Security in Branchless Banking

Final Assignment of Information Security Course

II3230

By

Feby Eliana Tengry

18217030

Information System and technology

School of Electrical Engineering and Informatics

Bandung Institute of Technology

2020

18217030@std.stei.itb.ac.id

Content

I. Abstract

Branchless Banking is a new approach to serve people who live in rural areas with banking services. With this approach, a bank does not need to build a physical branch in the remote area. To give banking services, branchless utilize agents who carry a card-reading POS terminal and mobile device to facilitate transactions. This concept requires lower cost and much more feasible to be implemented in rural areas than the conventional branch. However, just like conventional banking, information security is of the utmost importance of the system. This paper discusses the processes that make up the trust model in branchless banking and the technology implemented by branchless banking to maintain its security.

Keywords: branchless banking, rural, security, verification, agents.

II. Introduction

A. Background

Banking is an industry that handles financial transactions. It is one of the key drivers of a country’s economy. In the last few decades, banks have been investing a lot in adopting Information Technology (IT) for the purpose of setting up net banking, ATM's, telebanking, debit cards, credit cards, mobile banking, electronic payments etc. This advancement in technology adopted by banks aimed at providing quality services to the customers. However, based on data from Worldbank [1], nearly 1.7 billion people in this world are still unbanked nowadays. These people are mostly people who live in rural areas with no banking services available near them.

The lack of infrastructure is one of the main reasons for the limited banking services in rural areas. Infrastructure development in rural areas is far behind the one in urban areas. The inadequate infrastructure, for instance the lack of network and transportation infrastructure, does not satisfy bank branch requirements in order to operate. Also, as the main motive of financial institutions is to achieve maximum profit they become hesitant to reach rural areas [2]. Opening a branch in a rural area might be unprofitable because of the high cost of establishing a rural financial network compared to small profits from a small loan and savings account with a small balance [3].

Despite all of the difficulties to serve people in rural areas with financial services, financial services is a basic right for every citizen that needs to be available. Hence an innovation is needed to fulfill the rural areas’ citizen needs. Branchless banking is a new innovative idea to reach to poor and unbanked people of rural areas. It is used to provide financial services without requiring the customer to go to a physical bank [4]. Branchless banking utilizes technology, such as mobile phones and card-reading point-of-sale (POS) terminals to conduct financial transactions electronically and remotely [2]. Branchless banking has great potential to extend the distribution of financial services to poor people who are not reached by traditional bank branch networks; it lowers the cost of delivery, including costs both to banks for building and maintaining a delivery channel and to customers of accessing services [5].

Branchless banking utilizes agents to deliver banking services. To reach inclusivity, everyone can be an agent as long as they fulfill the required requirements. With this scheme, it will be easier for branchless banking to scale but also increase the information security threats to the system. The agents who act as the bank's employee in remote areas are less monitored and trained than the employees in traditional branches.

Nevertheless, information security is very important in banking. Therefore, regardless of the medium that banks use to provide services, it is important for the banking system to make sure that every transaction is secure. This paper will focus on how branchless banking keeps each transaction's data safety and security.

B. Problem Statement

Looking at the difficulties faced to open a bank branch in a rural area, branchless banking is the answer to provide rural area citizens with banking services. Just like in traditional banks, information security is the utmost importance in branchless banking. Increasing security risks and threats facing the financial sector as the increased demand for security in the banking sector give rise to new challenges. The challenge is even higher in branchless banking since it relies on agents who are recruited from the local areas to deliver services. The amount of control that banks have to the remote areas is far less than the control they have in the traditional branch.

There are two main questions that are going to be discussed, they are:

1. What are the processes that make up a branchless banking trust model?
2. What are the technologies that are implemented in branchless banking for its security?

III. Branchless Banking Concept

Most banks do not serve the poor in remote locations especially in developing countries. There are several reasons for this, such as:

- Undeveloped infrastructure
- High cost to establish a rural financial service network
- Low profit from small loans and saving accounts
- Low literacy rate of potential customers

It will take a huge effort to tackle barriers in building a physical bank branch to finally serve poor people in rural areas with banking services. Hence, a new approach is needed to provide banking services in remote areas.

In the last decade, a new concept called branchless banking emerged as an alternative to serve rural areas in developing countries with banking services. It deploys last-mile technology that uses card-reading point-of-sale (POS) terminal and mobile banking technologies. These devices are necessary to provide an interface for the transaction and connect with the bank system. POS terminal is a must for branchless banking. It is used to provide the interface needed while conducting a service. POS terminals are equipped with printer, fingerprint sensor, online and offline mode of transaction, and card card reader [6]. POS terminals do not need to be connected to a central server to operate. They can operate offline and use a fingerprint for verification [7].

IV. Authentication Methods

Authentication is an action to verify the identity of a user or process. Authentication is categorized in three categories, such as [8]:

- Knowledge based (e.g., password)
- Object based (e.g., token)
- Biometric based (e.g., biometric)

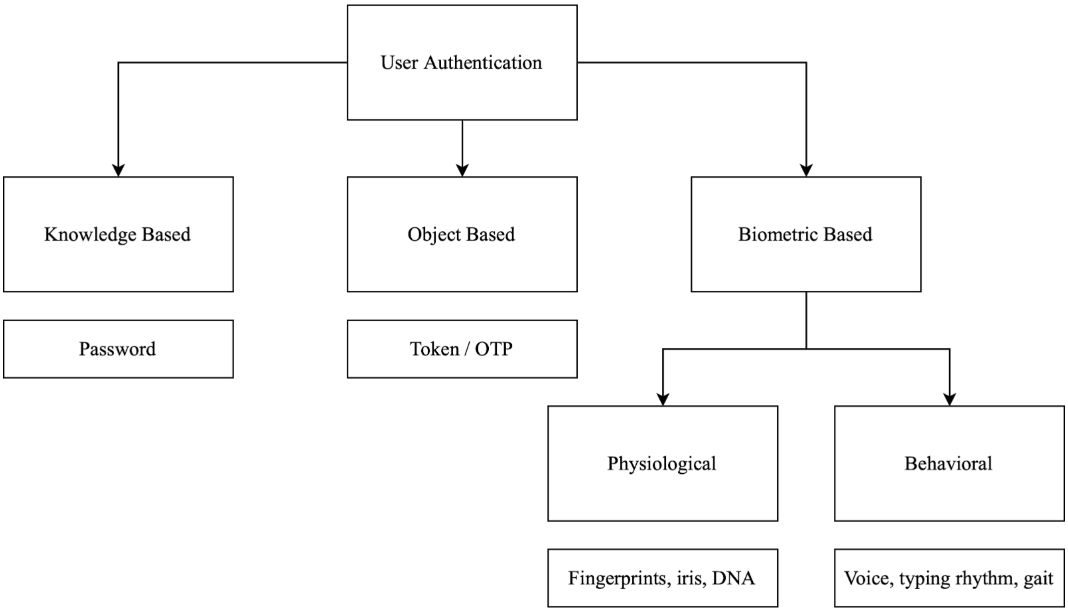

Figure 1. Authentication categories (source [8])

Password has been used as the standard for user authentication for decades. However, as time goes by, users are required to remember more complex and longer passwords. It is evident that a more convenient authentication method is necessary [9].

Another widely used authentication method is authorization code or OTP (One-time-password) for each transaction. In this method, the central system will send special authorization code as SMS messages to the user's mobile phone to authenticate a transaction. The code must be copied from the messages to the corresponding transaction interface [10]. After the code is typed and sent, the transaction will be executed. The main advantage of SMS-based authentication is that the messages sent by the bank to the user pass through cellular network which is independent from the internet. With this scheme, it is more difficult for the attacker to manipulate the transaction since they would need to steal the user's mobile phone or attack the cellular network. For instance if the attacker changes the destination account number and/or the amount on the client interface, the modified information will appear in the SMS message. However, this scheme relies on user awareness to check the correctness of the transaction in the SMS message.

The biometrics is a feature measured from the human body that is distinguishing enough to be used for user authentication [9]. This security system implementation relieves the burden of memorizing and memorizing passwords. Biometric identifiers are usually categorized as physiological or behavioral characteristics [11]. Physiological characteristics are related to the shape of the body for example but not limited to fingerprint, iris, and DNA. Behavioral characteristics are related to the pattern of behavior of a person, for instance but not limited to voice, typing rhythm, and gait [12].

For this discussion, we are focusing on fingerprint biometric because it is the commonly used biometric for branchless banking. Fingerprint biometric is stored through four steps as shown in Figure 3; first, several images from the individual's fingerprint is taken. These images are then read for its unique pattern. Finally, after the patterns are determined they are converted into representative binary numbers [13].

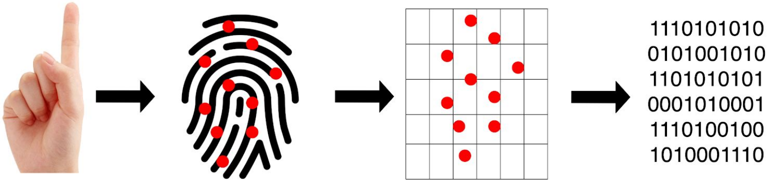

Figure 2. Fingerprint biometric storing process (source [13])

Fingerprint biometric is hard to fake out because they can’t be easily copied, duplicated, or even guessed. However, just like any other system it also has flaws. There are two basic types of recognition errors: false accept rate (FAR) and false reject rate (FRR). False Accept is when the system accepts a wrong biometric data as a match. False Reject is when a matching pair of biometric data is wrongly rejected by the system. Both errors are complementary which means trying to lower one error will increase the other error [13].

V. Trust Model in Branchless Banking

Branchless banking is an approach to serve people in remote rural areas with banking service. Unlike conventional banking that uses branches to serve their customers, branchless banking utilizes agents to give services. With this method, banks can provide financial services for poor people with lower cost of delivery. In order to deliver the services the agent needs to have a POS terminal and mobile device. Therefore, we will discuss the trust model and the technology to keep information security in branchless banking.

Branchless banking trust consists of processes to help preserve security, safety, and privacy of a transaction. In branchless banking, transaction is carried through the POS terminal that is carried by the agent. One of the key questions is how to make sure that the one who is doing a transaction is the account owner itself. This system has several processes to ensure that a transaction is valid and held by the account owner.

A. Customer identification

To proceed a transaction, firstly the system needs to identify who is the customer that is going to do the transaction. Every customer has their own bank card that is given when they open the bank account. This card has magnetic stripes behind it that contains personal information about the customer. Debit cards usually use high-coercivity magnetic stripe that can withstand the presence of a very strong magnetic field (~ 4000 Oersted). Data stored in high coercivity magnetic stripes is more difficult to erase because it requires a higher amount of magnetic energy to encode [14] . The data encoding in binary form is known as Frequency/Double Frequency (F2F) or Aiken Biphase technique. Before encoding, the cardholder’s alphanumeric information is coded into one (1) and zero (0) bits as per Coded Character Set tables in ISO/IEC 7811-2 standard [15].

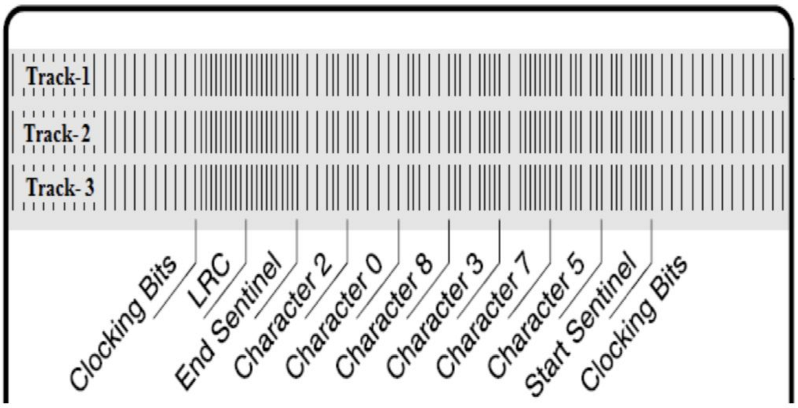

Figure 3. F2F encoding of character code on magnetic stripe of credit/debit card (source [15])

As in Figure 4, a stripe with a series of flux transitions is used to encode the customer data bits serially. This stripe will be read by the card reader on the POS terminal. Each transaction will be initiated by swiping the card to the POS terminal. Through this action, the system can identify which account is doing the transaction.

B. Customer Authentication

Even though by swiping the card the device can identify which account is requesting to do a transaction, it is still not sure whether the one who swiped the card is the card owner or not. In branchless banking, the common method used to authenticate a person is by using password and fingerprint scan.

In the next step the customer will need to input their password into the POS terminal. Ideally, a password should only be known by the password owner. Therefore, no other person than the password owner can do a transaction by using the owner identity. However, sometimes this password can be known by other parties intentionally or unintentionally. Passwords can be shared intentionally by the owner to their relatives. In the unintentional case, other parties might know the owner’s password due to the lack of security. For instance, the agent or other customer can eavesdrop on the information provided by a customer during transactions. It can be done easily by shoulder surfing or electronic tools like keyloggers. Once they know the password, it can be used again and again to do unauthorized transactions.

To increase the security for user authentication, POS terminals for branchless banking are complemented with biometric scanners. Fingerprint is the most commonly used biometric in branchless banking. Every person has a unique fingerprint hence it can be used as a unique identificator for users. However, the fingerprint biometric data is not stored as a highly detailed picture. It is stored as patterns in a series of points that are going to be converted into binary numbers. Sometimes, there is stored fingerprint data from an individual that matches with another individual's data. Therefore, to reduce the match rate, more than one fingerprint from a customer is used for user validation.

C. Transaction Verification

After the user and account are identified as valid, the transaction will be continued. Before finalizing the transaction, the bank server will send a verification to ensure that the transaction amount and account number is correct. The bank will send OTP via SMS messages to verify the transaction. Since the OTP is sent through a cellular network that is independent from the internet network, it will be harder for adversaries to attack transactions. For instance even if the adversary modifies the amount and account number of the transaction the modified messages will appear in the SMS messages.

VI. Technology Implemented in Branchless Banking Information Security

To maintain security, safety, and privacy in branchless banking, there are several technologies implemented in the system.

A. Magnetic Card Reader

Magnetic card reader is used to read the information stored in the customer's bank card. When a card with a magnetic strip is swiped over the 'reader head', a voltage is induced in the coils of the card reader device. The encoded flux in the magnetic stripe will be converted into positive and negative pulses when it is passing through a reader head [15], in this case the POS terminal, as shown in Figure 5. These pulses will be decoded into binary data later on.

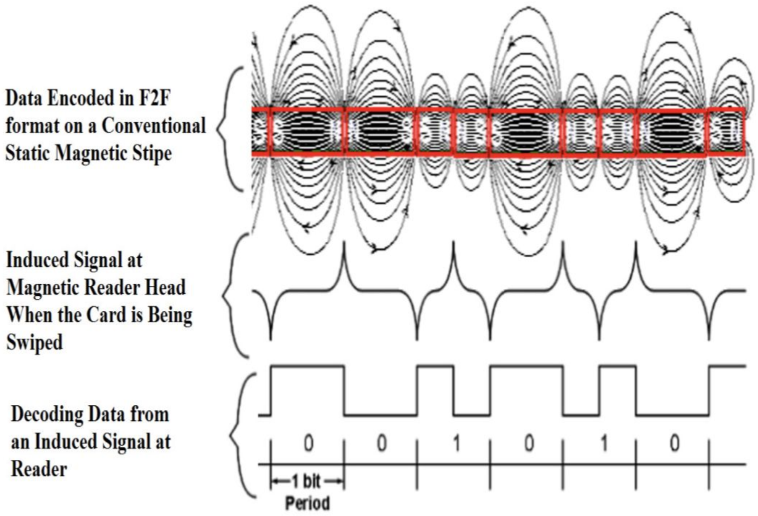
Data Encoded in F2F format on a Conventional Static Magnetic Stipe
Induced Signal at Magnetic Reader Head When the Card is Being Swiped
Decoding Data from an Induced Signal at Reader
0
0
1
0
1
0
1 bit Period

Figure 4. Encoded data on card's magnetic stripe and decoding it at magnetic reader when the card is swiped across the reader head. (source [15])

B. Fingerprint Scanner

There are two main stages involved in using a biometric authentication system, enrollment and authentication [16]. During the enrollment stage, the system learns about user features that are going to be used to verify transactions in the future.

Customer's fingerprints are scanned, analyzed, and then stored in the database by using the fingerprint scanner. The next stage is verification stage where customer's fingerprint will be read by the scanner and checked whether it is a valid fingerprint by comparing it with the data stored in the database.

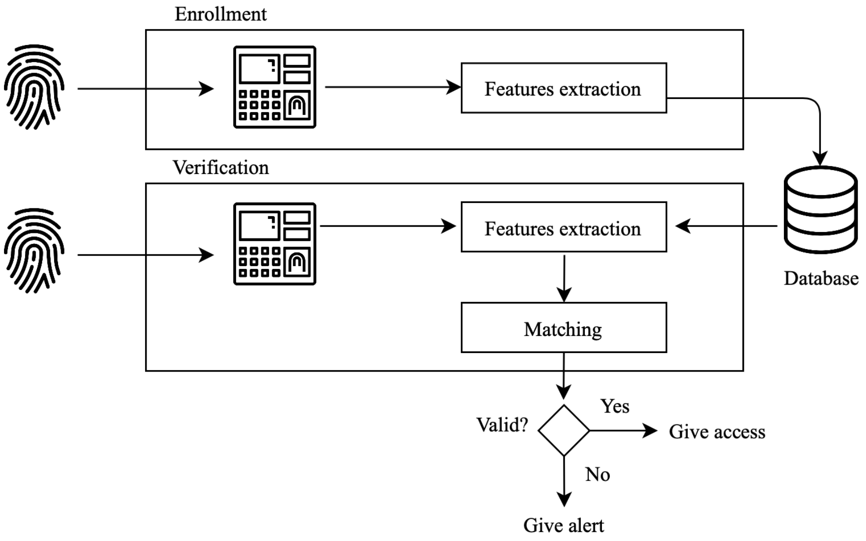

Figure 5. Fingerprint matching (adapted from source [16])

Branchless banking uses optical scanners that work by evaluating the reflection properties of the skin [17]. It will shine a bright light over the customer's fingerprint and produce a digital image by using a light-sensitive microchip. The light-sensitive microcip can be either a charge-coupled device or a CMOS image sensor [16]. The image is stored in flash memory and going to be analyzed and turned into a binary number. Typically, images captured this way are 512×512 pixels, and the standard image is 2.5cm (1 inch) square, 500 dots per inch, and 256 shades of gray.

C. One Time Password

Eavesdropping is one form of attack on network computing systems on network connections to obtain authentication information such as the login IDs and passwords of legitimate users. Once this information is captured, it can be used repeatedly to gain access to the system which is known as a replay attack. One time passwords (OTP), is one of the most popular possessions in two factor authentication (TFA) that can counter this attack. OTP can authenticate a transaction by agreeing on the possession of a pre-shared value [18].

After a transaction request is accepted by the bank server, an OTP code will be produced by the bank. The OTP code is produced by applying finite number secure hash functions to the output of the previous process which is accepting the transaction request message. Every transaction requires a different OTP. An eavesdropper would not be able to generate the required OTP because doing so would mean inverting the hash function. This OTP code will be sent through SMS messages to the customer. As stated before, SMS-based authentication brings benefits to the security system as well since it uses cellular network that is independent from internet network [10]. It creates difficulties on the attackers to manipulate a transaction since they.

VII. Conclusion

Banking services are a basic right for everyone. However, due to infrastructure limitations, the implementation of banking services in rural areas is not like the one in urban areas which is through bank branches. Branchless banking is an innovative approach to serve the poor in remote areas with banking services. Rather than utilizing physical building to provide services, this approach employs agents that carry POS terminals and mobile devices to facilitate transactions.

Information security is one of the main concerns in banking since the system deals with a huge amount of cash flows. From the discussion above, here are the conclusions that can be taken.

1. The trust model in branchless banking is made up by 3 main processes, they are:
    a. User validation

       This process is used by the system to identify which customer is about to make a transaction.

    b. User authentication

       Customers are authenticated to ensure that the one who does the transaction is the account owner itself. Password and fingerprint scan are used in this process.

    c. Transaction verification

       Before finalizing a transaction, the system will send a final verification utilizing OTP through the cellular network. This will ensure that the transaction details are correct.

2. There are three main technology used in branchless banking for its security, they are:
   a. Magnetic card reader

      When a magnetic stripe is swiped through a magnetic card reader, voltage is induced and causes the stripe to convert encoded flux into pulses. These pulses will be processed into binary data that can be converted into the card owner's data.
   b. Fingerprint scanner

      There are two steps in fingerprint biometric authentication system, enrollment and verification. Optical scanner is used in branchless banking to scan customer's fingerprints. Most branchless banking services scan more than 1 customer fingerprint to reduce false match rate.
   c. One time password

      One time password is a two factor authentication used by branchless banking to counter replay attacks.

References

[1] A. Demirgüç-Kunt, L. Klapper, D. Singer, S. Ansar, J. Hess, “The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution,” The World Bank , Washington, DC, Apr. 2018.

[2] M. Maharjan and S. Shakya, "System architecture for social security cash transfer through branchless banking in Nepal," in *Int. Conf. on Green Comput. and Internet of Things (ICGCIoT)*, Noida, India, 2015, pp. 60-64.

[3] L. Mohan and D. Potnis, "Mobile Banking for the Unbanked Poor without Mobile Phones: Comparing Three Innovative Mobile Banking Services in India," in *2015 48th Hawaii Int. Conf. on Syst. Sci.* Kauai, HI, USA, 2015, pp. 2168-2176.

[4] M. Saputra and S. H. Supangkat, "Financial technology business model as branchless banking for people in rural areas: Case study : Indonesia," in *2017 Int. Conf. on ICT For Smart Society (ICISS).*, Tangerang, Indonesia, 2017, pp. 1-6.

[5] G. Ivatury, I. Mas, "The Early Experience with Branchless Banking," CGAP Co., Washington, DC, USA, Rep. 46, Apr. 2008.

[6] M. Leger, “Bringing Financial Services to Emerging Countries,” Ingenico.co., Paris, France, White Paper, 2012, Accessed: Apr. 23, 2020. [Online]. Available: https://nocash.ro/wp-content/uploads/2012/02/Ingenico-White-paper-Bringing-Financial-Services-to-Emerging-Countries.pdf

[7] M. Pickens, D. Porteous, and S. Rottnan, "Banking the Poor via G2P Payments," CGAP Co.,Washington, DC, USA, Rep. 58, Dec. 2009.

[8] L. Long, "Biometrics: The future of mobile phones," in *Interactive Multimedia Conf.*, pp. 1-5, 2014.

[9] L. O. Gorman, "Comparing Passwords Tokens and Biometrics for User Authentication," *Proc. of the IEEE*, vol. 91, no. 12, Dec. 2003.

[10] M. Aizomai, A. Josang, A. McCullagh and E. Foo, "Strengthening SMS-Based Authentication through Usability," in *2008 IEEE Int. Symp. on Parallel and Distrib. Process. with Appl.*, Sydney, NSW, AAustralia, 2008, pp. 683-688.

[11] A. K. Jain, A. A. Ross, and K. Nandakumar, "Introduction to Biometrics" in *Handbook of Biometrics*. Berlin, Heidelberg: Springer, 2008, pp. 1-22.

[12] Sahidullah, Md, "Enhancement of Speaker Recognition Performance Using Block Level Relative and Temporal Information of Sub band Energies," Ph.D thesis, Indian Institute of Technology Kharagpur, Kharagpur, India, 2015.

[13] R. E. O. Paderes, "A Comparative Review of Biometric Security Systems," in *2015 8th Int. Conf. on Bio-Science and Bio-Technology (BSBT)*, Jeju, 2015, pp. 8-11.

[14] G. Masters and P. Turner, "Forensic data recovery and examination of magnetic swipe card cloning devices," *Digit. Investigation*, vol. 4, pp. 16–22, Sep. 2007.

[15] L. Honnegowda, S. Chan, and C.T Lau, "Security Enhancement for Magnetic Data Transaction in Electronic Payment and Healthcare Systems," *IACSIT Int. J. of Eng. and Technol.*, vol. 5, no. 2, Apr. 2013.

[16] S. Roy, S. Matloob, A. Seetharam, A. Rameshbabu, W. C. O'Dell, and W. I. Davis, "Biometrics Data Security Techniques for Portable Mobile Devices," *INAE Lett.*, vol. 2, no. 3, pp. 123–131, Aug. 2017.

[17] F. Alonso-Fernandez, F. Roli, G. L. Marcialis, J. Fierrez and J. Ortega-Garcia, "Comparison of fingerprint quality measures using an optical and a capacitive sensor," in *2007 First IEEE Int. Conf. on Biometrics: Theory, Appl., and Syst.,* Crystal City, VA, 2007, pp. 1-6.

[18] E. Erdem and M. T. Sandıkkaya, "OTPaaS—One Time Password as a Service," in *IEEE Trans. on Inf. Forensics and Secur.*, vol. 14, no. 3, pp. 743-756, March 2019.