International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 12, Number 12 (2019), pp. 2240-2245

Brain Signals Authentication on Cloud Computing

M. A. HADI[1], HANY S. ELNASHAR[2]

[1] Information Technology, Faculty of Computer and Information Systems, Princess Nourah bint Abdulrahman University, Riyadh, KSA.

[1]Cairo Higher Institute of Engineering and Computer Science, New Cairo, Egypt.

[2] Faculty of Computers and Artificial Intelligent, Beni-Suef University, Beni Suef, Egypt.

Abstract:

Recently, many organizations are using automated person Identification to rise their client needs. As Identifications are important in personal recognition process to promote the operating levels of their assets. Personal recognition scheme is a broad system used in deciding that an individual is utilizing their services. Thus, brain signals, electrical fields produced by the brain using Electroencephalogram (EEG), are used to as an approach of this recognition and, which serves as a type of cognitive Biometric. The advantage of both is popular, although a cloud provider provides them as a service

Keyword: Brain Signals, Cloud computing, Identification, Biometric.

I. INTRODUCTION

Biometric user authentication has received attention in recent years due to its protection and security. There are many types of characteristics, conventional and cognitive biometrics Conventional has physiological and behavioral characteristics, Physiological means the way the individual, and behavioral means the way the conduct. Cognitive is psychological brain states hence it measure the brain signal directly or indirectly

Recognition systems are categorized into three types first is Knowledge Approach that shows “what you know” like numbers, names, and Password, second is Token approaches that show “what you have” like cards, Passport; previous approaches mentioned can be lost at any time [1]; third is Biometric that show “who you are” like Fingerprint and iris recognition. A Biometric is a biological feature and alternative of traditional authentication approaches. It cannot be stolen or lost because it depends on physiological or behavioral features. Hence, the present paper presents a brain signals as a Biometric attribute. Author name used brain waves as a cognitive biometric attribute for recognition system.[2]. They also have signals that can read and measure each person' status. These signals follow the body actions, then measure the neurons electrical activity, finally record it through EGG [3]. Now, cloud computing security issues are solved by combining the biometric technology to a cloud computing platform that will merge the cloud computing security objectives such as: availability, authentication, accountability, confidentiality, integrity, portability, with the accuracy of biometric systems. Consequently, biometric technology is skilled to take care of issues identified with the present age of cloud computing technology. In any case, moving biometric technology to the cloud computing security is an entangled errand. Researchers and developers who endeavoring to handle this errand need to know about [4, 5]: This research paper attempts to examine the above security issues and give dynamic scientists and designers with some vital rules on the best way to move biometric technology to a cloud computing stage as a novel security benefit. The paper portrays the most widely recognized security issues that confronting the advancement work and gives new bearing for staying away from them. Moreover, it provides a case study on employing biometric user authentication in the cloud. as a result of cloud computing security and biometric application development the paper suggest use brain signal as attribute for authentication. The rest of the paper is organized as follows. Section two presents some basic characteristics of cloud computing. Section three introduces issues related to authentication in cloud computing, in addition to brain signals, feature, and classification. Section 4 handles the proposed approach for brain signals authentication as a cloud computing service. Finally, the paper is concluded in section 6

II. CLOUD COMPUTING ARCHITECTURE

Much research in recent years has focused on the use of cloud computing, the fifth generation of network engineering in information technology. It is a highly successful model of service-oriented computing and has led to the development of the use and management of computing infrastructure. It is a model of hosting resources and providing consumers with services. It provides convenient on-demand access to a central shared store of computing resources that can be used at the lowest administrative cost and with high efficiency. Cloud computing relies on the use of WAN as a supported Internet communications medium to deliver IT resources to its users on a pay as you go basis [6] . Cloud computing has been defined in different methods. In this paper, the definition was selected by the National Institute of Standards and Technology (NIST) [7]. As defined by NIST, the cloud model promotes availability and consists of five key features that provide (1) availability and reliability, (2) high scalability and flexibility, (3) management and interoperability, (4) performance and optimization, and (5) accessibility and portability. The architecture of cloud computing consists of three service layers

named: Software as a Service (SaaS); Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The models in cloud computing is designed of five buildings: platforms, infrastructure, customers, applications, and servers. McKendrick J. Priyanka Chauhan [8, 9] current clouds are as follows:

1. Community cloud: one or additional organizations could manage the cloud manage the cloud infrastructure that is provided for specific use by its specific community of consumer that have shared concerns (e.g., mission, security necessities, policy, and compliance concerns
2. Private cloud: a specific organization manages the cloud infrastructure which is used privately by its multiple users.
3. Hybrid cloud: The cloud infrastructure includes two or more cloud infrastructures.
4. Public cloud: a service provider manages and operates the cloud infrastructure which is provided for the general public.

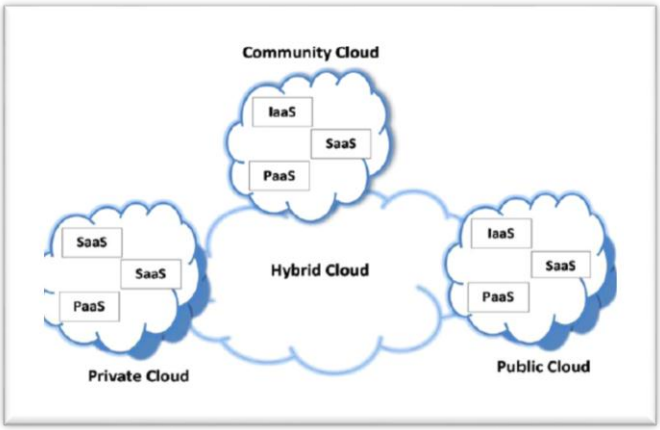

Fig.1. The distribution of cloud models and infrastructures

In Figure 1, cloud deployment models are shown together. Cloud computing providers offer previous cloud services as pay-per-use. As such, the use of servers, storage, processing, databases, and all resources, is provided to customers by the provider. These services are provided through contracts in the form of Service Level Agreements (SLA). SLA provides and determines the level of service and quality required by the organization.

III. AUTHENTICATION SECURITY IN CLOUD

Security in cloud computing is important in developing cloud-based systems, especially in building cloud services. Research shows that "security" is one of the five main issues, namely, cloud security. These problems arise because client data, information, and software are stored on cloud service provider servers [10]. In general, cloud security defines the following important objectives:

- Confidentiality: Make cloud systems available only to qualified individuals and only user data can access them.
- Authentication: Ensure individual identity in web communication.
- Integrity: The accuracy and consistency of the stored data that ensures the data as it is processed over the cloud, however, has not been altered by cloud-based systems.
- Availability: Always make services available to users anytime, anywhere.
- Accountability: Cloud computing systems to calculate their activities, accept responsibility for them, and disclose results in a transparent manner.

There is a need to easily use specific security technologies and services to achieve the above objectives. Security technology can be introduced as a process aimed at exploring or preventing a security attack, while a security service can be defined as a process aimed at enhancing the security of data and information. These services are assets in the face of security attacks, using one or more security technologies to achieve their objectives [11]. Security is the most regulated view of any kind of computing, making it obvious that security concerns are urgent for cloud computing as well. Because both sensitive data retain the end of each client as well as in cloud servers, identity management and authentication are important in cloud computing [12]. Verifying qualified users is a very important part of cloud security concerns, as violating these areas can result in undiscovered security rupture. Cloud computing may track different results and difficulties imaginable throughout. One, security is seen as a key to the progress of cloud computing. The challenges of cloud security are dynamic and large data localization is an important goal in the level of cloud computing security [13]. Regarding the security of customers' personal or business data, the strategic policies of cloud providers are of paramount importance [14]

IV. BRAIN SIGNALS, FEATURE, AND CLASSIFICATION

Electroencephalogram (EEG) is electrical induced signals from the human brain. EEG recordings are known as cheap and relatively easy devices. Thus, electrodes are placed in the setting surface that restricts the number of electrodes present in the entire scalp [15]. 5 frequency can be recorded by measuring the electrical activity of neurons. EEG is the brain activity that results from performing mental activities such as deep sleep, relaxation, moving reading, spelling, etc.

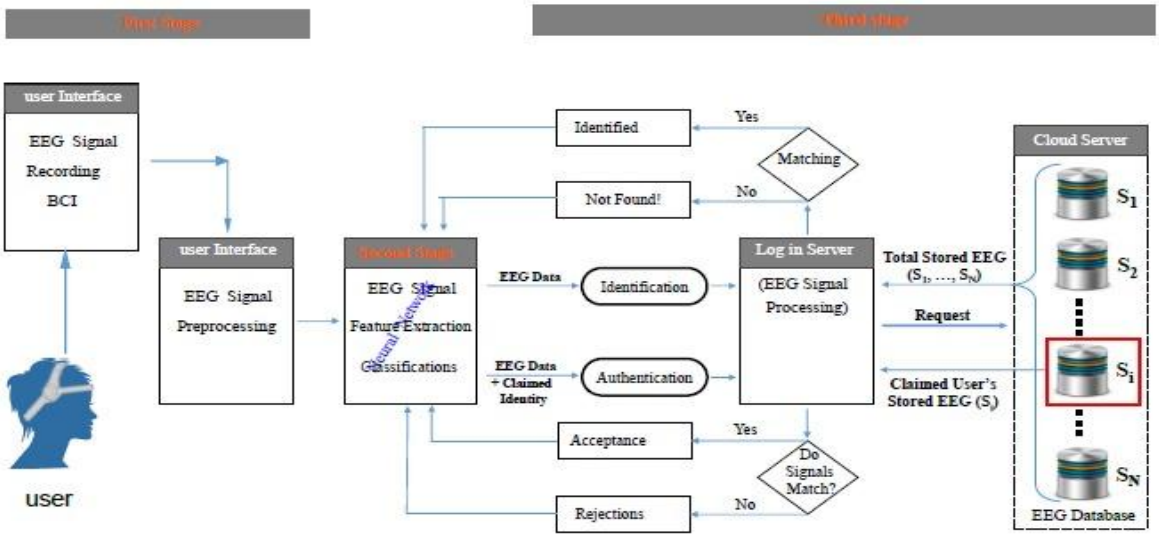

Fig.2. Brain signals recording and usability of Brain signal

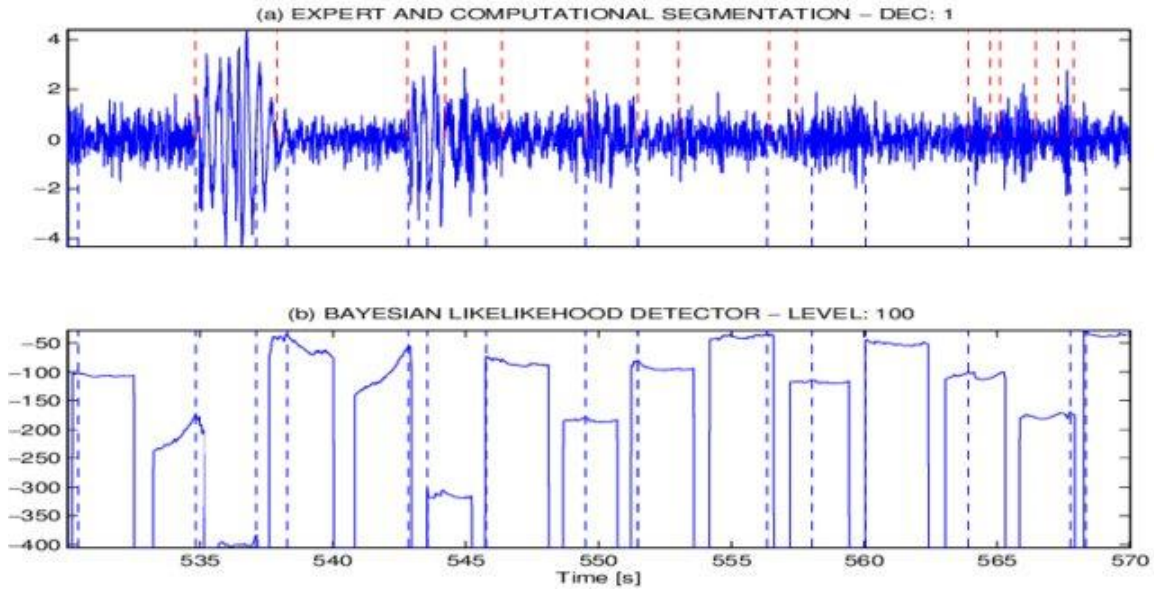

Fig. 3 Signal pattern presenting (a) segment by an experts (red) and by a Bayesian form of change-point detection (blue) and (b) a probability to detect change-points [29]

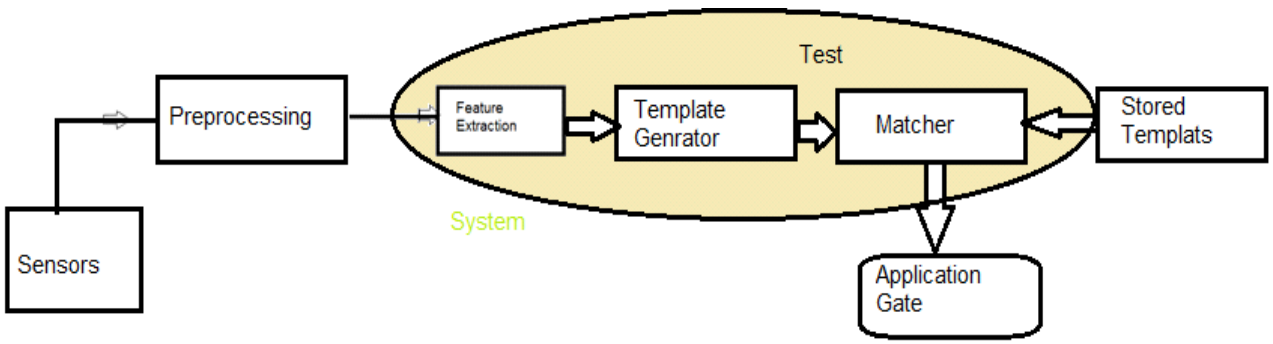

Fig.4: General System

The recorded EEG signals have 5 frequency elements: [0.5 - 4 Hz] called delta, [4-8 Hz] as theta, [8-14 Hz] as alpha, [14-30 Hz] as beta, and [> 30 Hz]] As gamma [16]. Delta and theta are slow, but beta and gamma are effective. Brain signals recorded by the pre-processing of the EEG signal indicate that the raw data is provided for further signal analysis and removal characteristics. These preparations are compromised: band pass filtering, baseline removal, mobility, artifact removal, and finally enhanced useful EEG data using independent component analysis [17]. EEG data to show that part of the tens values signals for the delta component frequency band (0: 5 to 4Hz) particularly satisfies user identification with a high accurate value.

Data sets:

The data was collected from four people (2 male, 2 female) for 60 seconds per state - relaxed, concentrating, and neutral. We used a Muse EEG headband which recorded the TP9, AF7, AF8 and TP10 EEG placements via dry electrodes [18][19].

A. Feature Extraction:

Time-based analysis, frequency-based analysis, time-frequency analysis, time-space frequency analysis, and wavelet transformation are all used to extract features from brain waves [18]. The wavelet converter is used to transfer a signal to a different shape, displaying the hidden properties in the original signal. It is also a small, oscillating wave that resembles time-focused energy; thus, changing window sizes enable the analysis of different frequency components in the form of a signal 3.

B. Classification

The neural network (NN) was defined for the measurement network of biological neurons. Currently, ANN usually refers to artificial neural networks (ANN) that are artificial neurons or nodes. This biological neural network consists of real biological neurons functionally linked to the nervous system. In neuroscience, they are often known as groups of neurons that perform a certain physiological function in laboratory analysis. In addition, ANN consists of interconnected synthetic neurons used to understand biological neural networks [20], or to solve artificial intelligence problems that do not need to build a model for a real ecosystem. Now, synthetic neuron networks, trained using an algorithm called posterior diffusion, are used to classify extracted EEG features. The process that binds each element of a given group with one or more elements of a second set domain is said to be set to f, where f is obtained from the training set T.

V. THE PROPOSED APPROACH

Develop the tools used to lock / unlock the screen. Named the authentication system. Starting from, the locked screen and the user's brain signals are recorded for two mental tasks and stored as reference data through training can be called the training phase.

When the screen is locked, the user's brain waves are recorded again and matched with the previously stored sample. If there is a match, the screen will be unlocked, or it will remain closed.

The prototype of the work is described as follows:

A. Training System:

The brain waves are recorded to the user when he performs mental tasks such as meditation and math activity.

B. Extract Feature:

The spectral power of the channel is calculated in the alpha, beta and gamma spectral bands for both mental tasks. Feature reduction technology is implemented to reduce the dimension of features.

C. Create a user profile:

These features are stored in a separate file as a user profile.

D.. Documentation:

A person's brain waves are recorded in real time for the same set of activities as in training, from which we extract features. Reduce the feature compared to previously stored features.

E. methodology

The biometric system includes two basic modes of operation. Verification and verification, first performs a comparison between the captured feature and a sample stored in a biometric database to verify that the person is an authenticated person. Three steps involved in this process.

- Database reference samples
- Samples are matched with reference samples to obtain scores of matching factors and calculate threshold value
- Inspection step: Use the ID number to indicate which template should be used for comparison.

Identification mode performs a comparison against a sample database, to verify identity. If comparing the biometric sample with the template in the database falls within a predefined threshold value, the system will succeed in identifying the individual. Figure 3 includes some changes in Figure 1 to be a generic identification system

VI. EXPERIMENTAL AND DATA ANALYSIS

EEG signals are often contaminated with the at least 50Hz line frequency interference, light fluorescents and other environmental which are recorded by the electrodes and acquisition system. They are separated in several channels of EEG and can make a mistake in the analysis of the record. So, it is necessary to begin line noise filtrations to attenuate artefacts of EEG signals using 60 HZ filter. Next, the EOG artefacts are removed from the signals by independent component analysis (ICA), using a method presented in [21].

a. PROPOSED METHODS

Perform this process from data in IV:

- Store data for authenticated person
- Read new persons say subject1 from dataset
- Run system
- Get system output
- Authenticated subject: matched
- Unauthenticated Subject: look the service

VII. CONCLUSION

This paper presents how the brain is used to identify the user. Biometrics are a valid means of identification, and depend on the behavioral or physiological features of a person. Therefore, Brain Biometric provides the highest degree of recognition, because Brain has enormous properties (discrimination, authenticity of deceptive attacks, unique identification and non-repetition of signals produced) in biometrics to enhance different safety levels and more reliable than other biotechnologies. The NN rating was run on EEG data for healthy people, and now the current method has met the correct grading scores from 97% to 100%. The results in the same line of relevant research show that EEG carries specific and unique information, as well as give a high degree of identification and recognition.

ACKNOWLEDGEMENT

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

REFERENCE

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition 1," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, 2004.

[2] V. Štruc and J. Žganec Recognition Technology for Biometrics service," in: pp. 68-75, 2012.

[3] J. Bule and P. Peer, "Fingerprint Verification as a Service in KC CLASS," in: 2012, pp. 76-82, 2012.

[4] Rakhshanda B., Ghazal N. Abdulhaq K., "Biometric Authentication in Cloud Computing". International Journal of Computer Applications (0975 – 8887). Volume 129 – No.11, November, 2015

[5] K.-S. W. and M.-H. Kim, "TOWARDS BIOMETRIC-BASED AUTHENTICATION FOR CLOUD COMPUTING," in 2nd International Conference on Cloud Computing and Services Science, p. pages 501–510. "http://v1.wcsit.org/media/pub/2015/vol.5.no.2/Secu

[6] Jain, P.; Rane, D.; Patidar, S. A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. In Proceedings of the 2011 World Congress on Information and Communication Technologies (WICT), Mumbai, India, 11–14 December 2011; pp. 456–461.

[7] Gowrigolla, B.; Sivaji, S.; Masillamani, M.R. Design and auditing of cloud computing security. In Proceedings of the 2010 5th International Conference on Information and Automation for Sustainability (ICIAFs), Colombo, Sri Lanka, 17–19 December 2010; pp. 292–297

[8] McKendrick J., (2011), "Loud Divide: Senior Executives Want Cloud, Security and IT Managers are Nervous", [Accessed 15-12-2017]:http://www.zdnet.com/ blog/ serviceoriented/ cloud-divide-senior-executives-want-cloud-security-and-it-managers-are-nervous/6484

[9] Priyanka Chouhan, Rajendra Singh. "Security Attacks on Cloud Computing With Possible Solution", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, ISSN: 2277 128X. January 2016.

[10] Rashmi, G. Sahoo, and Mehfuz, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions," Int. J. Cloud Comput. Serv. Archit., vol. 3, no. 4, 2013.

[11] S. T. Krishna, "Cloud Computing : A Cloud Security Issues," vol. 3, no. 2, pp. 67–75, 2015.

[12] A. Joint and E. Baker, "Knowing the past to understand the present," Comput. Law Secur. Rev., vol. 27, no. 4, pp. 407–415, 2011.

[13] M. H. ; Hany Elnashar, "CLASSIFICATION OF EEG SIGNALS USING FUZZY DEMPSTER," Int. J. Adv. Sci. Eng. Technol., vol. 5, no. 2, pp. 20–23, 2017.

[14] N. Elsayed, Z. S. Zaghloul, and M. Bayoumi, "Brain Computer Interface: EEG Signal Preprocessing Issues and Solutions," Int. J. Comput. Appl., vol. 169, no. 3, pp. 975–8887, 2017.

[15] G. Geetha and S. N. Geethalakshmi, "Artifact removal from EEG using spatially constrained independent component analysis and wavelet denoising with Otsu's thresholding technique," Procedia Eng., vol. 30, no. 2011, pp. 1064–1071, 2012.

[16] C. E. M. Kumar and S. V. D. Kumar, "Wavelet Based Feature Extraction Scheme of

Electroencephalogram," Int. J. Innov. Res. Sci. Eng. Technol., vol. 3, no. 1, pp. 908–913, 2014.

[17] M. Nandish, S. Michahial, H. K. P, and F. Ahmed, "Feature Extraction and Classification of EEG Signal Using Neural Network Based Techniques," Int. J. Eng. Innov. Technol., vol. 2, no. 4, pp. 1–5, 2012.

[18] J. J. Bird, L. J. Manso, E. P. Ribiero, A. Ekart, and D. R. Faria, "A study on mental state classification using eeg-based brain-machine interface,"in 9th International Conference on Intelligent Systems, IEEE, 2018.

[19] J. J. Bird, A. Ekart, C. D. Buckingham, and D. R. Faria, "Mental emotional sentiment classification with an eeg-based brain-machine interface," in The International Conference on Digital Image and Signal Processing (DISP'19), Springer, 2019.

[20] C. Republic, N. Caregroup, and C. Republic, "Wavelet Transform Use for Feature Extraction and EEG Signal Segments Classification," pp. 1–4.

[21] S. Duer, K. Zajkowski. Taking decisions in the expert intelligent system to support maintenance of a technical object on the basis information from an artificial neural network. Neural Computing & Applications 23(7), 2185-2197 (2013).