한국정보보호학회
Korea Institute of Information Security & Cryptology

2020년 한국정보보호학회 동계학술대회

CISC-W'20

Conference on Information Security and Cryptography-Winter 2020

일자 2020년 11월 28일 (토) **장소** 온라인 컨퍼런스

접속 및 시청방법 등록자에 한하여 개별 공지

Proceedings

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology **주관** 서울대학교 SEOUL NATIONAL UNIVERSITY

후원 국가정보원 National Intelligence Service Korea, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소, cen 아이티센 ITCen

IoT 기반 고위험 의료장치의 신뢰성 보장을 위한 횟수제어 기반 소자 설계

안성규* 주재경* 최기철* 정혜림* 박기웅†

*세종대학교 시스템보안연구실† 세종대학교 정보보호학과

Time control-based device design to ensure reliability of high-risk IoT medical devices

Ahn Sung-Kyu* Ju Jae Gyeong* Choi Gi-Choel* Jung Hye-Lim*

Ki-Woong Park†

*System Security Laboratory, Sejong Unibersity

† Department of Computer and Information Security, Sejong University

요 약

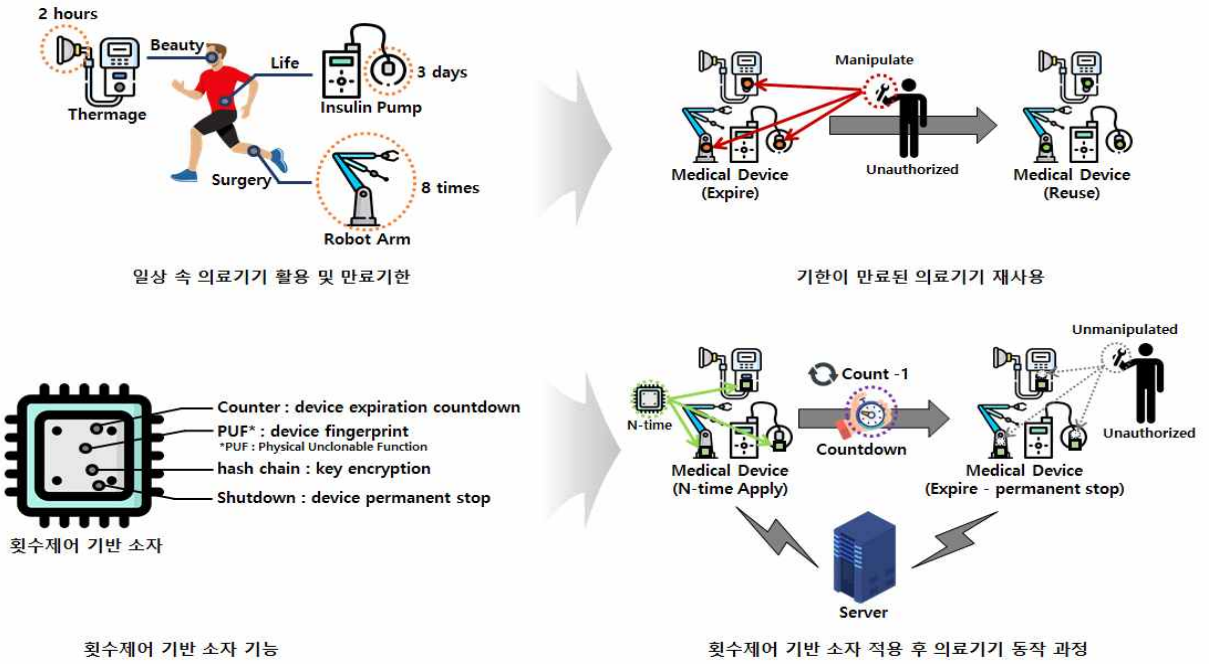
최근 의료 및 건강 분야에 IoT 기술을 융합하는 IoMT(Internet of Medical Things) 및 IoT Healthcare 등과 같이 의료 및 건강 분야에 대한 IoT 솔루션 시장이 확대되고 있다. 이와 같이 의료목적을 위한 IoT 기기의 안전한 운용을 위해 다양한 보안 관련 제도 또는 법안이 적용되었다. 하지만 저전력, 소형화를 추구하는 IoT 기기의 특성상 의료기기의 안전을 위한 고도의 보안 솔루션을 적용하기 어렵다. 본 논문에서는 이러한 IoT 의료기기의 안전성과 효율성을 위해 PUF(Physical Unclonable Function)기능을 활용한 보안 솔루션인 의료장치의 신뢰성 보장을 위한 횟수제어 기반 소자의 구성 방안 제안한다. 횟수제어 기반 소자는 IoT 의료장치가 정해진 시간 또는 횟수 이상으로 사용되는 것을 방지한다. 또한, IoT 의료기기를 장착 또는 실시간으로 사용되고 있는 상황에서 기기의 비정상 동작이나 악의적인 행위를 방어할 수 있다. 본 논문에서는 이러한 솔루션을 통해 의료기기의 오남용을 방지하고 IoT 의료기기를 대상으로 하는 악성행위로 인한 의료사고를 방지할 수 있을 것으로 기대한다.

I. 서론

최근 IoT와 의료 및 건강관리분야의 융합을 통해 구성된 IoMT(Internet of Medical Things), Healthcare IoT 등 의료 및 건강 분야에 대한 IoT 솔루션의 규모가 점진적으로 확대되고 있다.[1] IoT가 적용된 의료기기의 특징으로는 사용자의 신체와 물리적으로 밀접한 위치에서 기능을 수행함으로서 비정상적인 동작이나, 악의적인 공격자에 의한 공격이 인명 피해로 직결되는 상황이 발생할 수 있다. 이러한 상황을 방지하기 위해 의료기기의 올바른 사용법 및 오남용 방지규정 등의 강력한 제재 및 관련 법률 등이 필요하다.[2] 이러한 제재 및 법률에 속해있는 의료기기의 예로 신체 부착형 인슐린 펌프는 최대 3일을 최대 작동시간으로 하며[3], 수술용 로봇팔의 경우 최대 8회만을 수술 용도로 사용할 수 있다.[4] 또한, 피부과에서 사용되는 의료기기인 써마지(Thermage)의 경우에도 지정된 횟수와 사용시간을 준수하는 올바른 사용법으로 사용되어야 한다.[5] 그러나 이러한 규제와 법률을 무시한 채 무분별하게 의료기기를 재사용하거나 IoT의 기술적 취약점을 악용하여 의료기기 사용자에게 상해를 입히는 사고가 발

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 지원(No. 2019-0-00426)을 받아 수행된 연구임.



[그림 1] 횟수제어 기반 소자 기능 및 적용

생하기도 한다.[6] 이러한 위험성을 해소하고 안전한 IoT 의료기기 시스템을 구성하기 위해 본 논문에서는 정해진 횟수만 수행된 후 영구적으로 정지되는 횟수제어 기반 소자를 제안하여 의료기기의 수행 횟수를 제한한다. 또한, 물리적 복제 방지 기능을 활용하여 의료기기에 유일성을 부여하여 해당 의료기기의 사용이 관리 시스템에 기록하고 이를 통해 의료기기의 비정상적인 동작이나 오남용하는 경우를 방지하는 솔루션을 제시한다.

횟수제어 기반 소자는 IoT 기기의 특징인 저전력, 소형화를 만족하기 위해 저전력으로 수행하는 소자 형태로 디자인하였으며, 적용의 예는 [그림 1]과 같다.

[그림 1]은 우리의 일상 속에서 접하게 되는 의료기기 중 사용기한이 존재하는 제품군을 볼 수 있다. 해당 제품들은 각각 매뉴얼 상으로 사용횟수 및 사용시간이 지정되어 있지만 사용자가 인가되지 않은 임의의 방법으로 조작해 재사용하여 환자의 생명까지 위협할 수 있는 악용 사례가 있을 만큼 보안성이 충분히 확보되지 않은 경우가 많다. 따라서 사용횟수나 시간이 만료되면 재사용할 수 없도록 기기의 작동을 정지시키는 하드웨어 기반의 횟수제어 기반 소자를 통해 의료기기의 재사용을 방지하고자 한다. 횟수제어 기반 소자는 의료기기의 사용기한 메커니즘(시간,횟수)에 에 따라 n-times COUNT-DOWN을 진행하고 서버와 통신하여 Chip의 보안성을 확보한다. COUNT-DOWN으로 횟수가 0이 되면, 의료기기는 작동 불능 상태가 된다. 이를 통해 인가되지 않은 사용자가 재사용을 위해 조작을 시도하지 못하도록 하여 의료기기의 남용을 방지할 수 있게 된다.

본 논문에서 제안하는 횟수제어 기반 소자는 PUF(Physical Unclonable Function)와 해시(Hash)의 일방향성 특징을 활용한 역해시체인 기술을 적용하여 의료기기의 동작횟수를 제어한다. PUF는 전자기기 고유의 전기적 패턴에서 각 기기만의 유일성을 보유한 ID 값을 얻을 수 있다. 이는 암호알고리즘에서 키 값으로 사용될 수 있으며, 키가 별도로 저장되지 않기 때문에 보안성이 높다. 또한, 저전력으로 수행되기 때문에 IoT 환경에 적합하다. 횟수제어 기반 소자는 소자 형태로 PUF 칩을 내장하고 있다. IoT 의료기기에서 특정 연산 후에 횟수제어 기반 소자로부터 카운팅을 요청하면 PUF의 키값을 측정한다. PUF 키 값이 외부로 유출될 경우 유일성이 침해될 수 있는 위협에 취약해지므로

이를 해결하기 위해 횟수제어 기반 소자에서는 PUF 키 값에 역해시 체인을 적용하여 이를 유일성을 보장한다. 횟수제어 기반 소자가 적용된 IoT 의료기기에서 서버 시스템으로 역해시의 값을 전달하면 시스템에서 이를 통해 IoT 의료기기의 수행횟수를 카운팅하고 의료기기를 올바른 사용법으로 사용할 수 있게 된다. 또한, 소자 형태로 수행되어 악의적인 사용자가 이를 교체하더라도 이전에 서버에 등록된 PUF 의 해시값을 비교하여 악의적인 사용자의 소자 교체 여부를 파악하여 서버에서 IoT 의료기기를 제어할 수 있다. 이를 통해 의료기기의 무분별한 사용을 제어하고 비정상적인 행위를 방지한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 연구와 관련 연구를 서술하고 본 논문에서 제안하는 연구의 이점에 관해 서술한다. 3장에서는 본 논문에서 제안하는 연구에 대해 구체적인 동작 과정과 함께 IoT 의료기기에 횟수제어 기반 소자의 적용과 이를 통한 이점에 관해 서술한다. 4장에서는 본 논문의 결론으로 맺음말과 추후 연구에 관해 서술한다.

II. 관련연구

본 장에서는 본 논문에서 제안하는 연구와 관련된 연구에 관해 설명하며, 이와 관련하여 본 논문에서 제안하는 연구의 목표 및 장점을 설명한다.

2.1. IoT 기반의 의료기기의 취약점 및 보안 솔루션의 필요성

IoT 환경의 의료기기가 네트워크에 연결됨에 따라 의료기기에 대한 모니터링 및 진단에 필요한 정보를 편리하게 접근할 수 있다는 점은 의료 종사자와 환자에게 편의성과 접근성을 제공한다. 하지만 의료기기의 특성상 환자의 안전에 직접적으로 영향을 미칠 수 있어 다른 네트워크 기반의 컴퓨팅 시스템보다 보안 취약점이 차지하는 비중이 치명적일 수 있다.[7]

의료기기가 네트워크를 연결하는 방법이 증가함에 따라 해커가 악용 가능한 공격 접점도 증가하였으며 이로 인해 의료기기의 취약점도 증가하게 되었다. 또한, 환자가 사용하는 의료기기 단말이 접점이 되어 해커에게 병원의 의료 네트워크에 접근할 수 있는 수단을 할 수 있어 네트워크와 연결된 의료기기에 대한 보안은 필수적이라 할 수 있다.

2.2. PUF(Physical Unclonable Function)

여러 분야와 종류의 IoT기기가 출시되고 있지만, 아직 이에 대한 보안은 미흡하다. IoT 기기의 특성상 저전력을 이유로 낮은 컴퓨팅 성능을 가지고 있어 높은 컴퓨팅 자원을 요구하는 기존의 소프트웨어 방식의 보안 솔루션을 적용하기 어렵다. 따라서 물리적으로 복제할 수 없으며 저전력으로 사용 가능한 PUF(Physical Unclonable Function) 기술이 주목받고 있다. PUF는 반도체 제조 공정상에서 발생하는 예측 불가능한 미세한 물리적 구조 차이를 이용한 기법으로 같은 공정으로 제조된 칩이라도 시도 값에 대하여 서로 다른 응답이 나오는 특성을 활용하는 특징이다. 따라서 주로 PUF의 응답값은 암호화의 개인 키로 많이 사용되며 처리속도가 빠르고 전력을 적게 사용하여 IoT 기기에 사용하기 적합하다.[8]

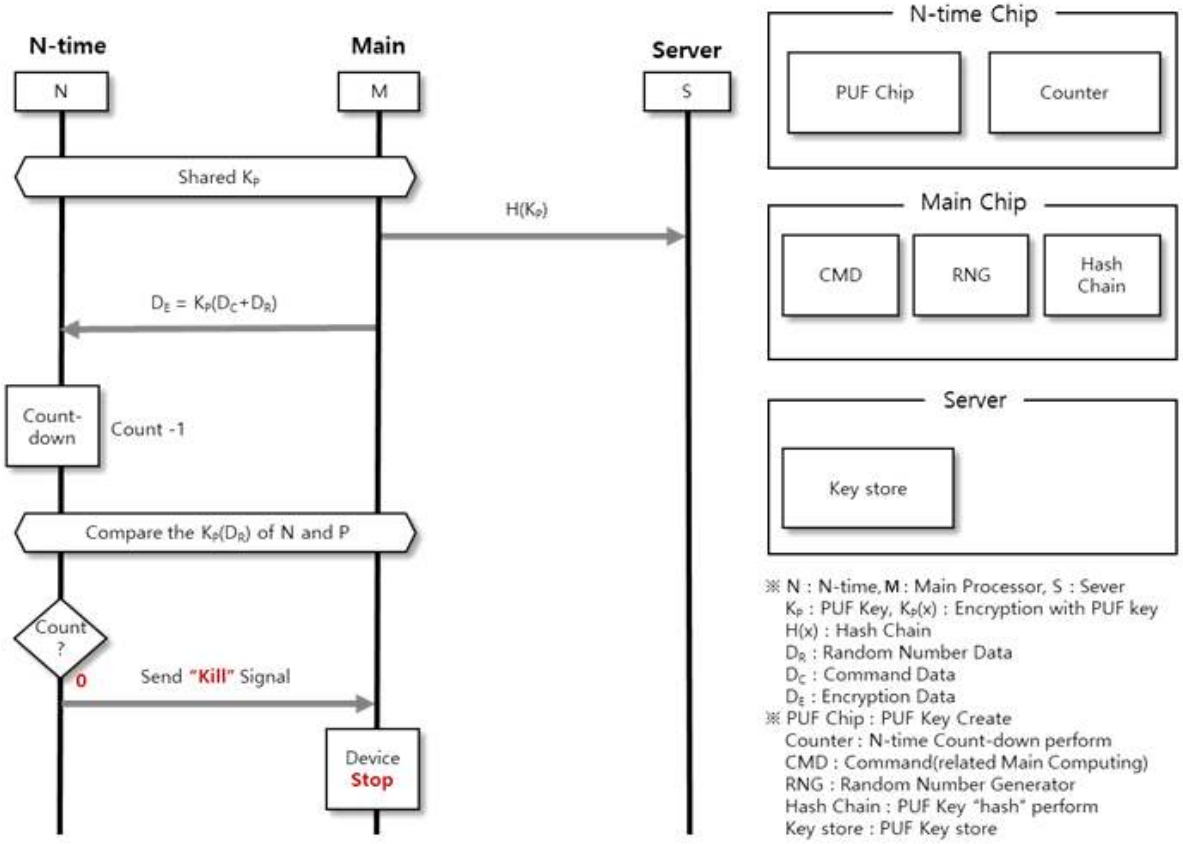
심전도(ECG), 심박수 가변성 (HRV) 및 SRAM Based PUF의 3가지 데이터를 결합하여 무작위성을 지닌 고유한 키를 생성하는 칩 기반의 하드웨어 보안 엔진 연구가 존재한다. 이 연구에서 생성된 고유한 키는 개인, 장치, 시간이 지남에 따라 지속적으로 변하여 데이터의 복호화 성공률을 크게 줄일 수 있고 소형 칩 형태로 제작되어 저전력을 요구하는 장비에서도 사용할 수 있다.

2.3. Monotonic Counter

Monotonic Counter와 같이 신뢰성을 보장하며 단방향 값 증가를 위해 관련 연구들도 진행되고 있다.[9] 이 기법의 활용 용도의 예는 다음과 같다.

- 특정 횟수만큼만 디스크에 데이터를 기록하거나 데이터에 접근하도록 제한
- 의료기기와 같은 횟수가 정해진 장치를 특정 횟수만 사용하고 폐기

본 논문에서 제안하는 연구는 IoT 기술기반



[그림 2] 횟수제어 기반 소자 내부 기술 진행 과정

의 의료기기에서 발생할 수 있는 보안 취약점으로부터 이를 막기 위해 의료기기의 기능을 횟수 제한하여 IoT 공격 및 오남용으로부터 사용자를 보호하는 연구이다. 본 논문에서 제안하는 횟수제어 기반 소자 연구는 소자 형태로 디자인하였으며, PUF 기술을 적용하여 의료기기의 식별 및 횟수를 카운트를 수행된다. 의료기기의 동작 횟수를 제어할 수 있으며 서버 시스템에서 기기 사용을 확인할 수 있으므로 의료기기의 통제가 가능해진다.

III. 횟수제어 기반 소자

본 장에서는 IoT 기반의 임베디드 시스템 플랫폼에서 활용될 수 있는 횟수제어 기반 소자의 구조 및 핵심 기술에 관해 설명한다. 본 논문에서 제시하는 횟수제어 기반 소자가 적용된 시스템은 공격자가 IoT 의료기기에 대한 물리적인 접촉 및 관찰과 프로빙 공격(Probing Attack)이 가능하다는 것을 가정한다.

3.1 횟수제어 기반 소자 구조

횟수제어 기반 소자는 의료기기 시스템 내부의 *n*-times counting chip 및 mainMain chip으로 구성된다. *n*-times counting chip은 PUF 기능을 지원하는 PUF Chip을 포함하고 있으며, 암·복호화 기능을 지원한다. Main chip은 횟수제어 기반 소자를 위한 *COUNT* 명령을 포함한 일반적으로 임베디드 시스템을 구동하기 위한 프로세서로 구동되어 있으며, RNG(Random Number Gernerator)기능과 암·복호화 기능을 지원하며, 네트워크를 기반으로 의료기기 관리 서버와 통신한다.

3.2 횟수제어 기반 소자 프로세스 구성

[그림 2]는 횟수제어 기반 소자의 동작 순서를 나타낸 것으로 *n*-times counting chip에서 PUF Key를 생성해 Main chip의 프로세서와 키를 공유하며 main Chip은 해당 키를 해쉬 체인 기술을 활용해 서버로 전달하여 해당 키의 유일성을 보장하도록 한다.

[그림 2]의 우측은 *n*-times counting chip, Main chip, server의 구조와 이해를 돕기 위한 플랫폼의 구성요소를 명시한다.횟수제어 기반 소자의 동작 순서는 [그림 2]와 같다. Main chip과 *n*-times counting chip은 의료기기의 동작 시작과 동시에 PUF key를 공유한다. 해당 PUF Key는 *n*-times counting chip의 무결성을 확보하기 위해 사용된다. PUF Key를 획득한 Main chip은 해당 PUF값의 해시연산을 연속적으로 수행하여 해시체인을 생성한 후 서버로 전달한다. 이후, Main chip의 RNG(Randome Number Generator)는 RN (Random Number)를 생성한다. 임베디드 장치에서 *COUNT* 이벤트(COUNT-DOWN, KILL)가 발생하거나 의료기기 관리 서버에서 이벤트 명령이 발생할 때마다, main chip은 Count 명령어와 RN을 조합한 데이터를 PUF값의 해시연산한 값을 Key로 사용하여 암호화하여 *n*-times counting chip으로 전달한다. *n*-times counting chip은 전달받은 암호화된 데이터를 PUF키를 사용하여 복호화한다. 복호화된 데이터는 RN과 COUNT 명령어로 구분되며, COUNT 명령에 따라 *n*-times counting chip의 *COUNT-DOWN* 명령을 수행한다.

명령이 정상적으로 수행되었을 때, *n*-times counting chip은 Main chip으로부터 전달받은 RN을 다시 PUF Key로 암호화하여 Main chip으로 전달하게 되며, main chip은 암호화된 RN 데이터를 PUF Key로 복호화 하여 명령어가 정상적으로 수행되었는지 검증할 수 있다. 만약 공격자에 공격 또는 하드웨어의 비정상적인 동작으로 인해 암호화된 RN이 Main chip에 전달되지 않을 경우, 임베디드 시스템이 비정상 상태이거나 공격받은 상태로 간주하여 실행되고 있던 모든 명령이 중단된다.

3.3 *n*-times counting chip COUNT 명령어 구성

main chip에서 생성되어 *n*-times counting chip으로 전달되는 명령어는 *COUNT-Down*과 *Kill* 명령의 두 가지로 구분된다. *COUNT-Down* 명령어는 *n*-times counting chip에서 저장하고 있는 COUNT 값을 기준으로 1만큼 감소하는 역할을 수행할 수 있는 명령어이며, *Kill* 명령어는 *n*-times counting chip이 가지고 있는 모든 COUNT가 소진되었을 때, *n*-times counting chip을 정지함으로써, 횟수제어 기반 소자가 부착된 임베디드 시스템이 재사용되는 것을 방지할 수 있다.

IV.결론

본 논문에서는 IoT 기반의 의료 및 건강 관리 디바이스의 오남용으로 인한 비정상 행위 또는 악의적인 공격을 방어하기 위한 횟수제어 기반 소자를 제안하였다. 본 논문에서 제안하는 횟수제어 기반 소자는 PUF(Physical Unclonable Function)을 사용하여 디바이스의 유일성을 부여함으로써 복제를 방지하고, 해당 PUF 값을 통신 암호화 KEY로 사용함으로써, 저전력 암호화 통신을 통해 버스 프로빙 공격등의 물리적인 인터페이스 공격을 방어할 수 있다. 또한, 횟수제어 기반 소자는 IoT-Cloud 플랫폼 형태로 구현되어 PUF의 유일성을 서버에 등록함으로써, 횟수제어 기반 소자가 복제되거나 중복으로 사용되는 것을 방지할 수 있다. 본 논문에서 제시하는 횟수제어 기반 소자를 활용함으로써 현재 활용되고 있는 IoT 기반 의료기기의 오남용 또는 악의적인 공격으로 인한 인명 피해를 방지할 수 있다고 예상한다. 후속 연구로는 본 논문에서 제시하는 횟수제어 기반 소자를 물리 소자 형태로 구현하여 다양한 IoT 기기에 능동적으로 적용할 수 있는 Pluggable 횟수제어 기반 소자를 연구할 계획이다. 또한, 본 연구의 추후 연구로 *n*-times counting chip의 COUNT-Down 0 단계에서 의료기기의 사용을 물리적으로 제한하기 위한 Kill의 메커니즘 연구가 추후 연구로 진행 중이다.

[참고문헌]

[1] PARK, Se-Hwan. IoT 기반 스마트 헬스케어 산업의 현재와 미래. The Magazine of the IEIE, 2017, 44.2: 24-28.

[2] D. Azariadi, V. Tsoutsouras, S. Xydis and D. Soudris, "ECG signal analysis and arrh

ythmia detection on IoT wearable medical devices," 2016 5th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, 2016, pp. 1-4, doi: 10.1109/MOCAST.2016.7495143.

[3] 장윤서, "11월부터 이식 의료기기 결함 발생 시 즉각 회수 시스템 가동", 조선비즈, 2020.07.09 https://biz.chosun.com/site/data/html_dir/2020/07/09/2020070902051.html

[4] 최락선, "세계 두 번째로 '일회용 부착형 인슐린 펌프' 개발한 이오플로우 김재진 대표 "웨어러블 인공췌장도 상용화할 것", 조선비즈, 2020.10.17. https://biz.chosun.com/site/data/html_dir/2020/10/16/2020101602436.html

[5] 백성주, "배 보다 배꼽 큰 로봇수술…병원들 고민 가중", 데일리메디, 2010.10.28. http://dailymedi.com/detail.php?number=720915

[6] 동아사이언스, http://m.dongascience.donga.com/news.php?idx=-107696

[7] 황규준, "써마지FLX 리프팅 시술 받기 전 확인해야 할 것", 스타데일리뉴스, 2019.10.21.

[8] LONZETTA, Angela M., et al. Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks, 2018, 7.3: 28.

[9] NAWIR, Mukrimah, et al. Internet of Things (IoT): Taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design (ICED). IEEE, 2016. p. 321-326.

[10] A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, M. Qbea'H and S. Alrabaee, "Security Vulnerabilities Detected in Medical Devices," 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC), Dubai, United Arab Emirates, 2020.

[11] S. K. Cherupally, S. Yin, D. Kadetotad, C. Bae, S. J. Kim and J. -s. Seo, "A Smart Hardware Security Engine Combining Entropy Sources of ECG, HRV, and SRAM PUF for Authentication and Secret Key Generation," in IEEE Journal of Solid-State Circuits, vol. 55, no. 10, pp. 2680-2690, Oct, 2020.

[12] Luis F. G. Sarmenta, Marten van Dijk, Charles W. O'Donnell, Jonathan Rhodes, and Srinivas Devadas, "Virtual monotonic counters and count-limited objects using a TPM without a trusted OS," in Proceedings of the first ACM workshop on Scalable trusted computing (STC '06), 2006.