Security Model for the privacy of Big Data in Health Care Cloud using Fog Computing

1st Shaldrin Emerson
Dept. Computer Science And Engineering
Mangalam College Of Engineering,
Ettumanoor, Kottayam
shaldrin.emerson2020@gmail.com

2nd Sruthy K Joseph
Dept. Computer Science And Engineering
Mangalam College Of Engineering,
Ettumanoor, Kottayam
sruthy.joseph@mangalam.in

***Abstract*—E-medicine is one of the new areas of e-health study. It is the distribution of health-related services and information via electronic information and telecommunication technologies. Electronic medical records, including medical big data, MBD, pictures, and interactive medical records, are relayed through insecure Online communications, as advised by distant doctors, in the E-medicine. Electronic Medical Records (EMR) must be stored with large amounts of data on the Medical Data cloud to provide effective access and facilitate mobility between health advisors and patients. Clinical-service Edge computing has various issues related to its security. As a result, we have put forth an approach that employs DMBD to safeguard Medical Big Data in the healthcare cloud. This method involves utilizing edge networking device plus pairing PKCs depending on cryptanalysis. Utilizing Pairing Based Cryptography(PBC)s for the storage and retrieval of MBD in the cloud, session keys will be created to ensure secure communication between participants. The use of a fog computing facility has focused on the secure storage of healthcare private data in the cloud.**

***Index Terms*—Medical Big Data, Fog Computing, Pairing Based Cryptography**

I. Introduction

Telemedicine includes the use of communication networks and digital solutions in providing health services and its popularity is increasing nowadays. Telecare aims to deliver healthcare services that are on par with in-person treatment in terms of quality. Its primary goal is to provide cost- effective medical services while also alleviating the pressure on healthcare systems. The ease of managing and tracking patient information is a benefit of healthcare cloud computing. However, this technology also poses security concerns that must be dealt with. Lack of transparency is also a consumer issue, which may come to light when consumers do not know where their data are physically kept or what will happen to them. Moreover, cyber security also poses a cloud security problem. Information input, information, and command out- put, sharing of property and physical infrastructure have all been identified as cyber security challenges. Therefore, we proposed a method to ensure that the MBDs are secured in healthcare cloud using DM BD and relying upon a combination of fog computing technology and paired cryptographically based encryption codes.

The large size and intricacy of these data sets make it challenging, and in some cases, not feasible to manage them using traditional software and hardware. The healthcare cloud infrastructure offers the advantage of seamlessly consolidating a patient's healthcare information, even as they transfer be- tween different hospitals or healthcare providers. This feature simplifies the regulation and observation of a patient's wellness data. Data theft attacks are the most serious security breaches of medical data in the Health Care cloud. The objective of this summary shall be to protect healthcare private information from cloud computing using fog computation technology. To notice the vulnerability concerns at healthcare cloud, Tripartite One Round Certificated Key Agreement Rule has contem- plated. This protocol uses additive coupling cryptology to generate secure interaction keys for participants to commu- nicate with each other in a safe and protected manner. Finally, implementation of a decoy technique will enable access and secure storage of private healthcare data.

II. Related Work

A. A 5G Cognitive System for Healthcare

This paper introduces a new system of healthcare based on 5G cognitive systems.Data Based on medical big data analysis, it is possible to control patient physiological and psychological status using cognitive intelligence. The 5G Tactile Internet technology is expected to revolutionize the healthcare industry by enabling real-time remote patient monitoring and diagnosis, as well as facilitating surgical procedures through haptic feedback. The technology is capable of providing high-speed, low-latency, and reliable connectivity, which is critical for applications such as telemedicine, remote surgery, and virtual and augmented reality (VR/AR) in healthcare. Moreover, the integration of machine learning and deep learning algorithms in the data cognitive engine can enhance the system's ability to analyze and interpret large volumes of healthcare data, includ- ing speech and emotion recognition. This can help improve the accuracy of medical diagnosis and treatment plans, as well as enable more personalized and efficient healthcare services. [1].

B. Healthcare Big Data Voice Pathology Assessment Framework

The study is related to the healthcare big data framework using voice pathology assessment (VPA). The processing of large amounts of heterogeneous healthcare data can be a

challenging task that requires careful consideration of the algorithm used. It is essential to have an algorithm that can effectively handle different types of data, such as numeric, alphanumeric, and textual data, without compromising the integrity of the data. Moreover, the algorithm should be able to process the data efficiently to avoid any delays in delivering healthcare services. Therefore, researchers often develop and evaluate various algorithms to find the most suitable one for processing heterogeneous healthcare data while maintaining the highest level of accuracy and speed [2].

C. Malady Prediction by Machine Learning over Big Health-care Data

This work streamlined predictive modeling algorithms for effective prediction of chronic disease outbreak in disease-frequent communities. Advancements in big data analytics technology have brought increased focus on anomaly pre-diction through big data analysis. Many studies have been conducted using automated selection of features from exten- sive data to enhance the precision of risk classification. A new convolutional neural network based multimodal disease risk prediction (CNN-MDRP) algorithm using structured and unstructured data from hospitals is proposed. Consider a simple disorder, hyperlipidemia, only a few features of structured data can get a good description of the disease, resulting in a fairly good effect of illness risk prediction. [3].

D. Wearable 2.0: Qualifying Human Cloud Integration in next generation Health Systems

The intention is to introduce a new generation healthcare system called Wearable 2.0, which improves the Quality of Experience (QoE) and Quality of Service (QoS). The collected data is then sent to the cloud where machine intelligence provides breakdown of impacts of the client's health and emotional status. The user's corporal data is collected pas-sively, and tailored patient care are offered through bulky data intelligence on the cloud. The editorial also addresses the system framework, operational elements, and configuration specifics of intelligent apparel. The healthcare implementa- tions of this system encompass supervision of chronic diseases, geriatric care, medical and health facilities, athletic training, and emotional support. [4].

E. Cloud - supported Industrial Internet of Things (IIoT) – capable platform for Vigor Investigation

The research work introduces a monitoring framework that is enabled by HealthIIoT. This framework allows for the collection of ECG and other data using mobile devices and sensors. The data collected is securely transmitted to the edge for seamless access by medical professionals. The proposed health monitoring approach involves signal enhancement, watermarking, feature extraction, ECG analysis, and signal re-construction. The framework is cloud-integrated and employs watermarking to ensure secure, safe, and high-quality health monitoring of healthcare data. [5].

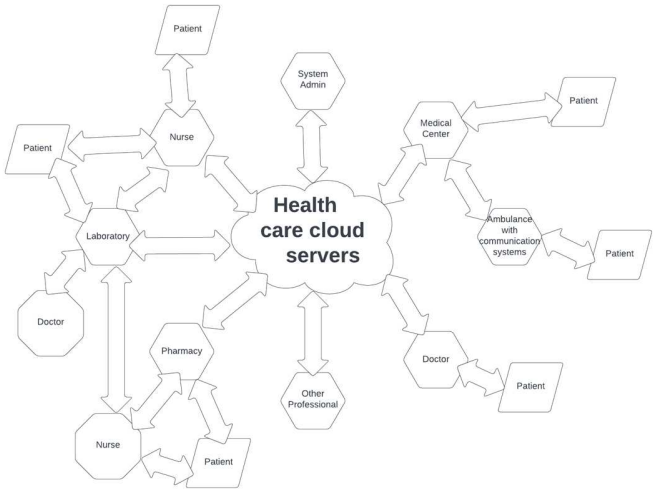

Fig. 1. High level Depiction of Health Care Cloud

III. EXISTING METHODOLOGY

CNNs are an advanced interpretation of deep neural net-works with spectral layers for learning lower and advanced level functions. CNNs are effective models for statistical forecasting, modeling, etc. The existing model presents an innovative aloofness-protecting solution termed sanitizer that utilizes neural learning to enhance therapeutics.[6] This miniature is founded on a Convolutional Neural Network with Bidirectional-LSTM and efficiently performs Medical Entity Recognition. sanitizer operates in a fog network-based smart healthcare system to curtail latency for medical applications that require timely response. The proposed solution can man-age varied data types, including numeric, alphanumeric, and textual data.[6]

To improve the model's accuracy, a hierarchical method based on weighted extreme gradient boosting was used [7]. This method continuously adds and trains new trees in each iteration to fit the residuals of the predicted values of the previous decision tree and the sum of the predicted values of all previous decision trees. Finally, the predicted values of all decision trees are summed together to obtain the final result.

IV. PROPOSED METHODOLOGY

Pairing-based cryptography (PBC) and a edge computing facility are required for the approach of securing the MBD in the healthcare cloud utilizing DMBD.By utilizing fog computing infrastructure and employing the decoy method, a Dummy Mobile Device (DMBD) is established. This approach can be perceived as an illusionary tactic since it deceives the attacker into thinking that they have gained access to the user's Mobile Device Database (MBD), when in reality, it is merely a simulated gallery meant to mislead them.

Consequently, as an initial measure, both authorized and unauthorized users will be directed towards the Dummy Mobile Device (DMBD), while legitimate authorized users will undergo verification and subsequently be directed to the

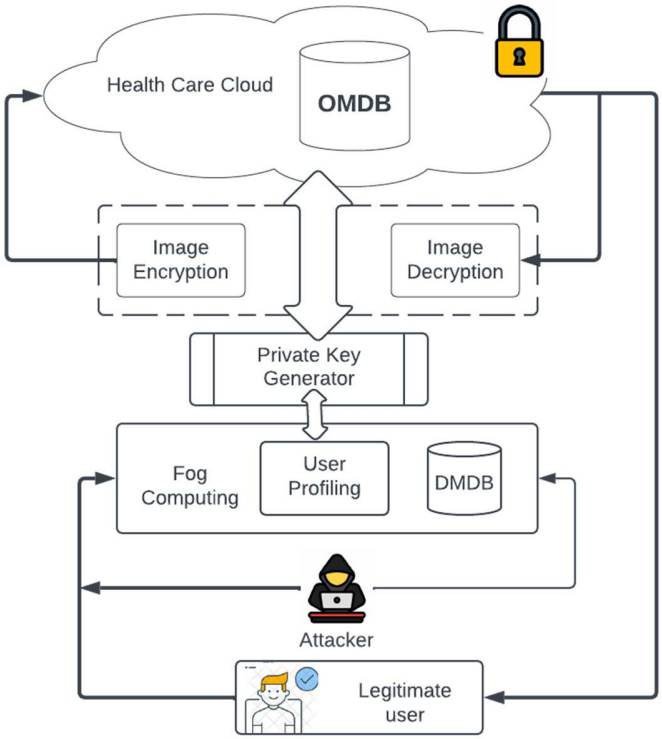

Fig. 2. Proposed System Architecture

Original Mobile Device Database (OMBD). Our belief is that by configuring the DMBD as the default option and keeping the OMBD hidden, we enhance the overall security of the original Mobile Device Database (MBD).

User profiling is a well-known technique that can be utilized to model how users access their information in the healthcare cloud, including when and to what extent. This behavior-based security method is commonly employed in fraud detection applications. Within the Dummy Mobile Device (DMBD), fabricated Mobile Device Databases (MBDs) are included to create the illusion that an attacker has gained access to the user's photos or medical images, when in reality, it is a decoy gallery. Legitimate users are already aware that the accessed gallery is not their original one, prompting them to proceed to the next step.

Upon advancing to the next step, legitimate users can access their Original Mobile Device Database (OMBD) after successfully completing a security challenge to verify their identity. The security challenge may involve a challenging security question or a verification code. Therefore, if a user successfully overcomes the security challenge, it confirms their legitimacy and grants them access to the OMBD, which is located in the cloud computing layer. In the event that a user only accesses the DMBD, a notification via SMS or email will be sent to the legitimate user, informing them of the unauthorized account access. The notification message will include details about the attacker, such as the access time, date, and IP address.

In order to ensure a significant resemblance between the two galleries, certain measures are taken. Whenever a legitimate user uploads a new photo or medical image to their account, a corresponding decoy photo from the fog computing system is automatically uploaded to their Dummy Mobile Device Database (DMBD). During the upload process, the user is expected to identify the category of the photo (such as ECG, X-ray, MRI, etc.). This category information is utilized by the fog computing system to select and add a photo belonging to the same category to the DMBD. This approach aims to make the decoy photo closely resemble the original photo, making it difficult for the attacker to differentiate between the real user's photo and the fake one. It is important to note that the responsibility of adding the decoy photo to the DMBD does not lie with the user. Instead, the decoy photo is automatically added to the DMBD while the user is uploading the original photo to the Original Mobile Device Database (OMBD).

When MBD is accessed and stored in the cloud via PBC, an access credential is produced for safe connection between the parties. This paper aims at safeguarding user multimedia data in the cloud , as part of ensuring a Cloud Data Mission. According to the studies, Blowfish is more effective because of its encryption and decryption time. Based on the size of the keys used, it's a bit safer than others. In addition, it does not require as much storage and capacity as remaining. Consequently, The most appropriate script is Blowfish for our proposed scheme and therefore best suited to use it.

V. CONCLUSION

In conclusion, the development of a security application aimed at safeguarding the Mobile Device Database (MDB) represents a promising field of research. This endeavor has the capacity to significantly enhance the security measures implemented in Healthcare Cloud environments. By focusing on the protection of sensitive healthcare data stored in mobile devices, this research has the potential to contribute to the overall security and privacy of healthcare systems. Continued advancements in this area can lead to improved security practices and ensure the confidentiality, integrity, and availability of healthcare data in cloud-based environments.

In this study, the main emphasis is on deploying a fog computing facility to safeguard sensitive healthcare data in the cloud. To do this, a tri-party one round authenticated key agreement protocol based on bilinear pairing cryptography has been presented. This protocol enables participants to generate a session key and safely interact with one another. Finally, a decoy approach is used to safely access and store the confidential healthcare data.

VI. FUTURE WORKS

Utilizing modern technologies such as machine learning, fuzzy logic, image processing, and others, it is possible to develop robust security systems for handling Medical Big Data. These technologies enable the creation of comparable security systems with enhanced accuracy and reliability.

Additionally, the development of new algorithms can further improve the performance of these systems. Cloud Computing, along with big data technologies like Hadoop, can be leveraged to efficiently manage and store vast amounts of data from users worldwide. In future research, the mentioned algorithms will be employed to enhance accuracy and improve diagnosis, particularly in scenarios where subtle data sets need to be analyzed. This holds great potential for advancing the field of medical data analysis and improving healthcare outcomes.

ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to all individuals who have contributed to the completion of this paper. We extend our sincere thanks to the authors of the relevant literature, whose valuable insights have played a crucial role in shaping our research. We also wish to express our appreciation to the reviewers and editors for their constructive feedback and suggestions, which have greatly contributed to the improvement of the paper's quality. Our gratitude extends to our institution for providing us with the necessary resources and facilities to carry out this research. Additionally, we would like to acknowledge the unwavering support we have received from our colleagues, friends, and families throughout this endeavor. Their encouragement and assistance have been pivotal in our success.

REFERENCES

[1] M. Chen, J. Yang, Y. Hao, , S. Mao, K. Hwang, "A 5G Cognitive System for Healthcare", Big Data and Cognitive Computing, Vol. 1, No. 1, DOI:10.3390/ bdcc1010002, 2017.

[2] M. S. Hossain, and G. Muhammad, "Healthcare Big Data Voice Pathology Assessment Framework," IEEE Access, vol. 4, no. 1, pp. 7806-7815, December 2016.

[3] M. Chen, Y. Hao , K. Hwang, L. Wang, L. Wang, "Disease Prediction by Machine Learning over Big Healthcare Data", IEEE Access, Vol. 5, No. 1, pp. 8869-8879, 2017.

[4] . Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, C. Youn, "Wearable 2.0: Enable HumanCloud Integration in Next Generation Healthcare System", IEEE Communications, Vol. 55, No. 1, pp. 54-61, Jan. 2017.

[5] M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT) - enabled framework for Health Monitoring," Elsevier Computer Networks, Vol. 101, No. (2016), pp.192-202, June 2016.

[6] A Deep Learning-Based Privacy-Preserving Model for Smart Healthcare in Internet of Medical Things Using Fog Computing Syed Atif Moqurrab, Noshina Tariq, Adeel Anjum, Alia Asheralieva, Saif U. R. Malik, Hassan Malik, Haris Pervaiz Sukhpal Singh Gill

[7] Hadeal Abdulaziz Al Hamid, Non-Member, IEEE, Sk Md Mizanur Rahman, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography".

[8] M. S. Hossain, G. Muhammad, Sk. M. M. Rahman, W. Abdul, A. Alelaiwi and A. Almari, "Towards End-to-End Biometrics-Based Security for IoT Infrastructure," IEEE Wireless Communication magazine, vol. 23. no. 5, pp. 45-51, October 2016