RESEARCH ARTICLE OPEN ACCESS

A Survey on Secure Medical Care Authentication in Cloud

K.Prem Kumar*, Kanishka B U**, Mythili J***, MythiliMeena D****
*(Computer Science and Engineering, M.Kumarasamy college of Engineering, Karur
Email: premkumark.cse@mkce.ac.in)
**(Computer Science and Engineering, M.Kumarasamy college of Engineering, Karur
Email: balukanishka@gmail.com)
***(Computer Science and Engineering, M.Kumarasamy college of Engineering, Karur
Email: mythilijayaraman97@gmail.com)
****(Computer Science and Engineering, M.Kumarasamy college of Engineering, Karur
Email: d.mythilimeena@gmail.com)

Abstract:

Telemedicine is one of the emerging fields for e-health research. To diagnose and evaluate a patient, the healthcare professionals need to access the electronic medical record (EMR) of the patient, which might contain huge multimedia big data including X-rays, ultrasounds, CT scans, and MRI reports. For efficient access and supporting mobility for both the healthcare professionals as well as the patients, the EMR needs to be kept in big data storage in the healthcare cloud. In spite of the popularity of the healthcare cloud, it faces different security issues; In the telemedicine service, EMRs including MBD, images, and multimedia medical data are transmitted on the fly over insecure internet connections as they are required by the remote doctors. Data theft attacks are considered to be one of the most serious security breaches of healthcare data in the cloud. The major vision of this project is to provide secure to medical big data that present in cloud using a fog computing facility. Here, a methodology is presented to secure patients' MBD in the healthcare cloud using the decoy technique with a fog computing facility. Proposed system uses Blow fish algorithm to encrypt the medical data before storing it on the cloud.

Keywords **—Decoy Technique, Tri-Party authentication key, Blowfish Encryption**

I. INTRODUCTION

Big data in healthcare refers to sets of electronic medical health data that are large and complex. Due to their huge volume and complexity, it is difficult (or infeasible) to man- age those data sets using traditional software and/or hard- ware. The diversity and volume of multimedia medical big data (MBD) and efficient accessibility of these datasets make it irresistible. MBD in the health-care industry includes patient data in electronic patient records (EPRs); clinical data from computerized physician order entries (CPOEs); machine generated/sensor data, such as from monitoring vital signs; clinical decision making systems (medical imaging, physician's written notes and prescriptions, insurance, laboratory, pharmacy, and other administrative data); social media posts, including Twitter feeds (so-called tweets), blogs, status updates on Facebook and other platforms, and web pages; and non-patient-specific information, including emergency care data, news

feeds, and articles in medical journals. Telemedicine is one of the emerging fields for e-health research. In the telemedicine service, EMRs including MBD, images, and multimedia medical data are transmitted on the fly over insecure internet connections as they are required by the remote doctors. The healthcare cloud infrastructure would make it much easier to pull all different healthcare information together for a patient while the patient moves from one hospital to another; as a result, the patients' information can be managed and tracked easily. The healthcare cloud is a cloud computing infrastructure where all the healthcare service providers and stakeholders can communicate with each other through the cloud servers. Healthcare cloud computing offers the benefit of both software and hardware through the provision of services over the Internet. Cloud computing is defined by ``a system for providing on-demand data access services through network to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". Similar to cloud computing, healthcare cloud computing has different issues related to its security, the most important of which are: legal and policy issues, data protection, privacy protection, lack of transparency, cyber security issues, absence of security standards, and software licensing. Each of these issues has different challenges that can be briefly discussed as follows. The challenges related to cloud computing legal and policy issues are: liability, applicable law, compliance, copyright, data portability, and data protection. Speaking about protection, privacy protection means to protect the personally identifiable information (PII), by making it clear to the consumer how it is used and where it is stored. Usually, privacy issues are all about three things, which are trust, uncertainty, and compliance. Also, another issue related to the consumer is lack of transparency, which may appear through the consumer not knowing where his/her data are physically stored or what happens to it. On the other hand, another cloud security issue is cyber security. In this paper, a methodology is presented to secure patients' MBD in the healthcare cloud using the decoy technique with a fog computing facility. It serves as a second gallery to contain decoy MBD (DMBD) that appear to the attacker as if it is the original MBD (OMBD). Unlike other methods, where the decoy files are called when an attacker is detected as accessing the system, in our proposed methodology the decoy files are retrieved from the beginning to ensure better security. Additionally, it uses a double security technique by encrypting the original file when an attacker recognizes that he/she is dealing with a decoy gallery; he/she would need to figure out how to decode the original gallery. As a result, our methodology ensures that the users' MBD are 100% secure and shortens the process. There is no need to worry if the user is an attacker, since by default it offers the decoy big data gallery directly to any user and keeps the original one hidden,

which is only made available to a legitimate user after successful verification.

II. RELATED WORKS

Secured Cloud Computing With Decoy Documents: Dnyanesh S. Patil, Suyash S. Patil, Deepak P. Pote, Nilesh V. Koli- Year: 2014

Cloud Computing is a virtualized compute power and storage delivered via platform-agnostic infrastructures ofabstracted hardware and software accessed over the Internet. These shared, on-demand IT resources, are created anddisposed of efficiently, are dynamically scalable through a variety of programmatic interfaces and Cloud computing is ageneral term for anything that involves delivering hosted services over the Internet. These services are broadly divided intothree categories: Infrastructureas- a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).. Withthese new computing and communications paradigms arise new data security challenges. Existing data protectionmechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to thecloud provider.

Our approach is to securing data in the cloud using offensive decoy & other various technologies. We monitor data access inthe cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challengequestions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protectsagainst the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approachmay provide unprecedented levels of user data security in a Cloud environment.

Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud: Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis- year: 2012

Cloud computing promises to significantly change the waywe use computers and access and store our personal and businessinformation. With these new computing and communicationsparadigms arise new data security challenges. Existingdata protection mechanisms such as encryption have failed inpreventing data theft attacks, especially those perpetrated byan insider to the cloud provider.We propose a different approach for securing data in thecloud using offensive decoy technology. We monitor dataaccess in the cloud and detect abnormal data access patterns.When unauthorized access is suspected and then verified usingchallenge questions, we launch a disinformation attack byreturning large amounts of decoy information to the attacker.This protects against the misuse of the user's real data.Experiments conducted in a local file setting provide evidencethat this approach may provide unprecedented levels of userdata security in a Cloud environment.

Data Security Issues and Strategy on Cloud Computing: Sonam Singh: 2013

Cloud Computing is a term, which involves virtualization, distributed computing, networking and web-services. It is a way of offering services to users by allowing them to tap into a massive pool of shared computing resources such as servers, storage and network. User can use services by simply plug into the cloud and pay only for what he uses. All these features made a cloud computing very advantageous and demanding. But the data privacy is a key security problem in cloud computing which comprises of data integrity, data confidentiality and user privacy specific concerns. Most of the persons do not prefer cloud to store their data as they are having a fear of losing the privacy of their confidential data. This paper introduces some cloud computing data security problem and its strategy to solve them which also satisfies the user regarding their data security.

Big data Security in HealthCare :Sudipta Chandra, Sowmys Ray and R.T. Goswami- year 2017

The present health care security situation in massive data environments has been summarized beside challenges featured and security problems that require attention. The volatility of massive data is what degree it changes, that's frequent change is often a challenge, they are doing not systematically monitor their data assets.

Ensuring Data Storage Security in Cloud Computing supported Hybrid Encryption:MrinalKanti Sarkar and Sanjay Kumar- year 2016

The authors propose an efficient and versatile data concealing scheme with explicit dynamic data support to make sure the protection of data once it's residing within the cloud data storage. Their scheme nearly guarantees the protection of data when it's residing in the data centre of any cloud service provider. They're not that specialize in the address concerning the error localization, communication overhead.

Cloud Computing is a virtual machine provide storage service through platform-agnostic infrastructures ofabstracted hardware and software accessed over the Internet. These shared, on-demand IT resources, are created anddisposed of efficiently, are dynamically scalable through a variety of programmatic interfaces and Cloud computing is ageneral term for anything that involves delivering hosted services over the Internet. Services of cloud are broadly divided intothree categories: Infrastructure-as- a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Withthese new computing and communications paradigms arise new data security challenges. Existing data protectionmechanisms such as encryption have failed in preventing data

theft attacks, especially those perpetrated by an insider to thecloud provider.

Our approach is to securing data in the cloud using offensive decoy & other various technologies. We monitor data access inthe cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challengequestions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This methodology protectsagainst the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approachmay provide unprecedented levels of user data security in a Cloud environment.

Conclusion

Thus the problem for securing the medical information will be solved by generating two photo galleries. The original multimedia big data wil be kept secret on the cloud and the decoy multimedia big data will be acting as a honeypot and this will be kept in the fog. When any unauthorized access is discovered, the user, by default, accesses the decoy file.

References

[1] M. Chen, J. Yang, Y. Hao, S. Mao, and K. Hwang, ``A 5G cognitive system for healthcare," Big Data Cognit. Comput., vol. 1, no. 1, p. 2, 2017, doi: 10.3390/.bdcc1010002.

[2] Frost & Sullivan: Drowning in Big Data? Reducing Information Technology Complexities and Costs for Healthcare Organizations.[Online]. Available: http://www.emc.com/collateral/analyst-reports/frost-sullivan-reducing-information-technology-complexities-ar.pdf

[3] M. Chen, S. Mao, and Y. Liu, ``Big data: A survey," Mobile Netw. Appl., vol. 19, no. 2, pp. 171_209, Apr. 2014.

[4] M. S. Hossain and G. Muhammad, ``Healthcare big data voice pathology assessment framework," IEEE Access, vol. 4, no. 1, pp. 7806_7815, Dec. 2016.

[5] M. Chen, Y. Hao, K. Hwang, L. Wang, and L. Wang, ``Disease prediction by machine learning over big data from healthcare communities," IEEEAccess, vol. 5, no. 1, pp. 8869_8879, 2017.

[6] M. Chen, P. Zhou, and G. Fortino, ``Emotion communication system," IEEE Access, vol. 5, pp. 326_337, 2017.

[7] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C.-H. Youn, ``Wearable 2.0: Enabling human-cloud integration in next genera- tion healthcare systems," IEEE Commun., vol. 55, no. 1, pp. 54_61, Jan. 2017.

[8] J. Bian, U. Topaloglu, and F. Yu, ``Towards large-scale twitter mining for drug-related adverse events," in Proc. SHB, Maui, HI, USA, 2012, pp. 25_32.

[9] M. S. Hossain and G. Muhammad, ``Cloud-assisted industrial Internet of Things (IIoT)_Enabled framework for health monitoring," Comput.Netw., vol. 101 pp. 192_202, Jun. 2016.

[10] W. Raghupathi and V. Raghupathi, ``An overview of health analytics," J. Health Med. Informat., vol. 4, no. 3, pp. 1_11, 2013.