Design of 3-Layered Authentication Mechanism using User's Biometrics Signals An Overview

[1]K.Bharathi SenthilKumar and [2]K.Jayalaksmi
[1]M.C.A,M.Phil., [2]M.Sc,M.Phil,SET.,
[1,2]Assistant Professor, PG & Research Department of Computer Science
Joseph Arts and Science College, Thirunavalur, India

Abstract *- In this paper, robust authentication mechanism using user's biometrics signals for complementing traditional authentication's weak points is proposed. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Nowadays, authentication system are developed using biometric. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. The different types of biometric used in authentication system are iris, fingerprint, vein pattern, hand geometry etc. A biometric system provides an automated method of identifying a human being based on his/her biometric characteristics. But there are some security problems. Some biometrics can be copied by a malicious user with scanners. All biometrics characteristics extracted from a user are not possible to maintain a steady normal condition. A biometrics signal is a pattern recognition that uniquely identifies human being based on his/her physiological traits. A biometrics signals should be impossible to masquerade or manipulate. This attribute is used as 3rd authentication phase. Proposed authentication mechanism is composed of 3 layered authentications; ID&P/W, PIN number or biometrics, and biometrics signals.*

Keywords: *Authentication, Biometrics Signal, Biometrics Security.*

I. INTRODUCTION

An authentication means to authenticate the user him/herself attempting to access the system after identifying user. To validate the user, Authentication is the first step of security requirement for any information communication environment. Authentication mechanism also prevents forgery and unauthorized access as well as identity check. Allowing access to only authorised users and disallowing access to the unauthorised ones is a fundamental aspect of authentication. Authentication processes are based largely on three methods. These methods include:

- What we know – passwords, pin codes and other personal details can be used to identify users of a particular system.
- What we have – tokens such as smartcards or key fob are also used for user authentication.
- What we are – here, biometric features such as fingerprint scans, iris scans, palm biometrics are deployed for allowing access to controlled environments.

Various authentication systems have been used in internet banking, access control system, credit card, and system security field. But password authentication is vulnerable to password hacking tools such as dictionary attack and brute-force attack. An authentication system using passwords can be replaced and/or intensified by accredited certificate, smartcard and any one of the biometrics. Smartcard also proved to be vulnerable to attack impersonation attack. Nowadays, authentication systems provide double authentication with password and smartcard or biometrics. Especially, biometrics provides a more reliability than other traditional authentication components[1, 2] .

Biometrics is widely used at various security fields. For example, fingerprint scanners have already used in smart phone and recognition sensors installed in automobiles. Biometrics has some limitations to be used alone because the fingerprint is often affected by handwork environment, and the voice is affected by flu or throat infection. So, complementary authentication factor is necessary to overcome these weak points. Recently, actively researching biometrics signals to apply to security system is done. Biometrics signals is a pattern recognition technology that is uniquely the automated identification of human being based on his/her physiological attributes. Biometrics signal is added to authentication mechanism for reinforcing reliability.

II. BIOMETRICS BASED AUTHENTICATION SYSTEM

Biometrics characteristics are a unique, measurable physiological and/or behavioral trait of a human being for automatically recognizing or verifying his/her identity. All human have their own unique biometrics in the overall human body structure. As mentioned above, biometrics classifies physiological and behavioral factors. Typical physiological factors are fingerprint, hand, face, iris, etc. Behavioral factors include keystroke, signature, voice, handwriting, etc.,

Biometrics is used to security system because it has inherent properties, universality, measurability, singularity and so on. Biometrics need not be remembered or had like passwords and smartcard. It is not easily lost or forged. And it should be collected in real time. So, biometrics based security system provides a more authentication reliability than traditional systems like passwords, smartcard, etc. Biometrics based security system provides verification of the user's identity by matching the measured biometrics attributes with his own biometric template stored in the database.

The collection sensor collects user's biometric characteristics using any sensors such as camera, fingerprint scanner, etc.The biometric characteristics may be fingerprint, speech etc.. The feature extractor processes extraction and encoding of specific characteristics from user's biometric characteristics to convert feature templates. In case of fingerprint, it extracts location and direction of the ridges and bifurcations from fingerprint image. And then the collected new feature template is compared with stored templates in a database to determine the degree of similarity or correlation. If new feature template is matched with individual templates stored in a database, it permits access to resources.

The biometric based security systems offer several advantages. It could be created specific personalized key for each user because biometrics is unique to each person. It also requires unchangeable authentication key periodically like password because biometrics characteristics are permanent and not changeable. No transferring or spoofing in their own biometrics characteristics to other users because biometrics characteristics are only measured in real time when user requests authentication to system. For these advantages, the biometrics is popularly used to security systems such as database security and access control in physical security like building, gate, and office.

It is essentially user characteristics recognition system that operates by extracting from physiological characteristics of a user into templates, and compares these templates set with the template set in the database like Fig. 1.

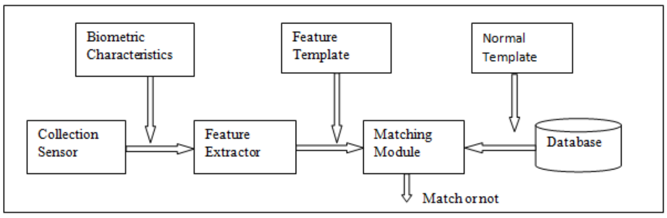

Figure1: Biometrics based Security System

But, there is not a biometrics based security system adequate to all application because biometrics characteristics have some inherent vulnerabilities. For example, it is impossible that all biometrics characteristics extracted from a user always keep a normal condition. Because it is difficult to extract accurate templates if human eats the food before sleeping. It is still needed to improve accuracy to reduce false rejection rate. So, it is better to use with another authentication factor to improve security performance[1-5].

III. DESIGN OF 3-LAYERED AUTHENTICATION MECHANISM

Authentication system aims to prevent forgery and unauthorized access as well as identity check. The common authentication approach is the use of passwords. But, using password for a long time, it is possible to copy by malicious user. Smartcard appears to resolve security problem of password in a secondary authentication approach. This also proved to be vulnerable to attack impersonation attack[6,7]. Recently, the biometrics based authentication techniques is popularly used in the security field. But even risk has been identified that hacker can steal biometrics from user and manipulates biometrics templates in the database by hacking.

In this paper, biometrics signals to authentication mechanism has been applied to complement traditional authentication factor's weak points. Biometrics signal is a natural, unique feature and an important physiological characteristic in the human body.

It is not ease to copy or imitate because it can collect from inside of human body[8]. Biometrics signals include EEG, pulse, and skin conductivity, etc., EEG (Electroencephalography) is the recording of electrical activity along the user's scalp. Pulse is a significant physiological signal that is the periodic wave of the arteries occurring by a human's heart beats. Skin conductivity is the electrical conductance of the user's skin, which varies with skin moisture. The concept of proposed 3-layered authentication mechanism is given in the following Fig. 2.

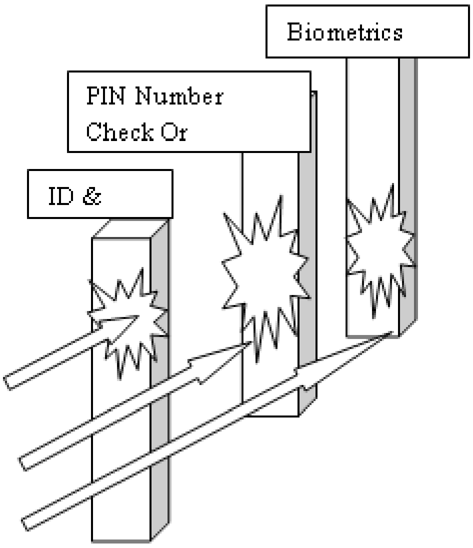

Figure2: The Concept of 3-Layered Authentication

The concept of the 3-layered authentication mechanism authenticates user step by step according to the importance of object which user tries to access. It doesn't request authentication by user's biometrics signals as soon as user firstly requests to access to system. In the first layer, user enters his/her ID&P/W when he/she access to network system. Second layer, user sends his/her PIN number or biometrics information captured with sensor to authentication server. In the last layer, when user requests access of critical data in the database, user should be measured his/her biometrics signal. If measured biometrics signal is matched the normal template in the database, user will be allowed to access the critical data he/she requested.

Proposed mechanism composed of a human interface, two modules and databases. Pulse is used as biometrics signal's factor because pulse is one of the feasible and easy measurable biometrics signal. First and second layered authentication mechanism is the same as traditional authentication method. The design of authentication mechanism using user's biometrics signals in given in the following Fig. 3.

In addition, a sensor device for the pulse is very convenient than other biometrics signal sensor device. And the two modules include Analysis module and Decision module.

•Human Interface: Input device is attached with sensor to collect user's live biometrics signal. Collection of sensor measures user's pulse, and sends measured feature to biometrics analysis module.

•Analysis Module: Composed of feature extractor and matching function. Feature extractor extracts specific features from the measured biometrics signal because full data of biometrics signal is not saved to the biometrics database. This convert's measured feature to template by mathematical algorithm, pattern recognition algorithm, etc., Conversion method could be varied from venders or modalities. Feature template is sent to matching function. Matching function performs to compare feature template with normal template in the biometrics database. Normal template, which is result from the average of the measured biometrics signal's specific feature for a few months, is enrolled in the biometrics database. Proposed mechanism's matching time is not long because some comparison objects were filtered by biometrics information in the 2nd layer. When a user requests to access critical data, one to one matching is processed with each single template recommended from 2nd layer in the database. Matching results is sent to a decision module.

•Decision Module: Determines whether access will be allowed or not. This module requests to measure a user's biometrics signal up to three times although the matching error is occurred in the first time. It will be considered the rate of false negatives of biometrics system. If a user is authenticated, user can access to data user requested. If a user does not pass authentication over three times, a user will be given a warning. In spite of a warning, if a user tries to continue to access data, this module rejects a user's all requests and block to access system. And then, the log file will be stored in the security policy database.

•Database: Composed of biometrics database and security policy database. The former stores user's biometrics information and biometrics signal templates. The latter stores security policies related to authentication, countermeasures, events logs, and so on.

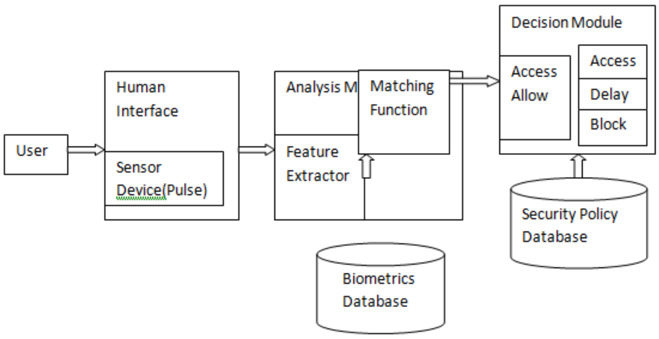

Figure3: The Design of Biometrics Signals based Authentication

IV. APPLICATION

Biometrics signals measurement system is composed of sensor, encoder and software made in Thought Technology. A BVP (Blood Volume Pulse) sensor can measure heart rate, pulse, temperature, and skin temperature. In this research, only pulse is used. BioGraph Infiniti program[9-11] presents biometrics signal and reaction times.

Raw data of three persons' pulse signals while repeated 10 times using BioGraph Infiniti program[12] is extracted. When calculating the mean of pulse graph, the graph beyond ordinary boundary was excluded. It is revealed a fact that the average graph cannot accurately represent pulse graph of the test subject due to the number of measurement and inaccurate results by the test subject's condition. While measurement is progressing, faced some problems could be affected test subjects. First of all, the measurement result is influenced by test subject's environment factors included indoor temperature, noise, air, smell etc. Secondly, the signal graph is irregular depending on the condition of the test subjects. After the test subject exercises or have a meal, span of the graph is narrow. When the test subject's condition is not good, span of the graph is wide. Lastly, when measuring, if the test subject moves, the value of biometric signals can't be accurately collected. Sensor of the measurement system is very sensitive to the movement of the subjects. These are identified through test subjects of three person's pulse signals.

This research is focused on biometrics signals based authentication system. It is mainly concerned with possibility of authentication using biometrics signals. The proposed authentication mechanism is still difficult to apply to security system because the problem with the sensor of the biometrics signals collection and the absence of the definition method of accurate normal biometrics signal templates. First of all, authentication optimized collection sensor is needed because the existing sensors is not appropriate to collect biometrics signal used to authentication system. Conventional sensors have a lot of noise when collecting biometrics signals. When noise happens frequently, the average of user's biometrics signals is not accurate. Also, if a user moves with wearing sensor, the value of measured biometrics signals is very irregular. So, motion avoided sensor which is not so sensitive to user's action is needed. If noise occurs, filtering technology could remove the unusable value is required. The accuracy of normal templates stored in the database is also a problem. For improving the accuracy, a huge amount of raw data is needed. It is not sufficient to calculate average with small data. Although the average was calculated with small data, it is easy to decide incorrect average value. So, most biometrics system research recommends mathematical and statistical algorithm to calculate normal templates. In addition, there are also many issues to address. For example, biometrics signal is not constant from the beginning to the end of measurement. Still these issues will be solved one by one as researching.

CONCLUSION

In this paper, a 3-layered authentication mechanism using user's biometrics signals for complementing traditional authentication's weak points is designed. Nowadays, authentication system are developed using biometric information. But there is also some security problem. Some biometrics is possible to copy by a malicious user with scanners. It is also impossible that all biometrics characteristics extracted from a user always keep a normal condition.

It is also proposed to apply biometrics signals to 3rd layered defense for improving authentication reliability. Biometrics signal is a natural, unique feature and an important physiological characteristic in the human body. It is difficult to copy or imitate because it can collect from only inside of human body in real time. The key of the 3-layered authentication mechanism is to request authentication factor to user based on biometrics signals.

The problem with the collection sensor for the biometrics signals collection and the absence of the definition method of accurate normal biometrics signal templates has to be solved.

Acknowledgment

"This paper is a revised version of a paper entitled [The Design of Robust Authentication Mechanism using User's Biometrics Signals] presented at [IJSIA 2014, volume 8]."

References

[1] R. Awasthi and R. A. Ingolikar, "A Study of Biometrics Security System", J. Innovative Research & Development, vol. 2, Issue 4, **(2013),** pp. 737-760.

[2] S. P. Cheon, J. M. Kang, M. W. Park and J. H. Eom, "The Scheme of 3-Level Authentication Mechanism for Preventing Internal Information Leakage In", The 4th International Conference on Digital Information and Communication Technology and its Application, **(2014),** pp. 154-157.

[3] "Biometrics Security Considerations", www.nsa.gov/snac.

[4] S. Rane, Y. Wang, S. C. Draper and P. Lshwar, "Secure Biometrics", IEEE Signal Processing Magazine, IEEE Press, **(2013)**.

[5] "The application and Problems of Biometrics", http://www.kipo.go.kr.

[6] W.-H. Yang and S.-P. Shieh, "Password Authentication Schemes with Smart Cards", J. Elsevier Computers & Security, vol. 18, no. 8, **(1999),** pp. 727-733.

[7] E.-J. Yoon, "Cryptanalysis of RSA based Password Authentication Scheme with Smart Card In", The International Summer Conference on IEIE, **(2012),** pp. 866-869

[8] T. Ye-wei, S. Xia, Z. Hui-xiang and W. Wei, "A Biometric Identification System Based on Heart Sound Signal In", The 3rd International Conference on Human System Interaction, IEEE Press, New York, pp. 67-75, **(2010)**.

[9] "SA7913 V5.1.2 BioGraph Infiniti Getting Started", pdf, http://www.thoughttechnology.com.

[10] S.-H. Lee, M.-W. Park, J.-H. Eom and T.-M. Chung, "PDT-BI: Proactive Detection Technology based on the Biometric Information for Preventing Internal Information Leakage", International Journal of Bio-Science and Bio-Technology, vol. 5, no. 5, **(2013),** pp. 187-196.

[11] H. Lee, J. Jung, T. Kim, M. Park, J. Eom and T. M Chung, "An Application of Data Leakage Prevention System based on Biometrics Signals Recognition Technology In", The 3rd International Conference on Networking and Technology, **(2014)**.

[12] Jungho E, " The Design of Robust Authentication Mechanism using User's Biometrics Signals", Vol.8,no.6, **(2014)**.