v. 2, n. 14, 2022

Journal of
Engineering
Research

CREATION OF DIGITAL SECURITY COMPONENTS FROM ELECTROENCEPHALOGIC SIGNALS

Javier Mascorro Pantoja
Department of systems and computing at the Technological Institute of Aguascalientes, Ags. Mexico

Ricardo Luna Carlos
Department of systems and computing at the Technological Institute of Aguascalientes, Ags. Mexico

Ilda Díaz Ramos
Department of systems and computing at the Technological Institute of Aguascalientes, Ags. Mexico

Miriam Malo Torres
Department of systems and computing at the Technological Institute of Aguascalientes, Ags. Mexico

David Rosas Vara
Department of systems and computing at the Technological Institute of Aguascalientes, Ags. Mexico

Durón De Luna Oscar Alejandro
Department of systems and computing at the Technological Institute of Aguascalientes, Ags. Mexico

Ramírez García Zabdi Zurisadai
Department of systems and computing at the Technological Institute of Aguascalientes, Ags. Mexico

Abstract: In a technological environment such as the current one, in which all daily digital tools are within the reach of a digital device, facilitating immediate access to information, various security tools in the area of information are implemented day by day based on in algorithms of various kinds, including both hardware and software tools; specifically, the tools of daily use such as: mail, social networks, education, banking applications allow the interconnection of multiple devices and thus have the availability of information in an interconnected manner, which implies a good level of aspects such as authentication and security management, key factors required to guarantee the availability, security and fidelity of information in an interconnected environment, promoting the creation of new security methods and paradigms.
Keywords: EEG(Electroencephalogram), Security, cryptography, Interconnection, Cloud.

INTRODUCCIÓN

On a daily basis, digital communications promote the immediate exchange of information between many people through mobile or portable devices, based on dimensionality to establish metrics of the interconnections between people and the information that is processed, recorded and stored; within the field of information technology[1], these applications are embedded within the contextual layers in the communication architecture, which is why events arise that can compromise information security at an abstraction level fuzzy logic in the cloud[2] that is vulnerable in certain sectors or applications, for which it is necessary that, directly to the growth of information and the means to communicate it, relevant tools and security measures with unique patterns are produced. Something basic in this area are the encryption tools and digital signatures, anticipating these situations that may present a risk to the confidentiality of the information and for which there would be a unique method such as the biometric pattern of a person at a particular moment in time. not reproducible, with this it is ensured that we will have a security component appropriate to the current era, in this case a digitized neural pattern is proposed from an EEG, converted into a digital key.

METHOD DESCRIPTION

OBJECTIVE

Generate a unique digital key from an EEG, through readings of biological patterns [3], specifically through brain waves, thus showing unique temporary security elements specific to information encryption, manifesting a degree of security and uniqueness that the information currently required to ensure that the user is not violated or their information is compromised [4].

THEORETICAL FRAMEWORK

Digital technology has historical elements that allow its origins to be contextualized and analyzed, and data and information encryption is no exception, since from the origins of communication and transmission of information, the importance of handling certain messages as private and within the same context, this being part of an area of study called cryptology which derives in two aspects [5], cryptography and cryptanalysis.

Within the current contextual framework that are focused on the protection of personal information and its confidentiality, there are tools such as GNU Privacy Guard (GnuPG or GPG), which are responsible for encrypting the information and generating digital signatures, authenticating and preserving the content of the same [6], it must be noted that this type of tools are based on [7]:

1. **Sign. In order to verify and ensure the integrity of the information.**

2. **Verify.** Check the digital signatures of third parties and regulate access to information.

3. **Encrypt/Decrypt.** Restrict and protect access to sensitive information, making it accessible only to those who have a signature and have been verified.

Additionally, all encryption tools are made up of processes for the management and protection of information through cryptographic methods, which are classified into two aspects, due to their high degree of reliability, the asymmetric cryptography method (public key) is frequently used., consisting of a pair of keys for sending messages: a public key to share with third parties and a private key for the owner of the content; This type of cryptography consists of three types of encryption algorithms[7]: RSA, DSA, and "ElGamal", the latter being of a higher degree of reliability[8] (Asymmetric (Public Key) Cryptography).

PROCESS

The procedure carried out to meet the stated objective consisted of a step-by-step approach consisting of three stages, evaluating the current methods, evaluating their performance and their implementation.

1. **Investigation.** An investigation was carried out regarding GPG, to determine the encryption method and algorithm for the data obtained [7].

2. **Selection.** Once the methodology to be used was understood, characteristic data were selected, which were previously obtained from biological EEG readings. [9].

3. **mplementation.** With the parameters and data defined, a key was generated based on characteristic data, and linked to the Bluemix platform [10].

RESOURCES

The resources used to carry out each of the stages mentioned in the previous section were:

1. A laptop with internet access.
2. 2. Linux operating system.
3. Netbeans programming environment.
4. Bluemix development platform.
5. Electrodes to obtain EEG data.

DEVELOPING

The steps that were performed in the stages mentioned above are described below:

1. First, the GPG[11] key generator was used, as shown in Figure 1, using the Linux command line.

2. The ElGamal[12] algorithm was adapted, so that the values on which the keys will be generated and based on data obtained from brain wave readings, due to having a higher precision index[13], the generated keys are shown in Figure 2.

3. The base of the encryption key was assigned to a Token[14], to serve as an identifier of a device oriented towards encryption[15], through MindWave Mobile EEG headsets, on the Bluemix platform, where the type of authentication can be chosen. to use, as shown in Figure 5.

FINAL COMMENTS

SUMMARY OF RESULTS

Through the implementation of data from unique readings based on biometric authentication by brain waves, and the application in the framework of computer security, the result was the generation of a unique access key reinforced with biometric

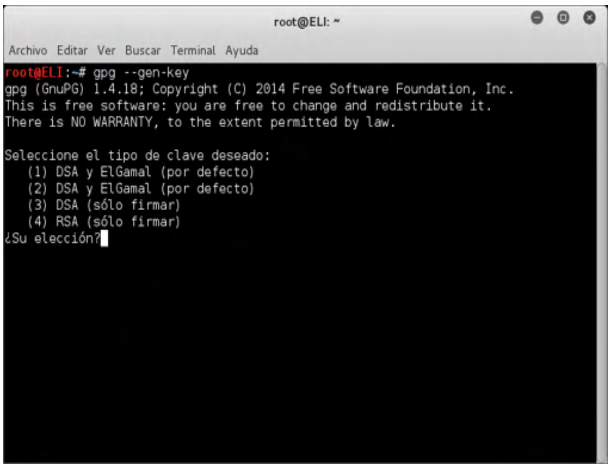

Figure 1. Initializing key generation on the command line.

```
Generated ID = 125131113018790896238684134 2
Public key = 116122050280182497989694093984150324164182
Private key = 495584442535467858441022650475761366817 12
```

Figure 2. Key generation.

Automatically generated authentication token
Allows the service to generate an authentication token for you. The token will be 18 characters long and will contain a mixture of alphanumeric characters and symbols. The signal will be indicated to you at the end of the registration process.
Authentication token provided

You can provide your own authentication token for the device. The token must be between 8 and 36 characters long and must contain a mix of upper and lower case letters, numbers, and symbols (hyphen, underscore, and period). The token must not contain repetitions, dictionary entries, usernames, or other predefined sequences. .

Provision of a signal (opcional)

Enter the authentication token here

Authentication tokens are encrypted before they are stored.
We can recover lost authentication tokens. Be sure to write down the authentication token after clicking Add

Figure 5. Implementation of the key in Bluemix.

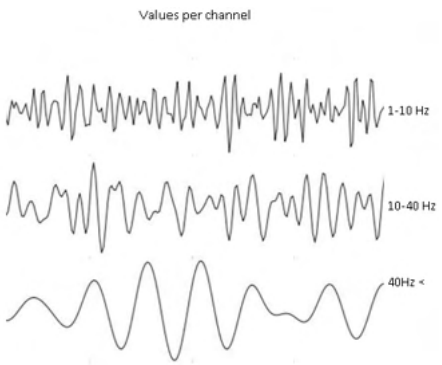

Figure 3. Base values per channel for the creation of digital security components.

techniques; The generated key can be applied in any system and guarantees a robust form of authentication, since the patterns in the initial configuration of the key are part of a unique and distinctive neural network. Figure 3 shows the biometric reading values. obtained through the electrodes on the subject's head and this is what was used to generate the personalized key.

CONCLUSIONS

Applications in information security based on unique temporary elements, represent an important aspect to protect information efficiently in any type of distributed systems such as the cloud, what is proposed in this article will facilitate its implementation in various systems and platforms, In addition, it proposes an improvement in information security with both spatial and temporal particular elements of a person, EEG patterns can generate as many keys as necessary, ensuring their spatial and temporal uniqueness, providing one more layer of the information security layer.

THANKS

This work was carried out thanks to the support of the Tecnológico Nacional de México, The present thanks are extended for providing the facilities and resources to carry out the investigation.

REFERENCES

[1] M. Rouse, "Internet of Things (IoT)," *WhatIs*, p. 6, 2014.

[2] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, p. 50, 2010.

[3] A. Cavoukian and A. Stoianov, "Biometric encryption," *Biometric Technol. Today*, vol. 15, no. 3, p. 11, 2007.

[4] F. Martín Moreno, "Criptografía y preservación de la seguridad de los sistemas de información," *Jornadas sobre Tecnol. la Inf. para la Mod. las Adm. Públicas*, vol. 10, 1998.

[5] M. Nogueira, A. Neto, H. Patil, and Í. Cunha, "Criptografia Baseada em Identidade: Uma Análise Comparativa sob a Perspectiva da Internet das Coisas," *An. - SBSEG 2015 XV Simpósio Bras. em Segurança da informação e Sist. Comput.*, p. 4, 2015.

[6] M. Girault, "Self-certified public keys," *Adv. Cryptol. — EUROCRYPT '91*, vol. 547, pp. 490–497, 1991.

[7] G. R. Blakley, "Safeguarding cryptographic keys," *Afips*, p. 313, 1979.

[8] S. Sharma, P. Sharma, and R. S. Dhakar, "RSA algorithm using modified subset sum cryptosystem," in *2011 2nd International Conference on Computer and Communication Technology, ICCCT-2011*, 2011, pp. 457–461.

[9] R. Vetter, "Authentication by biometric verification," *Computer*, vol. 43, no. 2. pp. 28–29, 2010.

[10] IBM, "Bluemix security," *ibm.com*, 2017. [Online]. Available: https://console.bluemix.net/docs/security/index.html#security.

[11] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter, "Public keys," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012, vol. 7417 LNCS, pp. 626–642.

[12] B. Chevallier-Mames, P. Paillier, and D. Pointcheva, "Encoding-free ElGamal encryption without random oracles," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006, vol. 3958 LNCS, pp. 91–104.

[13] E. R. Lewis, "Biological sensors," *Sensors and Actuators*, vol. 9, no. 1, pp. 9–17, 1986.

[14] M. Spain, B. Fuller, K. Ingols, and R. Cunningham, "Robust keys from physical unclonable functions," in *Proceedings of the 2014 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2014*, 2014, pp. 88–92.

[15] Z.-H. Qian and Y.-J. Wang, "IoT technology and application," *Tien Tzu Hsueh Pao/Acta Electron. Sin.*, vol. 40, no. 5, pp. 1023–1029, 2012.