International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com, Volume 5, Issue 2 (March - April 2017), PP. 34-37

VOICE BASED ACCESS CONTROL FOR PROVIDING HIGH SECURITY TO INTELLIGENT SYSTEM

[1] NIKHILN, [2] SHEETHAL.G, [3] RANJANA.R
[1]nnikzz76@gmail.com, [2]gsheethal12@gmail.com, [3]ranjanaramakrishna@gmail.com

***Abstract*— One of the hot topics in today's world is security. Providing security of data is an important task which can be done by bio-metric authentication. The existing techniques for authentication, involves the use of passwords, user IDs (identifiers) or RFID (radio frequency identification), PIN, iris recognition, finger print, face recognition. This survey presents use of security system for logical access control and device that has been developed for security purposes in various fields.**

***Index Terms*— Security, bio-metric, RFID, PIN, iris, face, finger print.**

I. INTRODUCTION

The value of authorized user authentication is not limited to just computer or network access. Various other applications in day-to-day life also requires user authentication, such as banking, e-commerce, and physical access control to computer resources, and could benefit from enhanced security. Authorized user authentication is an important task in the Web-enabled world. The result of an insecure authentication system in a corporate/enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity.

The existing techniques for user authentication, which involve the use of either passwords [1] and user IDs [3] (identifiers) or RFID [5] (radio frequency identification which is an automatic identification technology that uses a tag embedded in the target entity to mark it with a unique code like ATM cards) identification cards, PINs [3] (personal identification numbers) and tokens suffer from several limitations.

For instance, when a user's personal details such as user ID ,PIN and Password is shared with others the traditional authentication policy based on a simple combination of user ID and password becomes less efficient.

Bio-metric authentication technology is a rapidly advancing field that is concerned with recognizing a person based on an individual's physiological or behavioral characteristics. Examples for automated bio-metrics [2] include fingerprint, face, iris, palm print, hand geometry and speech recognition. User authentication methods can be broadly classified into three categories as shown below:

II. METHOD 1

The known techniques are:

EXAMPLES	PROPERTIES
USER ID and TOKENS	SHARED
PASSWORD	CAN BE GUESSED
PIN	COULD BE FORGOTTEN

A. TOKENS

Nguyen Van Duy et al [1] has described that a token can be a factor to authenticate user . Tokens can be used as an additional method to prove one's identity who he/she claims to be. A dynamically generated text using a hardware device or programs related to authentication can be used as the token to authenticate user. Tokens are divided into two mechanisms: 1) software-based 2) hardware-based physical electronic medium, such as USB-based devices for authentication.

Phin Shen Teh, Andrew Beng Jin Teoh [9] relates a token to an entity that requires a user to physically possess this for being authenticated.

They express that large scale implementation is simple and also that every system comes with its own weaknesses. They also have an opinion that tokens can be vulnerable to lose or theft as user may find it difficult to keep it safe at all times which is quite impossible. This implies that there is no assurance on uniquely identifying a genuine user even with the ownership of the token.

B. PASSWORD

Mahendra Chopra et al [1] expresses that password is commonly used as the authentication mechanism to access the web resources. However, knowing the password which is described as weakness and industry attacks surfaced in last few years, it clearly indicates that extra measures are required to protect confidential and crucial information. The second factor

secret can be the factor from the result of combining techniques like password or token/smart cards.

Bio-metric that makes the overall authentication stronger and more secure.

The author also claims that user may be challenged with two or more questions before the access to sensitive information is granted. The challenge question can be in the form of visuals displayed to the user or it can be transparent to user and read from the device without the user taking notice. It may not be necessary for every application or resource to use second factor but it is certainly for applications that control sensitive information.

III. METHOD 2

The existing techniques:

CARDS	**SHARED**
KEYS	**LOST OR STOLEN**
BADGES	**CAN BE DUPLICATED**

IV. METHOD 3

A. Combination of techniques

ATM CARD + PIN	SHARED PIN A WEAK LINK

B. ATM AND PIN (OTP)

Usually ATM SYSTEMS do not contain the OTP feature for money withdrawal. If an attacker manages to get hold of the ATM card and the PIN number he may easily use it to withdraw money fraudulently.

Using this authentication he may view details, and he is asked to enter an OTP as soon as he clicks money withdrawal option at this stage the system generates and sends a ONE TIME PASSWORD (OTP) to the registered mobile number to that particular user he now needs to enter the OTP in the system in order to withdraw money. Thus system provides a totally secure way to perform ATM transaction.

The user may have to face the following challenges:

- If CARD is lost there is no way to interact with system.
- Needs a security Guard at ATM center.
- OTP may take time to be received on mobile.

V. METHOD 4

SOMETHING UNIQUE ABOUT THE USER: Physiological or behavioral traits

FINGER PRINT	NOT POSSIBLE TO SHARE
FACE	REPUDIATION UNLIKELY
IRIS	FORGING DIFFICULT
VOICE PRINT	CANNOT BE LOST OR STOLEN

A. FINGER PRINT

Sulochana Sonkamble , Dr. Ravindra Thool [8] expresses that the finger prints of a person have been used as person identification from long time. Finger print is the pattern of ridges and valley on the surface of a finger-tip which is unique in every human being. The finger prints of the identical twins are different. It is made possible to scan finger prints of a person and it can be used through the computer for number of applications such as identifying a person etc.

This method is traditional and it gives accuracy for currently available Fingerprint Recognition Systems for authentication and authorization. This fingerprint recognition system is quite affordable in large number of applications such as banking, Passport etc., and it is quite useful.

The above method may have certain limitations. A few is as follows:

- Dry or dirty skin might intend to cause errors.
- It not applicable for differently abled people.
- Xinwei Liu et al [13] consider that a finger print sample may have lot of ambiguities because of many properties (scenery/imaging).

VI. HAND GEOMETRY

Odgerel Ayurzana et al [15] define hand geometry as a pattern of hand shape and palm contain much information for identifying person. Hand geometry which is used to identify unique pattern of hand, shape and also the palm lines. Hand-geometry were one of the first biometrics to prove practical in use across a variety of real-world applications.

Hand geometry systems work by taking a 3-dimensional view of the hand in order to determine the geometry and metrics.

Balwant Sonkamble [8] has explained that hand geometry recognition systems are basically related on a number of measurements taken (hand which includes its shape, length, palm size and many more.). This method is very simple and easy to use. There might be some effect of some factors such as environmental which might be weather or dry skin, this does not intend to have dry worst effects on the authentication accuracy but would vary if the person has any serious cuts/injury. There is a probability of change in the geometry.

The hand geometry is scanned and used for identification and recognition of a person [8].

Limitations: For example it's quite difficult for a person suffering from disease like arthritis to be comfortable with this kind of security system which deals with the hand geometry as they face a lot of health issues.

VII. FACE RECOGNITION

Sulochana Sonkamble [8] says that face recognition is the commonly used biometric technique for a person's recognition. The most reliable approaches to face recognition are based on shape of facial attributes, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes which define the human facial attire. This technique involves many facial elements; systems which deal with all these facial elements have some sort of difficulty in matching face images.

The face recognition systems which are used currently impose lot of restrictions on how facial images are obtained and how these images taken can be used for many applications. The face recognition system detects the authorized person's face image and is able to recognize the person's identity for any authentication purpose.

A. The challenges:

- 2D recognition is basically affected in many manners such as change of lighting while the recognition process is undergoing (which apparently keeps changing), person's hair that grows, age, and if the person is badly wounded.
- Requires camera which is the main requirement for user identification (probability of this being implemented until most PCs consist of camera as standard equipment is quite difficult).

B. IRIS

By Anas Aloudat, Katina Michael and Roba Abbas [14] define that iris is the colored part in the middle of the eye, just in front of the lens. The iris is "a thin diaphragm stretching across the anterior portion of the eye and supported by the lens".

Amena Khatun , A. K. M. Fazlul Haque [4] states that iris recognition is a biological feature in a human which implies for recognition. It is a unique structure of human which remains stable over a person lifetime unless we insist to change it. The iris is the annular region of the eye. Both left and right iris of an individual can be treated as separate unique identifier and can be used for many purposes. The iris information can be collected by taking an image of it. Regin Joy Conejar, JunWoo Jo, Jaeeon Bae, Haeng-Kon Kim analysis iris technology and has the opinion that the accuracy of iris based recognition system is promising. Each iris is believed to be distinctive and even the irises of identical twins are also different and this is the most important factor in a human life. The iris recognition system has become user friendly and cost effective which indeed helps people to approach it. The iris have a very low false accept rate as compared to other biometrics like finger print, face, hand geometry and voice as these lack in many factors.

There can be drawbacks to this recognition system as this may be intrusive and require a lot of memory to store data. This may not be cost effective.

VIII. VOICE BASED RECOGNITION SYSTEM:

Voice is the most natural way for humans to communicate .A voice recognition system is basically developed to identify an admin voice. MATLAB software which can be used for coding the voice recognition, the authorized person's voice can be authenticated and he can be identified. The key is to convert the speech waveform to a *.wav representation for further analysis and processing.[9] The database will be consisting of a different set of patterns which will represent the states required for the successful completion for a given phoneme. [11]

Devices are controlled by voice recognition process and in this system templates are stored in database according to the sampled speech power. The access may be processed by means of an enrolled user speaking into a microphone attached to the system which undergoes several processes. Then will decide whether the voice matches with the stored voice.

IX. ADVANTAGES:

Speech signal seems quite interesting as the basis for person identification. Features depend on the basis of structural parameters (dimension and proportions of the mouth, lips etc.,) and behavioral habits (individual ways of pronunciation, voice quality, prosodic properties, rhythm of speech etc.). It means that the protection given by speech signal treated as biometrical "key" to some system can be more effective than methods using solo the structural properties of the body of authorized person (e.g., fingerprints, palm shapes, face appearance, iris details etc.) [12]

CONCLUSION

In the voice based security system we can think of adding additional components like the wireless camera and a buzzer to monitor the person trying to access the system and alerting authorized user by means of a GSM model to know if an intruder is trying to access his system. In voice based recognition system if the voice matches then a DC Motor will rotate

To show that access is granted. If the voice mismatches then a buzzer will get activated and also a SMS will be sent to the concerned person using GSM modem. By the help of this method we will be able to give system the voice command to perform task and also to monitor using a wireless camera.

This may be used to extend the previously developed voice based security systems as a future work as it may provide a more efficient security system.

REFERENCES

[1] David Jaramillo,Richard Newhook,Nguyen Van Duy,Mahendra Chopra"Password-based Mobile Access, Alternatives and Experiences".Proceedings of the IEEE Southeast Con 2015, April 9 - 12, 2015 - Fort Lauderdale, Florida.

[2] F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "Quality measures in biometric systems," Security & Privacy, IEEE, vol. 10, no. 6, pp. 52– 62, 2012.

[3] Radek Holý1, Jana Kaliková2, Marek Kalika1,"Identification Persons - security components of ID card" .

[4] IAmena Khatun, 2A. K. M. Fazlul Haque, 3Sabbir Ahmed, 4Mohammad Mahfujur Rahman,"Design and Implementation of Iris Recognition Based Attendance Management System ".

[5] Yu-Chih Huang ,"Secure Access Control Scheme of RFID System Application".

[6] Silvy Achankunju, Chiranjeevi Mondikathi 1,International Journal of Emerging Trends in Electrical and Electronics (IJETEE –ISSN: 2320-9569) Vol. 11, Issue.2, June 2015"Voice & Speech Based Security System Using MATLAB".

[7] Silvy Achankunju,Chiranjeevi Mondikath"Voice Based Security System Using Matlab & Embedded System",Volume : 4 | Issue : 5 | May 2015 • ISSN No 2277 - 8179.

[8] SULOCHANA SONKAMBLE, 2DR. RAVINDRA THOOL, 3BALWANT SONKAMBLE 1Asstt Prof., Department of Information Technology , MMCOE, Pune, India-411052 Professor, Department of Information Technology, SGGSIE&T,Nanded, India -411017 3Asstt Prof., Department of Computer Engineering, PICT, Pune, India-411043

[9] Hairol Nizam Mohd. Shah*,Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin,Chow Kok Lin and Zalina Kamis

[10] Regin Joy Conejar, JunWoo Jo, Jaeeon Bae, Haeng-Kon Kim School of Information Technology.

[11] Anshul Gupta Jaypee University of Engineering & Technology, Guna M.P India. Nileshkumar Patel Jaypee University of Engineering & Technology, Guna M.P India. Shabana Khan Jaypee University of Engineering & Technology, Guna M.P India.

[12] Ryszard Tadeusiewicz Department of Automatic Control AGH University of Science and Technology Krakow, Poland rtad@agh.edu.pl Grażyna Demenko Phonetic Department, SpeechLab Adam Mickiewicz University Poznan, Poland

[13] Xinwei Liu1,2, Marius Pedersen1, Christophe Charrier2, Patrick Bours1,Christoph Busch11Norwegian University of Science and Technology, Gjøvik, Norway2E-payment and Biometric Research Unit, Laboratory GREYC,University of Caen, France

[14] By Anas Aloudat, Katina Michael, and Roba Abbas "THE IMPLICATIONS OF IRIS-RECOGNITION TECHNOLOGIES"

[15] Odgerel Ayurzana, **Bumduuren Pumbuurei, ***Hiesik Kim * Department of Computer Engineering, CSMS, MUST, Ulaanbaatar, Mongolia ** Department of Computer Engineering, CSMS,MUST,Ulaanbaatar, Mongolia *** Department of Electrical and Computer Engineering, University of Seoul, Seoul,Korea.