인공지능과 정보보안의 관계

서강대학교 ▌김종락

1. 인공지능의 역할

4차 산업혁명 시대의 근간이 되는 기술은 인공지능(AI)이다. 인공지능은 그동안 인류가 경험하지 못한 영역까지 확대될 것이 확실하다. 예를 들어 꿈의 자동차라고 할 수 있는 자율주행자동차의 경우만 보더라도 과거에는 상상도 못할 일이었다. 가끔 드라마나 영화에서 간단한 기계동작으로 운전자 없이 작동하는 경우는 있을 수 있지만 자동차 스스로 사물을 인식하고 그에 맞게 속력과 차선을 바꾸는 능력은 공상과학 소설에서나 가능한 일로 생각되어왔다.

그림 1 구글의 자율 주행 자동차 시제품

이뿐 만이 아니다. 공장에서 쏟아져 나오는 IoT 데이터는 Industry 4.0으로 발전되고 있다. 단순한 공장 자동화가 아니라 이른 바 "스마트 팩토리"의 실현이 점차로 진행되고 있다. 진정한 스마트 팩토리는 공장 설비의 노후화 예측, 생산되는 제품을 불량률을 예측하여 일정한 수준으로 줄이는 데 있다. 아직 국내 대기업에서 운영하는 공장에서는 독일 수준으로 혁신적인 Industry 4.0을 실천하고 있지 않으나 경쟁력을 높이기 위해서라도 시급히 이를 실천해야 한다.

헬스 IoT 역시 인공지능이 필요한 분야이다. 환자들의 건강 상태를 질문에 의존하지 않고 착용하기 쉬운

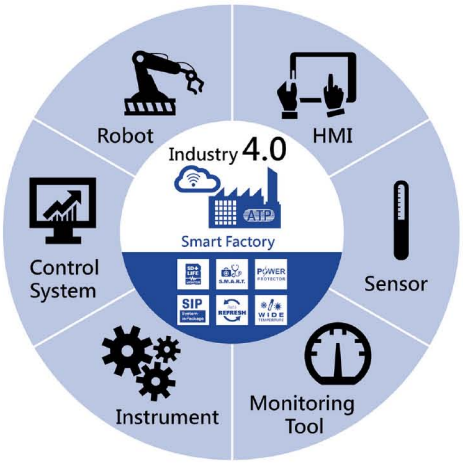


그림 2 출처 Embedded computing design(2015.12.3.)

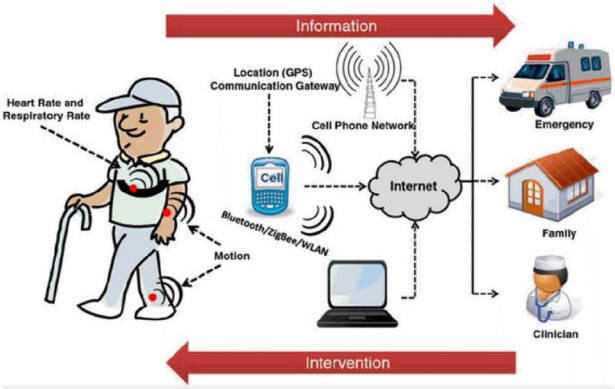


그림 3 출처 MedGIZMO (2016.8.24.)

센서를 몸의 다양한 부분에 부착하여 심박 상태, 혈압 여부, 심리적 상태 등에 대한 정보로 데이터화 할 수 있다. 많은 환자들의 데이터가 확보되어 있다면 이런 정보를 상호 비교하여 호전되는 사람들의 패턴과 악화되는 사람들의 패턴을 알아 낼 수 있다면 현재의 의료 체계를 획기적으로 변화시킬 수 있을 것이다.

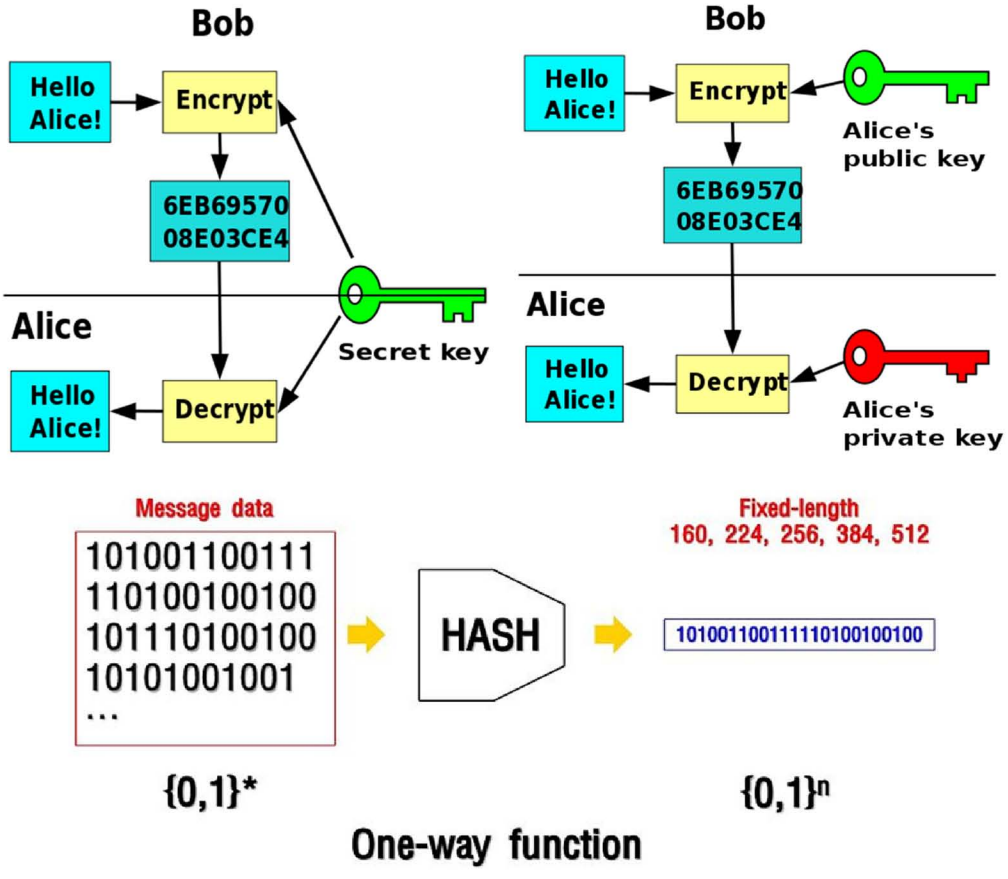
나는 이런 변화의 세계에 살게 된 것을 행운이라고 생각한다. 요즘 이틀 동안 생산되는 지구촌의 빅데이

터는 최근 인류가 생산한 모든 데이터와 맞먹는다고 한다. 다수의 컴퓨터로 연결되어 하나의 컴퓨터처럼 행동하는 AlphaGo가 바둑처럼 복잡한 게임을 인간과 겨룰 때 인간을 이긴다는 것을 우리는 목격하였다. 일본의 인공지능 컴퓨터인 '도(東)로봇 군'은 도쿄대에 들어갈 실력은 되지 못했으나 웬만한 사립대에 들어갈 실력을 갖추었다. 구글 번역기와 네이버의 파파고의 한글 번역 능력은 날이 갈수록 진화하고 있다. 음성인식 기술이 탑재된 제품이 이미 상용화되어 가정에 보급되고 있다. 애플의 시리, 구글 나우, MS의 코타나, 아마존의 알렉사, SKT의 누구 등은 비서처럼 가전제품 제어, 날씨나 일정 등의 정보를 안내해 준다. 이처럼 인공지능이 응용될 수 있는 분야는 무궁무진하다. 기존 암기식 지식의 습득이 무의미해질 날이 얼마 남지 않았다. 하지만 일반 사람들의 인공지능에 대한 지식은 아직 초보 단계여서 새로운 시대를 준비하기 보다는 가까운 미래에 필요한 스펙 쌓기에 몰두하고 있다. 미래학자 앨빈 토플러는 죽기 전에 한국의 젊은이들이 미래에 필요하지도 않은 지식과 존재하지도 않을 직업을 위해 하루 15시간이나 학교나 학원에서 시간을 낭비하고 있다고 안타까워하기도 했다.

2. 보안이 필요한 인공지능

인공지능에 대한 시대적 욕구가 팽배하고 있는 반면 많은 사람들이 간과하고 있는 분야가 정보보안(혹은 정보보호)이다. 정보보호는 암호보다 넓은 의미로 쓰이고 있다. 암호는 크게 대칭키 암호, 비대칭 암호인 공개키 암호, 그리고 해시 함수로 나뉜다. 대칭키 암호의 특징은 암호화와 복호화에 쓰이는 키가 본질적으로 같이 사용된다는 것이다. DES와 AES가 대표적이다. 이에 비해 공개키 암호는 암호화에 쓰이는 키와 복호화에 쓰이는 키가 다르다. 정수론 기반의 RSA 암호와 타원곡선론 기반의 타원곡선암호가 있다. 해시함수는 일방향 함수(one-way function)로써 주어진 데이터의 해시값은 쉽게 구하지만 주어진 해십값을 갖는 원래 입력값을 찾는 것은 거의 불가능하도록 만들어져야 한다. 현재에는 SHA-2 계열인 SHA-256, 384, 512가 가장 많이 쓰이고 있다. 조만간 SHA-3 계열이 상용화 될 것이다. 지금까지는 이런 암호 알고리즘을 기반으로 안전한 이메일 교환, 전자서명, 전자상거래 등이 활용되고 있다.

하지만 위에서 언급된 자율주행차, 스마트 팩토리, 헬스 IoT, 홈 IoT 분야에는 보안에 취약한 편이다. 센



서에서 생성되는 데이터는 암호화 되어야 된다. 그렇지 않으면 제 3자가 데이터를 쉽게 추출하거나 악의적으로 변형할 수가 있기 때문이다. 또한 센서에 사용되는 암호는 초절전 초경량이어야 한다. 그러다 보니 이런 암호는 전통적인 RSA 암호만큼 안전하지 않다. 이 부분을 어떻게 해결해야할지 아직도 큰 문제로 남아 있다.

IoT 데이터의 암호화이외에도 각 공공기관이나 기업이 보유하고 있는 빅데이터를 암호화 하여 외부에서 분석할 수 있는 방법이 제안되고 있다. 이를 완전동형암호라고 한다. 지금까지는 은행 정보를 직접 분석해야 하므로 데이터의 보안에 취약했다. 크레이그 젠트리는 2009년 데이터를 암호화한 암호문에 대한 덧셈과 곱셈을 자유롭게 할 수 있는 암호 시스템 즉, 완전동형암호를 제안하였다. 아직까지는 상용화가 되지 않았지만 조만간 상용화가 가능할 것으로 판단된다.

3. 인공지능을 활용한 보안 문제 해결

인공지능은 이러한 암호 응용 분야에 활용될 수 있다. 가장 간단한 예는 사용자 행위 분석을 통한 이상행위 탐지기능이다. 얼마 전 급히 다른 사람의 노트북을 빌려 Gmail에 접근한 적이 있다. 이때 Gmail은 바로 경고 메일을 보내서 경각심을 주었다. 이것은 평소 내가 쓰고 있던 노트북들의 IP를 저장하고 있다가 이와 다른 IP의 등장을 감지하고 바로 경고 메일을 보낸 것이다. 김종현의 <인공지능 기반 금융권 보안관제 동향 및 향후과제> (전자금융과 금융보안 제 8호 2017-04)에 의하면 다음과 같은 3가지 보안 분야에 인공지능이 활용될 수 있다.

사이버 공격에 의한 이상행위탐지를 모니터링하는 보안관제 분야에 인공지능이 효과적으로 사용될 수 있다. 이를 위해서는 방화벽, IDS(Intrusion Detection System), IPS(Intrusion Prevention System), 서버보안솔루션 등 다양한 보안 장비에서 빅데이터 수준으로 데이터를 생성해서 머신러닝을 위한 학습데이터로 활용하면 된다. 사이버 공격 이전까지의 이런 데이터를 잘 축척해 놓은 다음 이상행위가 탐지되었을 경우 바로 방어를 해야 할 것이다.

개인정보 오남용 모니터링 분야 또한 인공지능 기법이 효과적으로 작용할 수 있다. 종종 대기업이나 은행에서 운영하는 회원 정보가 유출되어 큰 사회적인 문제가 되고 있다. 이는 내부자 혹은 외부자가 내부자의 컴퓨터의 아이디와 패스워드를 알아내어 컴퓨터에 접근하여 회원의 정보를 탐색하고 복사해 간 것으로 볼 수 있다. 평소 그 아이디를 가진 내부자의 행동 패턴을 알고 있었다면 이런 정보의 탐색에 대하여 미리 경고를 주거나 확인 전화를 함으로써 그 상황을 미연에 방지할 수 있었을 것이다.

사기 거래탐지를 위한 FDS(Fraud Detection System)에 인공지능 기법이 유용하게 활용될 수 있다. 평소에 개인의 신용카드를 사용하는 장소, 시간대, 그리고 금액 등에 대한 정보가 있다고 하자. 늦은 밤 하와이에 있는 호텔에서 거액의 금액이 지출되었을 경우 이는 신용카드가 도용되었을 가능성이 무척 크다. 이런 경우 신용카드 승인을 하지 않고 사용자에게 전화로 문의해보는 시스템을 구축할 필요가 있다. 또한 이러한 사기 패턴들을 계속 업데이트하여 고객에게도 유사한 패턴이 보일 경우 어떤 집단에서 이 수법을 사용하는지 추적이 가능할 것이다.

4. 새로운 도전

지금까지 인공지능과 정보보안의 관계에 관하여 기술했다. 이 두 기술은 서로 보완을 하며 발전할 것이다. 이중 가장 극복할 문제는 양자 컴퓨터의 등장이다. 현재의 암호는 소인수 분해의 어려움과 이산로그 문제의 어려움에 기반을 두고 있지만 이는 양자 알고리즘에 의하여 다항식의 시간 안에 풀리는 것으로 이미 알려져 있다. 양자 컴퓨터가 완성된다면 기존 암호 체계가 붕괴가 되어 산업체 전반에서 대대적인 수술이 필요하다. 양자 컴퓨터의 등장에도 안전한 후양자 암호의 제안이 NIST(미국 국립표준기술 연구소)의 주관으로 2017년 11월부터 진행되고 있다. 1라운드에 69개의 알고리즘이 선정되었는데 그 중 5개는 한국에서 제안된 것이다. 2019년에 제 2라운드가 진행되고 몇 년 후에 최종적인 알고리즘이 결정될 것이다.

한편 해시 함수를 기반으로 하는 블록체인의 등장 역시 무시 못 할 혁신적인 사건이다. 블록체인의 핵심 아이디어는 정보를 공유한다는 것과 탈 중앙집권적이라는 것이다. 향후 개인 간의 거래가 누구의 간섭 없이 쉽게 진행될 것이다. 지금보다 많은 거래 데이터가 쌓일 것이다. 이런 데이터를 효율적으로 분석하고 관리하는 인공지능 기법과 이를 안전하게 처리하는 블록체인의 기법이 하이브리된 새로운 분야가 탄생될 것으로 전망된다. 결국 모든 것은 하나로 연결될 것이라는 신념이 미래에 다가올 5차 산업혁명의 핵심 철학이 아닐까 생각해본다.

참고문헌

[1] 김종현, "인공지능 기반 금융권 보안관 제 동향 및 향후 과제", 전자금융과 금융보안 제 8호, pp. 39-63, 2017.

약 력

김 종 락

1993 포스텍 수학과 졸업(학사)
1997 서울대학교 수학과 졸업(석사)
2002 미국 Univ. of Illinois at Chicago 졸업 (박사)
2002~2005 미국 Univ. of Nebraska 수학과 연구조교수
2005~2012 미국 Univ. of Louisville 수학과 조교수 및 부교수
2011 포스텍 방문교수
2012~현재 서강대학교 수학과 교수
2016~현재 (주) 감성수학레드 대표 및 창업자
관심분야: 부호론, 암호론, 산업수학, 인공지능
Email: ctryggoggo1@gmail.com