## Filed: NeuroSecurity (저널/컨퍼런스 다수 있음)

## Title: 실시간 EEG데이터 훼손을 막기 위한 블록체인 무결성 검증

## Introduction

1. Problems
   1. Brain Computer Interface(BCI) introduction
      1. 뇌파를 이용하여 사지마비 환자, 식물인간 그 밖에 근육을 움직이지 못하는 환자들과 의사 소통할 수 있는 분야에 대한 소개

1) Dong Ming et al.: Study on EEG-based mouse system by using brain-computer interface

2) A Lin et al.: The walk again project: Brain-controlled exoskeleton locomotion

3) Sorger B. et al.: A real-time fMRI-based spelling device immediately enabling robust motor-independent communication

* 1. NeuroSecurity의 정의 및 중요성
     + 1. 정의: Confidentiality + Integrity + Availability
       2. 중요성: BCI 첫 설계부터 보안이 포함되어야 한다(예: 인터넷)

1) Tamara D. et al.: Neurosecurity: security and privacy for neural devices

2) Kohno T et al.: Analysis of an electronic voting sytstem

3) Privacy by Design(accessed January 19, 2014)

* 1. Trends
     1. Opensource 개발킷 이용🡪 어플리케이션 개발 증가🡪오픈소스 보안취약

1) Tamara B. et al.: App Stores for the Brain: Privacy & Security in BCI

* 1. Limitations of existing BCI technics (limitations with ref. of previous research )
     1. 모든 BCI 연구과제들이 컴퓨터 SW/HW 기기를 이용하고 있기 때문에 해커에 의한 실시간 데이터 측정 정보 훼손의 가능성 존재

1) Halperin D et al.: Pacemakers and implantable cardiac defibrillators

2) A.B. Schwartz et al.: Brain-controlled interfaces: Movement restoration with neural prosthetics

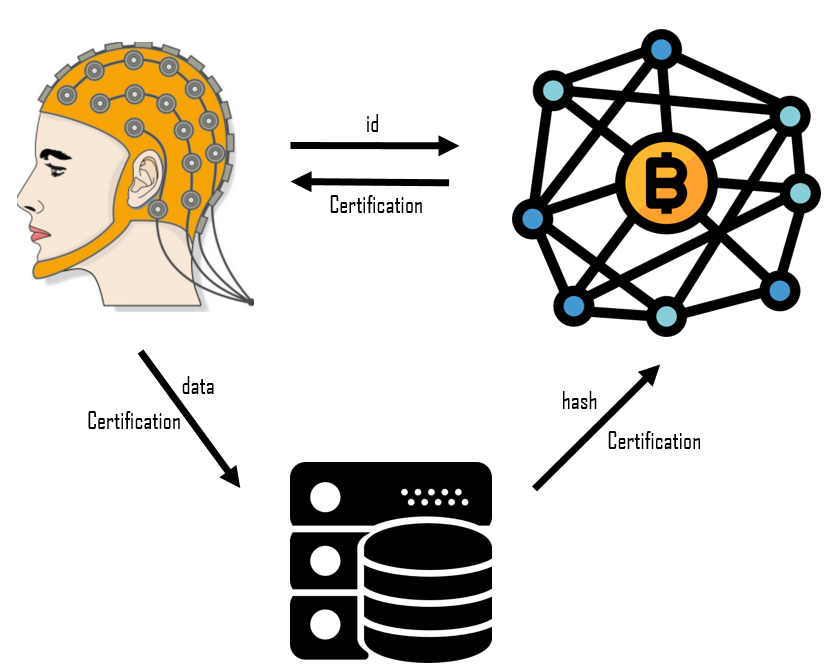
3) M. Conti et al: Can’t you hear me knocking: Identification of user actions on android apps via traffic analysis

* 1. The need for an object to pursue through experiments
     1. 근육을 움직일 수 없는 환자들의 안전한 의사소통의 길을 제시. 예를 들어, 공격자의 의한 환자 신체의 조절 및 제어 방지
     2. 마인드 리딩: 뇌파를 통해서 읽어낸 의도 역시 개인의 인적 정보에 해당하므로 일종의 개인정보로 분류 될 수 있으며, 개인정보 보호 및 정부기관의 개인 통제 수단으로 적용될 가능성에 대비
        1. Martinovic et al.: On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces.(사용자의 개인정보를 감지하기 위해 디자인된 해로운 어플리케이션 예시)

1. Purpose of the current research
   * 1. Method
        1. 시스템 구현 및 실험
     2. Purpose
        1. EEG 데이터 훼손 및 변경 가능성 실험을 통하여 문제의 심각성을 제시하고, 이러한 문제점을 블록 체인과 EEG데이터를 연동시켜 데이터가 훼손 될 수 없음을 확인하여 향후 BCI 잠재적 위험성을 방지
     3. How?
        1. 블록체인 적용 전/후의 EEG데이터를 측정한 후, 공격자의 데이터 훼손 결과 비교

## Method

1. Experiment
   * + 1. 실험 구조도(도식화)



* + - 1. 도구 및 환경
         1. NeuroSky: MindWave
         2. VMware, OS: Kali Linux 32bit
         3. Wallet: Metamask, SMART Contract
      2. 방법
         1. Metamask 설치
         2. 블록체인(SMART Contract) 발급

1) Ryan et al.: Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain

* + - * 1. 보급용 EEG를 이용하여 data측정
        2. Blockchain(SMART contract)와 EEG데이터 실시간 연동
        3. 공격: 데이터 훼손

## Results

1. 블록체인 사용 전
   1. Original EEG measurements Result
   2. Transformed EEG measurements Result by a intruder
   3. Related figure
2. 블록체인 사용 후
   1. EEG데이터가 변형되었지만, BlockChain의 구조 때문에 데이터가 변형되었음을 알 수 있음.
   2. Related figure
3. Experimental result
   1. Hash값 비교
   2. 데이터가 공격자에 의해 훼손되었음을 입증하는 figure와 데이터가 변형되었음을 알리는 figure 제시

## Discussion

* 1. 실험 목적을 한번 언급하고 그에 대한 해답 제시
     + 1. 목적: EEG 데이터의 훼손 및 변경 가능성 실험을 통하여 문제의 심각성을 충분히 제시했음을 서술
       2. 답변: 블록 체인과 EEG데이터를 연동시켜 데이터가 훼손 될 수 없음을 확인하고 향후 BCI 잠재적 위험성을 방지 했음을 서술
          1. 공개키 논문
  2. 블록체인 도입의 효과 및 이전 연구를 통한 블록체인의 다양한 보안성 검증
     + 1. 블록체인 사용 후 실험결과: 무결성 입증(데이터 변경 불가)
       2. 이를 통해, BCI의 안정적인 연구방향 제시 가능
       3. 이전 연구들에 의한 무결성이 검증된 블록체인 제시 인용
          1. Igor Zikratov et al.: Ensuring Data Integrity Using BlockChain Technology
          2. Gammon, K. et al.: Experimenting with blockchain Can one technology boost both data integrity and patients' pocketbooks?
  3. An opinion in favor of a conclusion

앞으로의 방향성 추구: 플랫폼 기반의 neural device를 개발해야 하고, 초기 개발부터 보안을 염두에 두고, 설계하여야 오늘날의 보안문제를 많이 커버할 수 있을 것이다.

* 1. A new attempt
     + 1. 새로운 BCI모델링임이자 이전에는 없었던 새로운 블록체인 활용방안

기존: 보험 및 금융분야

Gatteschi et al.: Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?(보험)

* 1. Limitation
     1. 데이터의 완전한 변경 방지가 아니라 블록체인 구조에 따른 데이터 변경 사항을 알림
  2. The importance of research
     1. 무결성 강화: EEG 데이터를 분산화된 데이터 저장소에 저장하며 기록된 데이터에 대해서는 그에 대한 해시 값을 블록체인에 기록함으로써 데이터의 무결성을 검증을 하며 이를 통하여 데이터 변경 불가능 또한 탈중앙화(CA) 시스템으로 정부 및 부정적 단체의 통제적 규제에서 벗어날 수 있는 방안 마련 가능
     2. 보급용 EEG와 블록체인 연동 비용 감소: 기존에 연구용 EEG비용이 상당하여 일반인들이 사용하기 힘들고, 향후에도 부자들에게만 이용될 것이라는 지적이 있었으나(마이클 교수) 가정용 EEG가 보급되어 많은 사람들이 이용할 수 있고 오픈소스모델인 블록체인을 이용하여 상당한 비용을 절약할 수 있게 됨
     3. BCI미래방향성을 위한 보안 모델 제시: 잠재적인 BCI의 위험성을 방지하기 위한 보안 모델 제시 뿐만 아니라, 근육을 움직일 수 없는 모든 환자들의 의사소통을 안전하게 수행할 수 있는 길을 제시

## Conclusion

* 1. 한 줄 요약
  2. Future research
     1. EEG-Command 시스템을 구현하고, 블록체인 적용
  3. Expectation effectiveness

상업적 비용 감소

위험 노출 방지