.

1. 서론 1)

블록체인 기술은 다양한 분야에서 사용되고 있으며 [1], 많은 관심을 끌고 있다. 그러나 블록체인 기술이 등장하면서 위·변조가 불가능한 신뢰기반의 시스템 구축의 중요성이 대두되고 있는데, 이는 반대로 말해 기존 IT시스템에 대한 불신이 가져온 환경 변화라고 이해할 수 있다. 국가와 사회에 큰 영향을 주는 시스템일수록 신뢰는 더욱 강조된다.

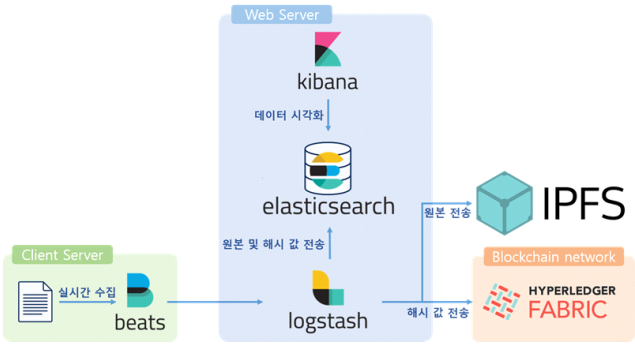
특히 로그는 시스템 운영에 큰 영향력을 가지고 있다. 로그란 시스템에서 발생하는 모든 기록을 담고 있는 데이터로, 시스템 문제에 대한 유일한 단서라고 볼 수 있다. 따라서 보안사고 발생 시 원인을 파악하기 위해선 필수적인 존재이다. 로그 분석을 통해 외부의 침입을 감지 및 추적할 수 있고 시스템의 장애 원인을 분석할 수 있다. 단순한 기록용 데이터가 아니라 모든 시스템에서 중요한 자산으로 사용되기 때문에 로그 데이터의 관리는 중요하다. 그러나 로그 파일은 쉽게 조작이 가능하여 보안에 취약하고 장기간 기록되어 그 양이 방대해 분석과 관리에 어려움이 있다.

이와 같은 문제를 해결하여 로그의 무결성을 확보하여 시스템을 보다 안정적으로 운용할 수 있도록 하는 것이 목표이다. 그리고 그에 대한 방법으로 공공의 데이터를 위·변조로부터 보호할 수 있고 효율적으로 분석할 수 있는 블록체인 기반의 로그관리시스템을 제안한다.

본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT멘토링 프로젝트 결과물입니다.

2. 블록체인 기반 로그관리서비스

대부분의 기관은 로그 데이터 조작에 대비해 별도 서버에 로그 파일을 백업해 놓지만 백업해 놓은 파일 역시 해킹을 당할 수 있다. 블록체인 기반의 로그관리서비스는 시스템에서 로그를 수집하고 별도의 서버에 저장하는 기존 서비스 기술을 활용하되 블록체인 기술을 적용하여 관리한다. 이 서비스를 개발하기 위해 ELK 스택, IPFS 프로토콜, Hyperledger Fabric [2] 을 사용한다.

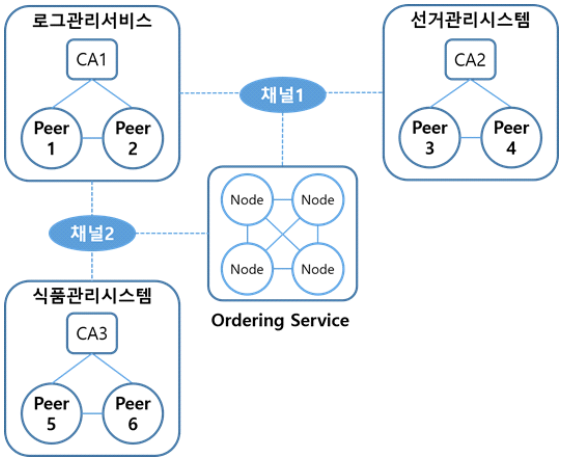


(그림 1) 로그관리시스템 시스템 구성도

(그림 1)은 로그관리시스템의 전체적인 시스템 구성도이다. ELK스택은 로그 데이터를 수집 및 저장하며 시각화 표현까지 제공 [3] 해 준다. IPFS는 분산형 P2P 파일 시스템으로, 블록체인 네트워크의 각 노드에 IPFS를 적용하여 네트워크를 구성하면 작은 블록 크기에도 대용량 파일을 저장할 수 있다. 대용량 파일을 IPFS로 분산 저장하고, 블록에는 IPFS와 해당 파일의 연결 정보만 저장하면 되기 때문이다. 로그 레벨에 따라 어마어마한 용량의 로그 파일이 산출될 수 있어 이를 분산원장에 직접 저장할 수 없는 문제점을 해결하기 위한 방안으로 고안하였다. Hyperledger Fabric은 데이터의 무결성을 보장해줄 가장 중요한 수단이다.

현재 다양한 종류의 블록체인이 존재하는데 로그관리시스템이 Hyperledger Fabric으로 구축되어야 하는 이유는 다음과 같다. Hyperledger Fabric은 허가형 프라이빗 블록체인의 형태로 [4], 누구나 자유롭게 참여가 가능한 기존 블록체인과 달리 인증 관리 시스템에 허가받은 사용자만 네트워크에 참여할 수 있다. 따라서 네트워크에 참여한 노드들은 이미 시스템에 의해 허가된, 신뢰를 가진 노드이다. 또한 전체 시스템을 다수의 채널로 구분해 채널별로 별도의 독립적인 블록체인 유지가 가능하다. 참여한 모든 노드에게 공유되는 기존 블록체인과 달리 시스템별로 별도의 원장을 생성하여 파일을 관리할 수 있다. 로그파일은 외부에 공개되는 것에 민감하기 때문에 채널별로 독립적인 원장이 필수적이다.

아래 그림은 로그관리시스템의 블록체인 네트워크 예시이다.



(그림 2) 로그관리시스템 블록체인 네트워크 구조

로그관리시스템은 대상 시스템의 예시인 선거관리시스템, 식품관리시스템과 채널을 통해 1:1로 연결된다. 하나의 네트워크 안에서 여러 참여자들과 연결되면서도 각 채널별로 프라이버시를 유지할 수 있다.

3. 핵심기능

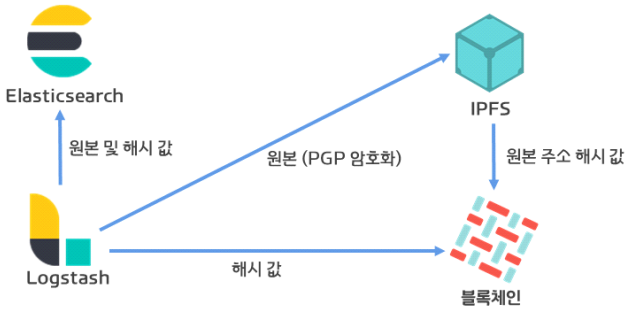
로그관리시스템의 핵심 기능과 동작 원리는 다음과 같다.

1) 수집

(그림 3) 로그 데이터 수집

로그 정보를 실시간으로 수집하기 위해 Filebeat는 클라이언트 서버에서 대상 시스템의 로그 파일을 감시한다. 라인이 추가되는 것을 감지하면 실시간으로 수집하여 웹 서버의 Logstash에 전송한다.

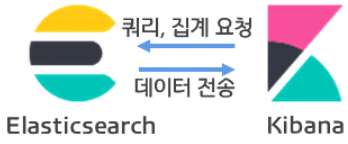
2) 저장



(그림 4) 로그 데이터 저장

수집단계에서 수집된 데이터들은 실시간 그리고 하루 단위로 저장된다. Logstash는 수집한 로그데이터를 실시간으로 Elasticsearch에 전송한다. 또한 Logstash는 하루 단위로 로그 파일을 묶어 fingerprint filter를 이용해 해시 값을 생성한다. 이 해시 값은 Elasticsearch와 Hyperledger Fabric에 전송하여 저장한다. 해시 알고리즘은 해시 값이 유출이 되었을 경우 로그 파일 원본으로 복호화 할 수 없도록 SHA 방식을 이용한다. SHA 방식은 원문메세지에 보안키를 추가하여 Verification Data를 생성한다. 이를 MAC(Message Authentication Code)라고 하는데 전송과정에서 보안키를 모르는 제 3자가 메시지를 변경하게 되면 수신자가 이를 검출할 수 있기 때문에 인증과 무결성을 동시에 제공할 수 있다. 또한 하루 단위로 묶어진 파일은 Elasticsearch와 IPFS 네트워크에 전송하여 저장한다. 그리고 IPFS에 저장된 원본 파일을 검색할 수 있는 해시 값을 Hyperledger Fabric에 저장한다. IPFS 네트워크에 저장되는 원본 파일은 PGP 방식으로 비대칭 암호화하여 저장한다. 파일을 검색하는 해시 값이 유출 되었을 경우 로그 원본 파일이 유출될 수 있기 때문에 공개키로 암호화된 파일을 개인키로 복호화 하도록 한다.

3) 조회



(그림 5) 로그 데이터 조회

Kibana는 Elasticsearch의 쿼리와 집계 기능을 이용하여 사용자들에게 시각화된 데이터를 제공한다. Elasticsearch의 기능을 이용하여 원하는 날짜와 시간을 선택해 조회하는 것 또한 가능하다.

4) 검증

(그림 6) 로그 데이터 검증

사용자는 검증하고자 하는 로그파일을 업로드하고 비교하고자 하는 날짜를 선택한다. Logstash는 업로드 한 파일의 해시 값을 생성하며, 웹 서버는 Elasticsearch에서 해당 날짜의 로그 파일과 해시 값을 불러온다. 두 해시 값과 로그 파일을 비교해서 1차적인 진위 여부를 파악한다. 그 후에 분산원장에서 해시 값을 불러오고 분산원장에 저장된 IPFS의 파일 해시 값을 이용해 파일 원본을 불러온다. 비교 대상 파일, Elasticsearch, 분산원장과 IPFS의 해시 값과 파일을 비교해 위변조 여부를 판단하고 위·변조된 부분을 사용자에게 보여준다.

위와 같은 시스템을 통해 위·변조가 불가능한 로그관리시스템을 구축하게 되면 해커가 로그 파일을 위변조하기 위해서 Logstash의 해시 생성 알고리즘을 알아야 하고 Elasticsearch의 로그 파일과 해시 값을 수정해야 한다. 이러한 과정이 성공했다고 하더라도 분산원장의 해시 값을 수정해야 하며 IPFS의 해시 값을 알아내어 파일을 찾아야 한다. 이후 사용자의 개인키를 습득하여 복호화를 진행한 다음 파일을 수정하여 공개키로 다시 암호화해야 한다. 이와 같은 과정은 사실상 불가능하므로 로그파일의 위·변조를 예방할 수 있을 것이라 기대된다.

4. 결론

본 논문에서는 사건, 사고의 원인을 파악하는데 중요한 역할을 하는 로그 데이터의 위·변조를 방지하기 위해 Hyperledger fabric을 이용한 블록체인 기반의 로그관리서비스 개발에 대해 제안했다. ELK 스택을 이용해 로그를 분석했고, 블록체인과 IPFS 프로토콜을 사용해 데이터의 무결성을 보증하고자 했다.

이 시스템은 분야에 상관없이 시스템을 운영하고 있어 로그 파일의 중요성이 강조되는 곳, 외부 시스템의 침입에 대한 대비나 분석을 위한 솔루션이 필요한 곳, 특히 높은 신뢰가 요구되는 시스템에서 유용하게 활용될 것으로 기대된다. 예를 들어 돈을 관리하는 금융기관, 높은 신뢰도가 요구되는 선거관리시스템, 높은 보안이 요구되는 민감한 자료가 오가는 국방망, 기타 여러 기업 등에서 사용될 수 있을 것이다.

참고문헌

[1] Pan The Duy “A survey on opportunities and challenges of Blockchain” SoICT 2018 Proceedings of the Ninth International Symposium on Information and Communication Technology, Pages 200-207
technology adoption for revolutionary innovation

[2] C. Cachin “Architecture of the Hyperledger Blockchain Fabric” Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016

[3] Sung Jun Son “Performance of ELK stack and commercial system in security log analysis” 2017 IEEE 13th Malaysia International Conference on Communications (MICC)

[4] E. Androulaki “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains” EuroSys '18 Proceedings of the Thirteenth EuroSys Conference, Article No. 30