https://doi.org/10.33778/kcsa.2024.24.2.133

동형암호를 활용한 DTC유전자검사 프라이버시모델★

진 혜 현*, 강 채 리**, 이 승 현**, 윤 지 희**, 김 경 진***

요 약

이용자가 직접 유전체 검사를 의뢰하는 DTC(Direct-to-Consumer) 유전자검사가 확산되고 있다. 수요 확대에 따라 인증제도를 통한 비 의료기관에 검사자격을 부여하고, 검사항목을 확대하였다. 그러나 제약이 적은 국외 사례와 달리 국내 제도에서는 여전히 질병 검사항목은 제외한다. 기존의 비식별 방식은 유전체 정보의 고유성과 가족 공유성에도 영향을 미쳐 충분한 활용 가능성을 보장하지 못한다. 따라서 본 연구는 서비스 활성화 및 검사 항목 확대를 위한 방안으로 분석과정에 완전동형암호를 적용하여 유전체 정보의 유용성을 보장하되, 유출 우려를 최소화한다. 또한 정보주체의 자기결정권 보장을 위해 Opt-out을 기반한 프라이버시 보존 모델을 제안한다. 이는 유전체 정보보호와 활용 가능성 유지를 목표로 하며, 이용자의 의사를 반영한 정보의 활용 가능성을 보장한다.

Privacy model for DTC genetic testing using fully homomorphic encryption

Hye-hyeon Jin*, Chae-ry Kang**, Seung-hyeon Lee**, Gee-hee Yun**, Kyoung-jin Kim***

ABSTRACT

The spread of Direct-to-Consumer (DTC) genetic testing, where users request tests directly, has been increasing. With growing demand, certification systems have been implemented to grant testing qualifications to non-medical institutions, and the scope of tests has been expanded. However, unlike cases in less regulated foreign countries, disease-related tests are still excluded from the domestic regulations. The existing de-identification method does not adequately ensure the uniqueness and familial sharing of genomic information, limiting its practical utility. Therefore, this study proposes the application of fully homomorphic encryption in the analysis process to guarantee the usefulness of genomic information while minimizing the risk of leakage. Additionally, to safeguard the individual's right to self-determination, a privacy preservation model based on Opt-out is suggested. This aims to balance genomic information protection with maintainability of usability, ensuring the availability of information in line with the user's preferences.

Key words : Direct-to-Consumer, genomic data, Fully Homomorphic Encryption, Opt-out

접수일(2023년 09월 30일), 수정일(1차: 2023년 10월 27일), 게재확정일(2023년 12월 27일)

★ 본 논문은 2024년도 산업통상자원부 및 한국산업기술진흥원의 산업혁신인재성장지원사업 (RS-2024-00415520)과 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0 사업의 연구결과로 수행되었음 (No. IITP-2022-RS-2022-00156310).

* 성신여자대학교/융합보안공학과(주저자)
** 성신여자대학교/융합보안공학과(공동저자)
** 성신여자대학교/융합보안공학과(공동저자)
** 성신여자대학교/마라융합기술공학과(공동저자)
*** 성신여자대학교/융합보안공학과(교신저자)

1. 서 론

유전체 데이터는 개인, 가족, 조상과 관련된 특별한 정보를 포함하며, 건강, 유전적 특성, 그리고 잠재적인 질병 정보와 같이 민감한 정보를 담고 있다. 이 정보는 고유성과 민감성으로 인해 안전하게 보호하고 다루는 것이 중요하다. 2013년, 미국 메사추세츠 공과대학(MIT) 연구소에서 공개한 DNA 정보를 통해 가계를 추적하고 유전적 정보를 추출하는 사례가 있었으며, 유전체 프로젝트(1000 Genome Project) 참가자의 기증 유전자 데이터를 사용하여 나이와 가족 관계를 파악하는 사례도 있었다[1]. 이에 따라, 개인의 전장 유전체 염기서열에 대한 정보보호의 중요성이 더욱 부각되었다.

DTC(Direct-to-Consumer) 유전자 검사는 질병에 미치는 유전적 연관성은 낮지만, 유전체 연구를 기반으로 특정 유전형과 검사대상자의 영양, 생활 습관, 신체적 특징 및 유전적 혈통과의 관계를 조사하는 검사이다[2]. 국외에서는 DTC 유전자 검사가 효과적으로 활용되어 많은 이용자를 확보하고 있으며, 글로벌 시장에서는 2020년 약 81억 달러에서 2025년에는 227억 달러로 22.8%의 성장률을 기대하고 있다[3]. 미국 식품의약국(FDA)은 현재는 안전성과 효과성을 검증한 후 86개 항목에 대한 유전자 검사를 허용하고 있다. 이러한 검사항목에는 치매, 파킨슨병, 그리고 유방암 BRCA 유전자 변이 검사 등이 포함된다.

국내에서도 DTC 유전자 검사가 확대되고 있으며, 「생명윤리법」 개정으로 인증 기관은 소비자를 대상 직접 검사가 가능하다. 그러나 질병 진단, 치료 및 예측을 위한 유전자 검사는 의료기관의 의뢰를 받아야 가능하다. 따라서 글로벌 수준과의 비교 시, 국내에서는 데이터 개방과 활용 측면에서 규제장벽을 가진다. 글로벌 시장 경쟁력 확보를 위해 검사 항목의 확대 및 안전한 유전자 데이터 처리, 이를 활용한 확장된 서비스를 제공하는 변화가 필요하다.

본 연구에서는 완전동형암호(FHE, Fully Homomorphic Encryption)를 활용하여 비식별 조치를 취하고, Opt-out 방식을 통해 정보 주체의 결정권한을 보장하는 프라이버시 보존형 DTC 유전자 검사 서비스 모델을 제시한다. 제2장 해외사례 및 선행연구에서는 Opt-out의 실적용 사례를 분석하고, 해당 제도 도입 시 사용자의 자기결정권에 미치는 영향도를 도출한 선행연구와 동형암호를 통한 유전체 분석 연산 선행연구를 분석한다. 제3장 프라이버시 보존형 DTC 유전자 검사 모델에서는 선행연구를 바탕으로 유전자 데이터의 안전성 향상 및 개인정보 자기결정권을 보장하는 프라이버시 보존형 DTC 유전자 검사 모델을 제안한다. 제4장 보안성 평가에서는 MITRE ATT&CK에서 제공하는 의료분야 민감정보 탈취 목적을 가진 공격자 그룹이 다수의 빈도로 사용하는 공격기법에 대해 기존 모델과 제안 모델과의 위험도 비교를 통해 제안 모델을 통해 위험도의 감소를 가져옴을 보인다.

2. 해외사례 및 선행연구

2.1 Opt-out 적용사례 및 선행연구

일본에서는 차세대의료기반법을 제정하며 Opt-in 방식에서 Opt-out 방식으로 전환하였고, 호주 정부는 Opt-out 방식을 기반으로 MHR(My Health Record) 시스템을 도입해 보건의료 빅데이터 활용을 강화하였다. 다양한 사례에서 볼 수 있는 Opt-out 방식의 장점을 고려하여, 본 연구에서는 이 방식을 도입함으로써 유전체 데이터 활용의 가능성을 확장하고자 한다.

조수진 외 1인(2022)[4]은 의료데이터 정보 주체의 인식을 설문조사를 통해 분석하였다. 이 연구는 보건의료 빅데이터에 대한 인식 및 활용에 대한 수용도를 파악하였으며, 응답자의 86.5%가 사후 동의 철회 절차에 대해 긍정적이었다. 빅데이터 연구에는 충분한 정보를 바탕으로 한 결정이 중요하다. 그러나, 임의적으로 제공되는 정보에는 한계와 불확실성이 존재할 수 있어 결과 도출에 영향을 미친다. 따라서 동의 범위 설정에 어려움이 존재한다. 이러한 문제점 해결을 위해, Opt-out 방식을 통해 개인정보 자기결정권을 보장과 확장된 활용가능성을 동시에 보장할 수 있다.

본 연구에서는 정보 소유 당사자가 정보수집을 명시적으로 거부할 때에만 정보수집을 중단하는

Opt-out 방식은 정보의 개방성과 정보 주체의 자율성을 동시에 존중하면서 빅데이터 활용의 효과를 극대화할 수 있다[5].

2.2 동형암호화된 유전데이터 분석

이원복(2018)[6]은 기존 프라이버시 보호 모델이 정보 활용성을 저해한다는 것을 근거로 완전동형암호(FHE, Fully homomorphic encryption)를 제시한다. 이를 통해 개별 데이터로 식별 불가하지만 활용 가능성은 유지할 수 있고, 유전정보 보호 법제에서 활용가능한 정보로 취급할 수 있다고 주장한다. 이를 통해 유전정보를 정보 주체의 동의 이상으로 정보 자체를 보호할 수 있다.

채승재 외 1인(2021)[7]의 연구는 대표적인 완전동형암호 알고리즘인 CKKS와 TFHE의 활용해 다자간 계산(Multi-Party Computation, MPC)을 통해 얻어진 데이터로 머신러닝 활용방법을 제시한다. 이를 통해 동형머신러닝이 가능함을 보인다.

유준수 외 1인(2021)[8]는 완전동형암호를 활용하여 사용자와 클라우드 간에 암호화된 유전자 서열을 분석하는 신개념 계산 모델을 발표하였다. 사용자는 유전자 서열을 암호화하여 클라우드로 전송하며, 클라우드는 받은 암호화된 데이터에서 질병과 관련된 위험인자가 있는지를 탐색한다. 이는 완전동형암호를 통해 암호화된 유전자 데이터의 분석이 가능하다는 것을 보여준다.

Cheon 외 3인(2017)[9]은 동형암호와 기계학습의 통합으로 보다 정밀하고 효율적인 유전자 데이터 분석 방법을 모색한다. 암호화된 메시지의 근사합과 근사곱을 가능케 하는 새로운 동형암호화 체계를 제안하며, 이 체계는 새로운 재조정 절차로 평문의 크기를 조절하며, 데이터의 보안성을 향상시키면서 정밀도를 유지하는 장점을 가진다.

Chen 외 2인(2019)[10]은 CKKS 근사 동형 암호화 기법의 신개념 부트스트래핑 방법론을 통해 데이터의 정밀한 분석과 동시에 보안을 강화한다. 이는 대규모의 복잡한 유전자 데이터를 대상으로, 복호화 과정 없이 암호화된 상태에서 다양한 함수를 통한 효율적인 평가를 가능하게 하여 유전자 데이터의 보안성, 분석 정확도, 및 실용성을 동시에 향상시킬 수 있다.

Liu(2015)[11]는 기존의 완전동형암호화 방식이 요구하는 필수 노이즈 감소 기술 없이도 실용적인 응용이 가능한 새로운 방법을 제안한다. 이를 유전자 데이터 분석에 적용하여, 노이즈로 인한 오차 없이 정확한 유전정보 분석이 가능해지고 연산속도에서 향상 가능성을 가질 수 있다.

본 연구에서는 '검체 전달 및 전처리 단계'에서 개인정보와 연구에 불필요한 정보를 삭제함으로써 연산속도의 향상을 기대하며, 단순 노이즈 제거를 넘어 프라이버시 보호를 통해 유전자 데이터의 활용을 보다 자유롭게 한다. 또한 기계 학습의 불확실성을 최소화하고, 암호화된 상태에서의 데이터 보안성을 확보하며 다양한 기계 학습 알고리즘에의 적용 가능성을 확장한다.

<표 1> 선행연구 비교 리스트

연구명	주요 특징	동형암호 사용	ML 가능성	차별점
본 연구	동형암호와 SNP의 통합	사용 (CKKS)	가능	Opt-out 도입
채승재 외 1인[7]	머신러닝에 암호화 데이터 활용	사용 (CKKS, TFHE)	가능	ML 결합
유준수 외 1인[8]	암호화된 유전자 서열 분석	사용 (Boolean Circuit)	가능	-
Cheon 외 3인[9]	근사 수 연산을 위한 동형암호기법	사용	불확실	근사 수 연산 특화
Chen 외 2인[10]	부트스트래핑 효율 향상	사용 (CKKS)	가능	CKKS 방식의 효율적 부트스트래핑
Liu[11]	노이즈 제거 완전동형암호 방안 제시	사용	가능	연산속도 개선

3. DTC 서비스 보안 아키텍처 제안

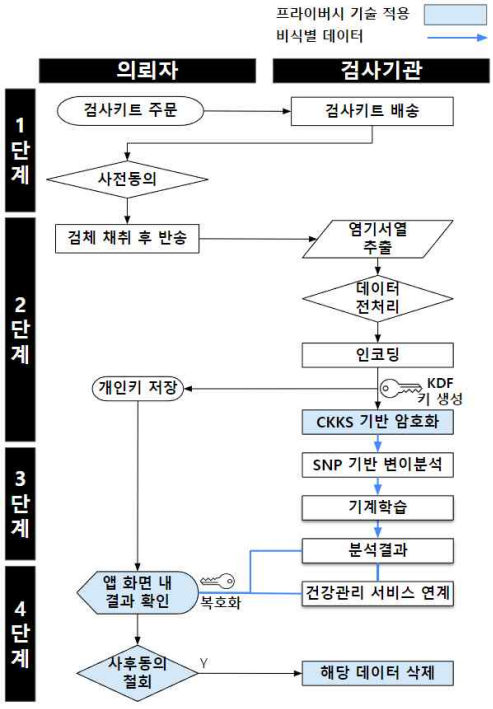
기존의 DTC 유전자 검사 프로세스에 다음의 프라이버시 보존 기술을 더해 유전자 데이터의 안전성 향상 및 개인정보 자기결정권을 보장할 수 있다.

첫 번째, 완전동형암호를 적용하여, 원본 데이터 노출 가능성을 제거한다. 검체 분석을 통해 도출되는 정보는 개인의 건강정보 및 질병 관련 민감정보를 포함할 수 있다. 따라서 기존의 분석 체계 내 검체 추출 및 데이터 분석단계에 완전동형

암호 CKKS 알고리즘을 적용한다. 해당 알고리즘은 부동소수점에 해당하는 수의 연산이 가능하여 유전자 데이터 암호화 후 데이터 분석 등 응용 단계에서도 암호화 데이터 연산이 가능하다. 추출된 DNA를 인코딩한 후 CKKS 연산 알고리즘을 기반한 완전 동형암호를 적용한다. SNP 분석을 수행결과 유전체의 특징과 변이정도를 도출하고, 동형기계학습을 통해 검사항목별 변이정도와 특징에 따라 필요한 건강관리 서비스 정보를 제공할 수 있다.

두 번째, Opt-out을 이용해 사전동의 내역에 대한 자기결정권을 보장한다. 유전체 정보는 고유성 및 가족 공유성이라는 민감성과 개인 식별 가능성을 가진다. 이러한 특성에 따라 유전체 데이터에 동형암호를 통한 비식별 조치와 함께 사전동의 사항에 대해 사용자 의사에 따른 재선택이 가능한 Opt-out을 적용하여 결정권을 보장한다.

프라이버시 보존형 DTC 유전자 검사 모델의 참여 주체를 의뢰자와 검사기관으로 나누고, 서비스 제공단계를 4단계를 구분하여 [그림 1]로 나타낸다.



(그림 1) 프라이버시 보존형 DTC 유전자 검사 모델

3.1 [1단계] 검사의뢰 단계

첫 번째, 검사의뢰 단계는 이용자가 서비스를 신청하고 사전동의를 받는 과정이다. 이때, 검사기관은 키트배송에 필요한 정보와 건강관리 서비스 제공에 필요한 건강검진이력 등의 정보를 수집한다. 이후 검사기관은 검사키트와 사전동의서를 함께 동봉하여 배송한다. 검체 수집 및 분석과정과 건강관리 서비스 과정에서의 수집 정보와 유전자 정보의 활용에 대한 사전동의를 수령한다. 사전동의서는 이용자가 이해할 수 있는 용어로 검사 내용과 정보의 수집 및 활용에 대해 상세히 서술한다. 특히 이용자의 유전체 정보를 활용해 추가적인 서비스를 제공하는 건강관리 서비스는 이용자의 자기결정권 보호를 위해 Opt-out을 제공한다. 사후 의사 변경 시 해당 의사 전달하여 자유롭게 서비스를 중단 및 재개 가능하다.

3.2 [2단계] 검체 전달 및 전처리

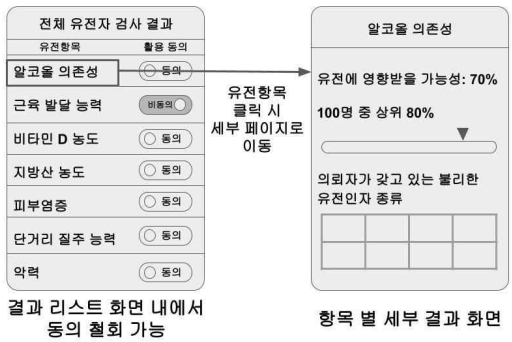
두 번째, 검체 전달 및 전처리 단계는 이용자 검체 채취 후 전달 및 검체 분석을 수행하는 과정이다. 이용자는 키트를 통해 채취한 검체를 검사기관에 반환한다, 검사기관은 사전동의서를 안전하게 보관하고, 검체로부터 유전자 정보를 추출을 수행한다. 검사기관은 검체 처리실에서 DNA 단편의 염기서열을 화학 반응 또는 광학적 반응을 활용해 하나씩 읽는 과정을 수행하며 염기서열을 파악하는 DNA 시퀀싱을 통해 문자형태의 염기서열[아데닌(A), 구아닌(G), 시토신(C), 티민(T)]을 추출한다. 이후, 원본데이터에서 반복 영역, 비 코딩 영역, 품질이 낮은 서열 데이터 등을 삭제하는 작업을 거친다. 염기서열 각각을 실수 형태의 숫자열로 매핑하여 문자열 형태의 데이터를 숫자열로 나타내는 인코딩을 수행한다. 이에 CKKS 알고리즘 기반 완전 동형암호화를 적용한다. 먼저, CKKS 알고리즘을 활용해 완전 동형암호화가 이뤄질 수 있도록 암호화 키를 키 더이스 함수(Key Derivation Function, KDF)를 활용하여 무작위성을 갖는 키로 생성한다. 생성된 암호화 키 중 복호화 키인 개인 키는 이용자의 단말기 내 안전한 저장소에 저장한다. 이후, 이용자의 개인정보보호를 위한 조치로 원본데이터를 파기한다.

3.3 [3단계] 암호화 데이터 분석

세 번째, 암호화 데이터 분석 단계에서는 동형 암호화한 유전정보에서 개인 특성을 찾아 분석한다. 검사기관은 암호화된 유전자 정보를 토대로 유전적 특성을 분석한다. 의미있는 유전자 변이 영역에 중점을 두고 고해상도의 DNA 시퀀싱을 수행한다. 시퀀싱된 데이터는 품질 제어 과정을 통해 잡음, 오류 및 반복 영역 등이 제거되거나 보정된다. 단일염기 다형성(SNP)는 각 개인의 유전적 특성과 건강상태에 결정적인 영향을 미치는 유전자 변이이므로, 최신 SNP 분석 모델을 통해 이용자의 염기서열을 정상 그룹과 이상치 그룹과 비교한다. 이 과정에서 이용자의 데이터 보안은 최우선적으로 고려하여 CKKS 동형 암호화로 원본 데이터의 보안성을 유지하면서도 정확한 SNP 및 유전변이 탐지가 가능하도록 한다. 분석된 SNP의 연관성에 기반해 SNP로 인한 기능적 영향성을 분석한다. 분석 결과를 동형기계학습 모델을 통해 이용자 유전체의 변이 정도에 따라 필요한 건강관리 서비스 유형을 도출한다.

3.4 [4단계] 분석결과 전달 및 건강관리서비스 제공

네 번째, 결과 전달 단계에서는 분석 결과를 사용자에게 전달하고 이를 이용해 필요한 건강관리 서비스를 제공한다. 분석 결과는 완전 동형암호화된 상태로 중앙 서버에 저장한다. 이용자는 모바일 앱을 통해 검사 결과지 형태로 열람 가능하다. 각 검사항목에 따른 변이형질 결과와 동형기계학습 모델을 통해 변이형질 수준에 따라 필요한 건강관리 서비스 유형을 제공한다. 이때 모든 데이터 전송은 SSL/TLS 같은 보안 프로토콜을 통해 진행하여 데이터 안전성을 확보한다. 또한 모바일 앱 로그인 단계에서 생체인증, 전자 증명서와 같은 인증방법을 이용한 본인인증을 진행한다. 정상적인 인증을 거친 이용자는 보유한 개인 키를 통해 진단 결과를 확인한다. 사용자 정보 자기결정권을 표현할 수 있는 수단인 opt-out을 이용해 [그림 2]와 같이 분석 결과 활용에 사용자의 의사를 반영할 수 있다. 검사기관은 실시간 모니터링 시스템을 도입하여 비동의로 전환된 정보를 즉시 인지하고, 지체 없이 이용자 관련 정보를 분리 및 삭제하며, 연관 프로세스에 사용자 의사를 반영하여 조치를 취한다.

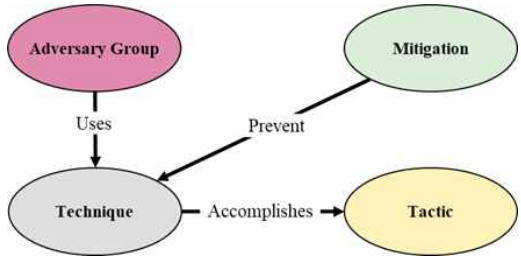


(그림 2) 동의철회(Opt-out) 앱 화면

4. 보안성 평가

4.1 MITRE ATT&CK Framework 및 보안성 평가방법

MITRE ATT&CK Framework는 알려진 전 세계 사이버 공격자 행위를 공격 생명주기에 따라 단계별로 정리한 지식 기반의 모델로, 공격전술(Tactics), 기법(Techniques), 절차(Procedures)로 분류한 체계 및 관계를 설명한다[12]. [그림 3]과 같이 공격자 그룹(Adversary Group)을 분석하여 공격 시 사용기법(Technique)을 파악하고, 이를 상위의 전술(Tactic) 범주에 묶는다. 파악된 기법은 완화(Mitigation) 방안을 마련하여 탐지 및 완화 방법을 소개한다.



(그림 3) MITRE ATT&CK Framework

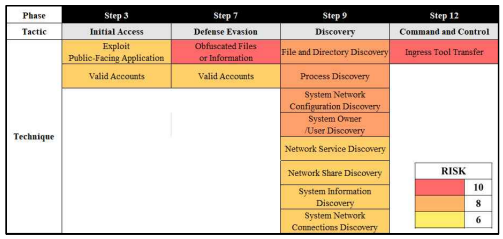
본 연구에서는 [표 2]와 같이 MITRE ATT&CK을 활용한 보안성 평가방법을 바탕으로 기존 모델 대비 제안 모델이 위험도를 감소함을 보인다.

<표 2> 보안성 평가 방법론

단계	설명
1	MITRE ATT&CK에서 제공하는 의료민감정보 탈취 공격 그룹 추출 및 프로파일링
2	MITRE ATT&CK Navigator를 이용해 추출한 공격자 그룹의 공격기술 분석 및 빈도별 위험도 도출
3	각 공격기술의 탐지 및 완화 방법 분석 및 위험도 도출 기준 수립 위험도 / 기준 1점 / 공격기술에 대한 완화 및 탐지 방안이 모두 존재하며, DTC 검사 모델에 구현 가능함 2점 / 공격기술에 대한 완화이나 탐지 방안중 하나가 존재하며, DTC 검사 모델 내 대체 가능한 보안 기능이 존재함 3점 / 공격기술에 대한 완화이나 탐지 방안중 하나가 존재하며, DTC 검사 모델내 구현된 기능이 부재함
4	기존 DTC 검사 방안과 제안 매커니즘의 위험도 비교 분석

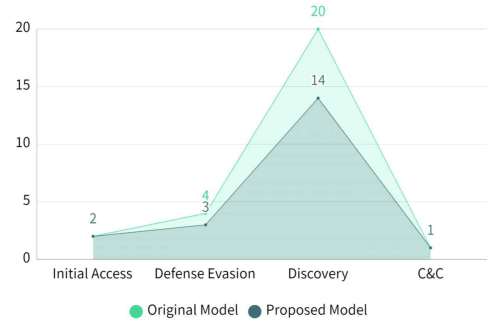
4.2 보안성 평가

단계별 보안성 평가를 위한 절차를 수행한다. 의료민감정보 탈취형 사이버 공격자 그룹인 FIN4와 Deep Panda 등의 8개 그룹을 선정하여 프로파일링한다. 공격그룹이 사용하는 Technique 각각에 '2'의 위험도를 부여하고, 상위 위험도를 가지는 4개의 Tactic과 최소 3개 그룹 이상이 활용하는 빈도 높은 technique을 위협 단계에 따라 [그림4]에 표기하였다. 공격자는 지속적으로 다양하게 알려지거나 알려지지 않은 공격을 실행하여 목표를 달성한다. 고위험 공격기술은 쉽게 목표에 도달할 수 있는 약한 연결고리 지점이 될 수 있다 [13].



(그림 4) 의료민감정보 탈취형 사이버 공격자 그룹의 활용도 높은 공격기술

의료민감정보 탈취형 공격은 특히 Discovery 단계에 다수 포진해 있다. 이는 시스템 환경 파악을 위한 정보수집 목적을 가지며, 해당 단계에서 수집하는 정보를 바탕으로 다음 단계의 공격을 결정할 수 있기에 공격자 입장에서 중요성을 가진다. 특히, Discovery 단계의 Technique의 75%는 시스템 기능의 남용을 기반으로 수행되기에 탐지 방안은 존재하나 완화 방안이 명확히 제시되지 않는다는 특징을 가진다.



(그림5) 보안성 평가 결과

기존모델과 제안모델의 보안성 평가결과는 [그림 5]와 같다. 기존모델 대비 제안모델은 원본 데이터에 동형암호를 적용하여 복호화 가능한 키를 가진 이용자의 키를 탈취해야만 공격을 통한 민감정보 탈취가 가능하다. 따라서 기존모델은 공격기법을 통한 권한 취득을 통한 정보 탈취 및 열람이 가능하나, 제안 모델은 이용자의 복호화 키를 함께 탈취하여야 하는 복잡성이 추가되고, 암호데이터 탈취 시 복호화가 불가능하여 탈취 목적달성이 불가능하므로 동형암호라는 대체 기능이 존재한

다. 따라서 Defense Evasion과 Discovery 단계에서 기존 모델 대비 위험도를 낮춰 26%의 위험도 감소 효과를 가진다.

5. 결론

유전체 데이터는 단순한 개인정보를 넘어서 가족과 조상에 이르는 광범위한 민감한 정보를 포함한다. 이러한 데이터의 특수성은 적극적인 서비스 수요에도 이를 이용한 개인 맞춤형 서비스 제공에 있어 제약을 유발한다. 따라서 본 연구에서는 프라이버시 보존형 DTC 유전자 검사 모델을 제안한다. 분석과정에 완전동형암호를 적용하여 유출을 통한 피해발생 우려를 최소화하고, 정보주체의 자기결정권을 보장할 수 있는 Opt-out 방식을 도입한다. 이를 통해 의료민감정보 탈취형 공격에 대해 기존모델 대비 26%의 위험도 감소율을 보인다.

본 연구를 기반으로 DTC 유전자 검사의 높은 수요에 따른 검사항목 확대와 서비스 활성화를 위한 방안이 지속적으로 개발되어야 하며, 안전성을 기반으로 이용자 개개인의 맞춤형 서비스로 이용자의 만족도를 높일 수 있다. 본 연구에서 제안하는 모델을 향후연구에서 인프라 제약을 최소화할 수 있는 클라우드 환경에서 실제 구현한다. 실질적인 분석 가능성과 분석단계의 연산 복잡도 및 시간 지연도를 고려한 활용 측면의 지표와 MITRE ATT&CK을 통한 공격 기술을 재현하여 데이터 탈취 상황에서의 프라이버시 노출도를 보호 측면의 지표로 함께 비교 분석하여 고도화된 모델을 제안을 목표로 한다.

참고문헌

[1] Melissa Gymrek, David Golan, Saharon Rosset and Yaniv Erlich. lobSTR: A short tandem repeat profiler for personal genomes. Genome Res. 2012 Jun; 22(6): 1154 - 1162.

[2] 보건복지부고시 제2022-43호,「의료기관이 아닌 유전자검사기관이 직접 실시할 수 있는 유전자검사 항목에 관한 규정」, 2022. 2. 22.

[3] EDGC, 한국IR협의회 기업리서치센터.

[4] 조수진, 최병인. (2022). “보건의료빅데이터 연구에 대한 대중의 인식도 조사 및 윤리적 고찰”, Journal of KAIRB 제4권 1호, 16-22. 대한기관윤리심의기구협의회.

[5] 이승현, 오정윤. (2018). "호주의 보건의료 빅데이터 활용을 위한 시스템연구: My Health Record의 2차적 사용", 보건산업브리프, Vol. 273, 한국보건산업진흥원.

[6] 이원복 (2018). “유전체 시대의 유전정보 보호와 공유를 위한 개인정보 보호법제의 고찰”, 법조, 67(3), 597-644.

[7] 채승재, 노종선. (2021). “정보보호 머신러닝에서의 완전동형암호와 다자간 계산의 활용”, 한국통신학회 학술대회논문집,Vol.2021 No.11, 581-582, 한국통신학회.

[8] 유준수, 윤지원(2021), “암호화된 유전자 서열 데이터 분석을 통한 질병 진단 방법에 관한 연구“, 한국통신학회 학술대회논문집, Vol.2021 No.11, 477-478, 한국통신학회.

[9] Cheon, J.H., Kim, A., Kim, M., & Song, Y. (2017). "Homomorphic Encryption for Arithmetic of Approximate Numbers", Advances in Cryptology ASIACRYPT, Part of the Lecture Notes in Computer Science book series, Vol.10624.

[10] Chen, H., Chillotti, I., & Song, Y. (2019). " Improved Bootstrapping for Approximate Homomorphic Encryption", Advances in Cryptology EUROCRYPT, Part of the Lecture Notes in Computer Science book series, Vol.11477.

[11] Liu, D. (2015). Practical Fully Homomorphic Encryption without Noise Reduction. IACR Cryptol. ePrint Arch., 2015, 468.

[12] Blake E. Storm at al., “MITRE ATT&CK : Design and Philosophy,” The MITRE Corporation, 2020.

[13] 윤지희 and 김경진. (2023). Enhancing the Cybersecurity Checklist for Mobile Applic

ations in DTx based on MITRE ATT&CK for Ensuring Privacy. 인터넷정보학회논문지, 24(4), 15-24.

〔저자소개〕

이 승 현 (Seung-hyeon Lee)
2021년 3월 ~ 현재 성신여자대학교 학사

email : 20210813@sungshin.ac.kr

진 혜 현 (Hye-hyeon Jin)
2019년 3월 ~ 현재 성신여자대학교 학사

email : hh991218@naver.com

윤 지 희 (Gee-hee Yun)
2019년 2월 학사
2018~2022 : F1Security 재직
2022년 9월 ~ 현재 성신여자대학교 석사

email : geehee_yun@naver.com

강 채 리 (Chae-ry Kang)
2021년 3월 ~ 현재 성신여자대학교 학사

email : charry501@naver.com

김 경 진 (Kyoung-jin Kim)
2007년 2월 성신여자대학교 학사
2009년 2월 성신여자대학교 석사
2013년 2월 성신여자대학교 박사
2016년 2월 고려대학교 무인자율 및 적응형 소프트웨어센터 연구교수
2017년 2월 성균관대학교 스마트핀테크연구센터 박사후과정
2017년 3월 ~ 현재 성신여자대학교 융합보안공학과 조교수

email : kyoungjin@sungshin.ac.kr