A Review on Healthcare Cloud using Decoy Technique and Fog Computing

Priyanka Khandge
Department of Computer Engineering
JSPM's Rajarshi Shahu College of Engineering
Pune, India
priyakhandge10@gmail.com

ABSTRACT

A health care cloud is a cloud computing service which is used by health care providers for storing, maintaining and backing up Personal Health Information (PHI). Today's world is the internet world; here all things are going through the web. Using telecommunication technology health professionals can diagnose, evaluate and treat the patients. For this purpose, health professionals access the Electronic Medical Record (EMR) of the patient from the cloud, which contains a large amount of data i.e. X-rays, ultrasound, CT scans, and MRI reports (whole patient information). In spite of the prevalence of restorative consideration cloud, addresses a few security issues, like data theft attacks which are considered one of the most serious attacks in the healthcare cloud. So the main goal of our system is to protect or provide the security to healthcare data, using fog computing. If user behavior finds as an attacker then instead of original data, he or she will get fake data and for fake data generation users decoy technique. As well as using key agreement protocol, the key generator generates key among the users, using this key user can communicate with each other by the secure way.

Keywords— Decoy technique; Blowfish algorithm; Fog computing; User profiling.

I. INTRODUCTION

Telemedicine is one of the emerging fields for e-health research. In the telemedicine service, EMRs including Medical Big Data (MBD), images, and multimedia medical data which are transmitted on over insecure internet connections and this data accessed by the remote doctors. The healthcare cloud can access or pull all different information together for a patient because the patient moves from one hospital to another; as a result, the patients' information can be overseen and followed effectively. But healthcare cloud has different issues related to its security, the most important of which are: legal and policy issues, data protection, privacy protection, lack of transparency, cybersecurity issues, the absence of security standards, and software licensing. To overcome such problems, a methodology is presented to secure the patient's MBD in the healthcare cloud using the decoy technique with a fog computing facility.

Data about the decoy, such as recovery documents, and other false information, can be generated upon request and used to detect unauthorized access to information and poison the filtered information of the thief. The use of reminders will confuse an attacker by making him believe he has useful information when he is not. This technology can be integrated with user behavior profile technology to protect a user's data in the cloud. Whenever you notice abnormal and unauthorized access to a cloud service, the information about the bait can be returned from the cloud and delivered in such a way that it seems completely normal and legitimate.

This paper is organized as follows: Section II describes the related work. Section III describes the structure of the system. Section IV describes the methodology to implement the system. Section V derives the conclusion.

II. RELATED WORK

J. Thakur et al. [1] the creator gives a reasonable examination between the three most basic symmetric key cryptography calculations: DES, AES, and Blowfish. Since primary worry here is the execution of calculations under various settings, the exhibited correlation thinks about the conduct and the execution of the calculation when distinctive information loads are utilized. The examination is made based on these parameters: speed, square size, and key size.

B. Nayak [2] signcryption is cryptographic crude which all the while give both the capacity of computerized signature and open key encryption in a solitary legitimate advance. Personality-based cryptography is an option in contrast to the customary authentication based cryptosystem. The creator present new signcryption plans are dependent on elliptic

bend cryptography. The security of proposed plans depends on elliptic bend discrete logarithm issue (ECDLP) and elliptic bend Diffie-hellman issue (ECDHP).

A. Jain et al. [3] web and systems applications are becoming exceptionally quick, so the requirements to ensure such applications are expanded. Encryption calculations assume a principal job in data security frameworks. On the opposite side, those calculations expend a lot of processing assets, for example, CPU time, memory, and battery control. This paper gives an assessment of five of the most widely recognized encryption calculations in particular: AES (Rijndael), DES, 3DES, RC2, and RC6.

H. Gohel [4] computational innovation is an extremely famous and late zone of innovative work. It is exceptionally valuable to accomplish computational things by utilizing calculations. There are different calculations are accessible and there are likewise numerous computational methods are accessible to perform different errands. In any case, these standard calculations and processing methods is insufficient valuable for giving just as upgrading security to the web.

P. Gaur et al. [5] in the present time, to send and get data, the web is the primary media. This data might be content, sound, and video and so on. There are numerous focal points of the web. The web gives snappiest information conveyance administrations; security of information is a real worry for all web clients. We can get these targets with cryptography which is just the study of anchoring delicate and secret data as it is put away on media or transmitted through correspondence organize ways. Blowfish algorithm, a sort of symmetric key cryptography is the best answer for this.

Ashadeep et al. [6] distributed storage is being utilized massively in different mechanical areas. Despite the plentiful preferences of putting away information on the cloud, security still remains a noteworthy obstacle which should be prevailed. Information on the cloud is being gotten to with the new correspondence and registering ideal models which further emerges new information security challenges. An adjusted methodology is utilized known as mist registering which utilizes the two procedures viz. client behavior profiling and decoy technology. In spite of these strategies, there happens an issue of the wrong data appearing to the right client and furthermore the misidentification of the client as an aggressor then the circumstance goes upside down and client's faces bother and disappointment.

S. Khairnar et al. [7] in cloud clients pay for what they use and have not to pay for nearby assets which they need, for example, foundation. So this is the fundamental preferred standpoint of distributed computing and primary purpose behind picking up fame in today's world. Also distributed computing is a standout amongst the most energizing innovation because of its capacity to decrease cost related with registering while at the same time expanding adaptability and versatility for PC forms. But in the cloud the principle issue that happens is security. And nowadays security and protection both are principle worry that should have been considered. Fog computing isn't a substitution of cloud it simply broadens the distributed computing by giving security in the cloud condition. With fog administrations, we can improve the cloud understanding by confining client’s information that needs to live on the edge.

Aruna et al. [8] the creators propose a totally extraordinary way to deal with anchoring the cloud utilizing bait data innovation, that they have come to call fog registering. They utilize this innovation to dispatch disinformation assaults against malevolent insiders, keeping them from recognizing the genuine delicate client information from phony useless information. Associations utilize the cloud in a wide range of administration models (SaaS, PaaS, and IaaS) and sending models (Private, Public, and Hybrid).

A. Aljumah et al. [9] mist frameworks are fit for handling a lot of information locally, work on-start, are completely compact, and can be introduced on heterogeneous equipment. These highlights make the fog stage exceptionally reasonable for time and area delicate applications. This wide scope of user-driven applications heightens numerous security issues with respect to information, virtualization, isolation, arrange and observing. Most the fog applications are propelled by the longing for usefulness and end-client necessities, while the security viewpoints are regularly disregarded or considered as an untimely idea.

S. P. Karekar et al. [10] distributed computing offers to altogether change the manner in which the creators use PCs and access and store their own information and business data. New figuring, correspondences standards emerge new information security challenges. Existing information security instruments like encryption were not effective in anchoring information control assaults, particularly those submitted by an insider to the cloud supplier. The screen information access in the cloud and distinguish irregular information get to designs.

III. STRUCTURE OF THE SYSTEM

The first user has to register to the system (i.e. create an account) then only he/she can access the system. After login successfully user is able to upload the data, for this he/she needs encryption key, which is requested to key generator,

after getting key user can upload data successfully. The same process will continue for the download data. Key generator when the generator gets requests from a user for keys than using the key agreement protocol key generator is responsible for generates a key (encryption key/decryption key). Fog computing monitor user profiling i.e. user behavior and generate decoy file which is store in DMBD. User behavior profiling is expected that access to the information of a user in the cloud shows a normal means of access. The user profile is a well-known technique that can be applied here to model how, when and how much a user accesses their information in the cloud. This "normal user" behavior can be continuously verified to determine if abnormal access to a user's information occurs. Decoys information on the release, such as recall documents, is delivered to the attacker when unauthorized access is detected. The file that was sent to the attacker is in an encrypted format.

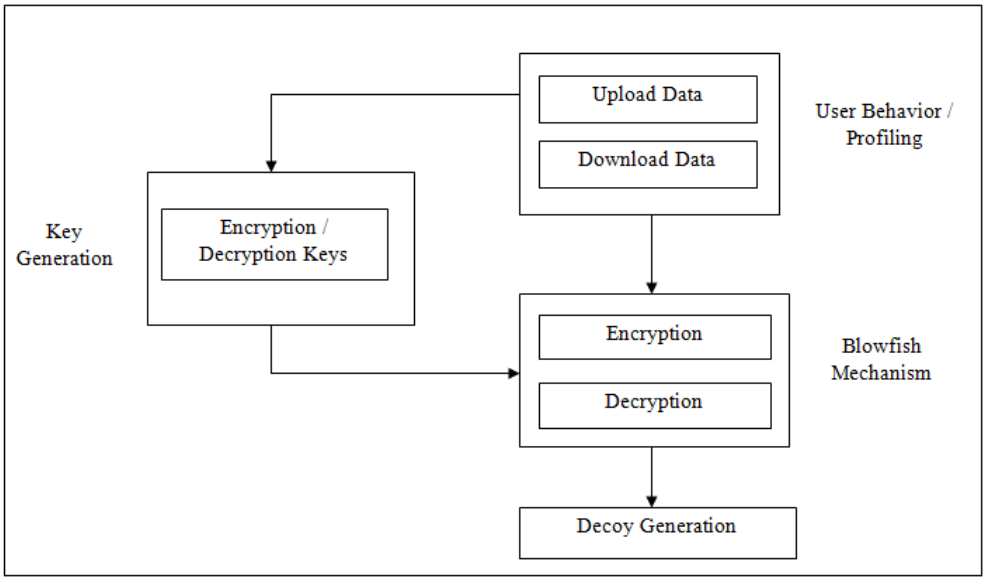

Figure 1: System Overview

However, when opponents try to use the system, they are certainly attracted to inflicting information, as their task is to explore confidential data and steal it for monetary and other benefits. Bait technology is very useful because it deceives the bad guys. When the technology comes out is used together with user profiles, it is possible to know the suspicious behavior of the users and in this way, it is possible to prevent the theft of internal data. The cloud is not a physical entity, but a vast network of remote servers all over the world that are connected and intended to function as a single ecosystem. These servers are designed to store and manage data, run applications or deliver content or services such as video streaming, webmail, office productivity software or social networks. Here cloud is responsible to authenticate user which are registered to the system and store OMBD (original data) in the ciphertext, to encrypt and decrypt the data here blowfish algorithm is used.

IV. METHODOLOGY TO IMPLEMENT THE SYSTEM

A. Fog Computing

Cloud computing is a decentralized computerized structure, where resources, including data and applications, are in logical positions between the data source and the cloud; It is also known by the terms "fogging" and "fog network". The goal is to bring basic analytical services to the edge of the network, improving performance by identifying the processing resources that are closest to where they are needed, thus reducing the distance that data needs to be transported across the network, improving efficiency and the general performance of the network. Computer fog can also be implemented for security reasons, as it has the ability to segment bandwidth traffic and introduce additional firewalls into a network for added security. Cloud computing has its origins as an extension of cloud computing, which is the paradigm for having data, storage and applications on a remote server and not hosted locally. With the cloud computing model, the customer can buy the services of a supplier, offering not only the service but also maintenance and upgrades, with the advantage that it can be accessed anywhere and provide the work of the teams.

B. Decoy Technique

Recovery data, such as recovery documents, honey files, honeypots, and various alternative counterfeit data can be generated on demand and function as a form of unauthorized access to the data and to "poison" the ex-filtered data of the thief. Withdrawals to the service can confuse and confuse someone in the basic cognitive process; they need filtered data, once they have not done so. This technology could also be integrated with user behavior identification technology to protect a user's data within the cloud. Each time abnormal access to a cloud service is detected, the bait data can also

be captured from the cloud and delivered in such a simple way that it seems to be totally legitimate and traditional. user of the truth, the agency of the United Nations (UN) is that the owner of the knowledge will determine without delay the data of the falsification that comes from the cloud and, therefore, could alter the answers of the cloud through a series of means which, like the challenge questions, tell the security system in the cloud that is detected incorrectly. Unauthorized access. In the event that access is known as unauthorized access, the cloud security system will provide unlimited amounts of falsified data to someone, thus protecting the user's actual information against unauthorized language acts. Therefore, calls have two purposes:

1. To confirm whether access to information is permitted or not when abnormal access to the data is detected.
2. To confuse the offender with falsified data.

We tend to postulate that the combination of these two security measures can offer security levels that are not optimal for the cloud. There is no security mechanism in the current cloud that has this level of security. We have applied these ideas to find illegitimate information about access to information contained in an area storage system by intruders, for example, UN agents who attack the impersonation of legitimate users once their credentials are stolen. You could consider illegitimate access to cloud information by an infamous corporate executive due to the malicious act of a masquerade. Our experimentation ends in an area storage system that shows that by combining each technique we obtain better detection results and our results recommend that this approach can be adapted in an extremely cloud environment since the cloud is designed to be clear to the user as a system area file. In the following, we tend to briefly review a series of experimental results obtained through the victimization of this approach to find the masking activity in an extremely native file configuration.

V. CONCLUSION

As part of the protection of data mission in the cloud, this document focuses on protecting the user's multimedia data within the cloud using fog computing. For this purpose, two photo galleries are generated the OMBD is kept secret in the cloud and DMBD is used as a honey pot and kept in the fog. Therefore, instead of recovering the DMBD only when unauthorized access is detected, the user, by default, accesses the DMBD. The OMBD is accessible only from up to the user after verifying the authenticity of the user. So the original multimedia data becomes more secure by configuring the default value of the DMBD, while the OMBD is stored in a hidden gallery. To facilitate the above process, an efficient key agreement protocol authenticated by a key generator which generates keys and gives to the user. User profiling algorithm is used to detect user behavior, if the behavior is attacker then generate fake data using the decoy technique of fog computing.

VI. ACKNOWLEDGMENTS

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally, I wish to thank all my friends and well-wishers who supported us in completing this paper successfully I am especially grateful to my guide Prof. S. B. Javheri for time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] Nagesh Kumar and Jawahar Thakur, ``DES, AES, and blowfish: Symmetric key cryptography algorithms simulation based performance analysis," In International Journal of Emerging Technology and Advanced Engineering, pp. 6-12, 2011.
[2] Biswojit Nayak, ``Signcryption schemes based on elliptic curve cryptography," Department of Computer Science Engineering, India, 2014.
[3] Amit Jain and Divya Bhatnagar, ``A comparative study of symmetric key encryption algorithms," In IJCSN, pp.298-303, 2014.
[4] Hardik Gohel, ``Design and development of combined algorithm computing technique to enhance web security," International Journal of Innovative Emerging Research Engineering, no. 1, pp. 76-79, 2015.
[5] Preeti Gaur and Neeraj Manglani, ``A survey on image encryption and decryption using blowfish & watermarking," International Journal on Recent Innovation Trend Computing and Communication, no. 5, pp. 3285-3288, 2015.
[6] Ashadeep and Sachin Majithia, ``Hindering data theft attacks in the cloud using fog computing,"In IJRASET, pp. 335-343, 2014.
[7] S. Khairnar and D. Borkar, ``Fog computing: A new concept to minimize the attacks and to provide security in cloud computing environment," International Journal Research Engineering Technology, no. 6, pp. 124-127, 2014.
[8] Aruna, C. Prasad, and M. A. Reddy, ``Securing the cloud using decoy information technology to preventing them from distinguishing the real sensitive data from fake worthless data," In IJARCSSE, vol. 3, pp. 292-299, 2013.
[9] Abdullah Aljumah and Tariq Ahamed Ahanger, ``Fog computing and security issues: A review,"In International Conference on Computers Communications and Control (ICCCC), pp. 237-239, IEEE, 2018.
[10] S. P. Karekar and S. M. Vaidya, ``Perspective of decoy technique using mobile fog computing with effect to wireless environment,"*Int. J. Sci. Eng. Technol. Res.*, no. 14, pp. 2620-2626, 2015.