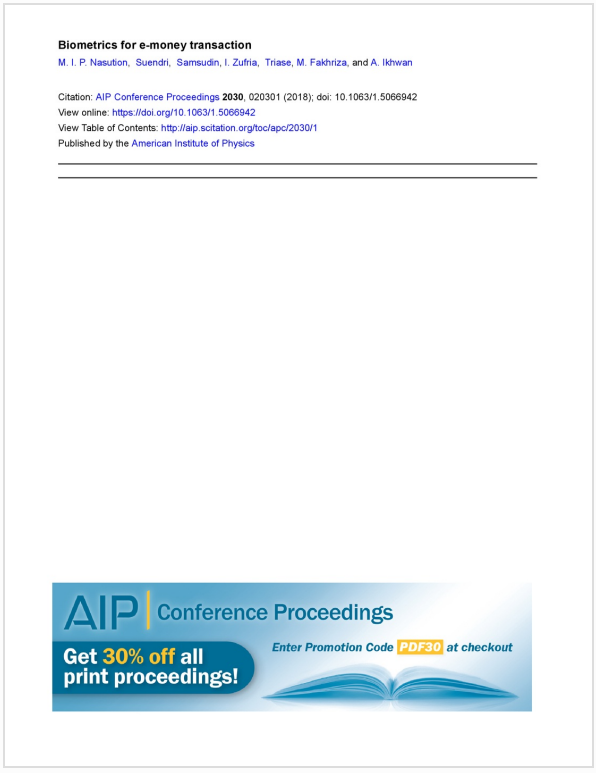
Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Muhammad Irwan Padli Nasution
Assignment title:	Reviewer
Submission title:	Biometrics for e-Money Transaction
File name:	1.5066942.pdf
File size:	924.76K
Page count:	7
Word count:	2,396
Character count:	12,798
Submission date:	07-Oct-2019 11:54AM (UTC-0700)
Submission ID:	1188003370



Biometrics for e-money transaction

M. I. P. Nasution, Suendri, Samsudin, I. Zufria, Triase, M. Fakhriza, and A. Ikhwan

Citation: AIP Conference Proceedings **2030**, 020301 (2018); doi: 10.1063/1.5066942
View online: https://doi.org/10.1063/1.5066942
View Table of Contents: http://aip.scitation.org/toc/apc/2030/1
Published by the American Institute of Physics

Biometrics for e-Money Transaction

by Muhammad Irwan Padli Nasution

Submission date: 07-Oct-2019 11:54AM (UTC-0700)
Submission ID: 1188003370
File name: 1.5066942.pdf (924.76K)
Word count: 2396
Character count: 12798

Biometrics for e-money transaction

M. I. P. Nasution, Suendri, Samsudin, I. Zufria, Triase, M. Fakhriza, and A. Ikhwan

Citation: AIP Conference Proceedings **2030**, 020301 (2018); doi: 10.1063/1.5066942
View online: https://doi.org/10.1063/1.5066942
View Table of Contents: http://aip.scitation.org/toc/apc/2030/1
Published by the American Institute of Physics

Biometrics for e-Money Transaction

M I P Nasution[1,a)], Suendri[1,b)], Samsudin[1,c)], I Zufria[1,d)], Triase[1,e)], M Fakhriza[1,f)], and A Ikhwan[1g)]

[1]*Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan, Indonesia*

[a)]Corresponding author: irwannst@uinsu.ac.id,
[b)]suendri@uinsu.ac.id,
[c)]samsudin@uinsu.ac.id,
[d)]ilkazufria@uinsu.ac.id,
[e)]triase@uinsu.ac.id,
[f)]fakhriza@uinsu.ac.id,
[g)]ali_ikhwan@uinsu.ac.id

Abstract. The rapid development of Information and Communication Technology has had an impact on all social aspects of society. Currently, there are many various forms of electronic money (e-money) that have used in buying and selling transactions both in traditional markets and in the online market. Various companies have issued their own electronic money. Initially the use of electronic money is still in the company's cooperation network. Thus, electronic payment transactions will continue to increase. This is a necessary mechanism of security that can make sure a sense of security for consumers in making payment transactions electronically. A security solution could be developed using consumer biometric elements. So in making payment transactions will be safer because biometric for everyone is not the same.

Keyword: e-money, biometrics, business, consumers

INTRODUCTION

The development of information and communication technology has changed the way of life and human interaction. Special innovations in payment transactions continue to expand, the traditional ways of monetary exchange have been replaced into electronic payments. Today, electronic money has become increasingly popular among people all over the world. Especially in Indonesia the first e-money permit in 2009 based on Bank Indonesia Regulation Number: 11/12 / PBI / 2009 on e-money, then in 2014 changes are made according to Bank Indonesia Regulation Number 16/8 / PBI / 2014, then another change was made in 2016 to Bank Indonesia Regulation Number 18/17/2016. Based on data from Bank Indonesia, the number of electronic money in circulation in 2016 is 51.3 million cards. Meanwhile, the volume of transactions through e-money reached 683.2 million times with a value of Rp.7.1 trillion. When viewed in number, transactions, and volume, then the use of e-money continues to increase from year to year. Data from Bank Indonesia reported that in the period of 2016, e-money grew by double digits in both terms of card number, transaction volume and transaction value. The amount of electronic money at the end of 2016 grew 49.22% to 51.20 million compared to the end of the previous year amounted to 34.31 million. The registered electronic publisher reached 20 companies consisting of nine banks and 11 telecommunications companies. On the one hand with the widespread use of e-money may reduce the use of cash. Communities already enjoy using electronic money can make more efficient payments, lower transaction costs than using other means of payment. This digitalization of financial services will continue to increase the use of e-money in payment

Green Design and Manufacture: Advanced and Emerging Applications
AIP Conf. Proc. 2030, 020301-1–020301-6; https://doi.org/10.1063/1.5066942
Published by AIP Publishing. 978-0-7354-1752-6/$30.00

transactions. For now the use of e-money in Indonesia is booming because e-money has been widely used to support routine transactions conducted by the community. For example, paying the entrance fee, paying for parking, public transportation tickets such as Commuter Line or Trans-Jakarta, and so forth.

Non-cash payment instrument in the form of e-money refers to smartcard. Basically, the security and comfort aspects become a very important factor in making the transaction. On electronic money has a stored-value or prepaid value in which a certain amount of money is stored in an electronic media owned by a person. The value of money stored in the form of stored balance on the chip e-money card will be reduced when the consumer uses it for payment. The balance can be replenished (top up) through a wide selection of scattered channels. For verification of identity data in a computer system is done using key, card, password, PIN and so on. However, this method has a shortcoming such as easily forgotten (password, PIN), hacked, or can be changed by irresponsible people.

The following are the security risk factors in the use of electronic money.

1. Theft. The simplest form of e-money crime is to steal another person's e-money card and then use the remaining funds. Theft can also be done by unscrupulous organizers of e-money, for example by charging funds illegally. Theft can also be done, for example by stealing a cryptographic key without the company's knowledge.
2. Duplication of devices. The risk of this crime is an attempt to duplicate the original card, so it can be used to make payment transactions like the original card. This type of crime is quite complicated and carried out by unscrupulous individuals with high levels of technical expertise. Because the offender must have different types of chips and operating system exactly the same as the original card.
3. Alteration or duplication of data / software This risk is a Crime Risk through attempts to change or modify data or applications contained on the original card, in such a way that the offender receives a financial gain. For example, adding e-money or changing the internal system of the application, so the calculation procedure is not working properly. Can also through 'physical attacks' against the chip itself.
4. Alteration of the message. This risk through the effort of change / intervention when the electronic data / message is sent, at the time of transaction. This potential risk is more likely to occur when e-money is used for internet payments.
5. Transaction denial (repudiation). Another misuse of e-money is the denial of transactions. The potential risk is an e-money-based software and uses message delivery when transactions over the internet network.
6. Malfunction. It risks can be corrupt or missing data, malfunctioning of the application or failure in message delivery. The risk of malfunction can be caused by physical or electronic disturbance of the instrument or due to interruptions in the transmission of messages between the transacting parties.

Thus, it is possible to develop techniques for the identification or verification of reliable and accurate use of biometric technology that utilizes special characteristics of the individual, such as face, iris, fingerprint, signature, etc. The main uses of biometrics include the identification of individuals to be able to access certain facilities as well as various applications to overcome and prevent crime. Physiological biometric data deals with the physical aspects of a person's body, such as face scans, fingerprints, hand lines, retinal scans, and DNA.

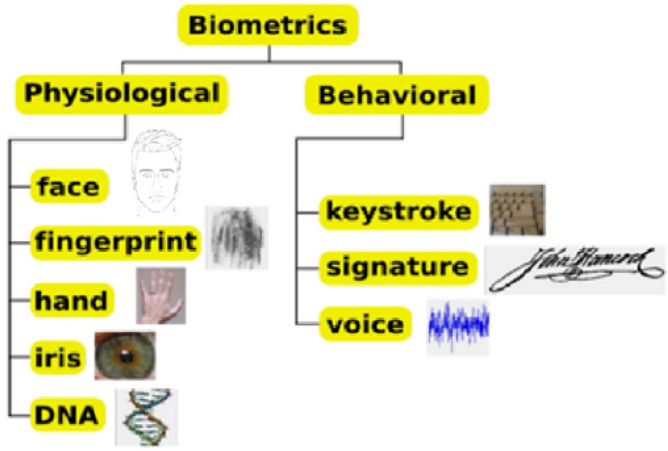


FIGURE 1. Biometric characteristic under verification conditions, biometric technology performs a singular comparison of the data presented with the previously stored template.

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds
Accuracy	High	High	Very High	Very High	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Long-Term Stability	High	Medium	High	High	Medium	Medium	Medium

FIGURE 2. Comparison of biometric techniques

From various research shows can be seen in Figure 2 that biometric data of fingerprint become an appropriate choice as authentication for the following reason: 1) The cheapest cost, more economical than other biometrics because of its easy and inexpensive data recording device, 2) The shape can be kept unchanged, so it can be used for long periods of time, 3) Uniquely, there is no possibility even though twins.

If using a biometric technique, it is no longer necessary to remember the PIN and or multiple password because the security device is the body itself so it will be difficult to duplicate or stolen by people. Thus will facilitate the mobility of every person to make payment transactions anywhere without having to be bothered because they have to carry cards.

METHODOLOGY

Biometric systems can seem complicated, but they all use the same three steps:

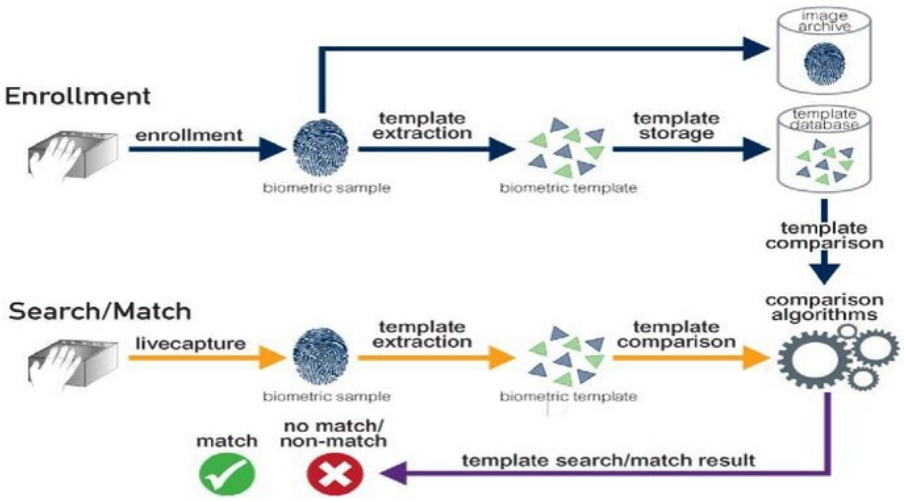


FIGURE 3. Biometric system processes

Enrollment: The first time you use a biometric system, it records basic information about you, like your name or an identification number. It then captures an image or recording of your specific trait. Fingerprint identification is the method of identification based on the different patterns of human fingers, which is actually unique among each person. It is the most popular way of acquiring details of any person and is the most easy and convenient way of identifying a person. An advantage of fingerprint identification method is that the fingerprints pattern remains same for a person throughout his/her life, making it an infallible method of human identification. This process is done by using equipment that has sensors to retrieve data digitally such as a fingerprint reader, digital cameras and smartphones. Performance of biometric systems is dependent on the quality of the acquired input samples. If quality can be improved, either by sensor design, by user interface design, or by standards compliance, better performance can be realized. For those aspects of quality that cannot be designed-in, an ability to analyze the quality of a live sample is needed. So, selecting the right fingerprint reader is a very important step.

1. Storage: Contrary to what you may see in movies, most systems don't store the complete image or recording. They instead analyze your trait and translate it into a code or graph. Some systems also record this data onto a smart card that you carry with you. A fingerprint pattern is stored into the database because it is a solid and invariable template object.
2. Comparison: The next time you use the system, it compares the trait you present to the information on file. Then, it either accepts or rejects that you are who you claim to be. This process is to identify and authenticate (authentication) or match the owner's original security device with the template stored in the database. The data with the owner and the database is authentic if both are the same.

The weakness of fingerprint technology is the process of storing and transmitting fingerprint information. The small fingerprint data must be stored as a template in the database on the server, thus, it becomes vulnerable if the weakness of the computer network security. Fingerprint data must also be sent to the server, so the data transmission process can also be an easy target for hackers. Thus, in conducting e-money transactions are necessary how to protect the fingerprint template to stay safe. Security in a system can be divided into three aspects, namely aspects of people, aspects of the process, and aspects of technology. Aspects of people discuss the security of the human side of the system implementers, such as how awareness of things that broken with system security, such as password security. Aspects of the process discuss the security of the side of the process undertaken. That is, every process that exists on the system is made so that the security of the system can be maintained. This aspect of the process should arise in every standard operating procedure (SOP). The technology aspect discusses the security of the technology side that can be applied to secure the system.

RESULTS

The mechanism of payment transactions with e-money as can be explained in Figure 4. Subsystems that exist in payment transactions with e-money usually contain four functions, namely loading agent, user (customer), seller (merchant) and collecting agent. Loading and collecting agent is usually a bank. Loading agent converts from monetary value to another form into electronic monetary value on this electronic money system. Collecting agents work the other way around, converting from money to electronic money systems to monetary value in other forms (e.g. banknotes). If using an e-money card, then the payment transaction is done by taking the value of money recorded digitally on the e-money card. However, if a fingerprint is used instead of an e-money card, it is necessary for the party to store the biometric by digitally recording the value of money in the fingerprint template, so that the payment mechanism of e-money with fingerprint can be explained in Figure 5. Wallet is a customer account that stores the value of money in accordance with their own biometric fingerprint, so everyone will have different wallet. The process of payment transactions to the merchant occurs of course, when fingerprint authentication gives successful results that the fingerprint read on the sensor in accordance with the owner. For top-up the money can be done by transfer to the wallet fingerprint account of the consumer.

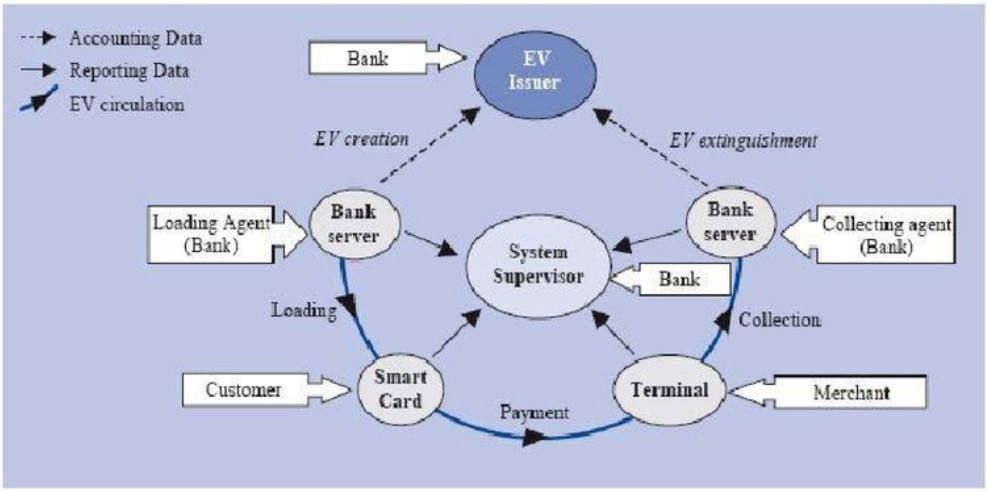


FIGURE 4. e-Money transaction using card

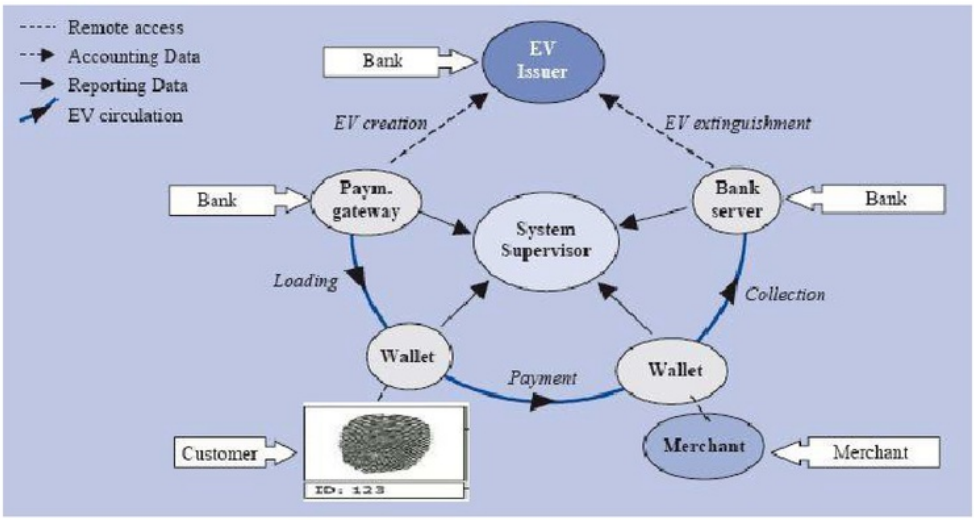


FIGURE 5. e-Money transaction using fingerprint

CONCLUSION

Biometrics are our most unique physical (and behavioral) features that can be practically sensed by devices and interpreted by computers so that they may be used as proxies of our physical selves in the digital realm. In this way we can bond digital data to our identity with permanency, consistency, and unambiguity, and retrieve that data using computers in a rapid and automated fashion. If using biometric techniques, it is no longer necessary to remember the PIN and / or password because the security device is the body itself so it will facilitate the mobility of every person to make payment transactions anywhere without having to be bothered to bring e-money card. Biometric technology has several implementation issues related to its extensive development and distribution. Problems that arise include the lack of biometric standards internationally and also privacy and security issues

become potential that affect the growth, distribution, and implementation of its services. It is therefore necessary for the regulation of the Government to regulate how the form of its authenticity authentication method is strongly attached to identification. When the level of security and comfort has been enjoyed by many people to various forms of retail sale and purchase, of course the use of biometrics in e-money transactions will grow rapidly.

REFERENCES

1. Vatsa M., Singh R., et al. Biometric Technology dalam Encyclopedia of Multimedia Technology and Networking / editor: Margherita Pagani. Hershey: Idea Group, Inc., 2005.
2. Muhammad Irwan Padli Nasution, Urgensi Keamanan Pada Sistem Informasi, Jurnal Iqra' Volume 2 No. 2, 2008.
3. Ali Akbar, Kriptografi Dalam Sistem Uang Elektronik (Electronic Money System), http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah2/Makalah-011.pdf, 2006.
4. Tracy V.Wilson, How Biometrics Works, retrieved on 05 December 2017 from https://science.howstuffworks.com/biometrics.htm
5. http://www.bi.go.id/id/peraturan/sistem-pembayaran

Biometrics for e-Money Transaction

ORIGINALITY REPORT

16%	16%	%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	how-does-things-work.blogspot.com Internet Source	4%
2	eprints.unm.ac.id Internet Source	3%
3	www.touchngoid.com Internet Source	3%
4	www.aware.com Internet Source	3%
5	minnesotafuturists.pbwiki.com Internet Source	1%
6	generalimpactfactor.com Internet Source	1%
7	www.scribd.com Internet Source	1%
8	www.cimbniaga.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		