Secure User Authentication by using Biometric and Keystroke in Cloud

Sagar Shankarrao Dake Hemanta kumar Mohanta Yechuri Durga Prasad

ABSTRACT
In last few years the data usage from internet has been increased at very high rate. The adaption of cloud in business organizations increased exponentially. But unfortunately the attacks on that data and transactions are also increasing. As the every authorized user has their own username and password to access their personal accounts, but as these details can be misused by an authorized user so there is a requirement of additional authentication step. The combination of keystroke biometric, voice authentication and cryptography is more efficient to authenticate the user and provide more security. Keystroke biometrics is based on the assumption the typing pattern of each user is unique and cryptography in use to secure the password. By using voice authentication password will reset. In this paper, looking forward at several processes for keystroke biometrics to enhance user authentication. The objective is to collect a keystroke-dynamics dataset, to develop a repeatable evaluation procedure, and to measure the performance of a range of detectors so that the results can be compared more accurately. The database is used to degree of variance of the user and to detect the authorization of the user.

Keywords
Biometric, cryptography, voice authentication, ZCR, MFCC, DTW

1. INTRODUCTION
In early days Biometric is the most secure and convenient authentication process. The password authentication is most important to detect correct person and correct place. The Biometric can't be borrowed, stolen or forgotten and forging one is practically impossible the security field uses three different type of authentication,[6],[1]

1) You know your password, PIN.

2) Something you have a card key, smart card or token.

3) Something you know biometric.

But in early days the hacking will be done easily by the hackers. They will easily hack your ID by using your ID IP, and session etc. In the physical biometric include finger print, hand or palm geometry and retina; iris or facial character behavior character includes signature, voice, keystroke pattern and gain. These all type of security are used for the security purpose. Neurophysiologic factor make written signature unique per person. These factors are also expected to make typing per person. By hackers the biometric method hacking are easier than the keystroke dynamic method the keystroke have based on behavior of typing keys. In early days virtual keyboards are used in banks authentication and personal laptop, it's take lot of time by user to find the special keys etc.[2]

The keystroke are require the software and hardware and keyboard are need to input using keyboard it can check the human typing password behavior, what shortcut keys, special keys, character used by user. These are thing are different in every human and these behavior used to achieve a particular result in authentication performance of keystroke dynamic is depend on what type of keyboard is used by user.

2. KEYSTROKE DYNAMIC FEATURES
These are several features which can be used to user process on keyboard [9],[3]

1) Pressing time (Key will held down)

2) Releasing time (Key will held up)

3) Latency between two key pressing and releasing.

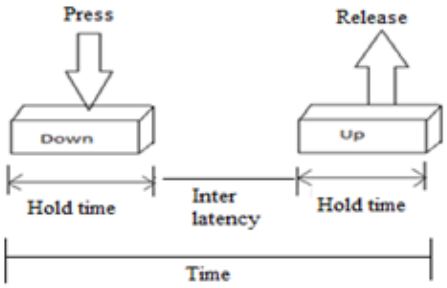

Figure 1

3. RELATED WORK
3.1 Voice: [5] In early days continued rise of identity theft and also the desire by companies to securely help customer's access information as rapidly as possible, "voice biometrics" has emerged as a way to answer these challenges and secure data. Voice biometrics can be used alone to provide a convenient method of authentication or as part of a two-factor authentication process, combined with something the customer "knows" (like a password or keystroke) to provide an extra layer of security for sensitive information and financial transactions.

Accuracy of Voice Authentication: The Accuracy of Voice Authentication is very important for several factors. The major difference of telephone and voice authentication, like enrolling with a home telephone and then trying to authenticate on a cell phone can be enough of a difference to cause a false rejection. Because of background noise, illness, and vocal changes from age can all affect accuracy

Accuracy of biometrics is measured in three categories:[7]
1. Failure to enroll – user's registration into the system is not successful
2. False acceptance –user is authenticated when she should not be
3. False rejection –user is not authenticated when she should be

3.1.1 Methodology:

End Point Detection

When there is an input voice signal, the initial step is to detect the beginning and ending point of the vocal signal. The reason of this process is to remove the silence sound such that the processing is only focusing on the main part of the sound. For this system, the end point detection algorithm will be using the zero-crossing rate, ZCR based algorithm. The ZCR is known as the number of times the sound sequence change its sign per frame and it is given as

$$z(n) = \frac{1}{2}\sum_{m=1}^{n} sgn[x(m+1)] - sgn[x(m)]$$

Where:

$$sgn[x(m)] = \begin{cases} +1 & x(m \geq 0) \\ -1 & x(m < 0) \end{cases}$$

This ZCR method is used in order to count the frequent of the signal that crosses over the zero axes. It is a very useful method for detecting the occurrence of silence sound.

3.1.2 Feature Extraction [8][10]

For the feature extraction section, the used algorithm is Calculating the Mel-Frequency Cepstral Coefficients (MFCC).The aim of this feature extraction process is to obtain a new voice representation which is more compact, less redundant, and more suitable for statistical modeling. The MFCC is based on the known variation of the human ear's critical bandwidths with frequency, where it filters the space linearly at low frequencies and logarithmically at high frequencies. It is used in order to capture the phonetically important characteristics of the voice. There are several steps in order to implement the MFCC as shown in the Figure 2

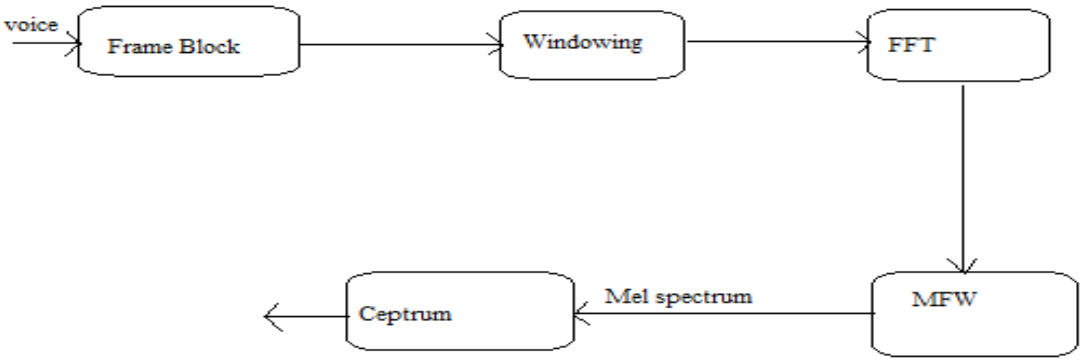

Figure 2 Computation of Mel Frequncy Cepstral Coefficients (MFCC)

3.1.2.1 Process A: Frame Blocking

The framing process is firstly applied to the voice signal of the producer. This signal is partitioned or blocked into *N* segments (frames).

3.1.2.2 Process B: Windowing

The second process of the processing is to window each of the individual frame such to minimize the signal discontinuities at the beginning and end of each frame.

3.1.2.3 Process C: Fast Fourier transform

The next process is the Fast Fourier Transform (FFT) Where each frame of *N* samples is converted from time domain to frequency domain.

3.1.2.4 Process D: Mel-Frequency Wrapping

The obtained spectrum from the FFT process is then Mel Frequency Wrapped. The major aim of this process is to convert the frequency spectrum to the Mel spectrum.

3.1.2.5 Process E: Cepstrum

In the final process, the log Mel spectrum is then converted back to time domain and the result is called the Mel frequency Cepstrum Coefficients (MFCC).

3.1.3Pattern Classification

After the feature extraction process, the next process is Matching two signals in order to undergo the verification Process. However, the voice input signal may be vary in term of speed or time when compare with the reference voice Signal. Therefore, these two signals must be aligned in order to get the optimal match between them. This process is called as the Dynamic Time Warping (DTW) algorithm.

3.2 Cryptography [12] is the practice and study of techniques for secure communication in the presence of third parties. It is about constructing and analyzing protocol that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.[13]

One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. When you consider the millions of electronic messages that traverse the Internet each day, it is easy to see how a well-placed network sniffer might capture a wealth of information that users would not like to have disclosed to unintended readers. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture. Encryption is the process of translating information from its original form (called plaintext) into an encoded, incomprehensible form (called cipher text). Decryption refers to the process of taking cipher text and translating it back into plaintext. Any type of data may be encrypted, including digitized images and sounds.

Cryptography secures information by protecting its confidentiality. Cryptography can also be used to protect information about the integrity and authenticity of data. For example, checksums are often used to verify the integrity of a block of information. A checksum, which is a number calculated from the contents of a file, can be used to determine if the contents are correct. An intruder, however, may be able to forge the checksum after modifying the block of information. Unless the checksum is protected, such modification might not be detected. Cryptographic checksums (also called message digests) help prevent undetected modification of information by encrypting the checksum in a way that makes the checksum unique. [14] The authenticity of data can be protected in a similar way. For example, to transmit information to a colleague by E-mail, the sender the information to protect its confidentiality and then attaches an encrypted digital signature to the message. When the colleague receives the message, he or she checks the origin of the message by using a key to verify the sender's digital signature and decrypts the information using the corresponding decryption key.[4] To protect against the chance of intruders modifying or forging the information in transit, digital signatures are formed by encrypting a combination of a checksum of the information and the author's unique private key. A side effect of such authentication is the concept of nonrepudiation. A person who places their cryptographic digital signature on an electronic document cannot later claim that they did not sign it, since in theory they are the only one who could have created the correct signature. Current laws in several countries, including the United States, restrict cryptographic technology from export or import across national borders. In the era of the Internet, it is particularly important to be aware of all applicable local and foreign regulations governing the use of cryptography.

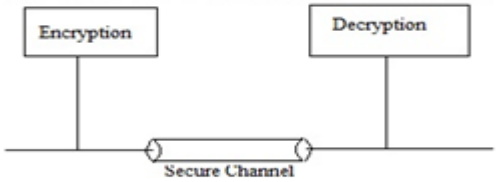

Fig. 3

4. ALGORITHM CRYPTOGRAPHIC EFFICIENTES

4.1 Feistel Networks

O Data Encryption Standard (DES) was developed by Feistel (1973), for IBM and initially called Lucifer, and was transformed into the official standard for digital security of theUnited States in 1977, being used on a large scale by computer networks. The cryptographic scheme model used by the DES is called Feistel Network, and is adopted by many other ciphers. In a Feistel network input data *X*i of size n is divided into two or more parts, *Ei*and *Di*. Then the right side *Di* is altered according to a function *F* (Feistel function), that may be defined by.[15][11]

F:{0,1}$n/2$ X {0,1}k ® {0,1}$n/2$

Where {0,1}k is the sub-key *Ki* to be applied in that round. The result of the function *F* is then combined with the exclusive OR operation or ⊕symbol XOR with the left half*Li*, that becomes part of the next round *Ri+1*, *Ri*p art and the part *Li+1* of the next round, forming the end *Xi+1*. The equation that represents this scheme is given by.

$$X_{i+1} = \begin{cases} R_{i+1} = L_i \oplus F(R_i, K_i), \\ L_{i+1} = R_i \\ where\ R_i = msb_{n/2}(X_i) \ominus L = lsb_{n/2}(X_i) \end{cases}$$

The decryption scheme is similar to, not needing to invert the function *F*, has to only perform the operation in reverse order, as represented.

$$X_{i-1} = \begin{cases} L_{i-1} = R_i \oplus F(L_i, K_i), \\ R_{i-1} = L_i \end{cases}$$

4.2 Advanced Encryption Standard

The AES (Advanced Encryption Standard) is the algorithm chosen by the U.S. government to protect data exchanged digitally. Formerly known as Rijndael, you may use keys of 128, 192 and 256 bits. The key used has size of 128 bits. The algorithm considers groups of 16 bytes to be a *state*, that in other terms is simply a 4x4 matrix with each element being a byte. From then performs four basic operations: **AddRoundKey**: Each byte of the state is combined with a byte key by operating Bitwise X-OR (Exclusive OR).**SubBytes**: A nonlinear substitution where each byte is replaced by another according to a lookup table. **ShiftRows**: The bytes of each row undergo a cyclic shift by a given number of steps. **MixColumns**: Each column of the state A(x) is combined according to a known matrix C(x) 4x4, which multiplied by columns of the state returns a new column to the resulting state B(x). The operation is invertible, simply multiply the columns of the state B(x) by a matrix D(x), the result is the state A(x).The security of the AES algorithm is still strong, but not unquestionable. There are several attempted attacks partially successful run in weakened AES versions. An attack is considered effective when the number of operations executed to break the security to discover the key is smaller than the number of possible keys. For the AES with 256-bit keys, the algorithm with up to 11 rounds have been broken with good efficiency.

5. PROPOSED MODEL

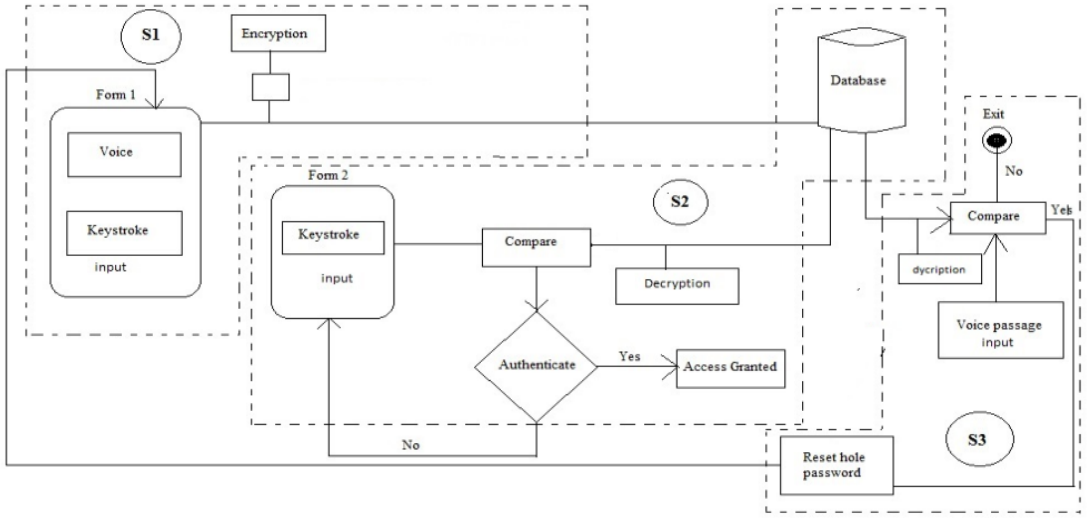

Figure 4

5.1 Description of Proposed Model:

STAGE 1:
CLIENT:
1) INPUT (TYPING SPEED, VOICE)
2) ENCRYPT (INPUT)
3) SEND-CLOUD SERVER

SERVER:
1) STORE INPUT (DATABASE)
STAGE 2:
AUTHENTICATION:

1) INPUT KEY(TIME);
2) RETRIVE INFORMATION FROM DATABASE DECRYPT INFORMATION
3) IF(YPING SPEED 1 = TYPING SPEED 2) LOGIN USER AUTHENTICATION
4) ELSE
Return step 1.
For (int i; i++; i<3);

ELSE GOTO stage 3

STAGE 3:
RESET PASSWORD
1) INPUT (VOICE)
2) RETRIVE INFORMATION FROM DATABASE DECRYPT INFORMATION
3) COMPARE (VOICE 2 = VOICE 1)
4) IF YES
5) RESET PASSWORD
6) ELSE EXIT

5.2 Description of stages

Stage 1:
In proposed model there are mainly three model s1, s2.s3. In s1 model the form1 used. In
Stage 1 first of all user will read the one paragraph (with clear voice, no illness, no distribution voice) then after that the user will type the user password with four times then this typing speed biometric will encrypt data by using AES algorithm and then it will store in cloud storage.

Stage 2:
In stage 2 there is use second form 2 to taking input as user authentication. The user will type his/her own password with same speed and then it will pass data to compare model, in this it will compare your input data and cloud storage database, if both are same equal to each other than user are granted to access, or else it will move to form 2 module to type again password

Stage 3:
Stage 3 is final; stage in this it will reset your whole password with your biometric voice authentication. If voice 1 and voice 2 is match then it will move to form 1 to enter new voice and keystroke else it will exit from window.

6. CONCLUSION:

The proposed work is described theoretically for secure authentication in cloud network and client server model. The encryption algorithm can ensure safe communication by encrypting and decryption module of network. In this paper, AES encryption algorithm is embedded in the drive program to encrypt and decrypt the initial key. In this paper voice authentication is used for password recovery, and keystroke dynamic for password authentication.

7. REFERENCES

[1] Yekta Said Can, FatihAlagöz, BilgisayarMühendisli˘giBölümüBo˘gaziçiÜniversitesi˙Istanbul, Türkiye.”Tu¸slaraBasmaDinamikleriKullanılarakKullanıcıTanımlama User Identification Using Keystroke Dynamics”

[2] Sally DafaallahAbualgasim, Izzeldin Osman, “An Application of the Keystroke Dynamic Biometric for Securing PINs and Passwords,” World of Computer Science and Information Technology Journal(WCSIT) Vol 1, No 9,398-404, 2011

[3] D. Shanmugapriya, DR. G. Padmavathi, “Virtual Key Force- A New Feature For eystroke,” International Journal Of Engineering Science And Technology(IJEST) Vol.3, No.10 October 2012

[4] MaximilianoBertacchini, Carlos E. Benitez and Pablo I.Fierens, "User Clustering Based On Keystroke Dynamics,"CongresoArgentino De Ciencias De La Computación CACIC2010-XVI

[5] Che Yong Yeo, S.A.R. Al-Haddad, Chee Kyun Ng Department of Computer & Communication. Faculty of Engineering, University Putra Malaysia, "Animal voice recognition for identification detect

[6] Luciano Bello, MaximilianoBertacchini, Carlos Benitez, Juan Carlos Pizzoni and Marcelo Cipriano, " Collection And Publication of a Fixed Text Keystroke Dynamics Dataset,"

[7] Edmond Lau, Xia Liu, Chen Xiao, and Xiao Yu, "Enhanced User Authentication Through Keystroke Biometrics,"International conference on biometrics dec 9, 2004

[8] Fabian Monrsone, Aviel D. Rubin, "keystroke dynamics as a biometrics for authentication," preprint submitted to ElservierPreprinter march1,2000

[9] N. S. Behbahan and Z. Musavinasab, "Design And Implementation An Identification System Based On Typing Rhythm On Keyboard",International Journal of Advanced Research in IT and Engineering, vol. 2,no. 11 ,pp. 54-65, November 2013.

[10] Kevin S. Killourhy and Roy A. Maxion. "Comparing Anomaly Detectors for Keystroke Dynamics," in Proceedings of the 39th Annual International Conference on Dependable Systems and Networks (DSN-2009), pages 125-134, Estoril, Lisbon, Portugal, June 29-July 2, 2009. IEEE Computer Society Press, Los Alamitos, California, 2009.

[11] Rybnik, M.; Panasiuk, P.; Saeed, K., "User Authentication with Keystroke Dynamics Using Fixed Text," Biometrics and Kansei Engineering, 2009. ICBAKE 2009. International Conference on , vol., no., pp.70,75, 25-28June 2009.

[12] Rybnik, M.; Tabedzki, M.; Saeed, K., "A Keystroke Dynamics Based System for User Identification," Computer Information Systems and Industrial Management Applications, 2008. CISIM '08. 7th , vol., no., pp.225,230, 26-28 June 2008.

[13] Stephen M. Stigler, "Thomas Bayes' Bayesian Inference," Journal of the Royal Statistical Society, Series A, 145, 1982, pp. 250–258.

[14] Coppersmith, D., S. J. Hong, and J. R. M. Hosking. "Partitioning Nominal Attributes in Decision Trees." Data Mining and Knowledge Discovery, Vol. 3, 1999, pp. 197–217.

[15] Rodrigo s semente, Andres O. Salazar "Cryseed an automatic 8-bit cryptographic Algorithm developed with genetic programming"