FOR SECURITY IN THE HEALTHCARE CLOUD, FOG COMPUTING AND DECOY TECHNIQUE

Lynn Lawrence[1], Anu M.V[2]

[1] *(Mtech Cyber Security,Department Of Computer Sceience And Engineering,Met's School Of Engineering,Mala Email:lynnlawrencelynn@gmail.com)*
[2] *(Assistant Professor,Department Of Computer Sceience And Engineering,Met's School Of Engineering,Mala Email:anumundadan@gmail.com)*

ABSTRACT

Electronic Medical Records (EMR) are used by healthcare practitioners to keep track of a patient's lab results, X-rays, Computed Tomography (CT) scans, ultrasounds, and other medical records. All of this information is stored in the healthcare cloud, which offers services such as patient data management and backup (PHI). Knowledge theft assaults, which are the most serious kind of threats, are a constant threat to the healthcare cloud. As a result, the most important purpose of our technology is to make data theft attacks more difficult for attackers. To do this, we are employing the decoy strategy to obtain phoney PHI data that can be supplied to the user if the user's behaviour is detected as that of the attacker. The key agreement protocol allows authorised users to speak with each other over a secure channel. The original PHI is securely stored by encrypting it with the blowfish technique. To make information transfer smooth and efficient, we use fog computing, which can assist in data security by keeping it at the sting.

Keywords:-*Fog Computing, Cloud Computing, Decoy Technique, User Profiling, Key Generator, Blowfish are some of the terms used to describe fog computing and cloud computing.*

1. INTRODUCTION

To store medical data, healthcare cloud infrastructure is used. It aids with the management and tracking of a patient's medical information, even if the patient travels between cities. Privacy protection, lack of security standards, legal and policy challenges, lack of transparency, data protection, and licencing are all security concerns in the healthcare cloud [7]. The purpose of this study is to provide a safe healthcare

cloud. To achieve this, a solution is proposed that uses the fog computing facility in conjunction with the decoy technique to safeguard the patient's Medical Big Data (MBD) [1], [15]. The remainder of this research paper's sections are organised as follows: Section 2 describes the literature review. In section 3, the suggested technique is described in depth, including the system architecture and algorithm to be used. The technical background is described in Section 4. Section 5 has the conclusion.

2. SURVEY OF LITERATURE

M. Chen et al. [4] stated a social insurance architecture that enables human-cloud integration to increase QoS and QoE of cutting-edge medicinal services in next-generation healthcare systems. Ahmed et al. [5] discussed the potential of constant mobile edge computing application scenarios. The report also depicts fundamental aspects of scientific categorization of mobile edge computing. In this study, H. Li et al. [6] look at the evolution of Mobile Edge Computing (MEC) and suggest WiCloud to provide edge organizing, proximal figuring, and data procurement for creative administrations. The paper by C. Pahl et al. [11] discusses the edge cloud, fog computing, and the integration of IoT and network integration. With an example, H. Gohel [8] described algorithm computing. They also go through how to improve online security by using an algorithm computing technique. In this study, P. Gaur et al. [9] proposed a cryptographic procedure that encrypts images before transmission and decrypts them upon receipt, using the Blowfish algorithm. S. P. Karekar et al. [10] suggested a volatile and broad decoy strategy for data security, in which they monitor data access in the cloud to detect suspicious patterns. By allowing a cognitive support application, M. Satyanarayanan et al. [12] shown how cloudlets can boost human perception and cognition. In the present fog computing paradigm, Stojmenovic et al. [13] highlighted privacy difficulties. In this study, S. Khairnar et al. [14] examined fog services and how they are an extension of the cloud computing experience. By employing an algorithm that effectively estimates average fluctuations and detects changes in user access patterns, Ashadeep et al. [15] suggested a way to improve insider data theft threat detection. N. Kumar et al. [16] compared the DES, AES, and Blowfish algorithms in this article based on performance, block size, and key size.

3. METHODOLOGY PROPOSED

A cryptography procedure that encrypts and decrypts images before transmitting and receiving them using the Blowfish algorithm. S. P. Karekar et al. [10] suggested a volatile and broad decoy strategy for data security, in which they monitor data access in the cloud to detect suspicious patterns. By allowing a cognitive support application, M. Satyanarayanan et al. [12] shown how cloudlets can boost human perception and cognition. In the present fog computing paradigm, Stojmenovic et al. [13] highlighted privacy difficulties. In this study, S. Khairnar et al. [14] examined fog services and how they are an extension of the cloud computing experience. By employing an algorithm that effectively estimates average fluctuations and detects changes in user access patterns, Ashadeep et al. [15] suggested a way to improve insider data theft threat detection.

3.1 Architecture

To safeguard user's multimedia data, the suggested system uses fog computing and a decoy approach over the cloud. Two photo galleries are created as a result of the procedure. The first is called Original Photo Gallery (OPG), while the second is called Decoy Photo Gallery. The Decoy Medical Big Data (DMBD) has been released.

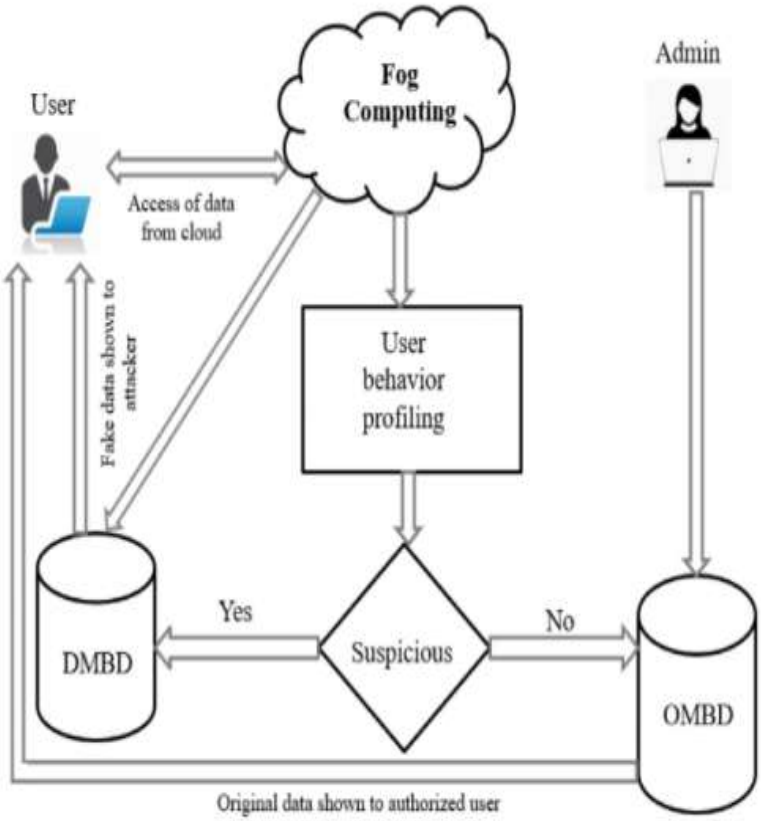

Fig-1:shows the proposed system's architecture.

The Original Medical Big Data (OMBD) is secured over cloud in OPG by using a fog as a honeypot in DPG. As a result, the user has access to the DMBD by default, but the OMBD is only accessible to authenticated users. A pairing cryptography-based tri-party authenticated key agreement protocol between the user, DPG, and OPG is presented to promote this process. Uploading and downloading data is the responsibility of the user. The key generator is in charge of creating a key (encryption/decryption key). User profiling, or user behavior, is monitored by fog computing, which generates a decoy file that is stored in the DMBD. A cloud server is in charge of verifying the user's identity and storing OMBD (original data).

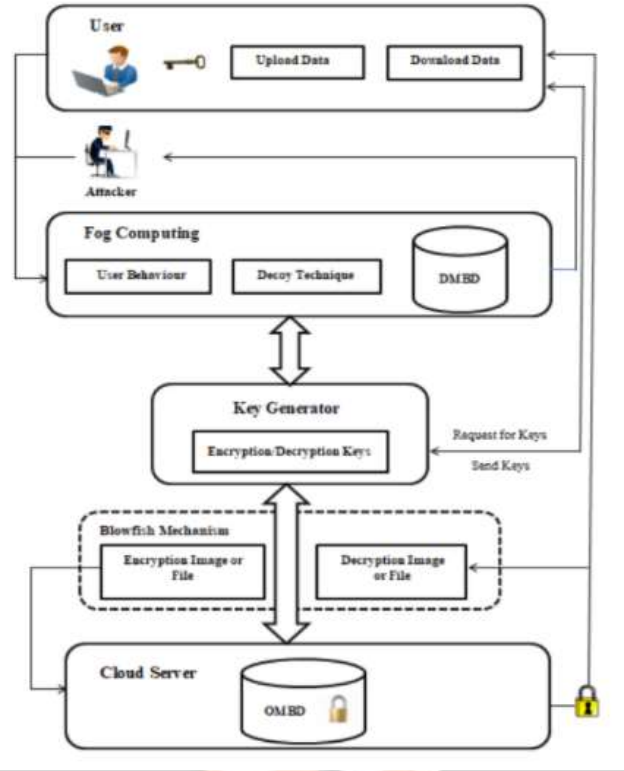

Fig-2 shows the fog computing setup.

3.2Algorithms

1) User Profiling: We employed user profiling to determine the legitimacy of the user. The system keeps track of the user's actions, such as the number of failed login attempts, data downloaded, and security questions, among other things.

• First, cntLoginFailincrease the number of user login failures.

• Next, raise cntDataDownload to calculate the amount of downloaded data.

• cntSecQueFail increases for the third time while calculating the number of security questions that fail.

• Detect attacker if cntLoginFail > 3 && cntDataDownload > 3 && cntSecQueFail > 3 && Key matches at that moment; otherwise, user is real.

2) Key Generation: The keys are created by following the instructions below:

• To begin, choose two prime numbers, p and q. The integers p and q should be picked at random and have similar bit lengths for security reasons. A primality test is frequently used to locate prime integers.

Then compute n = pq, where n is the modulus key, and (n) = (p – 1) (q – 1) is Euler's totient labor.

• Calculate d = e–1 mod Where d is the multiplicative inverse of e mod e mod e mod e mod e mod e mod e mod e mod e mod e Solve for d given (d * e)mod (n) = 1 in a more straightforward manner. This is frequently

registered in order to make use of the extended euclidean algorithm. Furthermore, d is retained as a personal key exponent. The public key is made up of the modulus n and the public (or encryption) exponent e, while the general public key is made up of the modulus n and the private (or decryption) exponent d, which must be kept secret.

3) Blowfish

a) The encryption algorithm is as follows: Blowfish is a 16-round game. A 64-bit data element, X, could be used as the input.

Divide the 64-bit plaintext value X into two 32-bit halves: XLand XR is a game developed by XLand.

XL = XL XOR P[i] for I = 1 to 16

F[XL] OR XR = XR

XL and XR should be swapped.

Then P[17] = XR = XR XOR XR = XR XOR XOR XOR XOR XOR X

P[18] XL = XL XOR

Finally, join XL and XR to form a 64-bit cypher text value.

The process of picture or file encryption is shown in Figure 2.

b) The decryption algorithm is as follows: The identical approach is used to decode the ultimate value back to the first one, with the exception that the array p is walked backward. Split the 64-bit value X in the cypher text into two 32-bit halves: XL and XR.

Step 1: XL = XL XOR P[i] for I = 18 to three.

F[XL] OR XR = XR

XL and XR should be swapped.

Then XR = XR XOR P[2] becomes XR = XR XOR P[2].

XL = XL XOR P[1] XL = XL XOR P[1] XL = XL

Finally, combine the XL and XR values into a 64-bit textual value.

4. INTRODUCTION TO TECHNICAL BACKGROUND

A. Cloud Computing

Cloud computing, according to the National Institute of Standards and Technology (NIST), is an on-demand, convenient, and ubiquitous service that provides access to a shared pool of resources such as servers, storage, networks, and other resources that can be provisioned and released with minimal interaction with the service provider [7]. Cloud services are used to meet end-user business demands. The three types of cloud computing services are as follows: (1) Infrastructure as a Service (IAAS) is a service that provides infrastructure components to clients. (2) PAAS: Platform as a Service (PAAS) provides a client with a pre-built application platform. (3) SAAS: Software as a Service (SAAS) gives you the ability to use cloud apps.

B. Decoy Methodology

The decoy approach aids in the generation of fake information on demand and the detection of unwanted access to data. Integrating decoy technology with cloud-based user behaviour profiling can aid in data security by deceiving attackers with the fake document.

C.Fog Computing

Fog computing brings data storage, processing, and communication closer to the user. It facilitates data sharing and storage by allowing local decision-making over peer-to-peer communication. Fog computing is used in the proposed system to monitor user profiling and generate decoy file stores in DMBD.

5. CONCLUSIONS

This document focuses on protecting the user's MBD in the cloud using fog computing as part of the protection of knowledge mission within the cloud. Two photo galleries, OPG and DPG, are created for this purpose. Within the OPG, the OMBD is kept a secret. DPG contains DMBD, which is used as a honeypot. By default, the user has access to DMBD, so access to OMBD is granted only after the user's authenticity has been verified. As a result, the OMBD becomes safer by storing it in the hidden gallery. Between the user, OPG, and DPG, a tri-party key agreement protocol based on pairing cryptography is used to help with this process.

ACKNOWLEDGEMENT

First and foremost, I thank God, without whose blessings, I would not have been able to finish my paper work. Mr. SUNIL S.S., the Head of the Department of Computer Science, deserves special thanks for his constant guidance and assistance. My heartfelt gratitude to our Project Coordinator, Mrs.ANU MV, M.TECH., faculty of computer science, for her assistance with this project. We gratefully acknowledge his contributions, constant support, and encouragement in the preparation of this paper. And the computer science faculty for their assistance in shaping my paper into what it is now. I appreciate my parents' mental support during the project, especially when my energy levels were at their lowest.

REFERENCES

[1] A. Aljumah and T. A. Ahanger, "Fog computing and security issues: A review," in 7th International Conference on Cloud Computing and Communications, pp. 292-303, 2018.

[2] H. A. A. Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. A. Alamri, “A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography,” IEEE Access, vol. 22, no. 2, pp. 22313-22328, 2017.

[3] H. A. Al-Hamid and S. M.M. Rahman, "Securing photos in the cloud using decoy photo gallery," Proc. IEEE Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET), pp. 816-822, 2017.

[4] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C.-H. Youn, "Wearable 2.0: Enabling human-cloud integration in next-generation healthcare systems," IEEE Communications, vol. 54, no. 1, 2017, pp. 54-61.

[5] Ahmed and E. Ahmed, “A survey on mobile edge computing,” in IEEE 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–8, 2016.

[6] H. Li, G. Shou, Y. Hu, and Z. Guo, “Mobile edge computing: progress and challenges,” in 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 83–84, 2016.

[7] D. Sangita, C. Ankita, and P. Reshamlal, "A review on issues and challenges of cloud computing," in IJIACS, vol. 1, no. 1, pp. 81-88, 2015.

[8] H. Gohel, "Design and development of a combined algorithm computing technique to improve web security," Int. J. Recent Innov. Emerg. Res. Eng., 76-79, 2015.

[9] P. Gaur and N. Manglani, "A survey on image encryption and decryption using blowfish and watermarking," Int. J. bRecent Innov. Trend Comput. Commun., vol. 15, no. 3, pp. 3285-3288, 2015.

[10] S. P. Karekar and S. M. Vaidya, "Perspective of decoy technique using mobile fog computing with effect on wireless environment," International Journal of Science, Engineering, and Technology Research, pp. 2620-2626, 2015.

[11] C. Pahl and B. Lee, "Containers and clusters for edge cloud architectures–a technology review," in IEEE 3rd International Conference on Future Internet of Things and Cloud (FiCloud), pp. 379–386, 2015.

[12] M. Satyanarayanan, Z. Chen, K. Ha, W. Hu, W. Richter, and P. Pillai, "Cloudlets: at the cutting edge of mobile-cloud convergence," in IEEE 6th International Conference on Mobile Computing, Applications, and Services (MobiCASE), pp. 1–9.

[13] Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in IEEE Federated Conference on Computer Science and Information Systems, pp. 1–8, 2014.

[14] S. Khairnar and D. Borkar, "Fog computing: A new concept for minimising attacks and providing security in cloud computing environments," in IJRET, vol. 4, no. 1, pp. 124-127, 2014.

[15] 'Hindering data theft attacks in the cloud using fog computing," Ashadeep, S. Majithia, 427-429 in Int. J. Res. Eng. Technol., 2014.

[16] N. Kumar and J. Thakur, "DES, AES, and Blowfish: Simulation-Based Performance Analysis of Symmetric Key Cryptography Algorithms," 6-12 in Int. J. Emerg. Technol. Adv. Eng., 2011.