"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST / DOAJ / DRJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Crossref /
Academic Keys / ROAD Open Access / OAJI / Academic Resources / Scientific Indexing Services / SCIPIO

BIOMETRIC MULTI-FACTOR AUTHENTICATION SCHEME IN CLOUD COMPUTING

Violeta N. OPRIS[1]
Sergiu EFTIMIE[2]
Ciprian RACUCIU[3]
[1]Ph.D. Student The Military Technical Academy, Faculty of Military Electronic and Information Systems, Bucharest
[2]Ph.D. Student The Military Technical Academy, Faculty of Military Electronic and Information Systems, Bucharest
[3]Ph.D. Professor The Titu Maiorescu University, Computer Science Department, Bucharest

Abstract: *The biometric Multi-Factor authentication represents the next generation computing authentication infrastructure. This paper proposes a novel multi-factor authentication scheme based on biometrics concepts. Biometrics is a process used to identify or authenticate an individual's identity using any of a series of physical or behavior characteristics. Interconnecting biometric technologies with cloud infrastructure improves speed, secure communication, scalability, identity and access management, reliability, automation.*

Keywords: *biometric, Cloud computing, security, authentication methods, authorized user*

Introduction

The word "biometrics" comes from Greek:bio (life) and metric (to measure). The biometrics authentication refers to identification of humans by their characteristics or traits [1].
In 1870 Alphonse Bertillon developed "Bertillonge"(anthropometrics). This was a method for identifying individualsbased on detailed records of their body measurements, physical descriptions and photographs [2].
The biometrics systems offer essential benefits in the cyber space and improve the security mechanism.
A biometric identifier is a physiological or behavioral characteristic of the person.This technology represents a unique method for recognizing individuals [3]. The characteristic are shown in figure 1.
The physiological biometrics is based on measurements (fingerprint, iris-scan, facial recognition, hand geometry) and behavioral characteristics (signature-scan, keystroke-scan, voice recognition).

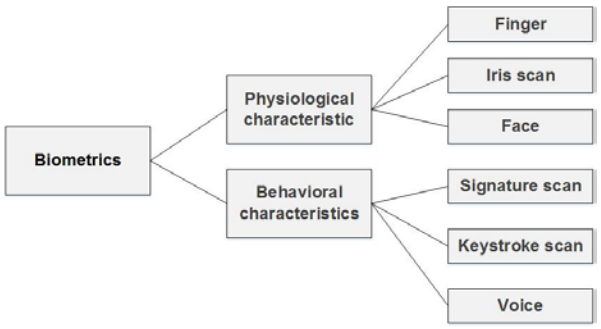

Figure 1.Physiological and behavioral characteristics

In recent years, many business, including many retailers and government agencies, have been testing different forms of biometrics.
This paper refers to interconnected biometric techniques and cloud computing for multi-factor authentication.
Cloud computing is described as a model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources [6]. Figure number two represents the NIST definition of cloud computing.

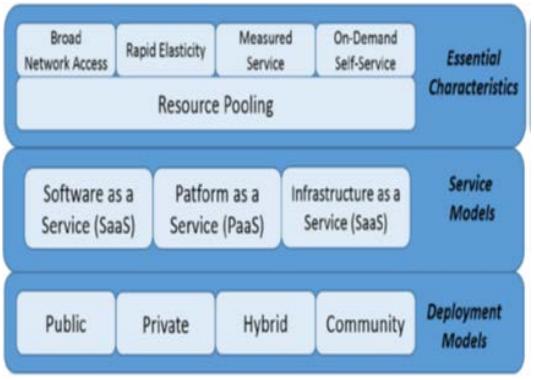

Figure 2. NIST- Cloud Computing

It provides three different service modals. Software as a Service (SaaS) that provide any software running on the cloud infrastructure.
In Platform as a Service (PaaS) capability provided to the consumer is to deploy anything onto the cloud infrastructure anything.
Infrastructure as a Service (IaaS) facilitates the user by providing storage, networks, and other

DOI: 10.21279/1454-864X-16-I1-079

fundamental computing resources where the consumer is able to deploy and run arbitrary.
Cloud computing is used for deployment modals: public, community, private and hybrid.
Currently, we are assisting a considerable evolution of the cloud computing architecture. It has been widely recognized as the next generation computing infrastructure.
Michael Dell (Chairman & CEO, Dell Inc., 2015) said that cloud computing is not a destination or a singular path, is a transformation that places IT squarely at the center of the enterprise [7].
Recently, the most important cloud vendors are: Amazon, Azure (Microsoft), Cisco Systems, Dell, Google, HP, IBM, Virtustream and Rackspace.
This paper is divided into four section. The first section represents an overview of biometric and cloud computing technology. The second section contains a review of current biometric. The third part presents the proposed multi-factor scheme, and in the fourthsections reveals the conclusions of the paper.

Review of current biometrics solutions

In this section there are emphasize the current solutions generated by the cloud computing architecture and biometrics from the last years.To know where we are going, it is necessary to look where we've come from.
Biometrics techniques are largely centered on face recognition, fingerprint scanning, face recognition, hand geometry and palm print scanning, iris scanning, voice recognition and signature recognition
In 1982, Francis Galton developed a classification system for fingerprints. The characteristics are still used today [2].
In 1975 FBI funded the development of scanners extracting technology.In 1988, the Lakewood Division of the Los Angeles County Sheriff's Department began using composite drawings of a suspect to conduct a database search of digitized mugshots [2].
Biometric technologies are already being implemented in a variety of systems. At Park Avenue Elementary School in the United States, students must first stare into a box before the doors of the school will open.
United States, Illionis was the first state that used face recognitions technology in its Department of Motor Vehicles (2011).
Diebold, a large producer of security software, has tested ATMs with iris scans, but banks have yet to adopt scanning because the systems were expensive and cameras too large for small ATMs (Hannah, 2005).
Pugazhenthi et al. (2013) describe a multiple biometric security in Cloud Computing. The paper proposes a new model of security system, users are to provide multiple biometric finger prints during Enrollment for a service [4].
An important current solution was proposed bySelvarani et al. (2015). This study presents a multi-modal bio-cryptographic authentication in cloud storage sharing for higher security, using fingerprint and Iris biometric technology.

The Multi-Factor authentication scheme

Building the cloud security Infrastucture with biometric technology will secure the data from unauthorized users.
In the virtualization space, the development of more authentication mechanism has becomea demand, especially when cloud computing technology is used.
This paper proposes interconnecting biometrics and cloud innovation, to take network users to the next level and improve the authentication mechanism.
As security is the main concern in using cloud computing fused biometric authentication techniques, which can be secure and reliable.
The article concentrates on a multi-factor scheme in cloud computing using biometrics authentication scheme. Theoretically, biometrics is a great way of authenticating a user.
The idea of this paper starts from Frong, Zhuang and Fister (2013). The authors describe an image-based, biometric authentication model for hand gestures captured by video recording [9].
The gestures serve as what the authors refer to as a "biometrics password" and provide context for biometric feature extraction and biometric matching based on the "hand shape and the postures in doing those signs" [10]. Figure three represents a biometric method for authentication.

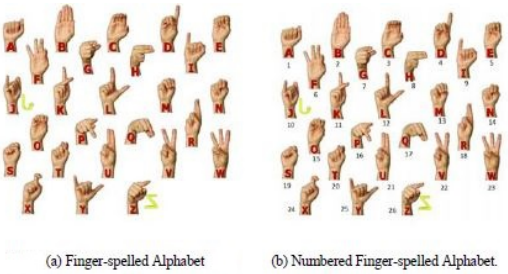

Figure 3. Gesture authentication [9]

The proposed multi-factor authentication scheme is centered on the iris scans, finger prints and gesture authentication in cloud computing, with three levels of security.
Iris scans are highly accurate and require low storage space. Iris scanning identifies the feature of the eye's iris. This is one of the most promising biometric tools.
A digital camera captures an image of the eye and registers unique patterns found in each person's

DOI: 10.21279/1454-864X-16-I1-079

iris. In the United States, iris scan technology is used at secure government installations and high-tech corporate headquarters.
In China, this biometric method is preferable than the fingerprint because customers feel that an iris scan is more sanitary.
Fingerprints have been used in forensics for more than a 100 years. This technology is incorporated into many firms as a payment mechanism or to verify employee attendance. In hospitals, it has been used to access control medicines and drugs.
The gesture method represents an innovative mechanism. This method is based on "sequence of hand sings". Those representing the letters "i", "l", " o", "v", "e", and "u" can be encoded as a series of gesture image and used to authenticate the claimed identity of the individual.
Figure fourshows the novel biometric multi-factor authentication scheme. The scheme is centered around of biometrics mechanism: iris scans, finger prints and gesture scans.
This mechanism secures authentication in the Cloud using three biometric level of security.

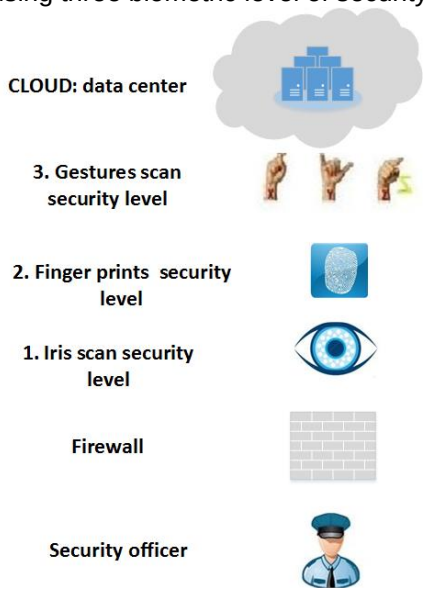

Figure 4. Biometric Multi-factor scheme

The first biometric level of security is iris scan, the second level is finger print and the last one is gesture scans.
The workflow of the scheme starts from the security officer and pass throwa firewall and three security levels for authentication in cloud.By interconnecting cloud with biometrics methods a security communication tunneling is obtained.
Biometrics increased security in cloud computing. The security officer enrolls with the biometrics characteristics provided by a cloud. Once the identity is registered, the biometric authentication details are stored in cloud service provider database.
The fourthsecurity level, gesture scan, represents a cryptographic method to achieving secure authentication. In the Fong, Zhuang, and Fister's model, each hand sign is associated with one character, a letter of the alphabet.

CONCLUSIONS

In this paper we have presented a novel multi-factor authentication scheme based on biometrics innovation for secure authentication in cloud.
The first part of the paper presents a descriptive introduction of the cloud computing and biometrics methods. The second part is a review of current solution, used by organizations.
The third part of the article represents the proposed multi-factor authentication scheme in cloud. This scheme presents innovative benefits, like on-demand secure communications, scalability, secure authentication, automation, identity and access management, efficient costs, high reliability, elasticity.
The result of this study can overcome some of the limitations of using a single biometric technology. The combination of those innovation secured data from unauthorized users in cloud environment.

DOI: 10.21279/1454-864X-16-I1-079

BIBLIOGRAPHY

[1] Vallabhu, H., Satyanaryana R. Biometric Authentication as a service on Cloud: Novel Solution. International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-4, September 2012.
[2] Biometrics History, http://www.biometrics.gov/
[3] Chakroborty, S., Bhattacharya, I., Chatterjee, A., A palmprint based biometric authentication system using dual tree complex wavelet transform, Measurement 46 (2013) 4179-4188
[4] Pugazhenthi, D.,Vidya,Sree., Multipe Biometric Security in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.
[5] Clodfelter, R., Biometrics technology in retailing: Will consumers accept fingerprint authentication?
[6] NIST- Cloud Computing, http://www.nist.gov/itl/cloud/
[7] Dell – Cloud Computing.http://www.dell.com/
[8] Hannah, J., 2005. Privacy concerns, expense keep biometrics put of US ATMs, Information Week October 12.
[9] Fong, S., Zhuang, Y., Fister, I.(2013) A biometric authentication model using hand gesture image. Biometrical engineering online, 12 (1), 111. Retrieved June 12, 2015, from http:// www.biometrical-engineering-online.com

DOI: 10.21279/1454-864X-16-I1-079