특집 05

국내 금융기관의 챗봇(ChatBot)서비스의 개인정보보호방안

이기혁 (중앙대학교)

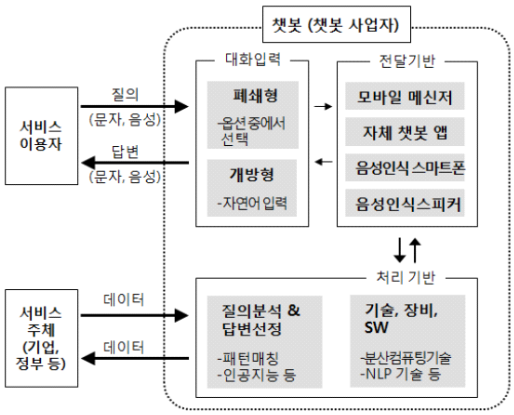
목 차

1. 서 론

Open AI사에서 개발한 챗GPT를 출시하면서 대화형 인공지능 서비스가 급속히 확산되고 있다. 일부 금융기관에서는 24시간 응대와 맞춤형 서비스를 제공하고자, 인공지능의 자연어 처리 기술을 기반으로 대화형 인터페이스를 적용한 챗봇 서비스를 활발하게 도입하고 있다. 챗봇(ChatBot)은 채팅(chatting)과 로봇(robot)을 결합한 표현으로 빅데이터 및 인공지능 기술을 활용하여 인간과 채팅이 가능한 프로그램을 말한다.

국내 금융기관은 각종 인건비와 관리비의 절감 및 고객응대등의 감성적인 노동 강도 등의 이유로 인공지능 기술이 적용된 '고객상담 챗봇'을 많이 도입하고 있다. 이와 같이 챗봇이 인기 있는 이유 중의 하나는 상담원과의 전화통화는 평균 10분이 걸리나, 챗봇은 평균 45초 이내에 원하는 답을 빠르게 응대할 수 있기 때문이다. 이러한 챗봇 서비스의 성공과 확대에 있어서, 사용자로 하여금 챗봇 서비스에 대해 긍정적인 경험을 갖게 함으로써 사용자의 만족도와 이에 따르는 지속적인 활용 의도를 높이는 것이 주요 영향 요인이 될 수 있다

챗봇 서비스를 도입한 금융기관은 챗봇 서비스가 잘못된 고객 응대를 하지 않도록 대화 이력을 검증하는 품질 향상 전담 부서도 같이 두고 있다. 예를 들어, 신한은행의 경우에는 쏠(SOL) 앱에 탑재되어 있는 챗봇은 관련 전담팀이 있으며, 매일 상담 이력을 확인하여서, 사용자들이 긍정적인 경험을 가질 수 있도록 하고 있다.



(그림 1) 챗봇 서비스의 구성

2. 서비스 유형

챗봇 서비스는 크게 2가지로 구분한다. 첫째는 시나리오 기반의 챗봇 서비스가 있다. 초기 금융기관의 시나리오 기반의 챗봇 서비스는 고객과의 대화 시나리오를 사전에 정의한 후, 사용자가 입력하는 키워드에 따라 금융상품소개, 영업점 안내 등 간단한 업무 위주의 서비스를 제공하는 방식으로 제한적 질문에 대한 정해진 답을 출력하여 새로운 보안위협에는 크게 문제가 되지 않았다. 둘째는 최근 AI기술을 적용한 챗봇 서비스를 시작하면서 복잡한 질문에도 응답할 수 있고, 자기 학습도 가능하여 AI기반의 서비스 제공이 가능함에 따라 개인정보 및 중요정보 유출이 가능하여 챗봇의 자기학습으로 인한 이상 동작 가능성 등 새로운 보안 위협이 예상된다.

금융감독원의 자료에 따르면 금융기관 352개사 중에 챗봇 운영 금융기관은 26개사로 시나리오기반의 서비스보다는 대부분이 인공지능 기반의 챗봇 서비스를 운영하고 있는 것으로 나타났다. 특히 최근 챗GTP의 붐으로 인해서 거의 대부분 인공지능기반의 챗봇 서비스로 전환 예정으로 나타나고 있다.

위와 같이 금융기관의 챗봇은 주로 금융상품 상담에 쓰인다. 은행의 챗봇 서비스는 주로 예금이나 적금 상품을 안내하고, 투자 포트폴리오를 제공한다. 보통 인터넷뱅킹이나 은행 모바일 앱에서 이용할 수 있으며, 챗봇 프로그램은 간편 송금, 계좌 조회는 물론이고 질문의 키워드에 따라 금융상품을 추천한다.

챗봇이 추천한 상품 중 비대면 계좌 개설이 가능한 상품은 바로 가입할 수도 있는 경우도 있다. 보험회사의 경우는 보험금도 챗봇 서비스로 간편하게 청구할 수 있다. 청구에 필요한 서류를 사진으로 전송하면 된다. 보험 회사의 챗봇은 해당 회사의 앱으로 실행하거나 카카오톡, 라인 등의 메신저를 활용하기도 한다. 전화보다 빠르게 상담할 수 있어 활용도가 높은 편이다. 신용카드 회사에서도 챗봇 서비스를 제공하고 있다. 개인 정보 변경, 대금 결제일 변경, 대출 한도 조회, 이자율 조회 등 변경 사항이나 간단한 궁금증도 해결하는 서비스를 제공한다. 증권사에서도 챗봇 서비스를 운영한다. 종목을 검색하거나 시세를 조회하는 등 질문만으로 필요한 정보를 얻을 수 있다. 조건을 제시하고 펀드를 추천 받을 수도 있다. 챗봇은 주어진 데이터로 학습해 새로운 것을 만들어 내는 능력이 있다. 발전 가능성은 무궁무진하다. 이런 맥락에서 챗봇은 반짝 유행하다 사라질 기술이 아니다. 챗봇은 AI의 발전과 함께하므로 시간이 지

〈표 1〉 국내 금융기관의 챗봇서비스 현황

유형	기관명	챗봇명	플랫폼	도입시기	제공 서비스
닫힌 대화	웰컴저축은행	웰컴봇	카카오톡	2017.09	대출신청, 상품문의, 한도조회
	대신증권	벤자민	카카오톡	2017.06	FAQ, 금융정보제공, 투자상품추천
	신한카드	신한카드	네이버 톡톡	2017.06	카드추천
열린 대화	현대카드	버디	자체앱, 카카오톡	2017.08	금융정보제공, 카드추천
	우리은행	위비봇	자체앱	2018.09	음성명령 송금, 계좌조회, 공과금납부, 환전
	KEB 하나은행	HAI	SMS	2017.07	계좌조회, 계좌이체
혼합 대화	신한은행	쏠메이트	자체앱	2018.02	예금, 대출 ,외환, 펀드 상담 등
	국민은행	똑똑이	자체앱	2017.07	계좌조회, 이체, 카드, 퇴직연금, 회자인증
	KEB 하나은행	HAI	자체앱	2017.09	지출분석(투자, 재테크 상담, 적금가입, 환전 시청, 자산현황)
	OK 저축은행	오키톡	카카오톡, 네이버톡톡	2017.09	시나리오 기반 금리, 한도 문의, 개인 거래정보 확인
	JT 친애 저축은행	JT 친애 저축은행	카카오톡	2017.08	시나리오 기반 증명서 발급절차, 지점안내
	삼성 생명	따봇	자체앱	2018.05	내 보험 조회, 보험대출, 지점찾기, FAQ

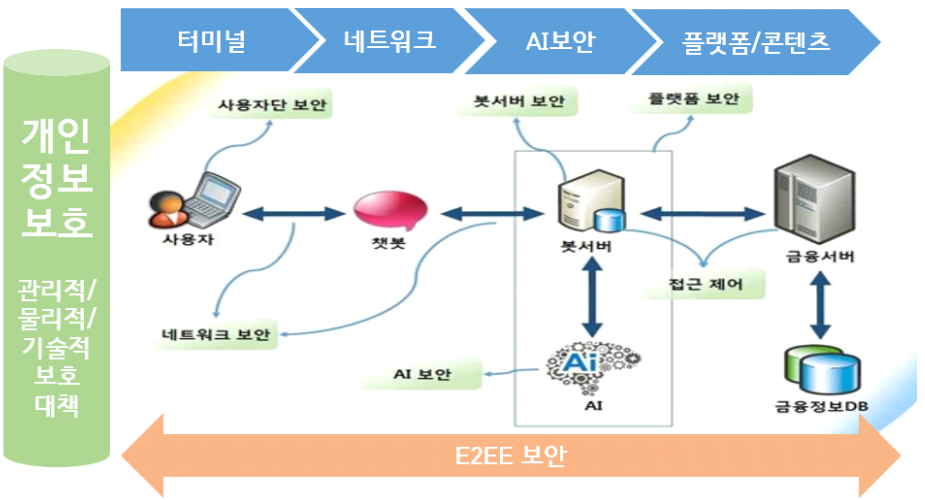
(자료출처 : https://m.fntimes.com/html/view.php?ud=2020010322251944436dd55077bc2_18)

날수록 더욱 정교해지고 사용하기 편리하게 바뀔 것으로 판단된다.

챗봇 서비스의 장점으로는 인간의 언어를 이용하여 대화하는 형태로 운영되므로 발전단계에 따라 다양한 서비스 제공이 가능하고, 비대면 금융거래가 활성화됨에 따라 단순 안내에서 카드발급, 대출, 보험계약 등 다양한 업무처리 가능하다. 그리고 인건비를 절약하면서 업무 시간의 중단 없이 고객에게 서비스를 제공할 수 있고, 고객의 입장에서도 필요한 시간에 신속하게 서비스를 제공받을 수 있다. 단점으로는 인공지능의 이상 작동 시 서비스 제공이 원활하지 않을 우려가 가장 크며 보안대책이 미흡할 경우 개인정보와 프라이버시 보호 측면에서의 부작용이 발생할 수 있다. 또한 이에 대한 적절한 보안 가이드나 사고 대응 매뉴얼이 존재하지 않는다.

3. 보안 위협과 대응

챗봇 서비스의 보안 위협과 대응에 관하여 알아보고 개인정보관련된 보호 방안을 제시하고자 한다. 우선 기술적 고려사항은 콘텐츠 - 플랫폼 - 네트워크 - 터미널(C-P-N-T) 전반적인 모든 단계의 보안의 재설계와 구축을 하여야 한다. 우선 사용자 단(Terminal)에는 비정상적인 챗봇 설치로 인한 피싱과 파밍 공격 등의 보안 위협에 대응 해야한다. 특히 챗봇에 대한 식별 기능을 제공하여야 하고, 챗봇을 통해 입력되는 중요 정보를 사용자 단말기에 저장하지 않거나 불가피한 경우 안전한 암호 알고리즘을 적용하여 이용하여야 한다. 둘째는 챗봇 플랫폼(Platform)과 서버보안이다. 여러 다른 통신 채널 (Skype, SMS, 메일 및 기타)과의 연결을 통한 보안 위협이 있을 수 있다. 예를 들면 HTTPS만 사용하도록 봇의 구성 강화와 봇을 등록하고 해당 어플리케이션 ID 및 암호를 가져와 Bot Framework 인증을 사용하도록 설정하여 이용하여야 한다. 특히, 챗봇 서버 플랫폼 단의 보안은 콘텐츠 프로바이더 등의 타사 플랫폼을 연동, 이용을 통한 서비스를 제공할 경우 해당 플랫폼의 보안 취약점은 챗봇 서비스에도 반영하여야 한다. 플랫폼 보안의 경우, 해당 플랫폼의 보안취약점과 Contents 보안인 시큐어 코딩 점검 결과 등을 확인이 중요하다. 다음으로는 AI보안이다. 고객이 입력한 단어에 대해 AI가 의도치 않은 행



(그림 2) 챗봇 서비스의 보안 개념도

위를 수행하여 개인정보 유출 등의 보안 위협이 존재한다. AI 행위에 제한을 두어 이상 행위 수행을 제한하고 AI 대답에 개인정보 포함 여부 등을 확인해 필터링 수행해야 한다. 마지막으로는 접근제어, 네트워크 보안, 웹 서버 보안등 금융서비스에서 일반적으로 고려되는 보안 사항에 대해서도 대비는 기본적으로 필요하다. 특히 공통인프라 보안기술인 암호, 인증, 접근제어, LOG관리, 백업관리는 콘텐츠-플랫폼-네트워크-터미널의 모든영영에서 공통 보안 기술로 들어가 있어야 서비스가 가능하도록 해야 한다.

4. 개인정보보호 방안

일반적으로 개인정보는 개인에 관한 일반적인 정보이며, 프라이버시는 개인정보에 더해서 혼자 있을 권리와 자기 정보 통제권을 말한다. 개인정보보호측면을 살펴보면 기본적으로 관리적, 기술적, 물리적 보호조치가 되어야 한다.

개인정보법에 따라서 개인정보처리자가 개인정보를 안전하게 저장, 전송하는데 사용되는 암호화 기술을 개인정보보호법 제24조제3항에 적용된 조치를 반드시 시행해야 한다.

챗봇이 주민등록번호등의 질의나 신분증 사진 등을 촬영 후에 별도의 기준을 마련하여 단대단(E2EE) 암호화 관리 해야 한다. 챗봇을 통한 서비스 상당 시 수집하는 개인정보는 의무적으로 암호화를 제시한다. AI알고리즘을 AI가 공격을 하는 모델 중에는 기능 추출형 모델의 입력 값과 출력 값을 비교해 모델을 복제하는 공격과 입력에 대한 출력 값을 내는 AI모델의 분류 결과와 신뢰도를 분석하여 학습데이터를 복원하는 공격 등 AI를 이용하 AI모델을 역 추론하는 사이버 공격을 막은 방안이 별도로 마련되어야 한다.

금융서비스 제공자는 대화형 정보처리시스템(문자·음성을 이용하여 인간과 대화하는 방식으로 정보를 처리하는 시스템을 말한다)을 기반으로 하는 금융서비스를 제공하는 경우 상담 시 수집되는 개인정보의 단대단(E2EE) 암호화를 필수적으로 진행하여 무결성 메시지 보호와 전송을 위한 신뢰할 수 있는 연결을 하여야 한다. 그리고 안정성 확보를 위해서 공통 인프라보안기술인 인증, 접근제어, 로그 관리, 백업 관리를 하여 감사 로그를 남기도록하여야 한다.

금융 챗봇 서비스와 관련된 기록관리 작업을 하여 사용자에 의해서 비활성화 할 수 없는 경우를 제외하고 감사 로그 상태를 (활성화 또는 비활성화)를 기록하여야 한다. 기술적으로 비 활성화가 허용되는 기능은 한정된 사용자 집합을 정의하고 제한 하여야 한다. 감사 로그의 보호는 기술에 의해 변경, 덮어쓰기 또는 삭제할 수 없어야 한다. 사용자 권한에 어떤 변경도 추후 포렌식 재구성을 지원하는 방안으로 보호되어야 한다.

개인정보보호법 제7조의 개인정보의 안전성 확보 기준과 보호조치 기준에 따라서 저장, 보관, 이용되어야 한다. 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있어야 한다. 또한, 대화형 정보처리시스템인 챗봇이 사람으로 착각할 수 있으므로 이를 명확히 하기 위해서 사람이 아니고 챗봇이라는 챗봇 표시제를 도입하여야 한다.

챗봇은 사람이 아니고 인공지능 기술 등 융합기술을 접목한 챗봇 시스템의 기술이 지속적으로 고도화되면서 사용자의 정보접근성을 높여주는 서비스가 잇따라 등장하고 있다. 심지어는 챗GPT에서 작성한 글을 아바타를 통해서 대신 발표하거나 연설하는 서비스도 제공되곤 한다. 그러나 아바타의 그래픽 동작이나 음성이 진짜 사람인지 모르는 경우도 미국의 해킹사례에서 발생했다. 따라서 서

비스 신뢰 향상을 위해서 최소한의 제도적 장치를 마련하기 위해서 반드시 사람이 아님을 표시하는 제도 도입이 필요하다.

지금까지 해킹은 전문지식, 시간, 독창성, 운이 필요한 인간의 활동 영역 이였다면, 앞으로 인공지능이 해킹을 시작하면 해킹 속도, 규모, 범위 등 금융기관의 챗봇 서비스 설계자가 예상하지 못하고 원하지 않았던 새로운 방식의 프라이버시 해킹의 시대가 올 것이다. AI해킹이 가장 먼저 위협이 될 분야로는 금융 시스템이고 금융시스템은 알고리즘적으로 해킹 가능하도록 설계 되었기 때문이라고 미국의 저명한 암호학자이자 보안 기술 그루인 브루스 슈나이어가 2022 RSA컨퍼런스에서 발표하기도 했다.

다음은 정보주체의 권리보장을 위해서 챗봇 인증제를 도입하여야 한다. 공신력 있는 제3기관인 금융감독원등을 통해서 인증을 받아 그 사실을 사용자에게 시각적으로 보여주어야 한다. 최근에는 블록체인 기반의 AI 검증 플랫폼 등이 출시되었는데 이와 같은 시스템을 이용하여 파싱과 파밍으로 보안 위협 기능을 완화 해야 한다. 이를 위해서는 기존의 상위법인 개인정보보호법을 전문 개정이 필요하며, 이하 관련 금융기관의 개인정보보호 가이드라인도 챗봇 서비스등에 맞춤형으로 개정되어야 한다.

비대면 시대에 사람이 인지하지 못하는 상황에서 실시간으로 개인정보를 수집 가능하고, 대화내용이 사후적으로 결합하거나 분석되어 또다른 개인정보 생성이 가능하며, 요구하는 수준 이상의 개인정보를 정보주체가 스스로 제공할 가능성이 상존한다. 그러나 챗봇 등장 이전에 마련된 현행 정통망법과 개인정보보호법에서는 관련 규정을 어떻게 챗봇 서비스에 적용해야 할지 불확실하며 정보제공자가 과도한 정보 제공 시, 향후 보안사고 책임 소재도 불분명하다.

로그인 후에 챗봇 서비스를 이용한다고 해서 챗봇으로 수집되는 개인정보를 수집, 저장, 제공에 동의 한다고 할 수 없다. 챗봇 이용 시 사용자가 스스로 과도한 개인정보를 제공할 가능성을 존재한다는 것과 그러한 정보에 대한 해당 조직의 처리방침을 이용 약관에 넣어야 하며, 챗봇 이용 전에, 약관 동의를 받아야 하며, 그 내용에는 개인정보 수집, 활용 관련 내용, 정보주체의 과도한 정보제공 가능성과 책임의 소재에 대해 충분히 설명 및 고지 되어야 한다. 그러나 동의 만능주의가 되지 않도록 대화형 인공지능에 맞게 정리해야 한다. 예를 들면 정보통신서비스 제공자는 대화형 정보처리시스템(문자·음성을 이용하여 인간과 대화하는 방식으로 정보를 처리하는 시스템을 말한다)을 기반으로 하는 정보통신서비스를 제공하는 경우 그 서비스를 사용함에 있어 부득이하게 사용자 스스로가 목적 외 정보를 제공할 수 있음을 공지하여야 한다. 대화형 정보처리시스템을 통해 사용자가 제공한 목적 외 개인정보의 수집 및 처리 과정 등에 필요한 사항은 과학기술정보통신부령으로 정한다.라고 개정되어야 한다

금융기관에서 제공하는 챗봇 서비스는 개인정보 보호를 위해 정보 주체의 권리인 열람, 정정, 삭제를 보장하는 규정을 마련해야 합니다. 그러나 현재 챗봇 서비스는 암호화 의무 규정에 해당되지 않아 내부에서의 접근 통제 규정이 부족한 경우가 많습니다. 이를 해결하기 위해서는 개인정보에 대한 내부 접근 통제 규정을 수립하고 업무별, 관리자 별로 차등한 접근 권한을 부여하는 통제 절차가 필요합니다. 챗봇 서비스는 세계적으로 사용되고 있지만 법률 개정이 적용되는 경우는 제한적입니다. 유럽연합에서는 일부 국가에서 법률이 적용되고 있으며, 우리나라에서는 새로운 기술이 도입될 때 빠르게 법률 개정이 이루어져야 합니다. 이를 위해서는 포괄적인 상위법 제정과 하위법에도 적용 가능한 신속한 법제 개선이 필요합니다.

5. 결 론

미래 금융시장에서는 챗봇서비스와 같이 인공지능이 점점 중요해지면서 더 많은 금융서비스가 제공될 것이다. 그러나 새로운 위협을 발생시킬 수 있으며, 데이터와 개인정보의 유출, 취약한 챗봇 보안이슈등은 지속적으로 발생할 것으로 본다. 이에 따른 개인정보의 수집, 이용, 제공, 파기 등의 처리과정에서 발생하는 문제를 해결하고 금융 상담 특화된 챗봇용 AI서비스의 관리, 감독기능을 추가하여 안전한 서비스 환경을 구현하기 위해서는 위 제시한 영역 이외에 체계적인 연구가 필요하다. 이를 위해 금융 상담용 챗봇 AI 보안 기술을 기반으로 활용하여 챗봇용 AI서비스에서 발생하는 피해를 방지해야 한다. 그후 안전한 금융 챗봇용 AI서비스를 제공함에 있어서는 Privacy from AI, Privacy of AI, Privacy by AI 등 다양한 개인정보보호를 위한 기준과 가명화 처리, 익명화 처리 등의 챗봇용 AI 서비스에 맞는 새로운 정의가 필요하다.

앞으로 금융 챗봇용 AI서비스와 관련한 개인정보보호 연구를 다각적인 관점에서 접근하고, 금융기관의 특화된 AI용 서비스에 맞게 개인정보보호 프레임워크 체계를 구현하는 연구를 지속적으로 수행해야 한다. 금융 AI서비스에서의 세부적인 개인정보 보호 준수사항을 도출해야 하며 가장 약한 보안 취약 고리가 되는 것을 방지해야 한다. 끝.

참 고 문 헌

[1] 금융서비스 챗봇의 인터렉션 유형별 UX평가 2019년03 한국과학학회지, 조국애(홍익대학교)

[2] 이상일.텍스트의 재발견 금융권에서 '챗봇'으로 화려한 부활. http://ddaily.co.kr/m/m_article.html?no=151813 2018.10.1

[3] 강석태. 문답으로 알아보는 챗봇. https://blog.lgcns.com/1318 2018.12.1

[4] KB국민은행, 대고객 인공지능 챗봇 서비스 월 이용자 100만 돌파 〈 챗봇 〈 AI Industry 〈 기사본문 - 인공지능신문 (aitimes.kr)

[5] 국내 금융챗봇서비스 어디까지 왔나? 2022.7.21) https://digitalbonaza.co.kr

[6] "AI 해커가 온다". 보안 그루의 경고 - ZDNet korea 2022.06.09

[7] 금융권 챗봇서비스의 사용자 수용의도에 영향을 미치는 요인 2021 VOL 24 한국기술혁신학회

[8] 금융회사의 대화형 뱅킹 현황 및 발전현황 2022.1.6 코스콤 뉴스룸

[9] 개인정보보호와 활용 개론(2017.06, 진한N&B 이기혁)

[10] 보안거버넌스의 이해(2021.02, 진한N&B 이기혁)

저 자 약 력

이 기 혁

이메일 : kevinlee010@cau.ac.kr

- 중앙대학교 대학원 융합보안학과 교수
- (사)한국디지털인증협회 회장
- (사)한국FIDO 산업포럼 회장
- 한국보안정책개발원 원장
- 건국대학교 대학원 공학박사
- 관심분야 : 개인정보보호와 활용, 디지털 인증, 블록체인 기술과 서비스, 현대암호학, ICT융합보안, 보안거버넌스, 보안 문화와 역사, 데이터통신 및 무선인터넷 기술과 서비스 등