A Survey on a Security Model for Electronic Health Records in Healthcare Cloud using Fog Computing

R.Roshan Joshua[1], G.Raja[2]

M.E. Student[1], Assistant Professor[2]

Department of Computer Science and Engineering, JJ College of Engineering and Technology, Trichy, Tamil Nadu, India

***Abstract:* - Data safety is the most important undertaking faced through cloud garage. Cloud computing and garage solutions provide users and numerous corporations with several talents to keep and way their facts in third party facts centers. Here, imparting a way for securing statistics in cloud garage with fog computing. The need of rapid and comfortable transmission is critical in the healthcare environment. Nowadays, the transmission of scientific picture is an everyday habitual and it's miles essential to discover an efficient manner to transmit them over the internet. In this research, suggest a new method to encrypt an image for secure and denoised transmission. This survey deals with image cryptography, records hiding and steganography. To offer higher embedding potential without sacrificing the imperceptibility, a novel steganographic approach based totally on nine-pixel differencing with modified Least Significant Bit (LSB) substitution is proposed. After LSB substitution the pixel values are readjusted to minimize distortion such that those modified values do not disturb the embedded bits. Steganography is the approach to cover the message in virtual media. This survey shows a proposed hybrid model the usage of public key Elliptical Curve Cryptography (ECC) and Steganography offers extra security than a Single ECC or Steganography technique. Application of this research is to provide important data of net clients, navy, distinct corporate sectors those which might be often the usage of public community for communication.**

***Keywords:* - Medical image security, Image steganography, LSB encoding and decoding, Elliptic Curve Cryptography.**

I. INTRODUCTION

Fog Computing permits a new breed of programs and offerings, and that there is a fruitful interplay among the Cloud and the Fog, specially with regards to data management and analytics. Fog Computing extends the offerings of Cloud Computing paradigm to near to the network person. While Fog and Cloud use the identical sources (networking, compute, and garage), and share the various equal mechanisms and attributes (virtualization, multi-tenancy) The Fog goal and prescient was conceived to cope with packages and offerings that don't suit nicely the paradigm of the Cloud.Similar to cloud computing, healthcare cloud computing has extraordinary troubles associated with its security, the maximum essential of which might be: legal and policy coverage problems, facts safety, privacy safety, lack of transparency, cyber protection problems, absence of protection standards, and software licensing. In this survey, a new methodology is proposed to relaxed patients' MBD within the healthcare cloud using the decoy approach with a fog computing facility. It offers service like 2d gallery to incorporate decoy MBD (DMBD) that seem to the attacker as though it's far the authentic MBD (OMBD). Unlike other strategies, in which the decoy files are known as when an attacker is detected as accessing the system, in proposed method the decoy documents are retrieved from the start to make certain higher protection.

Decoy Technique

The basic concept behind this method is to limit the harm because of stolen facts with the aid of decreasing the value of the stolen facts. To acquire this, the decoy needs to have positive capabilities. First, it should be reliable. In the absence of any extra information, a perfectly believable decoy needs to make it impossible for an attacker to find out that the records are not real. Thus, the decoy has to seem believable and truthful. Second, the decoy must be enticing sufficient to of the attacker and make him/her open the file. Third, the decoy ought to be conspicuous, that's intently related to being enticing. Whereas attractive is related to how curious an attacker is ready a decoy, conspicuousness has to do with how clean a decoy is to get admission to. Therefore, the decoy ought to be without problems located through seek queries. Fourth, the decoy needs to be differentiable so that the real person can distinguish between the real and the decoy file. Balancing differentiability for real customers with believability for attackers is one of the crucial aspects of any decoy deployment device. Fifth, the decoy should be non-interfering in order that the actual person will now not accidentally misuse the artificial information contained inside the decoy. Finally, the decoy should be detectable; this feature refers back to the ability ofdecoys to alert their owners when they have been accessed.

Information Hiding using Steganography

Steganography is the art of hiding the truth that records exchange is taking place, with the resource of hiding statistics in exceptional facts. Many wonderful provider document carriers can be used, but digital pictures are the most popular due to their frequency on the Internet. For hiding secret information in pictures, there exists a massive form of steganographic techniques some are greater complex than others and they all have respective robust and weak points. Different packages have wonderful necessities of the steganography approach used. Since the rise of the Internet one of the maximum critical factors of records technology and communication has been the security of information. Cryptography is the technique by using which the facts to be transmitted is hidden in a manner such that handiest the meant recipient can apprehend it. The preliminary records are known as plaintext and the encrypted statistics is known as cipher text. A key is used to cover the records. There are different sorts relying on the wide variety and way wherein the keys are used.

Symmetric Key Cryptography is sincerely the method by means of which equal cryptographic keys are used for the motive of each encryption and decryption. The receiver can get back authentic data via using the important thing. The symmetric key cryptography affords high rates of record, utilization as primitives to construct various cryptographic mechanisms and can be blended to produce stronger ciphers. The foremost truth here is that the security of facts depends on the security of the key. So, care has to be taken even as changing keys between the sender and the receiver. Symmetric cryptosystem have a problem of key transportation. The secret key is to be transmitted to the receiving system earlier than the real message is to be transmitted. Every manner of electronic verbal exchange is insecure as it is not possible to assure that nobody will able to tab information exchange channels. So the simplest cozy way of exchanging keys might be exchanging personally. Symmetric cryptosystem can’t provide virtual signatures that can’t be repudiated.

This survey is organized as, the Section I consists of brief introduction of medical data security, impacts, data secure techniques. Section II elaborates the related work. Section III provides the details about existing methodologies. Section IV explains the proposed work with provides comparative analysis. Section V explains the proposed techniques for secure medical images. In Section VI, conclude the overall survey paper.

II. RELATED WORK

Saniket M. Kudoo, et al.[1] proposed a mechanism to helps security functions to statistics and thereby allows for detection of invalid get admission to and thereby its prevention to permit legitimate distribution of data. The decoy files deliver HMAC authentication code for every file user down load or get admission to. The HMAC is computed over the report’s content precise to each user. When decoy files loaded into memory confirm that weather document is decoy files by way of computing HMAC primarily based on all of the contents of that documents. For gaining access to or downloading any documents from surroundings this device will ask every time for user to insert passkey which they already got from machine at the time of registration into cloud surroundings. So each depended on or registered user has their respective passkey generated by the hash message get admission to control for whenever. Once unauthorized information get right of entry to or publicity is suspected in system and later tested with the passkey or challenge question and gadget can redirect her or him to fog statistics.

Salvatore J. Stolfo, et al.[2] proposed a method for securing facts inside the cloud using offensive decoy technology. Here reveal facts get right of entry to in the cloud and hit upon atypical information get admission to styles. When unauthorized get admission to is suspected and then validated using project questions, launch a disinformation attack by returning massive amounts of decoy facts to the attacker. This protects in opposition to the misuse of the consumer’s actual information. Experiments carried out in a neighborhood report putting provide evidence that this method may additionally offer unheard of stages of user records safety in a Cloud surroundings. Decoy documents stored within the Cloud along the person’s actual information additionally serve as sensors to come across illegitimate get admission to. Once unauthorized statistics access or publicity is suspected, and later demonstrated, with challenge questions as an instance, inundate the malicious insider with bogus information to be able to dilute the person’s real statistics.

Arwinder Singh, et al.[3] proposed a system for securing statistics saved within the cloud the use of decoy technology. In this technique display facts get right of entry to inside the cloud and stumble on abnormal statistics access. Whenunauthorized access is detected that customers, interest could be tracked in log details desk. Based on the sports done through unauthorized person. Admin will have blocked or delete that person. When a new consumer enters into this System, he has to register first. After successfully registered, that person gets a key via mail. And during login, if the user enters incorrect password constantly greater than three times, he'll get admission to and his hobby could be tracked on log info desk inside the database. And after this, something activities he is doing that also can be tracked within the log desk. If he downloads any file, he gained get unique file. Instead of that he's going to get decoy record. If a consumer entered accurate password and he'll get entry to.

G. Rathi, et al.[4] proposed a device that implements records classification based totally on the sensitivity levels of statistics i.e. For higher touchy statistics higher degree of encryption will be enforced and lower sensitive information will use decrease level of encryption. The machine allows the physician to upload the report after which health practitioner is asked his mystery key wherein the device makes use of this key along with the physician and affected person records to create a device generated key to encrypt the record. To gain pleasant grained and scalable information get entry to manipulate for clinical information saved in cloud servers, recommend Attribute Based Encryption (ABE) strategies including key coverage characteristic primarily based encryption, position based totally encryption, and so on. To encrypt each patient’s scientific report file. For this here describe an approach which allows garage that is comfortable and patient’s fitness facts with controlled sharing.

Kushan Shah, et al.[5] proposed a singular version for the identical, the CPRBAC version turned into more controllability, traceability of records and authentication preservation to such sources online underneath a great-grained information safety scheme. The information is saved in the shape of EHR – Electronic Health Records that is to be had online anytime and may be updated as and whilst the affected person undergoes any remedy of prognosis. The report data alongside the helping information like x-ray snap shots, test images, affected person private records and treatment procedure can be saved. The foremost problem that needs to be treated at this level is the security of the above mentioned information. These records can be misused very effortlessly and might cause harm to the person if fallen victim to such schemes. Encrypting the records stored on-line is as a consequence very important and the key for decrypting the information should most effective be made to be had to the medical doctors and involved stakeholders.

Yin Zhang, et al.[6] proposed a cyber-physical device for patient-centric healthcare packages and offerings, referred to as Health-CPS, built on cloud and huge records analytics technologies. This gadget consists of a statistics series layer with a unified standard, a statistics control layer for allotted storage and parallel computing, and a records-orientated provider layer. Patients usually will recognize extra than a doctor. As such, the facts and information base can be enriched and shared by way of the doctors over the cloud. The sufferers also can actively take part in medical sports assisted by using massive facts. Through smart phones, cloud computing, 3-D printing, gene sequencing, and Wi-Fi sensors, the clinical proper returns to the sufferers, and the position of a doctor is as a representative to offer choice help to the sufferers.

III. EXISTING METHODOLOGY

As increasingly more healthcare groups undertake Electronic Medical Records (EMRs), the case for cloud information garage will become compelling for deploying EHR structures: now not only is it cheaper but it also offers the flexible, extensive-place mobile access more and more needed within the current technology improved world. However, earlier than cloud-based EMR systems can come to be a fact, troubles of data protection, affected person privateness, and average performance need to be addressed.The secret key of a healthcare provider can decrypt a particular cipher-text only if the characteristic set of the healthcare company's key satisfies the access coverage related to that cipher-text. IBE sender can encrypt a message the use of best identification without want of public key certificates. Common function of IBE is that they view identities as a string of characters. Steganography is a science which deals with invisible communications, i.e., the embedding of secret messages that have to not be detected in the course of communication. Because steganography can be used as a device to preserve privacy in communications, it's miles herbal that humans assault it.

Medical Image Encryption

Few approaches had been proposed for the combination of image encryption and compression. A new idea is to use reversible statistics hiding algorithms on encrypted images via wishing to get rid of the embedded records earlier than the image decryption. In This method, encrypt the original image with percentage mechanism then embed the encrypted image with patient data through using LSB lossless embedding technique with records hiding key after that for more protection. Apply steganography in embedded image as secrete photograph and encrypted image of every other medical image as a cover picture.

Encryption Algorithms

Various algorithms were studied in the process to encrypt the EHRs that are to be stored on cloud. As every encryption algorithm has different encryption and decryption time. The encryption and decryption formula for RSA is given as C= (Pe mod n) and P= (Cd mod n) respectively which follows the polynomial time complexity whereas for attacker it is e√C mod n which follows modular exponential complexity. With traditional implementations, doubling the RSA key duration method that encryption could be 4 times slower, and decryption will be 8 times slower. RSA encryption is a lot quicker than RSA decryption.AES (Advanced Encryption Standard) algorithm is a non-Fiestel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12 or 14 rounds. The key size which can be 128, 192, or 256 bits, depends on the number of rounds. Depending on the key size there are three different versions of AES: AES-128, AES-192 and AES-256. Various algorithms are analyzed with their break time that can be used to achieve various levels of security.

Integrity algorithm:

When integrity algorithms are used such as SHA-1 for creating hashed digest where SHA-1 has larger states i.e. 160 bits and 80 rounds. SHA-1 rounds have an extra bit rotation which makes it much stronger against collision attacks. SHA-1 has extra bit rotation hence there is more confusion than the previous version. It is one-way transformation. SHA-1 hashing function is used for integrity of the data that is to be sent. Any change in the data with very high probability change the hash value and thus the receiver would know that the data has been changed.

IV. COMPARISON AND DISCUSSION

Author names	Methodology	Performance	Advantages	Disadvantages
Saniket M. Kudoo, et. al.,[1]	A key hash message authentication code (HMAC) mechanism	It calculates message authentication code containing cryptographic hash function in combination of secret cryptographic key.	It can block his access or declared as an invalid user.	Possible to data loss and data leakage issues.
Salvatore J. Stolfo,et. al.,[2]	Decoy technology	When unauthorized access is suspected, launch a disinformation attack by returning large amounts of decoy information to the attacker.	Detection of masquerade activity.	It does not provide solution to the levels of assurance most people desire.
Arwinder Singh, et. al.,[3]	Decoy technique with secure encryption	It monitor data access pattern in the cloud and also detect abnormal data access.	The dense geographical distribution and support mobility.	Does not focus on ways of secure the data from attacker.
G. Rathi, et. al.,[4]	Decoy Information Technology	In the occurrence of any abnormal information access detection it confuses the attacker with bogus information.	Efficient and effective for finding the fog misuse or attacker for cloud computing	Secret key easily leaked by malicious users
Kushan Shah, et. al.,[5]	CPRBAC (Cloud-based Privacy-aware Role Based Access Control) model.	EHRs which is available online anytime and can be updated.	Make it difficult for an intruder to understand the data.	Does not support for storing high level data like videos from ultrasound
Yin Zhang, et. al.,[6]	Pairing-based cryptography over an elliptic curve.	Two nodes communicateseparately and compute the same secret key properties.	No need to store any keys from the other nodes	Difficult to adopt various sensor nodes
R. Josephus Arunkumar, et.al.,[7]	Image Encryption	First convert image into pixels and then encrypting the converted pixels.	Helps to access EMR even if they're miles apart.	Risks vary depending on the data sensitivity level.

V. PROPOSED FRAMEWORK

Steganography and cryptography are very typical techniques used for making sure the safety of the electronic medical data over in the internet. Cryptography offers away the reality that a few critical records is present and is encrypted. But the attacker will must discover the right algorithm out of such lots of, that might have been used for encrypting and then find out the records from the cipher textual content. Steganography however hides the fact that the provider has something hidden in it. Many algorithms based totally on the two are to be had for the identical. Steganography is the artwork of writing hidden messages in the sort of way that no one, apart from the sender and the meant receiver, knows the lifestyles of the message. This differs from cryptography is the artwork of secret writing, which is used to make message unreadable to third party but does now not hide the existence of secret information sharing.Numerous approaches of preserving one's non-public, economical or medical information are consequently being used by individuals, organizations, and governments. When it comes to preserving patient facts in clinical photographs, developed an records hiding methodology that includes the ECC and nine pixel based hiding technique. With this machine, any scientific photograph a good way to be electronically transferred (i.e. Emailed, faxed, and many others.) could have the affected patient's information hidden and embedded in the image outside of the least significant bits.ECC is an approach to public key cryptography primarily based on the algebraic shape of elliptic curves over finite fields. Its protection is based on the opportunity of efficient additive exponentiation and absence of efficient (classical) algorithms for additive logarithm. In finite fields ECC is based totally on elliptic curves of algebraic shape. Key size is small while examine to different strategies. It can capable of compute factor multiplication. Input picture records are entered to encrypt the name of the game records.

LSB Steganography

The way of embedding the secret information within the cover file is called LSB insertion. In proposed technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image. If 24-bit color images are used to perform LSB, then the amount of modification will be small.

LSB Encoding

First the unique image and the compressed encrypted secret message are taken. Then the encrypted secret facts need to be transformed into binary format. Binary conversion is accomplished via taking the American Standard Code of Information Interchange (ASCII) values of the person and converting them into binary layout and producing move of bits. Similarly, in cover photo, bytes representing the pixels are taken in unmarried array and byte stream is generated. Message bits are taken sequentially after which are positioned in LSB little bit of image byte. Same process is followed till all the message bits are located in photograph bytes. Image generated is called 'Stego-Image'. It is prepared for transmission through the Internet.

Algorithm for hiding mystery facts in Cover image:

Step-1: Read the cover media image and secret information which is to be embedded in to the cover image.
Step-2: Compress the secret facts.
Step-3: Convert the compressed secrets into cipher textual content by means of using secret key shared by receiver and sender.
Step-4: Convert compressed encrypted textual content message into binary shape.
Step-5: Find LSBs value of each RGB pixels that present in cover image.
Step-6: Embed the secret data bits into bits of LSB of RGB pixels of the cover image on the basis of nine pixel strategy.
Step-7: Continue the procedure till the secret information is absolutely hidden into cover document.

LSB Decoding

First, 'Stego-Image' is taken and single array of bytes are generated as it become carried out at the time of encoding. The general number of bits of encrypted secret information and the bytes representing the pixels of stego-image are taken. Counter is to begin with set to 1, which in turn offers the index range of the pixel byte where secret message bit is available in LSB. The procedure is continued till very last secret message bit is reached. After this, the bit circulation of the message shall be generated. Available bits are grouped to shape bytes such that each byte represents single ASCII character. Characters are stored in textual content record which represents the encrypted embedded message. After that the decryption and decompression are to be done.

Algorithm for unhiding secret data from Stego image:

Step-1: First read out the stego image.
Step-2: Find LSBs value of each RGB pixel of the stego image.
Step-3: Find and retrieve the LSBs of every RGB pixel present in stego image.
Step-4: Continue the procedure till the message is absolutely extracted from stego image.
Step-5: Decompress the extracted secret facts.
Step-6: Using shared key, decrypt secret records to get original records.
Step-7: Reconstruct the secret statistics.

Elliptic Curve Cryptography

Elliptical curve cryptography (ECC) is a public key encryption method based on elliptic curve principle that can be used to create quicker, smaller, and extra efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation in preference to the traditional method of generation because the manufactured from very large prime numbers. The era may be used together with maximum public key encryption methods, consisting of RSA, and Diffie-Hellman. According to some researchers, ECC can yield a degree of safety with a 164-bit key that different structures require a 1,024-bit key to achieve.

ECC Algorithm Steps

Key Generation

Key generation is an important part where have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, to select a number**'d'** within the range of **'n'**. Using the following equation can generate the public key

$$\mathbf{Q = d * P}$$

d = the random number that have selected within the range of (**1 to n-1**). **P** is the point on the curve.

'Q' is the public key and**'d' is the private key.**

Encryption

Let 'm' be the message that are sending. Have to represent this message on the curve. These have in-depth implementation details.Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 – (n-1)].Two cipher texts will be generated let it be **C1** and **C2**.

$$\mathbf{C1 = k*P}$$
$$C2 = M + k*Q$$

C1 and C2 will be send.

Decryption

Have to get back the message 'm' that was send to us,

$M = C2 – d * C1$

M is the original message that has sent.

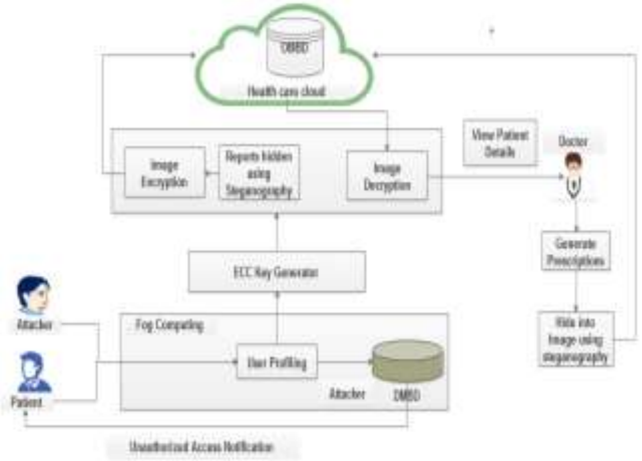

Fig 5.2 A Security model for Electronic Health Records in Healthcare Cloud using Fog Computing.

VI. CONCLUSION

The need of fast and secure transmission is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the net. This survey deals with image cryptography, data hiding and steganography. While protection of a patient's personal data is very crucial it is also important that the patient be reassured that the data being viewed is that of themselves. In this research a combined approach of cryptography, data hiding and steganography is used. In this method the original image is encrypted using ECC method then the encrypted image is embedded using LSB data hiding method with patient information. This survey shows, the proposed techniques provides more reliable and secure medical data sharing when compared to existing security mechanisms.

REFERENCES

[1]. Saniket M. Kudoo, Prof. Dilip Motwani, "Fog Computing: Data Theft Detection in Cloud with Behaviour Pattern & Decoy Stuff", International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2016,pp. 168-171.

[2]. Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2013, pp. 1–20.

[3]. Arwinder Singh, Abhishek Gautam, Hemant Kumar, Er. C.K. Raina, "Decoy Technology in Fog Computing", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 3, March 2017,pp. 798-804.

[4]. G. Rathi, Abinaya. M, Deepika. M¸ Kavyasri. T, "Healthcare Data Security in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015, pp. 1807-1815.

[5]. Kushan Shah and Vivek Prasad, "Security for Healthcare Data on Cloud" International Journal on Computer Science and Engineering (IJCSE), Vol. 9 No.05 May 2017, pp. 207-212.

[6]. Yin Zhang, Meikang Qiu, Chun-Wei and Atif Alamri, "Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data" in IEEE Systems Journal August 2015, pp. 1-8.

[7]. R. Josephus Arunkumar, R. Anbuselvi, "Enhancement of Cloud Computing Security in Health Care Sector" International Journal of Computer Science and Mobile Computing, Vol.6 Issue.8, August- 2017, pg. 23-31.

[8]. Divya Rayal and Smita Jangale, "Cloud based Information Security and Privacy in Healthcare", International Journal of Computer Applications (0975 – 8887) Volume 150 – No.4, September 2016, pp. 11-15.

[9]. Huaqun wang, "Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record", IEEE Trans. Inf. Forensics Security, vol. 10, no. 1, Jan. 2015,pp. 69-78.

[10]. Qinlong Huang, Wei Yue, Yue He, Yixian Yang, "Secure Identity-based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing" IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, Jul. 2014, pp. 1431-1441.