Patient Information Storing In Private Cloud Using Image Steganograhy With Advanced Encryption Standard(AES)

Praveen R[1], Rohit Kumar Jain R[2] ,Selva Shankaran S[3] ,Vishal Jain R[4],Jeyalakshmi S[5]
[1, 2, 3, 4, 5] Dept of Information Technology
[1, 2, 3, 4, 5] Valliammai Engineering College, TamilNadu, India.

Abstract- *Big data has brought a revolution in the universe of data conclusive. If the information is released or shared with the third party, it abuses the security of the data. So it is necessary to enhance the security over the personal sensitive data. Here we consider the data set as electronic health care records, which contain the personal sensitive data. Most of the existing systems are failed because of scalability, utilization of data and security of data on the public cloud. In proposed system it is mandatory to store the information in a secure format. For that an effective system or infrastructure is used. For the aid to provide support , they don't have to develop their own particular framework. As the result it can decrease estimated cost of utilization. All the data are stored on the cloud in the encoded form by utilizing an effective encryption calculation. Image steganography and cryptography approach is introduced to overcome the issue of existing system. To increase high adaptability of information PDE (Patient Data Encryption) algorithm is utilized for keeping both data secrecy and patient information on private cloud of an organisation. If the information is uploaded in private cloud it should ensure how safely the information are stored and it should also ensure the security provided over the sensitive information.*

Keywords- Big data, Sensitive information, Private and Public cloud, Image steganography, Fully Homomorphic Encryption, Patient Data Encryption (PDE).

I. INTRODUCTION

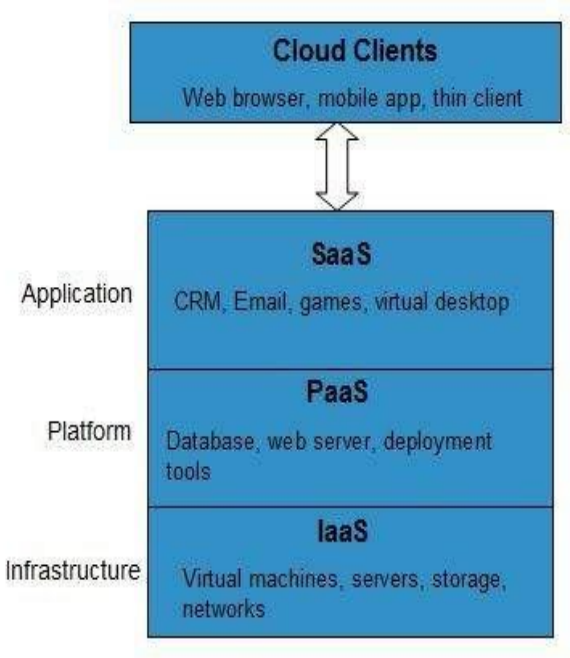
INTRODUCTION: Big data means really a large amount of data, it is a collection of large datasets that cannot be processed using old or traditional computing techniques. Big data is not exactly a data, rather it has become a complete subject, which involves various tools, techniques and frameworks. Big data involves the data produced by different devices and applications.

Thus Big Data includes huge volume, high velocity, and extensible variety of data.

The data in it will be of three types.

Structured data: Relational data.
Semi Structured data: XML data.
Unstructured data : Word, PDF, Text.

Big data and Cloud computing are the two important courses at present life, pose a substantial effect on current IT industry and research communities



1.1 OBJECTIVE OF THE PAPER

The main objective of this project is to provide secure and privacy data transmission in efficient way. It contains Content based image retrieval helps to get relevant images in the database. Through this concept we can achieve secure data transmission.

II. PREVIOUS WORKS

The previous system proposed about the fundamental parts of data hiding are steganography and steganalysis. Steganography is the specialty of hide confidential data or sensitive data into advanced media like images in order to have secure communication. steganalysis is the specialty of recognize the presence of steganography. In this work it describe about the crucial ideas of steganography, the advance of strategies for steganography for images in spatial representation. The synopsis of strategies for steganography is talked about [1].

cryptography and steganography helps us to keep message content in secret form. In cryptography it is illegal to utilize then all the things consider steganography is extremely helpful. steganography is the craft of concealing mystery or deleted data into computerized media like pictures in order to have secured correspondence[2].

The LSB and MSB based steganography with each other as indicated by the MSE (Mean square error) and PSNR (Peak signal to noise ratio) values. LSB works by replacing the least significant of the pixel estimation of the cover image (in the most of the cases eighth bit is replaced). In MSB most huge bit of the pixel value is changed in the cover image. Kanika Anand describes the outcomes demonstrate that LSB Based Steganography is superior to MSB construct steganography in light of the premise of MSE and PSNR values [9].

LSB based steganography and another encryption calculation. The current model is to first change over the information into encrypted form utilizing the proposed encryption algorithm and afterward fix the information in the cover image utilizing LSB based Steganography. Vikas Tyagi describes about Steganography should likewise be possible with Text, video, sound and protocol steganography [11].

AES is a standard used for encryption of data. AES is a symmetric-key computation which infers that same key is used for both decoding and encryption of data. AES is block cipher which uses bit sizes of 128, 168, 192, 224 and 256 bits. Douglas selent describes about additionally examines about declaring of AES and a few disadvantages of triple DES (3DES) and DES. AES utilizes Exclusive –OR operation and substitution and permutation operations, rows and column shifting [7].

AES is executed for 200 bit utilizing 5*5 state matrixes and AES 128 bit is also implementing for 200 bit utilizing 5*5 state matrixes. Ritu pahal compare with the 128, 192, 256 piece AES. Only the mix column transformation change is changed in this procedure. The outcomes demonstrate that the proposed calculation is 50% slower from AES-128, 40% from AES-192, and 25% from AES-256 [7].

Image steganography uses of the Advance Encryption Standard (AES) utilizing 128 bit block size of plaintext and 128 bits of Secrete key. Manoj Ramaiya describes about the pre-preparing give high level of security as extraction of picture is unrealistic without the information of mapping rules of AES and secret key [13].

Homomorphic encryption has various applications continuously. Gorti VNKV Subba Rao describes about the PC will play out the calculation on the scrambled information, subsequently without knowing anything of its real value. At last, it will send back the outcome, and that will be unscrambled. For coherence, the unscrambled result must be equivalent to the proposed registered esteem if performed on the original information [6].

Anonymization is to store the information in a safe organization. Visumathi describe about the data is exchange starting with one place then onto the next means how to safely exchange the information and furthermore how to give the protection over the sensitive information. For adminicle, they don't have to develop their own particular foundation. It can decrease the cost of utilization. All the data are put away on the cloud in the scrambled frame by utilizing an effective encryption calculation. Hybrid bunching technique procedure is presented for conquer the issue of existing framework. To increase high adaptability of information MapReduce calculation is utilized. For keeping both information privacy and patients personality on public cloud an association novel authorized [6].

Mbarek Marwan et al., has proposed to secure customers' information, however not very many of them are keen on database misuse. In this work it describes about homomorphic plan to secure this new worldview. Actually, this approach ensures information secrecy and empowers clients to perform math operation over scrambled information [10].

III. SYSTEM OVERVIEW

System architecture of the association is as exhibited in Fig 1. The information records discharged by the data owner that is patient is get by the data publisher and by utilizing the essential information like name, email id, company name, data publisher or user, the data publisher can make their own one of a kind id value. After login the data owner can transfer the information on private cloud .And

furthermore the data is shared with a unique id generated by the administrator. The whole data records about the patient are part into numerous lumps whenever it increases the maximum of 70MB.And afterward the piece records are to be encrypting then store by utilizing the key values in various cluster. The information records discharged by the data owner that is patient is get by the data publisher and by utilizing the fundamental information's the data owner can make their own particular profile. At whatever point the information records are required by the data publisher they encrypt by calculation of steganography with AES. And furthermore the data is shared id produced by the administrator.

The entire information records about the patient are part into numerous splits whenever it exceeds the limit of 70MB. And after that the part records are to be scrambled then stored by utilizing the key values in various clusters. Once data owner details are registered by the data publisher after login details are then disclosed to data owner.

Patient's details once upload on private cloud using image steganography with AES encryption techniques. After cloud encryption process is started. Whenever patient needs to retrieve the description and scan reports on public cloud through PDE decryption key.so only authorized person allow to access the patient details. Authorized data owner can easily to search the general medicine. Unauthorized user registers the basic details after user can access general medicine details on public cloud.

Registration and U-ID generation

This module is important for making patient record tool. Patient record is a device that can use to group, track and share past and stream information about your wellbeing or the soundness of somebody in your care. For a hospital to maintain or make one patient medicinal records implies we require a special identifier value for the patient in an association. For that the PDE algorithm is user to make individual user id value by utilizing the patient essential information. For doctor's facility every single user they have to play out an initial part determination. Depending upon the role selection the data is keeping in the cloud and maintained. Determine the role selection only for patient the unique user id is generated by the cloud Mongo lab.

Data Publisher to encrypt data Using Image Steganography with AES

Steganography is concealing patient secret information into cover information. Encryption is mainly used for encoding the content of an image, text, video and audio into something that cannot be understandable by unauthorized persons. AES technique focuses on improving the security of steganography images. This technique will provide better security and good quality encryption and decryption. Results shows that this method takes less time with the high quality of encrypted image to store the private cloud.

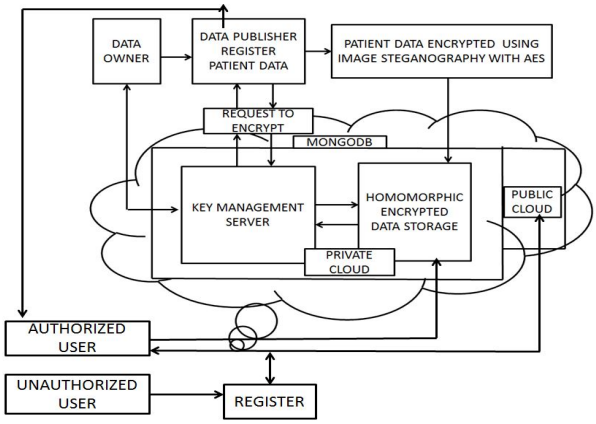


Fig.1. *System Architecture*

Patient Information Stored on MongoDB (Public and Private Database)

Mongo DB application make is utilized to store patients records. Every last information along with this metadata is to be store in a first place, it will improves the get to time of information and limit the utilization of joining the extreme modules. User file system is mechanically put in the Public and Private Cloud (i.e. Mongo DB) in view of the Sensitiveness of the Data. Design Files are coordinated in the Public Cloud, Assured Data in Private Cloud. Different Mongo DB Cloud is spread for quick Data Retrieval.

Cloud Encryption Using Homomorphic Encryption

Once data publisher sends request to cloud encryption after start the process of homomorphic encryption alludes to encryption where plain texts and cipher texts both are treated with an equivalent algebraic function. Homomorphic Encryption allows server to do operation on encrypted data without knowing the original plaintext. It can allow complex mathematical calculation to be performed on scramble information without using the original data. However, Data publisher need to decode hold information before handles them. Subsequently, these calculations are not appropriate for misusing the cloud database. Homomorphic encryption secure to patient information. This strategy is to complete calculations on scrambled information. Actually, homomorphic calculations enable one to calculate arithmetic calculations over encoded information without unscrambling them in this way, associations scramble their information

utilizing homomorphic calculations before transferring them into the cloud database.

Spark In memory Computation Algorithm for PDE

In our project we are dealing with massive amount of daily updatable patients records. For that Spark In memory Computation for PDE Encryption is used. We are providing input (fuel), the engine converts the input into output rapidly and expeditiously, and you get the outputs you need. Spark In memory Computation algorithm has several components like Spark API, MLlib, and Spark SQL. HDFS is fully used for data storage it contain both data node and the name node. And the Spark In memory Computation is utilizing for performing the operation by Sorting and shuffling the patient data.

Authorized Access of Records

This module allows only the Data owner or authorized person to send the request to cloud storage that time Key Server generate secret key send to the data publisher. After getting the secret key, data publisher sends it to the data owner. Data owner access the data once they received the secret key. The authorized person has full rights over the data. The indirectly authorized person has only rights to view general medicines data can view. But the unauthorized person has no rights over the data.

IV. ALGORITHM AND TECHNIQUES

IMAGE STEGANOGRAPHY WITH AES

Today's digital world is developing quickly over Internet technologies and its applications requiring abnormal state of shield for costly information amid transmission over the open correspondence channel. Image steganography is a technique for concealing data into a cover picture. Least Significant-Bit (LSB) substitution based strategy is most regular steganography procedure in spatial area attributable to its straightforwardness and concealing limit. The vast majority of existing methodologies concentrate on the implanting system with less consideration to the pre-preparing, for example, encryption of secret picture. The ordinary steganography calculation does not give the pre-processing required in picture for better security and protection. The proposed work exhibits an elite system for Image steganography in view of the Advance Encryption Standard (AES) utilizing 128 piece square size of plaintext and 128 bits of Secrete key. The pre-processing give abnormal state of security as extraction of picture is unrealistic without the information of mapping standards of AES and secret key.

Encoding Algorithm

Input: A Patient Secrete Image, A gray Level Cover of size.

Output: Stego Image of size.

Steps:

Input is sixteen pixel value of the patient secret image form block of 128 bits to the image encoding Function (AES), which generate the encrypted secret image.

Divide the each pixel values of four parts into two bits each in encoded patient secrete image.

Insert these pixel values into the LSB position of first four pixels in the cover image one by one.

End.

Decoding Algorithm

Input: Stego Image of size.

Output: A grey level Secrete Image.

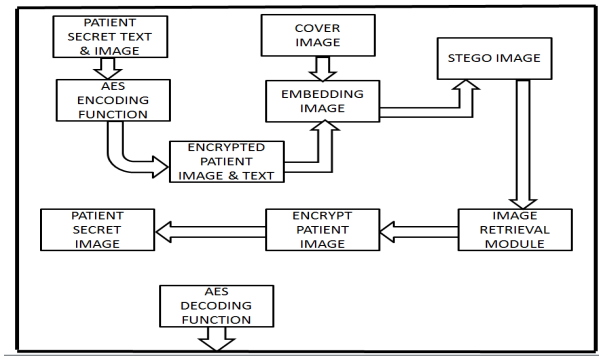


Fig.2. Steganography with AES

Steps:

Input each pixel and take two bit LSB from four consecutive pixel value of the stego image.

Concatenate four and 2bit of LSB to obtain 8 bits of each pixel value of encrypted secrete image.

Now sixteen consecutive pixel value forming block of 128 bits are inputted to decoding Function (AES)

Using same parameter but keys value used in reverse order, to get first eight pixel value of secrete image.

End.

This is a process of encoding and decoding process of Image steganography with AES.

LSB works by replacing the least significant bit of the Pixel estimation of the cover picture. 8 bits were to be inserted in the picture however just 4 bits were changed. Hence on a normal just 50% of the bits are changed in the inserting procedure. In LSB prepare we utilize BMP (bitmap) pictures since they are lossless compression pictures. In lossless compression size of record is diminished yet it doesn't affect the nature of document. The patient information in the document is restored when the record is uncompressed.

Homomorphic cryptosystem process

Homomorphic Cryptosystem (EHC) for homomorphic Encode/Decode with IND-CCA security procedure. Homomorphic encryption plans enable calculation to be performed on the encoded information, if the calculations are process on the plaintext. Homomorphic encryption has various groups of programs progressively. The PC will process the calculation on the encoded information, which does not know anything of its real value. At last, it will send back the outcome, and that will be decoded. For intelligibility, the decoded result must be equivalent to the suggest plan value if process on the authentic information. Consequently, the encryption plot needs to introduce a specific structure. By hold all the business requests we suggest new plan show preferable execution over existing plans chiefly in handling rate, memory and power utilization. Our construction is a non-deterministic and displays addition, multiplication, mixed addition and mixed multiplication operations.

Our plan to take large prime number "p" another prime number "q" such that $q < p$ are withdraw an arbitrary number "r" has withdrawn to build the plan non deterministic.

Consider the sorting of clear data Zp and the sorting of clear operations $\{+, -, *, /$and mixed$\}$ consist of independently, of the addition, subtraction, multiply and mixed multiply modulo m, with $m = p.q$. Give the figure a chance to content information list be Zc .the encryption key $k = (p, q, m, r)$ and $Ek(X) = (mod\ m)$.

Decoding process finished with the secret$key\ k = (p), X = Dk(Y) = C\ mod\ p$. In any case, can breach, if p could be found however which is an extremely intense to solve. A PC can consider that number decently fast however it fundamentally does it by trying a most of the possible combinations.

One can show two huge prime numbers, p and q that has 200 or may be 400 digits each. Q can be hold secret (It is secret key), and by multiplying both of them and to build a number $m = pq$. That number m is likewise a secret key to encode the information. It is generally simple to get m by multiply $p\ and\ q$. yet, in the event that anyone know m, it is essentially difficult to discover p and q. To get them, you have to element m, which is by all accounts an extraordinarily troublesome issue finding the "r" likewise troublesome as this value can be generate arbitrary. It is for the most part respected that m should to be at least 1024, if not 2048.

Homomorphic Addition Process

On a fundamental level, the Paillier encryption plan is made out of key generation, encode and decode functions. Along these lines, it takes as info two huge prime p and q to process the composite $n = p.q$. For producing keys, we pick g with such that n and $(g\lambda mod\ n2)$ are co-prime, where L means the capacity $L(u) = (u-1)/n$ and λ signifies the Carmichael work $\lambda(p.q) = lcm(p-1, q-1)$, where lcm stands for the least common multiple.

Taking after this, Paillier calculation ensures security, as well as performs numerical operations over scrambled information. In this specific situation, expect that $C1$ and $C2$ are two cipher texts of two plain texts $m1$ and $m2$ separately utilizing public key pk. Additionally refers to the encryption and D to decoding capacity

$$C_1 = E(m_1, p_k) \quad (1)$$

$$C_2 = g^{m_1} r_1^n \pmod{n^2} \quad (2)$$

$$C_2 = E(m_2, pk) \quad (3)$$

$$C_2 = g^{m_2} r_2^n \pmod{n^2} \quad (4)$$

$$C_1.C_2 = E(m_1, pk).E(m_2, pk) \quad (5)$$

$$C_1.C_2 = (g^{m_1} r_1^n)(g^{m_2} r_2^n) (\mathrm{mod} r^2) \quad (6)$$

$$C_1.C_2 = g^{m_1+m_2} (r_1 r_2)^n (\mathrm{mod} r^2) \quad (7)$$

$$C_1.C_2 = E(m_1 + m_2, pk) \quad (8)$$

$$E(m_1, pk).E(m_2, pk) = E(m_1 + m_2, pk) \quad (9)$$

Homomorphic Multiplication Process

In general, RSA is a public key encryption technique that enables one to perform multiplication over ciphertext. Actually, this calculation is an encryption plan that fulfills multiplicative homomorphic property. To accomplish this objective, the two huge primes p and q must be calculate.

$$n = p.q \quad (11)$$

Also, we choose e so that

$$\gcd(e, \varphi(pq)) = 1 \quad (12)$$

Where φ is Euler's totient work, the latter can be calculated as $\varphi(n) = (p-1)(q-1)$. On a basic level, the RSA conspire comprises of three main rules the key generation $(KeyGen)$, the encryption algorithm (Enc) and the decryption algorithm (Dec).

In such manner, accept that the public key $pk = (n, e)$ of the RSA scheme. In this way, assume $C1$ and $C2$ are two cipher texts of $m1$ and $m2$, to such that,

$$C_1.C_2 = E(m_1, pk).E(m_2, pk) \quad (13)$$
$$= m_1^e.m_2^e \pmod{n} \quad (14)$$
$$= (m_1.m_2)^e \pmod{n} \quad (15)$$
$$= E(m_1, m_2, pk) \quad (16)$$

Subsequently, the RSA strategy has multiplicative homomorphic property.

PATIENT DATA ENCRYPTION (PDE)

PDE algorithm is combination of both steganography and cryptography techniques. Which algorithm is mainly used to encrypt the patient image with securely, first encryption, the data publisher encrypt the patient image using steganography techniques with AES. Once completed steganography encryption process after Cryptography encryption process will be start, after encryption to store the patient data in private cloud. This PDE algorithm is very efficient to store the patient data with securely. It can access only authorized person. It is very difficult access the un-authorized person. The data owner wants to access the own data, first send the request to cloud, key server management (KMS) sends the key to data publisher, after verify the data publisher ,sends the secret key to data owner, once get the secret key from data publisher, it can access the patient data.

Steganography is the craft of concealing mystery or delicate data into computerized media like pictures in order to have secure correspondence. In steganography we conceal our mystery data in some cover picture with the end goal that one can't track the message. The first Image is called cover picture and the picture in which message is installed is called Stego-Image. Steganography should likewise be possible with Text, video, sound and convention steganography.

There is a contrast amongst cryptography and steganography. Cryptography helps us to keep message content in secret form while steganography keeps the presence of the message as a mystery. In the event that cryptography is illegal to utilize then all things considered steganography is extremely helpful.

Today there are numerous utilizations of steganography. It is utilized as a part of associations with the goal that information can be securely coursed it is utilized as a part of keen character cards where the data of the individual is furtively put away in the picture of the individual itself. Some different applications are medicinal imaging, web based voting framework etc.

The proposed algorithm is based on our advanced LSB coding method and the RSA and Paillier algorithm for encryption. In this an image file is taken for embedding the secret text. Both files are converted in binary equivalent. An operation is applied on embedding process to make the method more secure. The text is encrypted using the RSA algorithm and this encrypted text is embedded into binary converted image file. Encrypted text is embedded into the file LSB bit of each block. The embedded image file is called as stego image.

Cover Image is utilized to hold the mystery information. stego Image holding the implanted message. Mystery message is the mystery data which is to be installed with the cover picture.

PDE ALGORTHIM

STEP 1: Data owner details register by Data Publisher.
STEP 2: Data publisher encrypted the details using image steganography with AES.

STEP 3: A Data Publisher sends an encrypted data to cloud.

Eg: Let two encrypted number be a and b.

STEP 4: Data Publisher sends request to cloud for calculating function.

$$i.e.\ f(a,b)$$

STEP 5: Data Publisher and Cloud communicate through a cryptosystem based on homomorphic encryption.

In our propose plan is very security of the patient data to encrypt the very efficient. So we can support strongly our plan is more authenticate when compare to existing plan as follows:

This plan is very powerful as well as uses the secret keys $q, m\ and\ r$ and sharing key p for encoding. So it is very hard to find out the secret keys.

This plan only shares the shared key p only between the sender and receiver so it is very difficult to find out the $q\ and\ r$.

Arbitrary number 'r' can be generated randomly so that each time the same plaintext mapped to various cipher message so it is extremely difficult to track the plain content even with solid perception for unauthorized user.

Unauthorized did not get the secret value and arbitrary number.

This plan strongly believe supports Addition, Multiplication, Mixed addition and mixed multiplication.

We take huge prime number p decode the circle will be high so that second multiplication also possible.

It is very efficient compared to existing plan and consumes less power and memory.

STEP 6: Cloud stores encrypted data.

STEP 7: Cloud calculates the result of request sent by the data Publisher without knowing actual number.

$i.e.f(a,b)$ is calculated

STEP 8: Cloud then compute $f(Enc(a), Enc(b))$ without knowing a and b.

STEP 9: Data Publisher decrypts $f\ Enc(a), Enc\ (b))$ using its private key.

Both Cryptography and Steganography is to keep the data safe from unwanted parties. So both techniques alone cannot guarantee for better security because both techniques can be cracked after many attempts. It is necessary to develop a hybrid system of cryptography and steganography techniques. The advantages of both techniques combined together may provide better security. So many different combinations of cryptography and steganography techniques are used for securing the data.

The mystery message is encoded utilizing cryptography and afterward scrambled message is hidden utilizing steganography. At that point coming about stego picture can be sent to recipient without view the mystery data is being traded. Despite the fact that if the attacker knows the presence of mystery message in picture, attacker needs to know the private key to decode and get unique message. This crypto-stegano framework needs to conform to a couple of fundamental necessities. These necessities are imperceptibility, payload limit, against factual assaults, for example, repetitive sound, pressure, resize assault, robustness against picture control, free of record organization.

IV. CONCLUSION AND FUTURE ENHANCEMENTS

Cloud computing is the developing technology for the next generation of IT applications. The barrier towards the efficient growth of cloud computing are data security and privacy issues. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. In this paper we have discussed some key data security issues and also different techniques to provide data security. In this paper we have given some PDE scheme developed by researchers which allow us to perform computation on encrypted data without using secret key of client. It is nothing but a new layer applied to the cloud computation. In future, we are going to work on the behaviour of PDE compared to the length of the public key and the performance of the request by the cloud provider that depends on the size of encrypted messages.

Overall performance of the project is finding out by comparing our patient records with existing systems. In an existing system Ucloud service provider is used. Instead of Ucloud in our patient records we are using Mongolab service provider for security. Mongolab encrypt and maintain replica of both transformation of data and rest of the data.

FUTURE ENHANCEMENT

In future, we are going to work on the behaviour of PDE algorithm does not support patient audio, video files and also compare the length of the public key and the performance of the request by the cloud provider that depends on the size of encrypted messages.

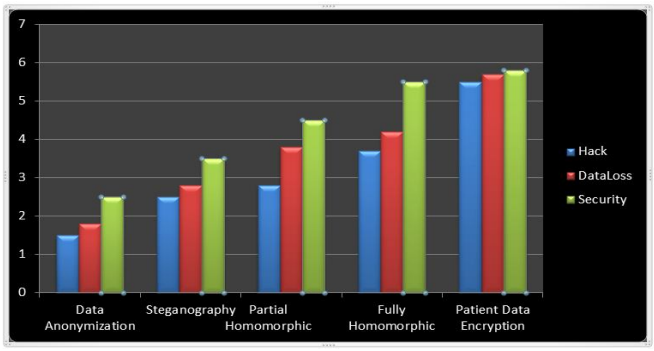


Figure 7.1: Performance of PDE Algorithm

REFERENCES

[1] "Artificial Neural Networks Applied to Image Steganography", A.S Brandao and D.C Jorge, March 2016

[2] J. Visumathi, P. Jesu Jayarin, P. Shyja Rose "Chunking and Storing of Sensitive Data in Public Cloud for Hospital Management Humanities", Asian Journal of research in social sciences and humanities,Vol.6,No.8,August 2016.

[3] Apoorva Shrivastava, Lokesh Singh N "A New Hybrid Encryption and Steganography techniques" ,International Journal of Advance Technology and Engineering Explorations,Vol 3(14),ISSN,2016.

[4] Veerabramachary.M, Sujatha.N "A Novel Additive multi keyword search for multiple data owners in Cloud Computing",International Journal of Computer Engineering in Research Trends,Vol 3,Issue 6,2016

[5] Jun Zhou, Xiaodong Lin "Patient self controllable and Privacy preserving cooperative Authentication in Distributed M-Healthcare systems",IEEE,2015.

[6] Lokesh Kumar, Dr.Shalini Rajawat, Krati joshi" Comparative analysis of NoSQL(MongoDB) with MySQL Database",2015.

[7] Utsav Sheth, Shiva Saxena "Image steganography using AES Encryption and Least significant bit",2016.