Pairing Based Cryptography for Privacy Medical data in a Healthcare Cloud using Fogcomputing Facility

Vijayanand.S[2], Mathipriya.R[1], Muthulakshmi.S [3], Reeva.T[4], Sandhiya.C[5]
1 (Computer Science, The Kavery Engineering College / Anna university,India)
2 (Computer Science, The Kavery Engineering College / Anna university,India)
3 (Computer Science, The Kavery Engineering College / Anna university,India)
4 (Computer Science, The Kavery Engineering College / Anna university,India)
5 (Computer Science, The Kavery Engineering College / Anna university,India)

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. It support esay access and 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.

Keyterms: ***electronic medical record (EMR), fog computing, Blow fish algorithm, healthcare cloud.***

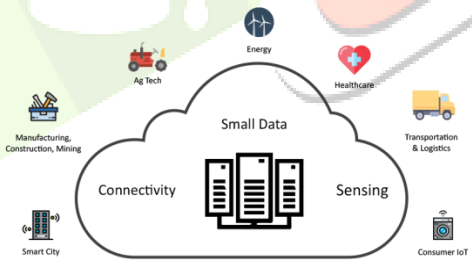
INTRODUCTION

Big data in healthcare refers to sets of eletronic 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 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); 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 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. Cyber security challenges are related to four factors which are: (1) information input, (2) information and commands output, (3) shared tenancy, and (4) physical infrastructure. Each one of these challenges contains different sub-challenges, for example information input challenges are categorized into three areas: (1) challenges related to the way of collecting and delivering the information to cloud computing applications, (2) challenges related to the mechanism used to transport the information from utility to cloud computing facility, and (3) challenges related to information storage facility. So, each cloud computing issue or challenge has different staff we need to know more about. At the end, to define the relations between consumers, utilities, and third parties in the cloud, a proper policy is needed in order to make sure that the cloud computing is secure. 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.

FOG COMPUTING

The concentration of computing resources (for example, servers, storage, applications and services) in data centers towards users for improving the quality of service and their experience. The fog computing ecosystem considered the user device layer comprises user devices that would traditionally communicate with the cloud. The edge node layer comprises multiple hierarchical levels of edge nodes. However, in the fog computing model, nodes close to the user are of particularinterest since the aim is to bring computing near user devices where data isgenerated. The different nodes, include traffic routing nodes (such as basestations, routers, switches and gateways), capability added nodes (such astraffic routing nodes, with additional computational capabilities or dedicated computational resources) and peer nodes (such as a collection of volunteereduser devices as a dynamic cloud). Workloads are executed in an offloading(both from user device to the edge and from the cloud to the edge), aggregatingand sharing models closer to the user.



Fog Computing

DATA SECURITY ISSUES AND SECURITY ON CLOUD COMPUTING

Lower down the stack the cloud vendor provides, the more security issues the consumer has to address or provide. 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 ssof 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.

IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM

Blowfish users must carefully select keys as there is a class of keys known to be weak, or switch to more modern alternatives like the Advanced Encryption Standard, Salsa20, or Blowfish's more modern successors Twofish

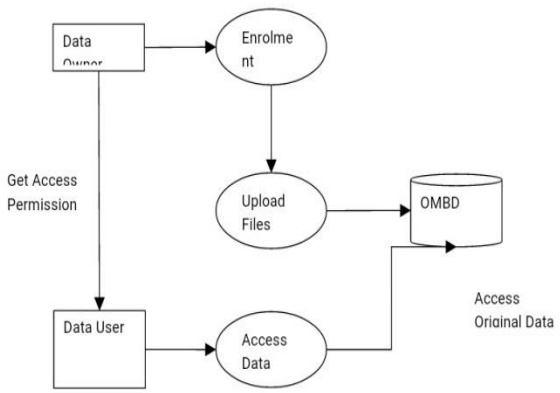
and Threefish.With the progress in data exchange by electronic system, the need of information security has become a necessity.Security becomes an important issue of communication and storage of images. This paper is about encryption and decryption of images using a secret-key.Encryption means conversion of plaintext into ciphertext.conversion of ciphertext into plain text is called as decryption. Blowfish designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits and default key is 64bits.It protect the system from the unauthorized persons and implemented faster than the popular other existing algorithms. The proposed algorithm is designed and realized using Visual basic.

PROPOSED SYSTEM

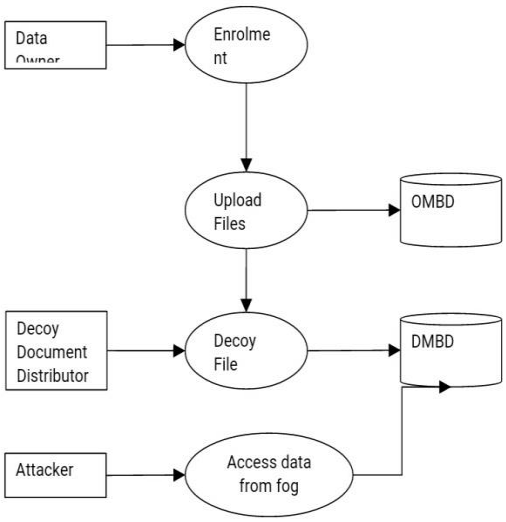
Proposed system is a new approach to provide security to the medical big data. Using fog computing facilities and the decoy technique, a DMBD is created. This technique can be considered as an illusion technique, as it makes the attacker believe that he/she has accessed the user's MBD while in fact it is just a decoy gallery. In our proposed system, once the user accesses his/her account, by default the DMBD is shown. Thus, both authorized and unauthorized users will be referred to the DMBD as the first step, while authorized legitimate users, as a second step, will be referred to the OMBD after being verified. We believe that by setting the default value of the DMBD as shown and the OMBD as hidden, we keep the original MBD more secure. Also, we believe that verifying that the user is legitimate is much easier than detecting the attacker, which is why we tried to deal with the attacker in the first place by offering the DMBD as the first step. When the user accesses his/her account, whether he/she is a legitimate user or an attacker, his/her first step would be accessing the DMBD, which is located in the fog computing layer side by side with user profiling. User profiling is a familiar technique that can be applied to model in what way, at what time, and how considerable users access their information in the healthcare cloud.The DMBD contains fake MBD, which are supposed to make an attacker believe that he/she has accessed the user's photos/medical image while in fact it is just a decoy gallery. The legitimate user already knows that the gallery he/she accessed is not his/her original one, so would move on to the next step. Moving to the next step, the legitimate user can access his/her OMBD after being verified by passing the security challenge. The security challenge might be a challenging security question or even a verification code. Thus, if he/she passes the security challenge, that means he/she is the legitimate user, so will be able to access the OMBD which is located on the cloud computing layer. In the event of the user accessing only the DMBD, an SMS or email will be sent to the legitimate user to inform him/her that his/her account has been accessed. The message will contain the attacker's information (e.g., access time and date and the IP address). When the user uploads the photo, he/she is supposed to recognize the photo category (ECG, X-ray, MRI, etc.), which will help fog computing to add the photo that belongs to the same category on the DMBD; this would make it closer to the original photo, so that the attacker would not differentiate between the real user's photo and the fake one. Thus, in our methodology, the user is not responsible for adding the decoy photo in his/her DMBD, since it will be added automatically

Data Flow Diagram

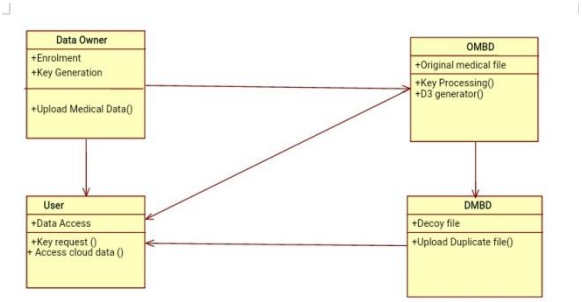
Level 0:



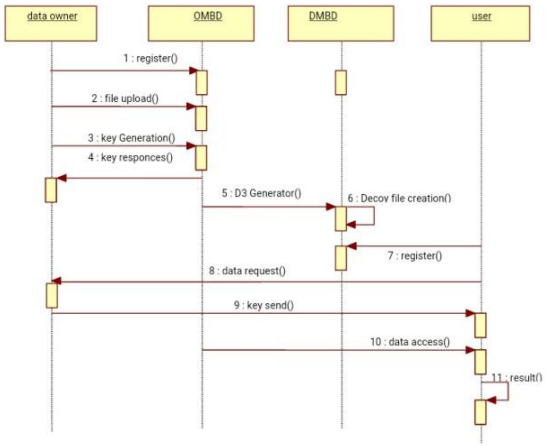
Level 1



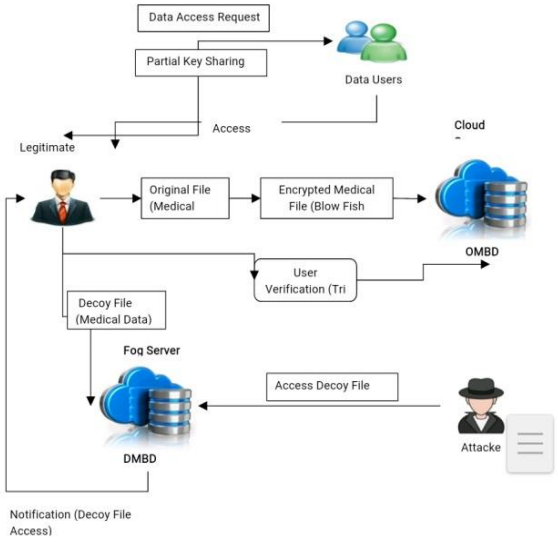
CLASS DIAGRAM



SEQUENCE DIAGRAM

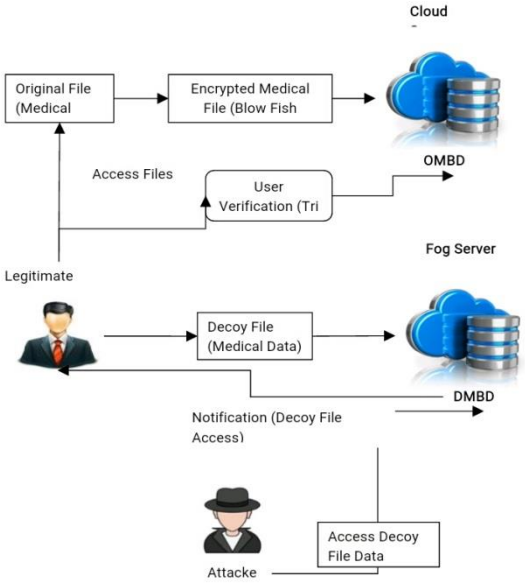


ARCHITECTURE



EXISTING SYSTEM

In existing there are different security issues in mobile cloud computing. These can be divided into five categories: (1) physical threats, which include mobile possession and lost or stolen devices; (2) application-based threats, such as those involving malware, spyware, privacy, and vulnerable applications; (3) network-based mobile security threats, including Wi-Fi sniffing, denial of service, and address impersonation; (4) web-based threats, such as phishing scams, drive-by downloads, browser exploits, and jail broken devices; and (5) other active attacks, including Internet protocol vulnerabilities, information recovery vulnerability, and unauthorized access to management interface. A decoy defense network can be deployed to bolster the security in different situations. One usage scenario involves using a decoy within a local computer, which means placing the decoy document within the same environment in which it was created. In another scenario, the decoy can be located on a network level. In both scenarios, the decoy is used to protect documents on different levels. However, a decoy can also be used to protect software, as by being made to look like a legitimate source code, decoy software can protect real software from unauthorized usage. Another decoy usage scenario applies a voicemail decoy to detect malicious activity; here the decoy is a legitimate voice message but contains false information. Lastly, a cloud-based decoy can be used to protect documents in the cloud against insider attacks. A few studies have focused on securing cloud data by using decoy documents. For instance, first carried out user behavior profiling to determine unauthorized access. When an attacker accesses the cloud, a decoy document is returned such that the real user's data are kept secure. Each decoy document header contains a hidden Hash-based Message Authentication Code (HMAC).Verification of whether or not the document is a decoy is done by calculating the HMAC based on the content of the document; if the two HMACs match, then the document is a decoy and an alert is issued. In this case, decoy documents are used for two purposes: first, to validate whether or not the data access is authorized when abnormal information access is detected and second, to confuse the attacker by providing false documents. It should be noted that only decoy documents are used in this study, and these are selected manually and added into the _le system by the user. In a similar technique carried out, malicious insider attacks were prevented by using decoy information technology. When abnormal information access is detected, the decoy helps to validate whether or not the access is authorized. Hence, when unauthorized data access is detected and verified, a malicious inside flood with bogus information is returned to dilute the real user data. Abnormal data access patterns are detected by monitoring the data access. When unauthorized access is detected and verified, a large amount of decoy information is returned to the attacker to protect the real data from any misuse. Such technology could offer exceptional levels of user data security in cloud computing and social networks as well. The protocol used an approach called selective encryption: because of performance issues, not all data can be encrypted, and to address this concern, only selected information that needs more security is encrypted. This is done by giving the user an option to completely encrypt, selectively encrypt, or not encrypt his/her data at all. To protect the data from insider attacks, a data cleaning approach is used. When the data are decrypted by a legitimate user, they are stored in the volatile memory of the physical machine for a temporary period, during which they could be misused by an insider attacker; a data cleaning technique is used to address this concern. As previously mentioned, besides selective encryption, fog computing is applied. To profile the user's search behavior, a neural network is used



PROPOSED ARCHITECTURE

ALGORITHM

Blowfish has been unique and an efficient algorithm that has become popular in the open source community.

- Blowfish is symmetric block cipher encryption algorithm.
- The Blowfish encryption algorithm operates on 64-bit bit blocks of plaintext.
- Supports variable key lengths ranging from 32 up to 448 bits; the default key length is 128 bit.

Main:

Get input
L = input[0-31]
R = input[32-63]
For i = 0 to i = 15 L = L XOR π
L = f-Function(L) (detailed F function below)
R = L XOR R
Swap L and R Swap L and R (intended to nullify the last swap)
L = L XOR P18
R = R XOR P17
output = combined result of L and R
return output

f-Function:

Get input
L = input[0-7]
centerL = input[8-15]
centerR = input[16-23]
R = input[24-31]
L = S-Box(L) (note that the result of the S-Box is a 32 bit data stream)
centerL = S-Box(centerL)
centerR = S-Box(centerR)
R = S-Box(R)
L = L + centerL (note: this is mod 232 addition)
L = L XOR centerR
L = L + R
return L

MODULES

DATA OWNERS

Data owners are may be a patient or doctor. Data owner want to register for data uploading. Data owner can login from anywhere using her/his username and password and upload file, using their own file key. And later she/he can download the file using the same key. When uploading the file the content will encrypted using Blowfish encryption before saved in to the database.

OMBD

OMBD is a cloud server that consists of Original Medical Big Data. When the user uploads new files, the OMBD is supposed to communicate with the DMBD to inform it to add a new decoy files. Moving to the next step, the legitimate user can access his/her OMBD after being verified by passing the security challenge. The security challenge might be a challenging security question or even a verification code. Thus, if he/she passes the security challenge, that means he/she is the legitimate user, so will be able to access the OMBD which is located on the cloud computing layer.

DMBD

Creating decoy information and locating it beside the real information in the cloud to hide the true data of the user is also called fog computing. DMBD is used as a trap gallery that makes it not of direct relevance to the legitimate user but it is used to secure users OMBD by distracting the attacker. DMBD is situate in the fog computing as a honeypot to secure the original one, which is located in the cloud. As noted, a number of anomaly-detection systems are provided by fog computing. Creating decoy information and locating it beside the real information in the cloud to hide the true data of the user is also called fog computing. DMBD is used as a trap gallery that makes it not of direct relevance to the legitimate user but it is used to secure users OMBD by distracting the attacker. DMBD is placed in the fog computing as a honeypot to protect the primal one, which is found in the cloud. As noted, a number of anomaly-detection systems are provided by fog computing such as user profiling and a decoy file system. Therefore, for each newly stevedore MBD in the OMBD, a decoy one will be situate on the DMBD. Therefore, for each newly uploaded MBD in the OMBD, a decoy one will be placed on the DMBD.The fast increase in the number of publications referring to “big data,” inattentive of disciplines, as well as those in the healthcare domain

Decoy Technique

Decoy is a file that consists of bogus information. This file is perfectly believable and should make it impossible for an attacker to find out that the data are not real. Fog computing can be considered as an alternative name for the Decoy Document Distributor (D3), which is a tool for generating and monitoring decoys. This strategy is used to protect the real, sensitive data by providing a fog of misinformation. The basic idea of decoy technique is to limit the damage caused by stolen data by decreasing the value of the stolen information.

SYSTEM TESTING

Software testing is a method of assessing the functionality of a software program. There are many different types of software testing but the two main categories are dynamic testing and static testing. Dynamic testing is an assessment that is conducted while the program is executed; static testing, on the other hand, is an examination of the program's code and associated documentation. Dynamic and static methods are often used together. The most common types of testing involved in the development process are: 1.Unit Test, 2.Integration Test,3.Validation Test

CONCLUSION

work concentrates on protecting user's multimedia data within the cloud by using fog computing. To this end, two photo galleries are generated. The OMBD is kept secretly in the cloud and the DMBD is used as a honeypot and is kept in the fog. Therefore, inlieu of recovering the DMBD only when any unauthorized access is discovered, the user, by default, accesses the DMBD. The OMBD is only accessible by a user after verifying the authenticity of the user. Thus, the original multimedia data become more secure by setting the default value of the DMBD, while the OMBD is kept in a hidden gallery.In future we can reduce the storage of the files. Use compression technique on data before storing it on cloud. This compression will help for data storage reduction.

REFERENCE

[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," IEEE Access, 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.