Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 1785-1800
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2021.5316

Implementation of hybrid cryptographic schemes in a cloud environment for enhanced medical data security

A. Priya[a,*], S. Saradha[a]

[a]*Department of Computer Science, VISTAS, Chennai, India.*

(Communicated by Madjid Eshaghi Gordji)

Abstract

Nowadays, several security architectures in cloud computing were employed in several applications, but they failed to secure the cloud data entirely. The current approaches use the ensemble algorithm for the decryption and encryption purpose to enhance the security technique. The input medical dataset is usually raw and might contain redundant packets and missing values. Initially, the data is preprocessed by means of the normalization technique. By using Enhanced Principal Component Analysis (EPCA) method, various attributes of the data can be obtained. After the extraction process, the classification mechanism is carried out for recognizing the attacks. The attack is predicted and is classified by means of the Adaptive AlexNet CNN classifier algorithm. A hybrid cryptographic technique in a cloud environment for improving the security rate and providing privacy preservation of the medical data in the cloud environment is presented. The proposed work mainly concentrates mostly on implementing hybrid cryptographic schemes which include AES algorithm, enhanced honeypot algorithm, SHA3 hashing and OTP in the cloud environment. It enhances the security of the data to a great extent. Thus, the presented technique is secured effectively that makes the intruders difficult to access the system as they need to attain control over servers.

Keywords: cloud computing, encryption, decryption, Enhanced Principal Component Analysis, Adaptive AlexNet CNN classifier, cryptographic technique, enhanced honeypot algorithm, SHA3 hashing and OTP.

*Corresponding author
Email addresses: vpriya172112@gmail.com (A. Priya), saradha.research@gmail.com (S. Saradha)

Received: January 2021 *Accepted:* June 2021

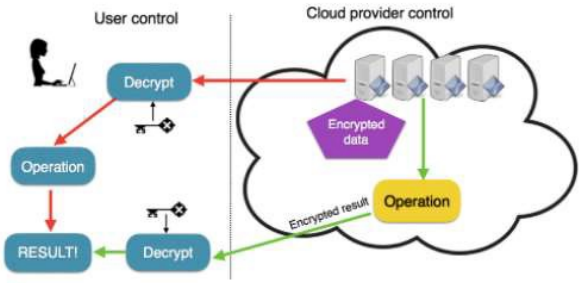


Figure 1: cryptography scheme in cloud framework

1. Introduction

Today, we are living in a world encompassed by technology. The utilization of technology is expanding step by step due to the Internet. A cloud computing normally indicates the information to be put away in cloud centrally and is accessible for shoppers over the span of thin clients and insignificant cell phones. Cloud computing is conceivable simply because of the great speed of Internet. Cloud symbol addresses the interaction over the Internet. Presently a day, numerous little and huge associations are quickly moving to the cloud network since, it gives quick admittance to the application and lessens the expense of the association. Cloud computing is a model and works as a service provider. It offers various types of assistance or assets to the client with the goal that an individual may not buy the necessary help in general yet can without much of a stretch access it by giving nominal charges to the services provider. There are number of dangers and difficulties that have arisen because of utilization of cloud computing. As of late, security of information is continuously winding up as a considerable one in the expanding number of private information that are interacted over the Internet of public or over third-party interaction. In the long run, there is a chief test as weaknesses and risks are developing with the upgrade of advances. Cybercrime's violations or Internet violations are unlawful act completed through the digital or Internet environmental factors through weaknesses. The maintenance of information is in this manner requires a more secured stage for the information storage. Inspired by earlier works the problem of secured data storage in cloud environment with high range of accuracy seems to be an important issue.

Present work indicates that the efficiency of the system is improved in terms of protection, durability and performance. Nowadays many security architectures in the cloud computing have been employed, but they failed to secure the cloud data completely. The current approaches use the SHA3 ensemble with AES and honeypot algorithm for the encryption and decryption purpose as the traditional work cannot give security to the entire cloud computing environment. Also, they are not cost effective. One of the main drawbacks of Blowfish algorithm is the time needed to initialize the algorithm with the key. Such techniques do not assure authentication and non-cancellation since two users possess the similar key.
The objectives of this work are listed below:
• To propose a hybrid cryptographic technique in cloud environment for improving the security rate and providing privacy preservation of the medical data in the cloud environment by identifying intruders.
• To detect and classify the intruders using Adaptive AlexNet CNN classifier scheme.
• To enable effective key management system using effective ensemble cryptographic techniques like AES, honeypot, SHA3.

• To implement the proposed scheme in the MATLAB environment and to evaluate its performance in terms of accuracy, specificity, precision, sensitivity, F-measure and recall.

2. Related Works

The author in the paper [15] triggers two level of encryption for achieving higher grade of security. First level is to encrypt the data by assigning hex codes to each character and for the generation of combination of secret key RSA and Enhanced ElGamal Algorithm is designed. Second level is that the generated key is converted into hex code and is added with the encrypted file which in turn provides strong encryption and high efficiency. Thereby, this work provides an application to encrypt the data using hex codes and RSA and Enhanced ElGamal to generate secret key as the password in turn to decrypt the file.
[13] and [23] presented the mechanism of security for the mode of virtualization. The algorithm of RSA was employed for the cloud security. The private and public key mechanisms decryption and encryption are combined in both virtual and also physical manners.
[24] enhanced the issues of safety considerate connected with storage of cloud and highpoints the importance schemes of data integrity for the outsourced data. In this, of existing data integrity schemes taxonomy was presented to employ cloud storage. A relative investigation of present systems is provided also with a complete conversation on probable attacks of security with their mitigations. Moreover, design challenges were discussed like communication efficiency, computational efficiency, storage efficiency, and condensed I/O in these systems.
[6] presented various data mining techniques involved and also analyzed their respective accuracy. This paper deployed tools like Modified J48 classifier which gives around 99 % accuracy rate by tools such as MATLAB and WEKA. It also deals with various data mining methodologies depending on the prediction performance. This paper achieved dataset accuracy up to 98 %.
[10] presented a newly developed framework in domain encryption for data hiding reversibly. This paper developed an efficient framework to encrypt domain for RDH (Reversible Data Hiding). Here, the plain images are represented in pixels that are divided into subcategories with the size of $m \times n$. Then with an encryption key a key stream is used.
[4] surveyed various existing feature selection techniques and algorithms. Naive Bayes, SVM Algorithms, J48 are the examples of various existing methodologies that are employed in prediction methods. This proposed work predicts disease occurrence at a very early stage, which will prevent it from becoming fatal [9]. This proposed methodology can provide automatic early diagnosis result.
[3] introduced an effective GPU encryption system to protect big data from attacks like data stealing, etc. This encryption system involves the process of bits scrambling which, in turn, resulted in avalanche effect. It has achieved high-security and high-performance rate.
[11] proposed the advantage of using AES –Advanced Encryption Standard. It also noted that if the number of rounds increased to 16, then the system will be more protected from outside attackers. This increase in number, in turn, increases the computational time. If the computational time is increased, then it will be complicated to the hacker, who tries to hack the system.
In [1] the cloud security was done using the genetic and Markov algorithm. [8] proposed a multican attribute based encryption system of hierarchical distribution (HD-MAABE) in which attributes are issued by organization and standard attribute bodies. [21] focused on MAABE (multi-authority attribute-based encryption) approaches, by compressing the least value attributes.
[14] proposed a Novel Approach for detection the intrusion. [2] proposed deep learning approaches for intrusion detection. [19] formulated the Current ABE Cities, an urban sensing encryption system

that resolves problems mentioned above, while ensuring a thorough access control over data through Attribute-based Encryption (ABE). [5] proposed an efficient file recovery using cloud-based attribute file encryption (ERFC).
The system has been developed for watermarking by [22] to protect data through authentication between the cloud and the users. The transmission errors could be reduced by integrating Reed–Solomon with water markup coding. In cryptographic techniques, the check capabilities were important and the versatility of access control by the proposed ABE method was increased by [12]. Because of its high expense, estimable difficulty, key problems and decryption were high in the ABE process. The customer and the authority side achieved constant performance. [7] presented the diabetes prediction by soft computing techniques. Neural networks are an effective technique utilized for diabetes prediction. Three layers included in the artificial neural network are input layer, output layer, and hidden layer. All attribute values are defined by the input layer.
[18] presents the public relations neighboring in the cloud the consumers are unwilling towards make a proposal for their business in the cloud. Generally, internal entities are responsible for the theft data, this leads to audit the data integrity by the third party. Whereas the sensitive information was external entities kept in the cloud throughout the intellectual query fired up on the cloud.
[16] Presents the Cloud computing technology is a stretchy, price- efficient and provides a nice stand for the trade opportunities and the customer services via network. It is the main route to improve the capacity or else add the capability with dynamism without investing in new infrastructure.
[20] presents the ICN privacy and security are explored and open challenges are presented. Especially, three extensive subjects: security threats, risks involved with privacy, access control management techniques are explored. Primary objective of ICN is to modify the present location-based IP network architecture to location-free and content-oriented network framework.
[17] Presents the cloud security research proposes an efficacious modeling and privacy protection framework utilizing an enhanced blowfish algorithm.

3. Proposed Work

This section is the thorough portrayal of projected method explanation. The overall flow of proposed system is shown below:

3.1. Pre-processing

The measured values of normalization at various balance to a notionally standard size often before the average is necessary to ensure data processing. Many forms of normalization require only a rescaling method to obtain the values for every other element. The errors are to be modified by merely adjusting the data parameters when they are known. The data values will typically be distributed instead of random distribution despite error adjustment. The first step in the normalization process is to get the z-score.

$$Z = [(z - \alpha)/\sigma] \tag{3.1}$$

Where α is the datamean, and the standard deviation of the data is σ. When the mean results and the standard variance are negative, the overall score is determined from the mean sample and overall sample variance.

$$Z = \frac{z - \overline{z}}{m} \tag{3.2}$$

Where $\overline{z}$ is the sample mean, and the standard deviation of the samples.
For this standardization step, the same values as the input values are used, and the errors have to be

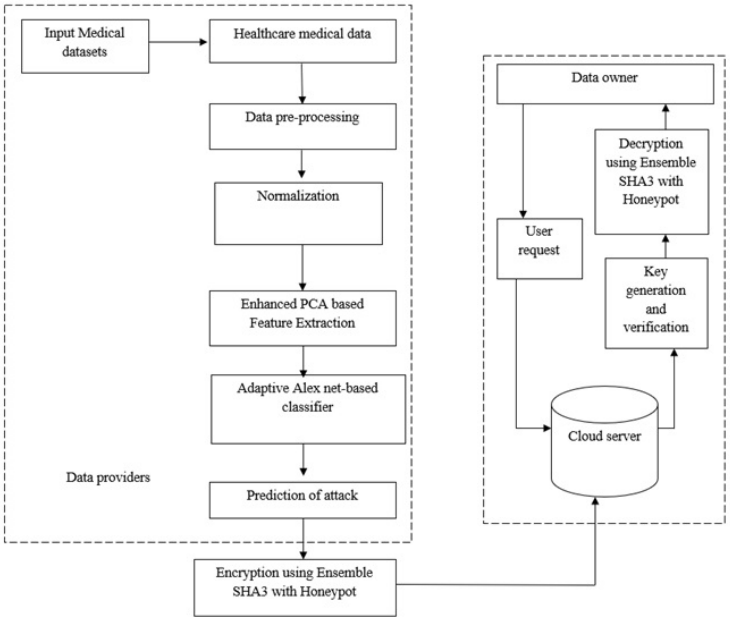


Figure 2: Flow 2 Proposed system flow diagram

changed such that the formula for the regression analysis is used to adjust the error function. Take a simple linear regression model first,

$$Y = \alpha_0 + \alpha_1 z + \in \tag{3.3}$$

The random sample is in the form of,

$$Y_i = \alpha_0 + \alpha_1 z_i + \in_i \tag{3.4}$$

Where
error is the $\in_i$,and it is dependent on the σ^2
The residuals are pseudo errors which can be created.

$$\sum_{i=1}^{n} \widehat{\in}_i = 0 \tag{3.5}$$

$$\sum_{i=1}^{n} \widehat{\in}_i \; z = 0 \tag{3.6}$$

$$H = X \times (z^T z)^{-1 z^T} \tag{3.7}$$

The variance for the Hat matrix is,

$$Var(\widehat{\in}_i) = \sigma^2(1 - h_{ii}) \tag{3.8}$$

$$Var(\widehat{\in}_i) = \sigma^2(1 - \frac{1}{n} - [(z_i - \overline{z}^2)/ \sum_{j=1}^{i}(z_j - \overline{z}^2)]) \tag{3.9}$$

Then the residual which can be calculated by

$$t_i = \frac{\widehat{\in}_i}{\overline{\sigma}} \sqrt{1 - h_{ii}} \tag{3.10}$$

Where $\overline{\sigma}$ is an estimate if the σ

$$\widehat{\sigma}^2 = \frac{1}{l-m}\sum_{j=1}^{n}\overline{\in}_j^2 \tag{3.11}$$

Where m is the parameters number.

$$\widehat{\sigma}^2{}_i = \frac{1}{l-m-1}\sum_{j=1\ j\neq 1}^{n}\overline{\in}_j^2 \tag{3.12}$$

The error is independent to each other and is signified as follows,

$$t_i \sim \sqrt{s}\frac{T}{\sqrt{t^2+v-1}} \tag{3.13}$$

Where t is a variable inrandom
The normalization of variable movement is signified by:

$$K = \frac{\mu^k}{o^k} \tag{3.14}$$

Where, moment scale is k.

$$\alpha^k = E(z-\mu)^K \tag{3.15}$$

Where E is the expected value, X is a random variable and

$$o^k = (\sqrt{E(z-\alpha)^K})^2 \tag{3.16}$$

For normalizing the distribution of the variable c_v can be calculated particularly for the normal orderly distribution.

$$C_v = \frac{s}{\overline{z}} \tag{3.17}$$

Where C_v is the coefficient of variance.
After that, the feature scaling process can be done to bring all the values in between 0 and 1. This technique is termed the unity-dependent normalization.

$$z' = \frac{(z-z_{min})}{(z_{max}-z_{min})} \tag{3.18}$$

3.2. Feature Extraction

Feature extraction is the most important step for accurate classification of disease. To make this extraction is an efficient way, this chapter proposes the EPCA based feature extraction approach. It is used mainly for dimensionality reduction or for compressing the data. It identifies the important features in dataset and removes the unwanted features. This feature extraction involves ranking the features based on their importance in descending order using the correlation criterion.
Modified Principal Component Analysis (MPCA) determines the Eigen vectors of co-variance matrix and by using these Eigen vectors, the data is projected into a new subspace of equal or less dimensions. In general, the correlation or the co-variance data matrix is created thereby computing the eigenvector matrix. The subset of variables is selected from a huge dataset depending on actual

Algorithm 1 Enhanced principal component analysis (EPCA)
Input: x← dataset Information
M← mean value
Output: T← feature selection
Step 1: for(x0……xn)
Step 2: o ← Eigen(x)
Step 3: R ←Cov (x0,x1)
Step 4: End for
Step 5: Eign t(x)
Step 6: for n=0 to # iterations
Step 7: m← n div length;
Step 8: s← m(n) mul(m(n))
Step 9: su← a(n) mul b(n)
Step 10: a ← s div su
Step 11: if(m > a)
Step 12: return n
Step 13: End if
Step 14: End for loop
Step 15: End method:
Step 16: cov (x,x)
Step 17: for x to n
Step 18: k ← x[i] add m
Step 19: h ← n[i]+ add m
Step 20: sum ← k mul h
Step 21: R ← sum div lenth;
Step 22: end loop
Step 23: end method

Table 1: Algorithm 1 Enhanced principal component analysis (EPCA)

variables which have a maximum correlation with the principal component.

$$T = \frac{\lambda_1 + \lambda_2 + \lambda_3 + ... + \lambda_k}{\lambda_1 + \lambda_2 + \lambda_3 + ... + \lambda_k + ... + \lambda_d} \tag{3.19}$$

λ is the Eigen value; k is the new set of features; d is the original features
To represent the data records with low dimensional vectors, firstly, n Eigen vectors need to be estimated corresponding to m largest Eigen values.
$\Phi = v_z, v_2, ..., v_m$
$A = diag(\lambda_1, \lambda_2, ..., \lambda_m)$
Here, A defines the diagonal matrix of Eigen values and the covariance matrix is arrived by,

$$C\Phi = \Phi A \tag{3.20}$$

Then, the number of features is determined by using the following criterion.

$$\frac{\sum_{i=1}^{T} \lambda_i}{\sum_{i=1}^{p} \lambda_i} > N \tag{3.21}$$

P is the total number of Eigen values
The indices are sorted out in the descending order and selecting the first set of features without modifying of original features values.

In this algorithm, initially, the mean value is assigned and the mean is subtracted from every dimension of data. Thus, it produces the dataset whose mean is zero and estimates covariance matrix. After that, it calculates Eigen vectors and Eigen values of covariance matrix. Then, it sorts the Eigen vectors by reducing Eigen values. Finally, it transforms the samples to a new subspace.

Algorithm 2: Classification using Adaptive AlexNet CNN

```
Start
    Step 1: Interpret the input feature data
    Step 2: Increase contrast type of original data using
        contrast stretched min-max algorithm
    Step 3: Transform the contrast stretched transformation.
    Step 4: Segment the data
    Step 5: Extract the features from extracteddata using
        EPCA
    Step 6: Assess images using training testing patterns.
    Step 7: Use AlexNet CNN classifier to classify data.
    Step 8: Distinguish Ground truth data to check if the
        region is malignant or benign.
    Step 9: Set the classifier label as 0 and 1, then
Apply state
if (result == 1)
helpdlg ('data is diseased)
disp ('Malignant')
else
helpdlg ('data is healthy)
disp ('Benign')
end
if (choice==3)
close all
return
end
    Step 10:  Return the results.
Stop
```

Table 2: Algorithm 2: Classification using Adaptive AlexNet CNN

3.3. Classification using AlexNet CNN

After the extraction process, the classification mechanism is carried out for recognizing the attacks. The classification stage is the final process in this work. The AlexNet CNN deep learning classifier in these approaches is used in segmented areas of with a malignancy or benignity label. The dataset has been subdivided into two phases to evaluate the regions for training and testing. This stage involves the training of vectors of the data set and its respective classes, whereas the output determines whether the nature of input image is fatal or mild. AlexNet CNN is trained and tested with RBF kernel functions to achieve good results. The AlexNet CNN algorithm is used in this paper to classify the areas of brain tumor.

The data in the words before step t in the CNN architecture is also used as input during word processing in step t. Earlier cell data are collected from the cell, and words are provided as inputs. Little references detect the repeated image through one cell. The sequence cells of the architecture are other references.

The text amount presented in each data example does not turn out to be a particular value in natural language processing problems. To execute every text, the dimensions of the arrangement are reduced to a value. If the value of the arrangement is less than the specified value, the sequence is filled into the value. If the size of the sequence exceeds the value mentioned, the excess is rejected.

AlexNet CNN 18 consists of five layers of convolution, one recurrent layer and two layers that are completely connected. The CNN layers are used to learn middle-level visual patterns similar to the first five layers of the popular Alex-Net seven layer. The RNN layer is used to learn space dependence between visual patterns of the middle level. In both final layers, the two fully connected RNN outputs are collected and a global image representation is learned. A softmax layer for classification shall be subsequently applied to the N-Way (N denotes class number).

3.4. Hybrid Cryptographic Algorithm

Hybrid cryptographic techniques are implemented for improving the security of the data. These include: AES Algorithm for file encryption, Enhanced Honeypot Algorithm for data security, SHA3 Hashing to secure tables, OTP for authentication. Advanced Encryption Standard (AES) Crypt is a file decryption and encryption software accessible on some system of operation which employs the industry normal AES to securely and easily encode files. Honeypot is the energetic protection technology, in which the reserves situated in a network through intending to monitor and confine the original attacks". This paper proposes a Honeypot-based prediction of Intrusion Detection System (IDS) to find a better use of data concerning the attacker. To identify the intrusion detection-based assaults such incredible problems get to establish with an extensively robust Honeypot based prediction method. The protection system is Honeypot's exploitation. A Honeypot is a vital security entity used for surrendering its benefit to unapproved admittances to calculate the possible vulnerabilities in operational structures and abolish the hazardous/danger. These are like catches for expecting user. To attract the attackers, Honeypot is established on a network. The Honeypot method utilized in different fields like Intrusion Detection System (IDS) that is the control system for the industrial areas, which gathers data and information from further attacks and intruders. If it is combined beside with Intrusion Detection System (IDS) and firewall, it holds the False Negative Rate (FNR) and False Positive Rate (FPR). Also, it includes another layer of Security based matter. Also, it is well-matched with encryption or communication during IPV6, not like other securities. The aim of the proposed work as, to predict the intrusions in the network through the feature extraction and feature selection initially gets established. Then, to form the clustering of data according to the features. The set of clusters achieves the intrusion formation where the intrusions present in the cluster formation. Each cluster groups contain the intrusions or may not have. The form of clusters applied to the Honeypot- based prediction of intrusions. Here, the Honeypot-based prediction approach helps to identify the intrusions present in the cluster formation according to the interaction level of the Honeypots. The involved steps in the proposed work as given as Normally, Honeypots are classified by the interaction level among intruder and the system that are: High-interaction, Less-interaction, and Medium-interaction. In High-interaction level, they either follow a complete operating system or utilize an actual installation of an operating system with the supplementary monitoring system. They not only handle demands but also permit malicious schemes completely interrelate and yet concession the suggested method. The several high-interaction honeypots also allow limited peripheral connections, creating the service emerge completely functional in DoS attacks whereas preventing it from receiving part, which causes massive traffic and losses in the network. In Less-interaction level, that follows network examines, somewhat than an entire system, only to the position that an intruder can monitor in but also execute no actions. This is an extremely secure resolution, which creates little threat to the atmosphere in which it is established. The less-interaction Honeypot suggests only the transport layer of the network on a solitary physical host and never utilized information gaining on the application layer. Attackers never interact with the real Operating System (OS), having entrée only to imitated services similar to a counterfeit web or mail server services. Though, the data collected by the less-interaction Honeypot can provide important information about the intrusion like as whether an attacker endeavored to utilize well-known vulnerabilities in definite services. Less-interaction honeypots change from IDS systems in two methods: 1. They project and identify attacks 2. The ability to actual login attempts, whereas IDS systems are passive. In Medium-interaction Honeypots, that is a mixture of less- interaction and High-interaction Honeypots, proficient of following complete services or explicit vulnerabilities. Similar to the less-interaction Honeypots, its primary intention is prediction and is established as a purpose on the host OS with merely the imitated services being there to the public services. In the

Pseudocode for IDS dataset SHA-Honeypot prediction

Input: *Intrusion History Database*
Output: *Revised inspection vector Curr O and P(O)*
Begin;
while *Intrusion is inferred,* ***do***
Choose similar intrusions from IHD;
if *the Possibility that intrusion persists is greater than intrusion discontinuing* ***then***
Honeypot permits the intrusion;
Reacts with a reply;
else
Honeypot obstructs the intrusion;
Falls the message of the intrusion;

Table 3: Pseudocode for IDS dataset SHA-Honeypot prediction

proposed work, Honeypot is utilized to establish the unauthorized exploit of an information system by analyzing the behavior of the attacker in an isolated and monitored environment. They can be cluster-based network but are extra frequently, but never the network-based interaction is typically achieved over a network association. The leading utility of a honeypot comes from the fact that it makes simpler the Intrusion Detection problem in terms of Intruded network or non-intruded network by having no genuine use. Thus, any movement on a Honeypot can be instantly defined as abnormal. The Honeypots characteristics create them well fitted to the malicious movement monitoring on the networks. Honeypots are intended to impersonate systems that an intruder would like to split into but boundary the intruder from containing contact to the complete structure.
In the proposed work, Honeypot is utilized to establish the unauthorized exploit of an information system by analyzing the behavior of the attacker in an isolated and monitored environment. They can be cluster-based network but are extra frequently, but never the network-based interaction is typically achieved over a network association. The leading utility of a honeypot comes from the fact that it makes simpler the Intrusion Detection problem in terms of Intruded network or non-intruded network by having no genuine use. Thus, any movement on a Honeypot can be instantly defined as abnormal. The Honeypots characteristics create them well fitted to the malicious movement monitoring on the networks. Honeypots are intended to impersonate systems that an intruder would like to split into but boundary the intruder from containing contact to the complete structure.
To maintain the attacker busy while intrusion, Honeypot either permits the attacker actions or obstructs the attacker actions. To choose the reply to the attacker, Honeypot removes the Associate's Position, $AP(Q_m)$ for each Q_m that occurs in $Curr\_O$. The term of $AP(Q_m)$ as given below:

$$AP(Q_m) = \{O_i/O_i \in O/O_r \ \& \ \{O_iO_r\} \in \Phi(T_i)\} \tag{3.22}$$

The Associate's Position of O_r, $AP(Q_m)$ is the group of observations, which reason any indication of T_i when occurred in combination with O_r. For every O_j in $AS(O_k)$, Honeypot reacts reply. Honeypot either replies with the subsequent message in progression as uttered by the specifications of the protocol or it never permits the additional expansion of the process. The Honeypot chooses the achievement by submitting to the IHD (Intrusion History Database) where IHD (Intrusion History Database) is the collection of intrusions in the network.

The intrusion predicted according to its interaction-level. If a honeypot is predicted successfully, the intruder will have no scheme that is scammed and observed. According to the interaction level (less, high, medium), the intrusion gets predicted, finally, calculate the intruded and non-intruded networks. If to evaluate the intrusion, the prediction accuracy (how precisely identified the intrusion)

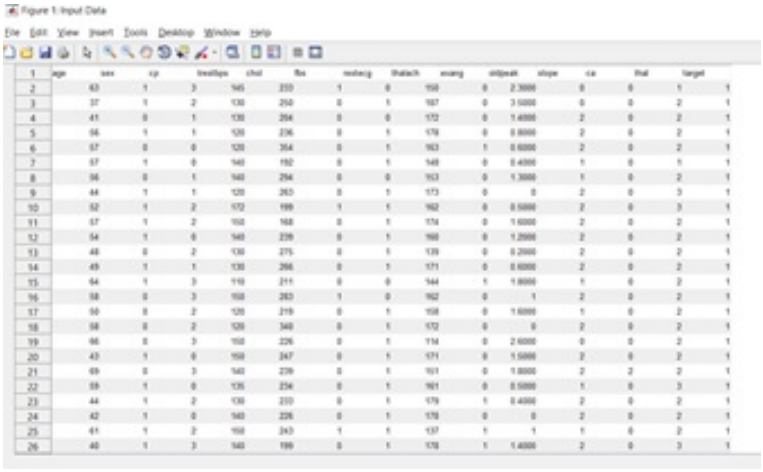


Figure 3: Input data representation

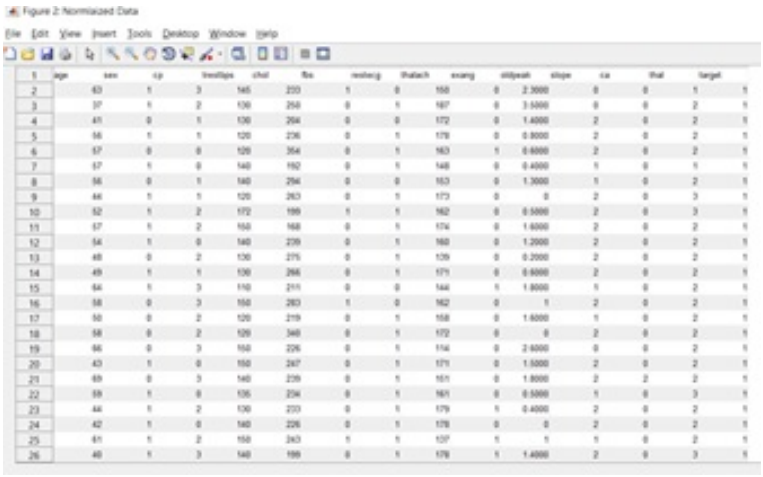


Figure 4: Normalized data depiction

gets evaluated. If there is no intrusion present in the network, the data gets stored in the cloud environment. In the proposed system, Honeypots offers efficient result to enhance the security in terms of non-intruded networks and consistency of the network. Also, the data establishes a secure manner as well as the there is no breakage to store the data; the security is the prime factor in the data storage with effective way.

4. Results

This section is the deliberation of performance analysis of the proposed system. The proposed system perfromance is evaluated and the outcomes attained are compared with existing techniques to prove the effectiveness of proposed system.

Figure 3 is the representation of input data and the normalized form of input data is depicted in figure 4 with the features data representation in figure 5. The features data is then clustered and the clustered form is shown in figure 6.

Figure 7 is the depiction of decrypted data. The preprocessed data is then stored in cloud server

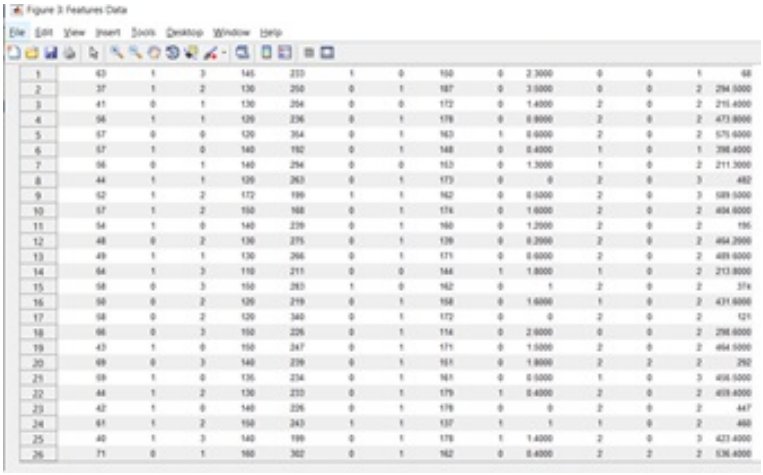
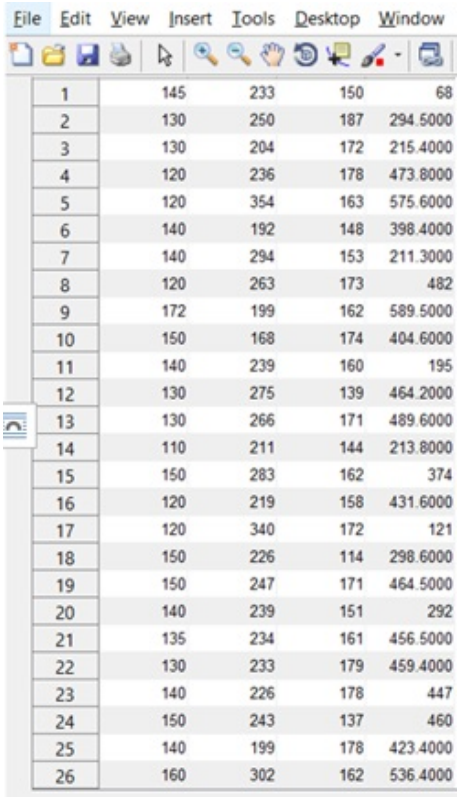


Figure 5: Features data illustration



1	145	233	150	68
2	130	250	187	294.5000
3	130	204	172	215.4000
4	120	236	178	473.8000
5	120	354	163	575.6000
6	140	192	148	398.4000
7	140	294	153	211.3000
8	120	263	173	482
9	172	199	162	589.5000
10	150	168	174	404.6000
11	140	239	160	195
12	130	275	139	464.2000
13	130	266	171	489.6000
14	110	211	144	213.8000
15	150	283	162	374
16	120	219	158	431.6000
17	120	340	172	121
18	150	226	114	298.6000
19	150	247	171	464.5000
20	140	239	151	292
21	135	234	161	456.5000
22	130	233	179	459.4000
23	140	226	178	447
24	150	243	137	460
25	140	199	178	423.4000
26	160	302	162	536.4000

Figure 6: representation of clustered form of features data

	1	2	3	4
1	63	1	3	0
2	37	1	2	0
3	41	0	1	0
4	56	1	1	120
5	57	0	0	120
6	57	1	0	0
7	56	0	1	0
8	44	1	1	120
9	52	1	2	0
10	57	1	2	0
11	54	1	0	0
12	48	0	2	0
13	49	1	1	0
14	64	1	3	110

Figure 7: decrypted data

	AlexNet_CNN	Basic CNN	Random Forest Classfier
Accuracy	99.5938	99.1875	99.0521
Sensitivity	100	82.3529	87.5000
Specificity	99.5859	99.5842	99.3080
Precision	82.3529	82.3529	73.6842
Recall	100	82.3529	87.5000
F-Measure	0.9032	0.8235	0.8000

Figure 8: Comparative analysis of the proposed and existing techniques

with some cryptographic strategy so as to ensure the security constraints of data. For this, the data accessed is decrypted after key verification and the decrypted data is shown in figure provided below.

Figure 8 is the comparative analysis of proposed and existing techniques in terms of accuracy, sensitivity, specificity, precision, recall, and F-measure. The comparison is made for proposed and the existing techniques like AlexNet CNN, Basic CNN, and Random Forest classifier. The analysis shows that the proposed system is better than proposed methodology.
Figure 9 is the comparative analysis of proposed and existing techniques in terms of $PSNR$, MSE,

	Proposed	Existing
PSNR	17.6761	13.6761
MSE	0.5856	0.7856
SSIM	0.9862	0.1951

Figure 9: Comparative analysis of proposed and existing techniques

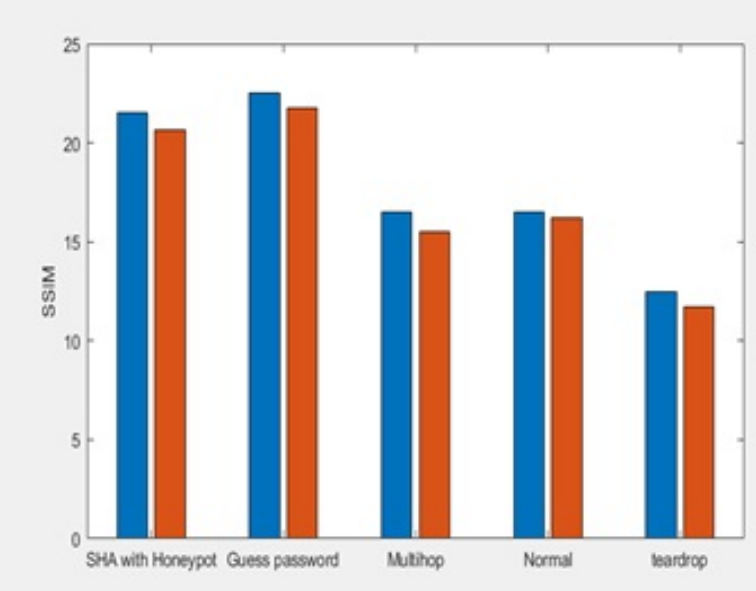


Figure 10: SSIM comparative analysis of existing and the proposed methods

and $SSIM$. The comparison is made for proposed and the existing techniques. The analysis shows that the proposed system is better than proposed methodology.
Figure 10 is the comparative analysis of existing and proposed techniques on behalf of $SSIM$. The comparison is made for proposed SHA with Honeypot algorithm and the existing techniques. The analysis shows that the proposed system is better than proposed methodology.
Figure 11 is the comparative analysis of existing and proposed techniques for $PSNR$. The comparison is made for proposed SHA with Honeypot algorithm and the existing techniques. The analysis shows that the proposed system is better than proposed methodology.
Figure 12 is the comparative analysis of proposed and existing techniques on behalf of MSE. The comparison is made for proposed SHA with Honeypot algorithm and the existing techniques. The analysis shows that the proposed system is better than proposed methodology

5. Conclusions

An approach of efficient cryptographic techniques for the detection and classification of attack in the medical data. The proposed approach with enhanced security of medical data employs cryptographic approaches so as to ensure the effective security constraints. The healthcare medical data is preprocessed by normalization approach and the features are extracted using Enhanced PCA. The classification of attack or intrusion is carried by means of AlexNet CNN classifier. Then the data is securely stored in cloud framework by encrypting the data using Hybrid AES with Honeypot algorithm using SHA3 for hashing function. Thus, the proposed ensemble technique effectively encrypts and decrypts the data with enhanced rate of security. Thus, the performance analysis is carried out by estimating parameters like accuracy, sensitivity, specificity, precision, recall, F-score, MSE, PSNR, and SSIM. Thus, the proposed technique is effective than existing techniques from the analysis.

References

[1] M. H. R. Al-Shaikhly, H. M. El-Bakry and A. A. Saleh, *Cloud security using Markov chain and genetic algorithm*, Int. J. Elect. Inf. Engin. 8(2) (2018) 96–106.

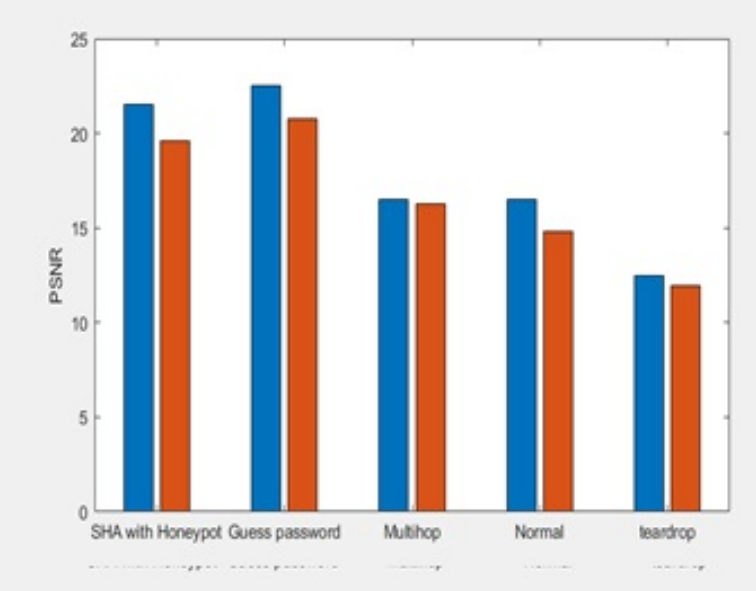


Figure 11: PSNR comparative analysis of existing and the proposed methods

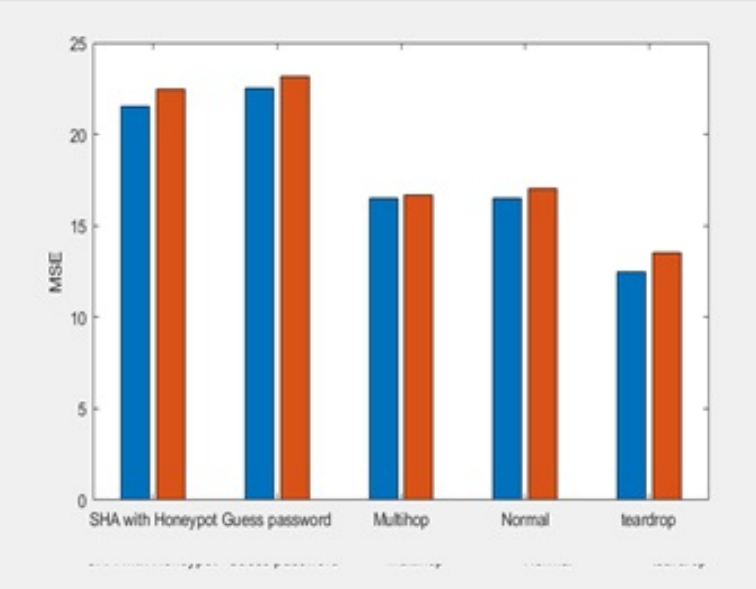


Figure 12: MSE Comparative analysis of existing and the proposed methods

[2] A. Aldweesh, A. Derhab and A. Z. Emam, *Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues*, Knowledge-Based Syst. 189(105124) (2020).
[3] SH. Aljawarneh, M. B. Yassein and W. A. Talafha, *A resource-efficient encryption algorithm for multimedia big data*, Mult. Tools Appl. 76(21) (2017) 22703–22724.
[4] CH. Beyene and P. Kamat, *Survey on Prediction and Analysis the Occurrence of Heart Disease Using Data Mining Techniques*, Int. J. Pure Appl. Math. 118(8) (2018) 165–174.
[5] N. Deepa and P. Pandiaraja, *E health care data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption*, J. Ambient Intel. Human. Comput. 12(5) (2020) 1–11.
[6] R. Devi and J. M. Shyla, *Analysis of various data mining techniques to predict diabetes mellitus*, Int. J. Appl. Engin. Res. 11(1) (2016) 727–730.
[7] M. Durairaj and G. Kalaiselvi, *Prediction of diabetes using soft computing techniques-A survey*, Int. J. Sci. Tech. Res. 4(3) (2015).
[8] R. Gupta, P. Kanungo and N. Dagdee, *HD-MAABE: Hierarchical Distributed Multi-Authority Attribute Based Encryption for Enabling Open Access to Shared Organizational Data*, In: G. S. Tomar, N. S. Chaudhari, J. L. V. Barbosa and M. K. Aghwariya (eds) International Conference on Intelligent Computing and Smart Communication 2019. Algorithms for Intelligent Systems. Springer, 2020.
[9] V. S. V. Hema and R. Kesavan, *ECC based secure sharing of healthcare data in the health cloud environment*, Wireless Personal Commun. 108(2) (2019) 1021–1035.
[10] F. Huang, J. Huang and Y. Shi, *New framework for reversible data hiding in encrypted domain*, IEEE Trans. Inf. Forensics Sec. 11(12) (2016) 2777–2789.
[11] P. Kumar and SH. B. Rana, *Development of modified AES algorithm for data security*, Optik-Int. J. Light Elect. Opt. 127(4) (2016) 2341–2345.
[12] S. S. Kumar, SH. Prasad, M. Parimala and DR. G. M. Someswar, *Scalable and secure sharing of personal health records in cloud computing using attribute based encryption*, Int. J. Adv. Comput. Tech. 5(6) (2016).
[13] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu and N. Kumar, *A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers*, J. Supercom. 74(12) (2018) 6428–6453.
[14] P. Nagar, H. K. Menaria and M. Tiwari, *Novel Approach of Intrusion Detection Classification Deeplearning Using SVM*, In: A. K. Luhach, J. A. Kosa, R. CH. Poonia, X. Gao and D. Singh (eds) First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019, Springer Nature, 2020.
[15] P. Preethi and R. Asokan, *A high secure medical image storing and sharing in cloud environment using hex code cryptography method—secure genius*, J. Med. Imag. Health Inf. 9(7) (2019) 1337–1345.
[16] A. Priya, Dr. S. Saradha, *A detailed survey of the security issues and defensive tactic in cloud background*, J. Adv. Res. Dyn. Cont. Syst. 11(11) (2019) 606–611.
[17] A. Priya, Dr. S. Saradha, *An efficient prediction and privacy preservation using enhanced blowfish cryptographic scheme for cloud security*, HTL J. 26(11) (2020) 1–9.
[18] A. Priya, Dr. S. Saradha, *An overview on cloud computing frameworks and review on cloud security schemes*, J. Crit. Rev. 7(17) (2020) 3303–3308.
[19] M. Rasori, P. Perazzo and G. Dini, *A lightweight and scalable attribute-based encryption system for smart cities*, Comput. Commun. 149(2020) (2020) 78–89.
[20] M. Sakthivanitha and S. Saradha, *Survey based on security aware caching scheme for IoT based information centric networking*, EAI Endorsed Trans. Energy Web 8(32) (2020) e2.
[21] F. Sammy and S. M. C. Vigila, *An Efficient Multiauthority Attribute-Based Encryption Technique for Storing Personal Health Record by Compressing the Attributes*, In: J. Jayakumari, G. K. Karagiannidis, M. Ma and S. A. Hossain (eds) Advances in Communication Systems and Networks. Lecture Notes in Electrical Engineering, Springer, Singapore, 2020.
[22] H. Wang, SH. Wu, M. Chen and W. Wang, *Security protection between users and the mobile media cloud*, IEEE Commun. Mag. 52(3) (2014) 73–79.
[23] H. Xiong, H. Zhang and J. Sun, *Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing*, IEEE Syst. J. 13(3) (2018) 2739–2750.
[24] F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, N. Javed, M. Alam and F. Jamil, *A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends*, Comput. Sec. 65(2017) (2017) 29–49.