Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 10. No. 4, December 2022 – Special Issue on Cryptography & Security Mechanisms

Article Citation Format
Darko, C.D. (2022): Data Security in the Cloud Using Multi-Modal Bio-Cryptographic Authentication. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 10, No. 2. Pp 9-14
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P2

Data Security in the Cloud Using Multi-Modal Bio-Cryptographic Authentication

Darko, Cyprian Danso
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: login2cyprian@gmail.com
Phone: +233)201692746

ABSTRACT

Bio Cryptography have been used to secure and protect systems for decades and a further development to employing multi modal bio cryptographic authentication in cloud security has become the best of practice to avert the problems associated with single-phased bio cryptographic techniques. Cloud security have seen improvements over time and higher data security can be achieved by using Multimodal bio cryptographic technique for data encryption and decryption to prevent the intruders from accessing the data. Application of one of the best algorithm-Bluefish to encrypt and decrypt data in the cloud.

Keywords: Bi- Cryptography, Data Decryption, Data Encryption, Cloud Security, Biometrics

1. INTRODUCTION

Cloud storage is the new order for information technology-driven systems world over and this has necessitated securing such system from intruders and hackers thus is an integral part of the process. Storing information in cloud computing is cost effective. But security is the concern in storing the data in cloud. Authorized owners are losing billions of dollars due to illegal activities like sharing and copying of digital data in cloud. So, it is very essential to protect the data in the cloud from unauthorized users. To overcome these difficulties bio-cryptography is used for encryption and decryption which is the best technique to further implement multi modal bio-cryptographic authentication.

The password-based authentication system is unsecure because, if the password is chosen easily, it is easy to guess and if the password is chosen very complex it is very hard to remember. To overcome these difficulties biometric system is used for encryption and decryption. Biometric system cannot be forgotten or easily stolen.

Biometric authentication is more powerful and it is alternative for traditional existing system. In the proposed system multimodal biometric authentication in cloud storage, security will be increased. Although biometric techniques show many advantages over conventional security techniques, biometric systems themselves are vulnerable against attacks. Biometric system protection schemes are in high demand. Bio-cryptography is an emerging technology which combines biometrics with cryptography. It inherits the advantages of both and provides a strong means to protect against biometric system attacks. Bio-cryptography is an emerging area involving many disciplines and has the potential to be a new foundation for next generation security systems.

Biometric Cryptography, also called Biometric Tokenization, refers to an authentication or other access system that combines inherence factors with public-key infrastructure (PKI). In particular, biometric cryptography is set up to take advantage of the convenience of authentication via fingerprint, face, eye, voice, palm, etc. — with none of the risks posed by having the biometrics take the form of a shared secret. https://www.hypr.com/security-encyclopedia/biometric-encryption

2. RELATED LITERATURE

In classical cryptography substitution ciphers, such as mono-alphabetic cipher, poly-alphabetic cipher, transposition/permutation cipher, have been studied and used for many years. Unfortunately, most of the traditional substitution ciphers have been broken and rendered non-usable. However, the substitution cipher created by nature in billions of years is still widely used in the biological world and shows its new value as a tool for information security. As aforementioned, the substitution cipher refers to the mapping between RNA and protein. As referenced by P. Selvarani and N. Malarvizhi that White (2004, p. 1) points out, “the genetic code is a substitution cipher, where codons are translated into amino acids. The substitution cipher has been known for about 50 years, but a logical origin of the cipher is still unknown. As a cipher, it is a molecular form of cryptography: meaning encoded in one molecular sequence and decoded into another.

Biometric cryptography enables the service provider to abandon the risks associated with central biometrics storage. The most glaring example of a biometrics breach to date is the US Office of Personnel Management 2015 data breach where millions of biometric templates were stolen among many millions more pieces of personally identifiable information (PII).
https://www.hypr.com/security-encyclopedia/biometric-encryption

S. Sumathi et.al. [14] proposed the multi biometric authentication using Discrete Wavelet Transform (DWT). A new novel technique based on DWT for identification of user. It utilizes support vector machine for the absolute result, the efficiency of the design is analyzed in terms of Genuine Acceptance Rate and False Acceptance Rate.BhawnaChouhan15 proposed the Image segmentation and feature extraction were focused in Iris recognition process. The performance depends on edge detection. Canny edge detector is used as a n image processing tool. In their article published in..., P. Selvarani* and N. Malarvizhi stated the need for data encryption and decryption in the cloud and gave the best algorithm of using the Bluefish which algorithm has 16 Iterations. The Input text is divided into block size of 64 bits, split the 64 bit block sizes into 32 bits.

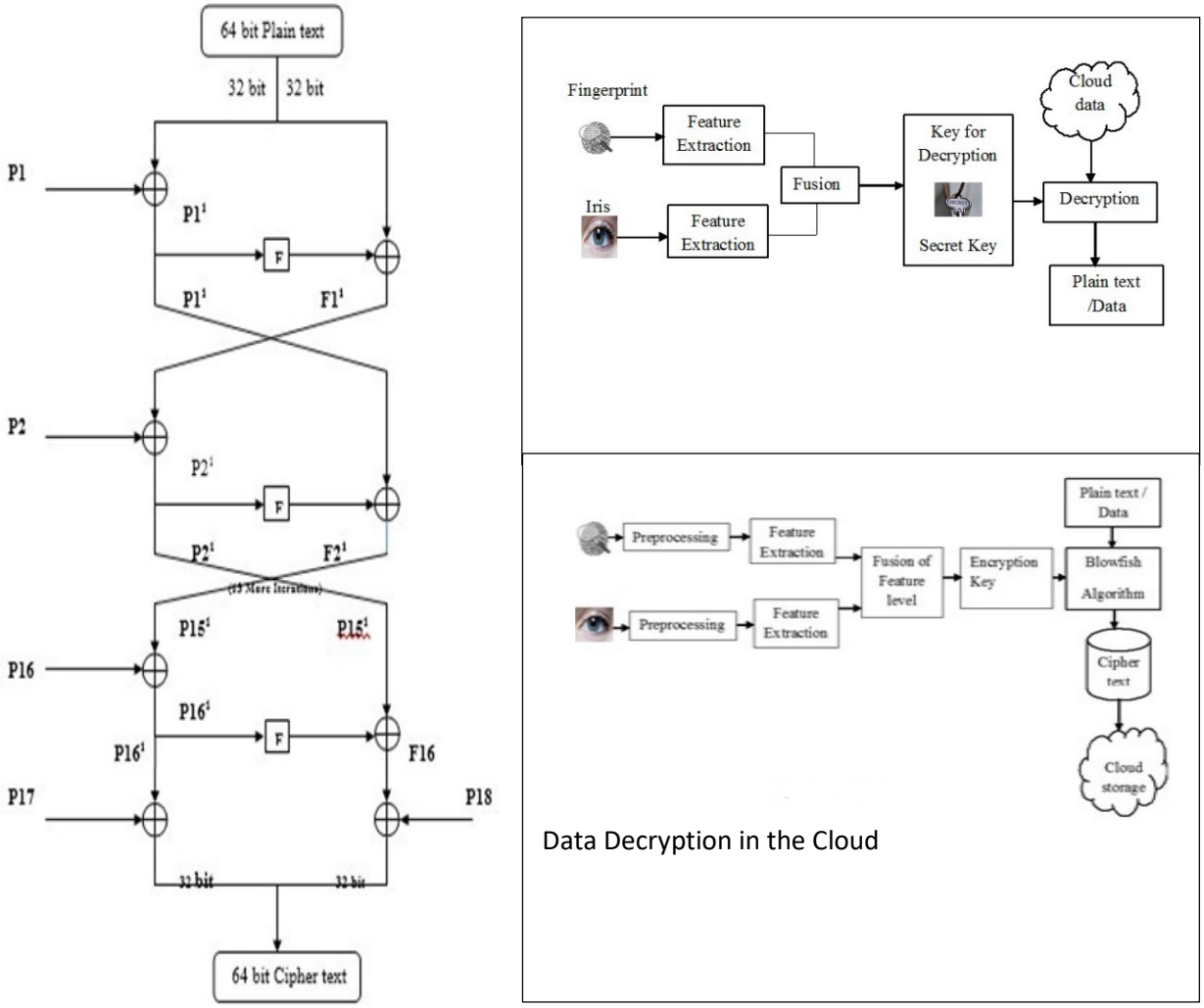

Fig.1 Bluefish Algorithm - Data Encryption in the cloud
Source: Indian Journal of Science and Technology, Vol 9(34)
DOI: 10.17485/ijst/2016/v9i34/86374, September 2016

3. RESEARCH GABS AND FINDINGS

Radha N. et.al. [13] proposed the biometric multimodal system using fingerprint and iris. They use Fisher Linear Discriminant and Principal Component Analysis (PCA) methodology for biometric recognition. This paper presents the difference between the logistic regression methods and bord a count method.

From the comparison results that the logistic regression approach with the rank level fusion and recognition rate were increased and error rate were decreased in Multibiometric system. By using multimodal biometric, like fingerprint, iris and secret key used to protect the data from unauthorized user. so the intruder cannot able to access the cloud storage data. Only authorized person is allowed to access the corresponding cloud data. Higher accuracy and more security have been provided by using fingerprint and iris. The total time taken for both decryption and encryption in the blowfish algorithm using multimodal biometric technique is very much reduced.

Strong Authentication can be provided to restrict the unauthorized person to access the cloud storage data. It was found that, bluefish algorithm is one the best and most recommended for the bio-encryption and bio-decryption of data in the cloud. The gabs left on all the research of the related work did not consider the weaknesses that are associated with the bio-cryptographic authentication and the security if offers in cloud services

4. RECOMMENDATIONS FOR POLICY AND PRACTICES

The use of multi modal bio-cryptography techniques to protect data in the cloud should be made a policy by the international governing organizations and International Professional and standardization organizations like IEEE, ISO, NIST and the Budapest conventions should make it a policy to collaborate with other stakeholders to set out rules for the implementation of multi modal bio-cryptography. They could achieve this by enforcing a policy that would coerce the cloud service providers to implement it at every level of authentication. Further, multi modal bio-cryptographic authentication methods should be used in authenticating logins on cloud systems by providing the needed hardware in computers and other devices that would allow such biometric authentications anywhere one is accessing the data from the cloud.

5. DIRECTIONS FOR FUTURE WORKS

The biometric-based blowfish method uses fingerprint and iris data as a secret key to save the data in a cloud environment. Future implementations of security methods for high-level encryption and decryption could improve security for cloud computing. In the future, further research should consider offering algorithm implementations to support the theories about cloud computing security and also delve into the weaknesses that may be associated with bio-cryptography and applying the multi modal bio-cryptographic authentication and suggest solutions to avert the outcomes.

REFERENCES

1. https://www.hypr.com/security-encyclopedia/biometric-encryption
2. Selvarani P, Visu P. Multi-model Bio-cryptographic Authentication in Cloud Storage Sharing for Higher Security. Maxwell Scientific Organization. 2015 Sep; 10(1):95-101
3. Radha.N, Kavitha A. Rank Level Fusion Using Fingerprint and Iris Biometrics. Indian Journal of Computer Science and Engineering (IJCSE). 2012; 2(6):917-23.
4. Sumathi S, Rani Hemamalini R. Multibiometric authentication, using DWT and score level fusion. European Journal of Scientific Research. 2012

5. Indian Journal of Science and Technology, Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/86374, September 2016
6. P. Selvarani* and N. Malarvizhi. Data Security in Cloud using Multi Modal Biocryptographic Authentication. Indian Journal of Science and Technology, Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/86374, September 2016.
7. Czaplewski, B. (2017). *Current trends in the field of steganalysis and guidelines for constructions of new steganalysis schemes Aktualne trendy w dziedzinie steganalizy oraz zalecenia dla konstrukcji*. *10*, 1121–1125. https://doi.org/10.15199/59.2017.10.3
8. Fridrich, J., Du, R., & Long, M. (2000). Staganalysis of LSB encoding in color images. *IEEE International Conference on Multi-Media and Expo*, *00*(III/WEDNESDAY), 1279–1282. https://doi.org/10.1109/icme.2000.871000
9. Fridrich, Jessica, Goljan, M., & Du, R. (2001). Reliable Detection of LSB Steganography in Grayscale and Color Images. *Proc. of the ACM Workshop on Multimedia Security*, 27–30.
10. Fridrich, Jessica, Goljan, M., & Soukal, D. (2003). *Higher-order statistical steganalysis of palette images*. *5020*, 178–190.
11. Fridrich, Jessica, Kodovský, J., Holub, V., & Goljan, M. (2011). Steganalysis of content-adaptive steganography in spatial domain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6958 LNCS*, 102–117. https://doi.org/10.1007/978-3-642-24178-9_8
12. Harmsen, J. J., & Pearlmana, W. A. (2003). Steganalysis of Additive Noise Modelable. *Transform*, *2003*(April), 131–142.
13. JinaChanu, Y., Manglem Singh, K., & Tuithung, T. (2012). Image Steganography and Steganalysis: A Survey. *International Journal of Computer Applications*, *52*(2), 1–11. https://doi.org/10.5120/8171-1484
14. Johnson, N. F., & Jajodia, S. (1998). Steganalysis: The investigation of hidden information. *1998 IEEE Information Technology Conference: Information Environment for the Future, IT 1998*, *1998-September*, 113–116. https://doi.org/10.1109/IT.1998.713394
15. Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications*, *40*, 217–235. https://doi.org/10.1016/j.jisa.2018.04.005
16. Ker, A. D. (2005). Steganalysis of LSB matching in grayscale images. *IEEE Signal Processing Letters*, *12*(6), 441–444. https://doi.org/10.1109/LSP.2005.847889
17. Mahdavi, M., Samavi, S., & Zaker, N. (2008). Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram. *Iranian Journal of Electrical & Electronic Engineering*, *4*(3), 59–70.
18. Sethi, P., & Kapoor, V. (2016). A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography. *Procedia Computer Science*, *87*, 61–66. https://doi.org/10.1016/j.procs.2016.05.127
19. Shukla, V. K. (2017). *AN OVERVIEW OF FEATURE BASED STEGANALYSIS*. *14*(2), 224–229.
20. Shyla, S. I., Adaptive, A. E., & Steganography, I. (2016). *Empirical Evaluation Of Image Steganography*. *3*(11), 74–76.

21. Westfeld, A., & Pfitzmann, A. (2000). *Attacks on Steganographic Systems*. 61–76. https://doi.org/10.1007/10719724_5
22. Yang, C., Liu, F., Lian, S., Luo, X., & Wang, D. (2012). Weighted stego-image steganalysis of messages hidden into each bit plane. *Computer Journal*, *55*(6), 717–727. https://doi.org/10.1093/comjnl/bxr112
23. Zhou, H., Zhang, W., Chen, K., Li, W., & Yu, N. (2021). Three-Dimensional Mesh Steganography and Steganalysis: A Review. *IEEE Transactions on Visualization and Computer Graphics*, *2626*(c), 1–20. https://doi.org/10.1109/TVCG.2021.3075136