디지털산업정보학회 논문지 제15권 제1호-2019년 3월
https://doi.org/10.17662/ksdim.2019.15.1.061

FinTech를 위한 다자간 컴퓨팅 암호기술

박 찬 길*·최 영 화**·이 철 희**

Secure Multi-Party Computation of Technology FinTech

Park Chankil·Choi Youngwha·Lee Cheulhee

〈Abstract〉

FinTech has expanded to the extent that not only businesses but almost everyone can feel the impact. The spread of the scope of use has introduced a variety of new financial services that are changing the way we live. In these environments, it is important to develop reliable security measures to protect against cyber attacks.

The number of mobile financial transactions in the financial sector is also increasing, making security vulnerable. In this study, we studied security through mutual authentication method that can safely handle financial security and focused on FinTech's security processing through multi-party mutual authentication method that strongly prevents leakage of information even in the event of continuous and sophisticated attacks.

Key Words : FinTech, Security, Information Leakage Prevention, Authentication, Secure Computation, Secure Multi-party Computation

Ⅰ. 서론

FinTech는 기업뿐만 아니라 거의 모든 사람들이 그 영향을 느낄 수 있는 지점으로 확장되었다. 사용 범위의 확산으로 새로운 금융 서비스가 다양하게 도입되어 우리가 생활 방식을 변화시키고 있다. 이러한 환경에서는 사이버 공격으로부터 보호 할 수 있는 안정적인 보안 조치를 개발하는 것이 중요하다. FinTech가 일상생활에서 보다 밀접하게 연결되면서 보안 침해는 엄청난 재정적 손실을 초래하고 기술 자체에 대한 신뢰를 떨어뜨릴 가능성이 있다. 특히, FinTech의 핵심 요소이며 편리한 서비스의 도입에 필수적인 스마트 폰의 사용은 보안에 취약하여, 정보 유출이라는 중요한 사이버 위협에 놓여있다. MacroMill의 2016년 연구에 따르면 FinTech에 대한 인상을 묻는 질문에서 사용자는 정보 유출에 대한 두려움을 가장 많이 꼽았다. 인증 정보의 유출은 스푸핑을 통해 위조 된 정착 및 대규모 누출로 이어질 수 있으므로 이를 방지하기 위해서는 강력한 조치가 필요하다. 패스워드가 없는 업계 컨소시엄 FIDO (Fast IDentity Online Alliance : 국제생체인증협회)의 사용자 생체 정보를 사용하여 공개키 암호화를 사용하여 안전한 인증 실행을 위한 프레임 워크를 지정하고 있다. 그러나 이것은 사용자의 생체 인식 및 비밀키가

* 숭실사이버대학교 정보보안학과 교수 (교신저자)
** 한국폴리텍대학 정수캠퍼스 모바일정보통신과 교수

사용자 단말기 또는 장치에 "안전하게" 저장된다는 가정에 기반 한다. 만일, 사용자가 장치를 분실했거나 악성코드가 침투하여 장치가 공격자가 액세스 할 수 있게 되면 데이터 보안을 더 이상 보장 할 수 없다. 또한 생체 인식 템플릿이 민감한 개인 정보라는 사실을 고려할 때 데이터의 누출을 방지하는 효과적인 방법을 개발하는 것이 중요하다. 이 연구에서는 지속적이고 정교한 공격에 대해서도 정보 유출을 강력하게 방지하는 암호화 기술의 일종인 보안처리에 중점을 두었다.

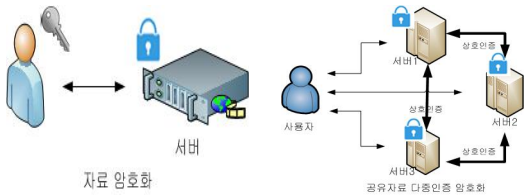
최근 많은 관심을 보이고 있는 FinTech 보안에서 안전한 다자간 정보인증을 통해 정보유출 방지 및 안전한 키관리 기법을 설계하였다. 본 논문에서는 1장에서 FinTech 보안의 문제점을 분석하였으며, 2장에는 안전한 보안관리 기술인 다중암호화기법, 3장은 SMPC를 활용한 FinTech 응용, 4장은 결론에서 향후 방향을 논하였다.

Ⅱ. 안전한 보안기술

암호화는 외부 공격으로부터 데이터를 도난당한 경우에도 정보 유출을 방지하는 효과적인 방법이다. 통상적으로, 암호화 된 데이터는 그것이 처리되기 전에 암호 해독되어야한다. 이를 통해 공격자는 관리자 권한을 얻을 수 있는 경우 원래 데이터를 복원하여 데이터를 얻을 수 있다. <그림 1>과 같이 암호화 된 데이터 자체가 처리되므로 침입자가 적절한 관리자 권한을 가질 수 있는 경우에도 정보 유출이 불가능하다.

보안을 위한 안전한 암호화 계산은 일반적으로 검색 가능한 암호화 및 준 유사 암호화와 같은 특수 암호화와 SMPC (Secure Multi-Party Computation) 방법을 활용하고 있다. <그림 2>에서 암호화 기법을 이

<그림 1> 정보유출 방지를 위한 안전한 암호화



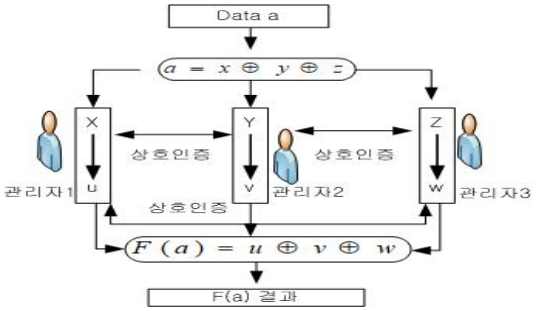
<그림 2> 안전한 상호인증을 통한 암호화

용하여 정보를 보호 하는 방법과 두 개 이상이 서로 가지고 있는 방법으로 암호화하여 정보를 보호하는 방법을 나타내고 있다. 전자의 경우 처리 과정에 따라 서로 다른 암호화 방법을 설계해야 한다. 후자의 경우 SMPC는 원칙적으로 "XOR"및 "AND"와 같은 기본 연산으로 빠르게 대량의 데이터 처리가 가능하도록 다자간 SMPC 알고리즘을 결합하여 임의의 데이터를 처리하는 기능을 갖추고 있다.

2.1 다중 보안 암호화 기법(SMPC)

SPMC의 처리 개념은 <그림 3>과 같다. 먼저 데이터 소유자는 비밀 공유 x, y, ...에 a를 안전하게 배포한 다음 x, y, ...를 각각에게 보낸다.

다른 서버에서 계산은 데이터가 항상 입력에서 출력으로 공유되는 비밀 상태에서 수행된다. 결과 F(a)는 출력 공유로 재구성 될 수 있다. a는 비밀 공유이므로 공격자가 도용 한 자료가 임계값을 초과하지 않는 한 유출 될 수 없다. 또한 SMPC는 데이터를 처리하는 동안에도 이 속성을 유지하므로 메모리에 a가 나타나지 않는다. 즉, 일부 컴퓨터가 공격자의 통



<그림 3> SMPC 개념도

제 하에 있더라도 데이터 보안을 보장 할 수 있다. SMPC는 침입자가 내부자 위협의 경우에도 침입자가 권한을 가지고 있으며 암호화와 같은 기존의 대응책이 작동하지 않는 경우에도 침입자가 액세스 할 수 없도록 한다. 이론적으로 SMPC는 위에 설명 된 상황을 처리 하여 컴퓨터 간 통신과 처리가 모두 엄청나게 늘어남에 효율적으로 활용 할 수 있게 되었다.

2.2 고속 SMPC

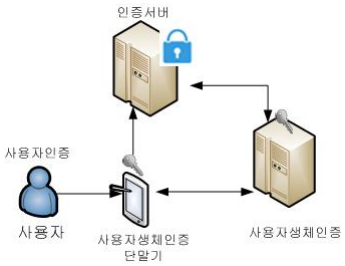
고속 SMPC 시스템은 3대의 컴퓨터에서 암호화 값을 실행하므로 공격자가 시스템 중 하나에 대한 제어권을 점유하더라도 정보 유출은 불가능하다. SMPC에서 데이터 처리는 "XOR"및 "AND"게이트의 논리적 표현으로 표현된다. 비밀 공유 방법을 통신 없이 각 시스템 내에서 계산할 수 있는 처리량을 최대화하고 처리 자체를 최적화함으로써 "AND"게이트 작업을 향상시킴으로써 속도를 향상 시킨다.

SMPC의 표준 성능 벤치마크에 사용되는 AES (Advanced Encryption Standard)에 적용되며, 비밀키와 데이터가 비밀 공유를 계속하면서 암호화가 수행된다. 한편 SMP의 보안 문제에는 공격자가 시스템을 인계하는 경우의 악의적인 조작 문제가 포함된다.

Ⅲ. SMPC를 활용한 FinTech 응용

3.1 인증 정보의 보호

사용자 및 장치 인증은 모바일 지불을 포함한 대부분의 FinTech 서비스의 보안을 위한 출발점이다. SMPC를 활용한 인증방법은 인증 데이터를 매우 강력하게 보호한다. 인증 데이터가 SMPC에 의해 보호되는 두 가지를 분석한다. 첫 번째 경우는 FIDO 기반 인증의 데이터 보호와 관련된다. FIDO 기반 인증은 생체 인식 데이터를 사용하여 사용자를 인증한다. 인증이 성공적이면, 사용자 단말기는 단말기에 디지털 서명을 생성하고 인증 서버는 서명을 검증한다. <그림 4>는 사용자의 생체 정보의 템플릿과 장치의 비밀키를 보호한다. 여기에서, 템플릿 및 비밀 키는 사용자 단말기 및 보안 컴퓨팅 서버에 안전하게 분배된다. 인증이 실행될 때, 사용자 단말기와 보안 컴퓨팅 서버는 통신하여 SMPC를 수행한다. 이 처리에 의해, 생체 인증을 검증 할 수 있고, 생체 템플릿 및 비밀키를 복원하지 않고, 장치 인증을 위한 서명을 생성할 수 있다. <그림 4>와 같이 RSA를 디바이스 인증에 사용하면 RSA의 특성을 이용하여 간단한 SMPC를 적용 할 수 있다 <그림 5>. RSA 비밀 키 d에서 d = d[1] - d[2]를 만족하도록 생성 된 두 개의 공유 d[1]과 d[2]. 사용자의 장치와 서버가 함께 작동하는 동안 사용자 장치는 인증 서버에서 보내는 RSA 인증

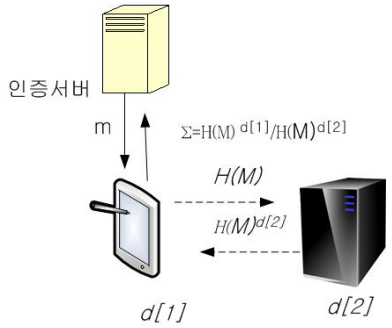


<그림 4> SMPC를 사용한 FIDO기반의 인증 보호

시도에 시간과 같은 정보를 추가하여 만든 데이터 M에 대한 서명 σ를 생성한다. 여기서 N은 RSA의 공개키이고 H는 서명 생성에 사용되는 해시 함수이다. SMPC 활용으로 서명 σ는 se를 복원하지 않고 생성될 수 있다.

<그림 5>에서 키 d. 두 번째 경우는 클라우드의 사용자 인증 플랫폼에서 인증 정보를 보호하는 경우이다. 이 경우 인증 플랫폼은 POS와 같은 다양한 단말기 및 서비스에 사용자 인증 기능을 제공한다고 가정한다. 엄청난 양의 인증 정보가 등록되면 인증 플랫폼은 매우 강력한 보호 기능을 필요로 한다. 많은 양의 인증 데이터를 여러 서버를 통해 안전하게 배포하여 SMPC를 수행하면 서버 중 하나가 공격자의 제어를 받더라도 정보 유출을 방지 할 수 있다. 생체 인증에서 단말기는 확인을 위해 생체 인식 템플릿을 안전하게 배포한다. 이러한 공유는 별도로 인코딩 되어 터미널과 서버 간에 전송되며, 생체 인식 템플릿에 등록 된 공유 자료는 서버에서 SMPC로 안전한 처리를 실행하는 데 사용된다. 이 사용 구성에서는 대용량 인증이 클라우드 측에서 구현되며, 여기에 사용된 SMPC로 계산되는 σ처리 방법이다.

$$\sigma = H(M)^d \bmod N = H(M)^{d[1]} / H(M)^{d[2]} \bmod N$$



<그림 5> FIDO 기반 RSA서명의 다중인증

3.2 고객 정보 보호

FinTech 회사는 구매 내역, SNS를 통한 인터넷 관련 정보 수집, API를 사용한 은행 계좌 정보, 고급 대출 및 자산 관리 등의 서비스를 지속적으로 제공한다. 이러한 서비스는 엄청난 양의 고객 데이터를 수집하고 처리하는 데 의존하므로 수집 된 고객 데이터의 누출을 확실하게 방지하는 향상된 보안 조치를 제공하는 것이 중요하다. SMPC는 데이터를 처리하고 관리자의 정보 유출을 방지하고 고객 정보를 전례없이 안전하게 보호 할 수있는 입증 된 솔루션이다. FinTech 회사가 수집 한 고객 데이터는 경쟁의 열쇠이다

공격자가 제어하는 시스템을 사용하면 보안 처리를 수행하고 예외를 감지 할 수 있어야한다. 시스템을 실용화하기 위해서는 탐지 능력이 중요하다. 악성 서버를 탐지 할 수 있는 고속의 안전한 시스템을 개발과 증가 된 속도에 대한 접근 방식은 논리 연산을 기반으로 SMPC에 적용 할 수 있을 뿐만 아니라 정수나 소수의 비밀 공유를 기반으로 하는 산술 연산의 합계 및 곱셈을 기반으로 하는 SMPC에도 적용 할 수 있다. 생체 인증 및 데이터 분석을 위해 산술 연산을 기반으로 SMPC를 적용하여 속도를 높일 수 있다.

Ⅳ. 결론

이 연구는 클라우드 컴퓨팅 환경에서 적용될 수 있는 암호인증 및 정보보안을 위한 다자간 상호인증을 통한 안전한 정보처리 시스템 개발이다. 시스템개발에 필요한 SMPC 알고리즘을 활용하여 대단위로 사용 가능한 FinTech 활성화를 위하여 대용량의 정보를 빠르게 처리하는 방법을 연구 하였으며, 향후 안전성 검증을 통한 활용을 기대 할 수 있다.

참고문헌

[1] About Macromill: http://www.macromill.com/honote/20160405/report. html

[2] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara, High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority. ACM CCS, 2016.

[3] J. Furukawa, Y. Lindell, A. Nof, and O. Weinstein, High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority, to appear in Eurocrypt2017

[4] MALKA, L. Vmcrypt: modular software architecture for scalable secure computation. In Proceedings of the 18th ACM conference on Computer and communications security (New York, NY, USA, 2011), CCS '11, ACM, pp. 715–724.

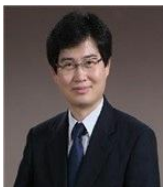
[5] MOHASSEL, P., AND FRANKLIN, M. Effi ciency tradeoffs for malicious two-party computation. InProceedingsofthe9thinternational conference on Theory and Practice of Public-Key Cryptography (Berlin, Heidelberg, 2006), PKC'06, Springer-Verlag, pp. 458–473.

[6] NIELSEN, J. B., NORDHOLT, P. S., ORLANDI, C., AND BURRA, S. S. A New Approach to Practical Active-Secure Two Party Computation. In Proceedings of the 32th Annual International Cryptology Conferenceon Advancesin Cryptology(2012), CRYPTO '12. http://eprint.iacr.org/2011/091.

[7] OSADCHY, M., PINKAS, B., JARROUS, A., AND MOSKOVICH, B. Scifi - a system for secure face identification. In Proceedings of the 2010 IEEE Symposium on Security and Privacy (Washington, DC, USA, 2010), SP '10, IEEE Computer Society, pp. 239– 254.

[8] 최희식, 조양현, "모바일 앱 서비스 이용 증가로 인한 보안 위협 분석," (사)디지털산업정보학회 논문지, 2018년3월, 14권1호, pp.45~55.

■ 저자소개 ■



박 찬 길
(Park, Chankil)

2010년 2월~현재 숭실사이버대학교 정보보안학과 교수
2006년 2월 숭실대학교 대학원 컴퓨터학과 (공학박사)
1994년 8월 서울과학기술대학교 컴퓨터공학과 (공학석사)
1991년 2월 서울과학기술대학교 컴퓨터공학과 (공학사)

관심분야 : 이동통신, IoT, 정보보안, 전자상거래
E-mail : ksdim@naver.com

최 영 화
(Choi Youngwha)

1993년 3월 ~ 현재 한국폴리텍대학 모바일정보통신과 교수
1987년 2월 인하대학교 응용물리학 석사
1985년 2월 단국대학교 응용물리학 학사

관심분야 : 이동통신, IoT, 정보보안
Email : choiyh@kopo.ac.kr

이 철 희
(Lee Cheulhee)

1997년 3월~현재 한국폴리텍대학 정수캠퍼스 모바일정보통신과 교수
2000년 8월 조선대학교 대학원 전자공학과 (공학박사)
1994년 8월 조선대학교 대학원 전자공학과 (공학석사)
1992년 2월 조선대학교 자연과학대학 물리학과 (이학사)

관심분야 : 이동통신, IoT, 정보보안
E-mail : lch@kopo.ac.kr

논문접수일 : 2018년 12월 17일
게재확정일 : 2018년 12월 26일