Journal of The Korea Society of Computer and Information
Vol. 22 No. 2, pp. 59-63, February 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.02.059

A Study on secure authentication system using integrated authentication service

Hyung-Su Lee*

Abstract

Recently, Certificate has been loosed 100 times in a four years as Phising or hacking. The service that use certificate in financial services occurs practical and secure issues. Therefore, the Korea government abolished the mandatory system used in the certificate service. However, they did not provide a replacing method for a certificate. And is not to fill the gaps of the certificate with one time password or secure card. Therefore this paper is propose the alternative method with total authentication service, that is lead the more secure electronic commercial.

▸ Keyword : Certificate, Electronic Commerce, Internet Banking, Total Authentication, Authentication Method

I. Introduction

최근 대규모의 개인정보가 유출되는 사건이 빈번하게 발생하고 있으며 개인정보 및 전자거래 보안에 대한 불안심리가 커지고 있다. 게다가 피싱이나 해킹 등으로 유출된 은행 공인인증서가 4년 새 100배나 증가한 것으로 나타났다[1]. 또한 전자상거래에 대한 직관적인 인증서비스로 보다 실용적이고 불안을 덜 수 있는 기술 및 제도가 필요한 시점이다. 2014년 전자금융거래법 및 전자서명법이 개정되어 해킹사고 발생 시 과실입증책임이 금융기관에 귀속되었으며 공인인증서를 이용한 강제적 전자상거래 조항도 삭제되었다[2]. 하지만 공인인증서를 대체할 만한 보안 수단이 마련되지 않은 상태에서 대체수단을 마련하는 것이 매우 시급한 실정이다. 현재의 보완 수단으로 사용되고 있는 기존 OTP(One Time Password) 및 스마트 OTP 역시 보안안전성 측면에서 미흡하다는 조사결과가 나왔다[3]. OTP는 보조적인 역할 일뿐 실제 전자상거래를 할 경우 핵심 비밀번호를 다시 입력해야 하는 문제는 여전히 남아 있다.

또한 해킹기법의 더욱 지능화에 따라 전자금융 거래 및 전자상거래 해킹 피해의 점진적인 증가 추세로 이어질 전망이며 부정거래 건수 및 금액이 훨씬 늘어날 전망이다. 이를 보완하기 위해 이중 채널 인증인 ARS 인증이나 SMS 인증 등의 보조적인 인증 기법이 확산되고 있으나 대포폰을 이용한 해킹 피해 사례도 보고되고 있다[4].

그간 마케팅 용도로 사용됐던 QR코드가 최근 문서 진본성 확인 및 인증 수단으로도 그 활용범위가 확대되고 있다. 하지만 진본여부를 가려내야 할 QR코드 자체가 위변조 될 가능성이 높은데다 진본성에 대한 법적 효력도 보장하지 못해 활용에 신중을 기해야 한다는 지적이 나온다[16]. [Fig. 1]에서 보는 바와 같이 QR코드 위변조를 통한 증명서를 위조한 사기 사건이 발생하였고 이를 일반이니 확인하기는 불가능한 일이다. 간단한 프로그램만 있으면 누구나 만들어 낼 수 있기 때문에 위변조 가능성이 매우 높은 실정이다[6].

• First Author: Hyung-Su Lee, Corresponding Author: Hyung-Su Lee
*Hyung-Su Lee (hyungsu.lee@gmail.com), Dept. of Computer, SoongSil University
• Received: 2017. 01. 26, Revised: 2017. 02. 14, Accepted: 2017. 02. 22.

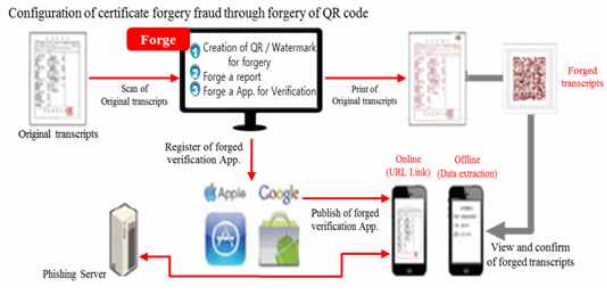

Fig. 1. Hacking Configuration

본 논문에서는 사용자가 간편하게 소유할 수 있는 인증 디바이스를 기반으로 통합인증 서비스 수행을 통해 기존의 공인인증서를 대체하고 기존의 보안 장치의 보안성을 뛰어넘는 통합인증 방안을 제안하고자 한다. [Fig. 2]에서 목표로 하는 것과 같이 통합인증 서비스는 향후 비대면 서비스가 활성화될 것을 고려하여 선제적이고 개방형 형태의 표준화 방안을 제안하고자 한다.

Fig. 2. The Goal of Proposed System

본 제안을 통해 향후 비대면 서비스의 보안을 보다 강화하고 모드 서비스가 표준화된 형태로 인증을 수행하며 보다 실용적이고 간편한 서비스가 될 수 있도록 제안하고자 한다.

II. Literature Review

1. Certificate and Active-X

공인인증서는 전자상거래를 할 때 신원을 확인하고, 문서의 위조와 변조, 거래 사실의 부인 방지 등을 목적으로 공인인증기관이 발행하는 전자적 정보로서, 일종의 사이버 거래용 인감증명서이다. 공인인증서가 도입된 지 10수 년이 지난 현재 공인인증서를 탈취하여 해킹 사례가 늘어나고 있으며 2014년 1만5376건에 달하는 것으로 확인됐다. 금융감독원이 새누리당 김태환(구미을) 국회의원에게 제출한 `은행별 공인인증서 유출로 인한 폐기현황' 자료에 따르면, 공인인증서의 유출로 폐기된 건수는 `11년 15건, `12년 8건에서 `13년 5871건으로 급증한 뒤 2016년 8월말까지 1만5376건의 유출사례가 발견됐다. 은행별로는 농협이 3946건으로 가장 많았고, 국민(3365건)과 신한이(2089건)이 뒤를 이었다. 농협과 국민, 신한은 2015년에도 각각 1540건, 1423건, 739건으로 공인인증서 유출사례가 가장 많았다[7].

액티브 X는 MS가 윈도 사용자들이 기존 응용 프로그램으로 작성한 문서 등을 인터넷과 연결시켜 그대로 사용할 수 있도록 개발한 기술이다. 예컨대 인터넷 뱅킹을 하려면 금융거래 및 보안 프로그램을 설치한 PC에서만 가능한데 액티브X는 이러한 프로그램을 유포하는 수단이다. 국내 인터넷 사이트의 대다수가 IE의 액티브X를 기반으로 하고 있어 파이어폭스 등 다른 웹브라우저로는 정상적으로 인터넷 서비스를 이용하기 어려운 경우가 많으며 많은 해킹의 대상이 액티브 X로 인해 발생하여 2015년 3월 정부에서도 이러한 액티브 X를 폐지하기에 이르렀다. 액티브엑스가 또 논란이 된 것은 보안에 있어 허점을 만들어왔다는 점이다. 이를테면 어떤 사이트에서 동영상을 재생하는데 필요한 액티브엑스 기반 프로그램을 다운로드 받으면 이 파일이 PC에 자동으로 설치돼 지워지지 않고 해킹에 악용될 수 있기 때문이다. 대표적인 피해 사례가 2009년 온 나라를 떠들썩하게 만든 7.7 디도스 사건이다. 당시 청와대 등을 일제히 공격했던 좀비PC를 만드는데 액티브엑스가 악용됐다는 지적을 받았다[8][15].

이러한 액티브엑스를 통한 해킹을 차단하기 위한 많은 연구가 있었으며 악성코드에 대한 근본적인 해결을 마련하여야 한다[11][12]. 또한 모바일 환경이 급속도로 발전하고 있으므로 유선 및 모바일 환경을 함께 고려한 시스템이 개발되어야 한다[13].

2. Smart OTP(One Time Password)

금융을 뜻하는 파이낸셜(financial)과 기술(technique)의 합성어로 모바일 결제 및 송금, 개인자산관리, 크라우드 펀딩 등 정보기술(IT)을 기반으로 한 새로운 형태의 금융 기술을 말한다. 핀테크 비즈니스 모델과 사업 영역을 분류하는 기준은 크게 은행업 및 금융 데이터 분석(Banking & Data Analytics), 지급결제(Payment), 자본시장 관련 기술(Capital Market Tech), 금융자산 관리(Finance Management) 등 4가지 영역으로 정리돼 가고 있다. 핀테크의 등장은 기존의 금융 질서를 파괴하며 창의와 혁신에 바탕을 둔 비즈니스 모델들을 쏟아내고 있다. 통화의 종류, 결제 시스템 같은 기존의 장벽을 허물고 보다 간편하고 보안 이슈까지 잡은 기술들이 속속 등장하기 때문이다. 최근 들어서는 단순한 결제나 송금 서비스뿐만 아니라 고객의 개인정보·신용도·금융사고 여부 등을 빅 데이터 분석으로 정확하게 파악하는 알고리즘 기술까지 등장해 개인 자산 관리 서비스까지 그 영역을 확대 중이다[9].

3. FinTech

소유기반의 인증방법인 OTP는 사용자만이 유일하게 가지고 있는 OTP token을 통해 일회용 패스워드를 생성하기 때문에

매우 강력한 안전성을 가지고 있다. 하지만 OTP token을 구매하고, 직접 은행에 찾아가 등록하고, 사용하기 위해 항상 휴대해야 하는 일들은 사용자들로 하여금 OTP를 사용함에 있어서 불편을 느끼게 하는 원인이 된다.

스마트 OTP는 이러한 OTP 인증방법의 문제점을 극복하고 사용자 효율성을 높이기 위해 OTP Token이 없이 일회용 패스워드를 소프트웨어적인 방법으로 생성하는 것을 말하며, 기본적으로 사용자와 컴퓨터 간에 공유하는 비밀정보를 기반으로 일회용 패스워드가 생성되기 때문에 지식기반의 인증으로 분류된다[14].

III. Main Subject

본 논문에서는 현재 공인인증서의 폐지에 따른 인증 문제를 해결하기 위해 통합인증 서비스를 제안하고자 한다. 본 서비스를 통해 향후 표준화되고 안전한 인증 체계를 갖추는데 밑거름이 될 수 있을 것이라 판단한다. 무엇보다도 향후의 인증 체계는 비대면 서비스가 주를 이룰 것으로 예상되므로 안전성, 개방형, 표준형을 갖춘 창조적이고 효율적인 시스템이어야 한다.

1. System Concept

본 논문에서 제안하는 통합인증의 개념으로 [Fig. 3]과 같이 제안하며 본인확인, 접속인증, 거래인증 등의 범용적인 통합인증 서비스를 제공하는 것을 목표로 한다.

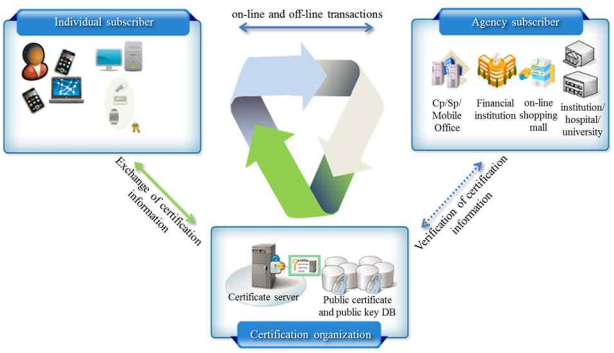

Fig. 3. Target System of Total Authentication

통합인증이라 함은 개인이 온라인이나 오프라인을 통해 신분을 인증 받거나 거래를 하기 위해 제 3의 인증기관이 인증을 대행해주는 형태를 말한다. 기존에는 인증을 본인이 직접 수행하였으므로 이를 해킹할 경우 본인으로 확신시키는 문제가 발생하였다. 또한 기존의 2채널 인증의 경우도 복제된 기기를 이용하는 등의 우회적인 방법이 존재하여 문제가 여전히 남아 있는 실정이다. 이를 해결하기 위해 기존의 공인인증서의 장점을 살리고 우회할 수 있는 방안을 제거함으로 보다 완벽한 형태의 인증을 제안하고자 한다.

2. System Structure

[Fig. 4]는 본 논문에서 제안한 통합인증의 시스템 구성을 나타내고 있다. 단말을 통해 인터넷으로 본인인증이나 거래를 할 사용자는 인증디바이스를 통해 거래에 필요한 인증값을 받아 거래기관에 제출하여 안전하게 거래를 진행 할 수 있다. 본 논문에서 제안한 개념은 기존의 공인인증 방식과는 달리 거래 시점에 사용자가 외부 기관을 통해 실시간으로 인증을 받는다는 점이 상이하다. 다만 사용자가 거래를 위한 임의의 값을 입력해야하지만 이 부분은 기술적으로 얼마든지 자동화가 가능하다. 즉, 향후 도입되는 스마트워치나 착용 디바이스 등을 활용하면 가능하며 현재의 스마트폰에서도 자동 인식 기능을 추가할 경우 자동화가 가능하다. 즉, 스마트폰과 사용자가 고유하게 보유하고 있는 디바이스를 상호 인식시켜 인증에 활용할 경우 복제나 해킹이 불가능하다.

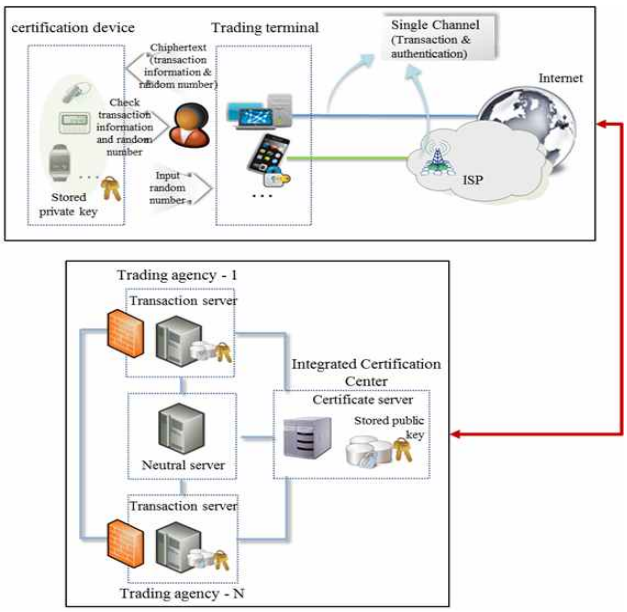

Fig. 4. System Diagram

최근의 대부분의 스마트기기는 블루투스나 NFC(Near Field Communication)를 지원하므로 해당 기기와의 인증을 토대로 복제 불가능한 인증값을 생성할 수 있다. 최근 핀테크의 관심으로 NFC에 대한 인증도 관심을 받고 있다[10]. 다만, 이렇듯 개인이 소유하고 복제가 불가능한 매체를 통해 난수를 발생시키고 이를 거래 기기에서 활용하는 방식은 기존에 도입된 적이 없으므로 인증 다바이스 활용 측면에서는 보다 검토할 필요가 있다. 하지만 앞에서도 언급했듯이 향후 디바이스들이 대부분 스마트를 표방하기 때문에 임의의 난수정도를 생산하는 기능은 그리 어려운 일이 아닐 것이다. 다음 절에서는 프로토콜 레벨로 본 제안 시스템을 설계하고자 한다.

IV. Design

본 논문에서 제안한 시스템에 대한 구체적인 설계를 제안하고자 한다. 우선 각각의 주체 및 객체에 따른 기능 정의를 하고 각 객체간의 인증 흐름을 제안하도록 한다. [Table 1]은 주체인 사용자의 단말과 사용자가 소유한 인증 디바이스의 기능을 명시하고 있고 [Table 2]는 객체인 거래서버 및 중립서버, 인증서버의 기능을 명시하고 있다.

Table 1. System Function List

Authentication Device	User's Terminal
Personal Key and Decoding	Load authentication program
Saving Algorithm	Receive coded information
Receive coded information	Send coded information
Decode information	Receive random number
Transaction confirmation information	Generate authenticator
Send random number	Send authenticator

Table 2. Object Function List

Transaction Server	Neutral Server	Authenticator Server
Generate and send transaction confirmation information	Receive transaction confirmation information	Send public key
Receive Authenticator	Generate Hash Value	Receive random number
Send coded information	Request and receive public key	Receive authenticator
Receive authenticator	Generate random number	Generate authenticator
Send authenticator	Send random number	Send certification result
Receive certification result	Encode public key	
Notify certification result	Send coded information	Mange public key

중립서버는 거래서버와 인증서버가 직접적으로 연결되어 해킹될 가능성을 완전히 배제하고 거래를 투명하게하기 위해 도입한 서버이다.

[Fig. 5]는 사용자가 소유한 단말 및 인증 디바이스의 인증 흐름을 나타내고 있다. 이때 사용자 단말은 암호화된 형태의 정보를 인증 다바이스에 전달하며 암호화된 내용을 복호화한 후 사용자를 인증한다.

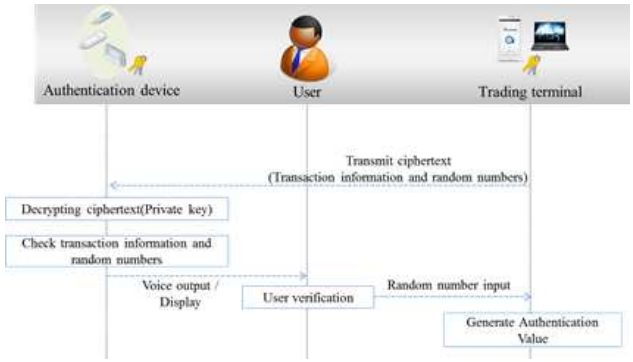

Fig. 5. Subject Authentication Flow

[Fig. 5]의 절차에 따라 인증값을 다음과 같이 확인하여 데이터와 난수를 확인한다.

$$E_{Public\text{-}key}(Data+Rand) \rightarrow D_{Private\text{-}key}(E_{Public\text{-}key}(Data+Rand))$$

- Data와 난수 확인
- 사용자 확인은 음성인식이나 얼굴인식 등의 생체인식을 활용하여 보안성을 강화한다.
- 단, 거래를 수행하기 전에 사용자는 인증서버에 자신이 거래할 때 사용할 공개키를 인증서버에 전달하여 향후 인증에 사용한다.

위의 과정을 통해 사용자의 인증값을 받아 거래서버로 전달을 한다. 거래서버는 중립서버에서 거래를 위한 난수를 생성하고 이를 다시 사용자에게 전달하여 개인키를 소유한 여부를 확인한다. 이 후 사용자의 인증 디바이스에서 생성된 인증값을 토대로 거래를 수행하게 된다.

본 논문에서 제안한 통합인증 서비스의 경우 기존의 공개키를 활용하여 인증을 수행하므로 인증서의 장점은 그대로 채용하였다. 또한 사용자가 소유하고 있는 인증 디바이스를 활용함으로 인증의 해킹이나 복제 등과 같은 원천적인 보안 문제를 해결할 수 있다. 그리고 인증서버를 실시간으로 활용함으로 인해 기존의 공인인증기관의 역할도 보존할 수 있는 방안을 마련하였다. 본 서비스를 활용할 경우 서비스에 제한이 없는 개방형 인증 서비스를 추구할 수 있다는 장점을 가진다.

[Fig. 6]에서와 같이 사용자는 사용자 단말을 이용하여 금융거래 서비스를 신청하며 이때 거래 확인 정보를 인증서버로부터 수신한다. 수신된 인증정보는 사용자의 공개키로 암호화되어 있어 사용자의 개인키로 복호화가 가능하므로 사용자 인증이 가능하다. 이후 사용자는 [Fig. 5]에서 제시한 인증 디바이스를 이용하여 인증값을 생성하고 이를 인증서버에 전송하므로 거래를 수행할 수 있는 권한을 승인받을 수 있다. 이와 같이 기존의 공인인증서 방식이 아닌 공개키 방식을 사용하므로 보안의 비도는 높게 유지하면서 사용자는 간편하게 거래를 위한 인증을 받을 수 있다. 따라서 근본적인 해킹이나 복제가 불가능한 서비스를 제공할 수 있다.

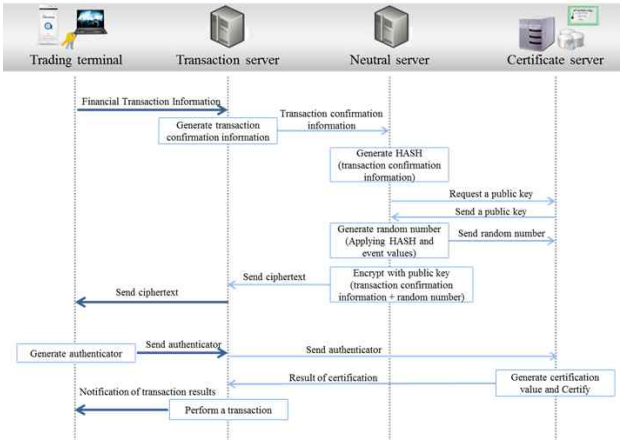

Fig. 6. Object Authentication Flow

V. Conclusions

본 논문에서 제안한 통합인증 서비스는 기존의 공인인증서 방식의 문제점을 해결하고 추가적인 인증 디바이스를 제안하여 보안성과 편의성을 모두 해결하였다. 향후 인증 디바이스 시장은 더욱 확대될 전망이다. 공인인증서 제도를 폐지함에 따라 거래 서비스를 제공하는 사업자나 기관은 별도의 인증 방식을 마련해야 한다. 이때 사용자가 간편하게 소유할 수 있는 인증 디바이스를 제공하여 통합인증 서비스를 수행한다면 비대면 서비스에서도 대면 서비스 못지않은 인증을 수행할 수 있다고 판단한다. 다만, 인증서버에 공개키를 저장하기 위한 초기 등록 절차를 보다 간편하게 할 수 있는 방안을 마련해야 할 것이다.

이러한 통합인증 서비스는 거래 서비스 이외에도 신분을 확인하기 위한 용도로도 활용이 가능하다. 신분증을 위조할 경우에 통합인증 서비스를 활용한다면 전자 신분증 제도로도 활용이 가능하다는 것이 매우 큰 장점이라고 할 수 있다.

REFERENCES

[1] NEWS1, *http://news1.kr/articles/?1906344*

[2] OpenNet, *http://opennet.or.kr/e-finance-e-signature-reform.pdf*

[3] Chosun Biz, *http://biz.chosun.com/site/data/html_dir/2015/04/20/2015042003040.html*

[4] Data Net, *http://www.datanet.co.kr/news/articleView.html?idxno=81727*

[5] Digital Times, *http://www.dt.co.kr/contents.html?article_no=2015041402100351800001*

[6] Gyeongbuk Dohmin Ilbo, *http://www.hidomin.com/news/articleView.html?idxno=249918*

[7] Gyeongbuk Dohmin Ilbo, *http://www.hidomin.com/news/articleView.html?idxno=249918*

[8] Asian Economy, *http://view.asiae.co.kr/news/view.htm?idxno=2015032509531946839*

[9] Naver, *http://terms.naver.com/entry.nhn?docId=2118001&cid=42107&categoryId=42107*

[10] IT Today, *http://www.ittoday.co.kr/news/articleView.html?idxno=59377*

[11] Jae-Kyung Park, Sang-Yong Choi, “Studing Security Weaknesses of Android System”, International Journal of Security and Its Applications, Vol. 9, No.3, pp. 7-12, 2015.

[12] Jae-Kyung Park, “A Realtime Malware Detection Technique Using Multiple Filter”, Journal of The Korea Society of Computer and Information, Vol. 19, No.7, pp. 77-85, July 2014.

[13] Hyo-Nam Kim, “Realtime hybrid analysis based on multiple profile for prevention of malware”, Hongik Univ. Feb. 2014.

[14] Seongmin Yoo, Jinseung Yu, Haegjin Jang and Jaecheol Ryou, “A Study on OTP Generation Method based on Software”, Journal of the HCI Society of Korea, HCI 2011, No. 1, pp. 173-176, 2011.

[15] Sangyoung Choi, “Trend of mobile malware spreading and responding”, Journal of The Korea Society of Computer and Information, v.22 No. 1, pp. 1-6, 2014.

[16] Gyeongyong Heo, Imgeun Lee, Some Sick Park, Young Woon Woo, “Development of Genuine Product Authentication Framework and Genuine Distinction Algorithm Using Design QR Code”, Journal of The Korea Society of Computer and Information, v.20 No. 6, pp. 13-20, 2015.

Authors

Hyung Su Lee received the B.S.,degrees in Electronic Engineering from SungKyunKwan University, in 1991. M.S. degrees and Doctorate in Computer Science from Soongsil University, in 2011 and 2013.

Mr. Lee joined the faculty of Consulting & Security SI at SK Infosec, Seoul, Korea, in 2011. He is currently a Professor in the Department of Information Security, Korea Polytechnics. He is interested in network security, cyber security, and information communication.