A NOVEL HOMOMORPHIC AND MATRIX OPERATION FOR RANDOMIZATION ENCRYPTION SCHEMES FOR PRIVACY IN CLOUD COMPUTING ARCHITECTURE

R. HARI KISHORE[1], A. CHANDRA SEKHAR[2], PRAMODA PATRO[3], PRAGATHI CHAGANTI[4]

[1]Department of Mathematics, Vasavi College of Engineering, Ibrahimbagh,
Hyderabad, Telangana, India, 500031
[1,2] Department of Mathematics, GITAM Institute of Science, GITAM University, Visakhapatnam, Andhra Pradesh, India, -530045
[3]Department of Engineering Mathematics, College of Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, Telengana, India, 500075,
[4]Department of Mathematics, GITAM, Rushikonda, Visakhapatnam, Andhra Pradesh 530003, India

E-maiL : [1]kishore.rh6@gmail.com, [2]cakkaped@gitam.edu, [3]pramoda.mtech09@gmail.com,
[4]pchagant@gitam.edu

ABSTRACT

Traditional outsourced methods are being replaced by the emerging cloud computing architecture, which offers adaptable services to clients in many regions through the Internet. Due to this, it becomes necessary for data categorization to be carried out by probably dangerous cloud servers. In this situation, clients can use a classification created by the server to categorize their unique cloud-based resource test results. The current study effort created a training approach that protects confidentiality using the Matrix Operation for Randomization and Encryption (MORE) scheme, allowing neural network model calculations. The neural unit of the model may retain certain critical data as a result of over-fitting during the deep learning training phase. It is possible for data privacy to be compromised whenever the intruder creates the appropriate assault scenario. In this research article, a Differential Privacy Subspace Approximation with Adjusted Bias (DPSaab) is proposed to train the Feed forward-designed Alexnet convolutional neural network (FF-ACNN). Initially, the data normalization is done by Min-Max normalization then the privacy-preserving training method based on A FF-Alexnet CNN model's calculations may be done immediately on floating point data. This is possible due the encryption technique MORE. In addition, the DPSaab method is used to maintain differentiated anonymity in FF - CNN's Alexnet. The efficacy of the suggested approach is tested on the MINST identification database using the DPSaab method, which meets the concept of differentiated secrecy.

Keywords: *Classification Problem, Homomorphic Encryption, MORE, MNIST Digit Recognition Problem, DPSaab, FF*-ACNN.

1. INTRODUCTION

The demand in cloud computing has grown significantly over the past several years as a result of its benefits, including accessibility and mobility in getting computer capabilities at a cheaper price. The concept of combining physical assets and representing them as virtual assets is the foundation of the abstraction known as "cloud computing". Providing services, developing applications, and enabling platform-independent user accessibility to functions through this architecture is undoubtedly innovative [1]. NIST's description of cloud computing is one of the ones that is most frequently utilised: Through the use of a common pool of reconfigurable computational capabilities that must be quickly supplied and delivered with little administration work or services carrier involvement, cloud computing is a concept for providing universal, practical, on-demand network connectivity [2]. One of the concepts of modern computing that is expanding the quickest is cloud computing. The initial expenditure required by enterprises to implement cloud computing is relatively inexpensive because consumers simply spend for the products they really utilize. Companies currently having the freedom to get assets or solutions as needed. Several of the polls do not address concerns related to administration, identification administration, admission protection, law, and accountability. the latest, most thorough taxonomy of cloud safety problems. To determine how many referrals there are for every type of problems and associated answers, they had adopted a statistical technique [3]. As a result, they had offered considerable insights into both the topics that scholars had focused on and the topics that haven't gotten any focus. They were successful in outlining a taxonomy of cloud privacy, but also avoided going into technological specifics.

On the other hand, Data classification in machine learning and artificial intelligence refers to the challenge of classifying an unexpected information item utilizing a classifier that is constructed from a training set of recognized data samples. It is impossible for persons or smaller companies to create their own classification since doing so required a huge quantity of acceptable learning data [4]. The data categorization should be outsourced to a third party as the only practical answer to this issue. The need for a significant number of correct training information examples, as well as expensive computing and memory capabilities on the part of the customer, is reduced when the data categorization is outsourced. Several approaches have been developed using different methods, including Secure Multiparty Computation (SMC), FHE, and PHE, to enable secure and privacy-preserving data processing in the cloud [5]. But none of them are able to solve the aforementioned three issues. The significant computational complexity of FHE-based techniques prevents flexibility accessibility to the outcomes of cipher text processing. Due to the complexity of secret key transformation amongst customers, it has also shown demonstrated that using cryptography alone is insufficient when data are distributed across several consumers. Consequently, various multi-server methods are suggested and created. However, they still have certain problems [6]. To accomplish calculations over cipher messages that were contracted by a number of clients having its own keys, for instance, a strategy depending on Paillier's cryptosystem was presented. But it can only support addition and multiplication. Another PHE-based technique accomplishes a variety of calculation tasks, but it has a significant computational cost, particularly when multiplying a large number of input data [7]. Using at least three servers, a well-known SMC technique enables safe addition and multiplication. perform additional calculations, but make managing the data more challenging and multiplying a large amount of data more complex.

Convolutional neural networks have demonstrated exceptional efficiency in a variety of disciplines, making it a more prevalent framework for deep learning today. Three factors determine if its use is effective: (1) a vast number of real databases [8], (2) effective optimizing techniques like SGD, Momentum, and Adam, and (3) outstanding deep learning open source frameworks like Tensor Flow, Pytorch, Paddle, and the GitHub code platform The backpropagation process using the stochastic gradient descent approach, which minimizes the loss function, determines all the model parameters given a CNN framework. This trained network is referred to as BP-CNN. Unfortunately, BP-CNN training consumes a significant amount of processing power, and the model itself lacks comprehensibility. a recurrent neural network architecture that uses feedback path. The BP and SGD algorithms are not required to be used in the training of the FF-ACNN [9]. By travelling in a feed-forward fashion, the model's parameters are acquired. The FF-ACNN performs better than BP-CNN under the same model framework and has a less sophisticated model than the latter. Deep learning's risks to security. Since the deep learning dataset includes a lot of particular security details, including the user's location, photos, medical, finances, and other sensitive details, deep learning privacy protection has gained attention as a study area in recently years [10]. An intruder would suffer unpredicted damages if they succeed in obtaining this knowledge, which would harm consumers. Deep learning has two key privacy risks: external causes and internal considerations. To breach the consumer 's confidentiality, the intruder, on the one hand, masters specific background knowledge and puts up assault situations that match to it, such as membership assaults and model inverting assaults. On the other side, over-fitting during the deep learning training phase might lead to the neural unit of the model remembering certain private data. Information security breaches might occur as a result of how the hacker creates the appropriate assault environment [12]. The advancement of deep learning is indeed greatly influenced by how to create an effective private protection system.

In this situation, users can use a classification created by the servers to categorize its own cloud-based information items. The existing research work, developed a privacy-preserving training method based on MORE scheme, enables the computations within a neural network model. The neural unit of the model might remember certain important details as a result of over-fitting during the deep learning training phase. It's possible for information security to be compromised whenever the hacker creates the appropriate assault scenario. So in order to mitigate the problem, this research work proposed a DPSaab the training data in order to FF-ACNN.

The remaining works are arranged in the following sections. In Section 2, discuss cloud computing implementation models and categorization issues. Describes the methods under consideration in Section 3. Findings and their discussions are presented in section 4 in detail in section 5, summarizing proposed work and the issues presented in the work.

2. LITERATURE REVIEW

Discussed some current methods for addressing categorization challenges and privacy concerns in cloud computing in this chapter.

Rahulamathavan et al [13] introduced a privacy-preserving (PP) With a server-side classifier that is hidden from the clients throughout the classification, the server is impossible to learn anything regarding the input data points from the clients. To make further precise, we suggest the first client-server supporting vector machine data categorization protocol that is currently available. Both two-class issues and issues with multiple classes can be classified using the suggested technique. The protocol uses safe two-party computing and the advantages of Pailler homomorphic encrypting. Our method's central idea is a safe method for extracting the Pailler encrypting numbers' sign that is both effective and innovative. A Homomorphic Re-Encryption Scheme was used to assist Ding et al. [14]'s suggested Privacy-Preserving Data Processing (PPDP) system (HRES). By allowing several customers to access processing cipher texts via cipher text re-encryption, the HRES converts partial HE from a single-user system to a multi-user one. Seven fundamental operations on cipher messages, including addition, subtraction, multiplication, sign acquisition, comparison, equivalent test, and variation, may be supported by the PPDP system with the help of a Data Service Provider (DSP) and an Access Control Server (ACS). We also employ numerous ACSs to manage the information from their own customers and construct computational operations across cipher texts belonging to different ACSs in order to increase the adaptability and reliability of the platform. After that, we analyze PPDP's performances and benefits in comparison to other recent work, show how secure it is, and verify its safety. We also show how efficient and successful it is in terms of huge data processing by simulating these processes. Li et al [15] developed a cutting-edge method based on a hybrid structure that combines completely homomorphic encryption with the double decryption process (FHE). Moreover, demonstrate the security of these two multi-key deep learning techniques over encrypted data. Briefly introducing classification algorithms and cloud computing in Zhou et al [17]. Work, they then analyse the drawbacks of the existing parallel classification methods and provide a novel paradigm of parallel classifying algorithms. Additionally, it primarily provides a parallel Map Reduce-based Naive Bayes categorization method, a straightforward yet effective parallel programming method. The empirical findings show that the new approach performs better than the original technique and can effectively handle big information on commodity hardware.

Wang et al [18] the use of homomorphic encryption, which may conceal important inputs and outputs from a counterparties, was suggested as the basis for an outsourcing privacy-preserving decisions tree categorization model. A safe exclusive OR (XOR) protocol has been developed; this protocol deftly computes the XOR of two sets of bit-encrypted data in order to get a third set of bit-encrypted results. According to the empirical findings, the suggested methods are especially effective for cloud-encrypted, outsourcing decisions trees. These decision trees are characteristic of categorization methods that were developed using actual databases, which range using the categorization of cancer to the diagnosis of heart disease. Through the use of encryption methods, Kaur et al [20]. Suggested work plan seeks to allay worries about database protection from various cloud users' perspectives. On order to guarantee the protection of content in the cloud, the model suggested several encryption techniques, including AES, DES, RSA, and Blowfish. We suggested these methods to account for diverse users' points of view. AES, a symmetric encryption method, was introduced by Pancholi et al (Advanced Encryption Standard). It is based on various permutations, replacements, and transformations. A non-interactive, privacy-preserving k-NN query and categorization technique was created by Du et al.

[22]. In order to protect the secrecy of encrypted outsourced data, data access patterns, and the query record, our suggested method is using two already-existing encryption systems: Order Preserving Encryption and the Paillier cryptosystem. It also makes use of the encrypted k-dimensional tree to improve the performance of the conventional k-NN algorithm. High query performance is something that our suggested system aims for when maintaining data security. Comprehensive empirical findings demonstrate that this technique achieves categorization performance that is extremely near to that of the strategy that uses unencrypted information and the scheme that already exists for non-interactively querying encrypted data. Compared to the currently used non-interactive k-NN query strategy, the query runtime of our approach is much faster.

Faheem et al. [23] presented symmetrical encryption using the AES method. Numerous permutations, replacements, and transformations constitute the foundation of it. It demonstrates the use of Secure Data Storage for Cloud Computing to increase security while demonstrating AES's resilience to a number of attacks, including difference, square, key, and key retrieval threats. As a result, the AES algorithm is a very reliable technique of encryption. The algorithms known as AES and Blowfish were developed by Gupta et al. [24]. The provision of protection against the illegal access to the data was the primary intention behind the development of the encryption method. The primary objective of this research is to propose a concept for combining these two methods in order to provide twice the protection for data that is kept inside the cloud. In addition to this, important considerations include efficiency as well as the cost of deployment. Mewada et al. [25] presented a security method, namely AES, DES, BLOWFISH, RSA, and MD5, for use on a single device as well as a cloud network for a variety of inputs. The performance of these algorithms is evaluated using two different parameters: the mean time and the speed-up ratio. Fully homomorphic encryption (FHE) on a symmetric basis is proposed, along with the Matrix Operation for Randomization and Encryption (MORE) technique, which enables unrestricted computation on encrypted data. In order to protect data privacy and improve the current MORE method, the suggested scheme makes use of the Secret Information Moduli Set (SIMS) [30].

3. PROPOSED METHODOLOGY

This research work proposed a Differential Privacy Subspace Approximation with Adjusted Bias (DPSaab) to safeguard the data used for training in Feed forward-designed Alexnet convolutional neural network (FF-ACNN). Here initially the data normalization is done by Min-Max normalization. And then the privacy-preserving training method based on encryption scheme, MORE, allows for the direct use of floating point data in the calculations carried out by an FF-Alexnet CNN model. Lastly, the FF-Alexnet CNN uses the DPSaab algorithm to maintain differential privacy. The process of the proposed methodology is shown in figure 1.

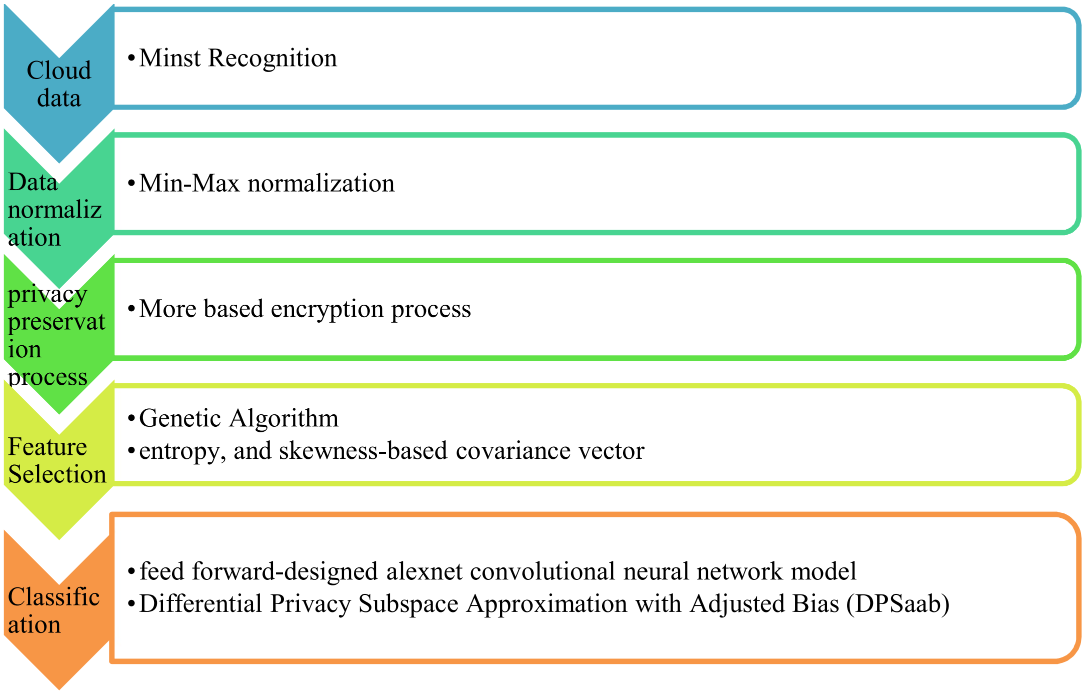
Cloud data
•Minst Recognition
Data normaliz ation
•Min-Max normalization
privacy preservat ion process
•More based encryption process
Feature Selection
•Genetic Algorithm
•entropy, and skewness-based covariance vector
Classific ation
•feed forward-designed alexnet convolutional neural network model
•Differential Privacy Subspace Approximation with Adjusted Bias (DPSaab)

Figure 1. Proposed Methodology

3.1. Problem Formulation: MNIST

Classification is a common topic explored in the NNs context. The challenge of image classification is highly particularly related to data displayed in images. MNIST [26] database comprises Graphics of handwritten numerals are often utilized as the starting point for images classifier systems. digit recognition problem was chosen for the first experiment to address the issues of privacy-preserving calculations in NN systems with the goal of giving important insights into the proposed technique's advantages and weaknesses in a real-world setting. Deep CNN models, on the other hand, have been proven to outperform other kinds of classification models on MNIST, resulting in the lowest reported test error. Furthermore, the error rate increased whenever matching shallow networks were used, underlining the necessity in depth modelling. Estimating the probability that a picture belongs to one of 10 groups is how the problem of digit recognition is put out (0–9 digits). Target labels are thus often represented as one-hot vectors with the values 1 for associated class and 0 for remainder. A NN system that has been trained to minimize the cross-entropy error between predicted (y I and expected (y) probability distributions may be used to solve this case of a multiclass classification problem (C = 10) which is defined in the following equation 1.

$$CE(y, \tilde{y}) = -\sum_{c=1}^{c=10} y_i \log(\tilde{y}_i) \qquad (1)$$

(1) Dataset

MNIST collection contains 70,000 gray-scale images with a relative small size of 28 28 pixels, every image tagged with digit which shows in Figure 2. In the images, the digits are size-normalized and centred. MNIST samples were divided into 3 databases, yielding 50,000 instances for training NN classification model, 10,000 for verifying trained model, 10,000 for evaluating performance of the classification method. To prevent class imbalance difficulties that frequently occur in classification, the training data were evenly distributed among the 10 classes.

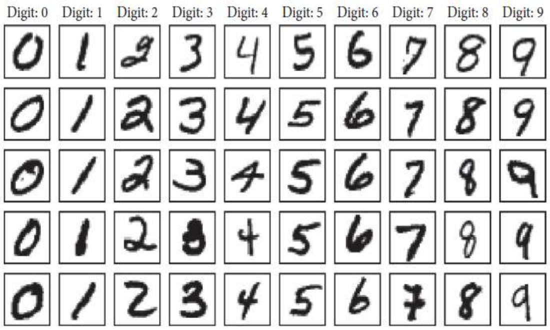

Figure 2: Mnist Database Sample Images [26]

Pixel values in MNIST images vary from 0 to 255. Pixel values are scaled between [0, 1] depending on the least and highest pixel intensity to facilitate training convergence. MNIST labels, which were expressed by numerical values ranging [0-9], are encoded to categorical data as one-hot vectors for neural network training. As a result, every digit was indicated by the vector with a length equivalent to total classes and a value of 1 for digit position in vector, with all other values set to 0.

3.2. Min-Max based Data Normalization

Min-Max normalization, z-score normalization, and decimal scaling normalization of data are examples of data normalization [27]. By applying a linear adjustment to the initial data, min-max normalization transforms it. Consider that the lowest and maximum values for attribute A are mina and maxa. Equation shows how to compute the min-max normalization, which converts a value of A, v, to v' in the range (2). Range transformation was chosen as the technique to adjust the normalizing result to the appropriate scale. The formula for range transformation used for normalizing is shown in equation (2):

$$v' = \left(\frac{(v - min_a)}{(max_a - mi\ \ _a)}\right) * \left((new - max_a) - (new - min_a)\right) + new - n \qquad (2)$$

In an effort to give each attribute the same weight, data is normalized. For categorization methods using neural networks or measures of distance, such as nearest-neighbor identification, normalizing is very beneficial.

3.3. Matrix-Based Data Randomization

More than one version of MORE encryption technique is explored and developed to work directly on floating-point data. A n n cipher text matrix is used to encrypt a plaintext scalar using the MORE encryption technique [28], Calculations on encrypted text may be made possible by the application of matrix algebra. As a consequence of this, each and every action performed on cipher text data is characterized as a matrix operation. For instance, the multiplication of plaintext scalars is referred to as the matrix multiplication of cipher text matrices. Sequence of matrices employed to encrypt a message is an essential aspect in determining the security-to-efficiency trade-off. The MORE cryptosystem is presented in Table 1 for a 2 × 2 configuration.

MORE method allows to do algebraic operations on cipher text matrices, that is., provided two encrypted matrices *C*1 =*SM*1*S*− 1 and *C*2 =*SM*2*S*− 1, for addition.

$$C_1 + C_2 = SM_1S^{-1} + SM_2S^{-1} = S(M_1 + M_2)S^{-1} \qquad (3)$$

which is the encryption of $M_1 + M_2$, and for multiplication

$$C_1C_2 = SM_1S^{-1}SM_2S^{-1} = SM_1M_2S^{-1} \qquad (4)$$

Subtraction and division, and also plaintext scalar operations, have the same characteristic, making the system completely homomorphic for algebraic process.

Table 1: More Encryption Scheme For Rational Numbers.

Message	**Scalar value m∈ ℝ**
Secret key generation	Invertible matrix $\boldsymbol{S} \in \mathbb{R}^{\mathbf{2*2}}$
Matrix construction	$M = \begin{pmatrix} m & 0 \\ 0 & r \end{pmatrix}$, where r∈ ℝ is a random parameter

Encryption operation	Encryption$(m) = C = SMS^{-1}$
Decryption operation	Decryption$(C) = K = (S^{-1}CS)$
Message recovery	$m = K_{(1,1)}$

- **Encryption of Rational Numbers**

Actual MORE method, the same as any FHE or PHE technique, is restricted to positive integer values modulo N, and all operations are carried out modulo N. This restriction applies to the full set of operations. In order for these systems to be able to function properly with rational numbers, an encoding method is used to a substantial extent. The end result of this process is that a real number is converted into an integer, the technique is then employed to homomorphically encrypt encoded numbers. The use of continued fractions is a common way to formulate the encoding. Even fundamental processes on numbers stated in this form are hard to execute, despite the fact that an accurate representation may be achieved. However, by multiplying rational integers with high scaling parameters, a simpler encoding may be inserted. Though much more permissive, it necessitates a scaling factor management method, that is problematic to implement some processes, such as division, when this factor is decreased. Furthermore, by expanding the methods to work on rational numbers, noise is often introduced into the cryptosystem. As a result, a noise-control technique must be implemented to keep the noise level to a minimum. Despite the fact that dealing with rational numbers seems to be a straightforward undertaking, there is not yet a solution that will allow them to be employed in higher education. The fact that the MORE encryption technique may be easily defined for rational numbers is one of its primary advantages.

- **Performing Operations over Encrypted Data**

With regard to basic algebraic operations, the MORE encryption method has been proven to be completely homomorphic. Nonlinear functions must be handled in real-world applications, with DL-based techniques. The majority of regular nonlinear process techniques are relied on notion the process, utilizing a finite polynomial series, of approximate the value that was provided. Nonlinear function calculation is based purely on algebraic operations in this technique, which is perfectly compatible with the MORE encryption setup. Nevertheless, a more practical method is feasible within the MORE cryptosystem. Provided the characteristic that govern encryption systems, as well as the fact that matrix algebra is required for cipher text-based procedures, nonlinear functions can be calculated in one of two ways: either (1) directly as matrix functions, or (2) through matrix deco, in which a message m that has been encrypted can always be found among the eigenvalues of the cipher text matrix C. Consider, in a 2 × 2 configuration, one of eigenvalues related to arbitrary value r used while matrix construction, whereas other relates to message m. A random number r is often chosen to be statistically indistinguishable from the message in order to ensure that it can only be decrypted properly and decoded using a secret key to identify the message. It is possible to use a function f on C cipher text data consequently equal to using f position. Whilst initial approach is straightforward, next method is formed on the property as said by directly on C eigenvalues. Hence, matrix decomposition $VLV-$ 1 is first utilised to break down the encrypted text matrix C into its eigenvalues L and eigenvectors V. Because of this, each eigenvalue of the nonlinear function that has to be evaluated has value on its own. Finally, the encrypted text matrix that has been created is reshaped as $Cf=Vf(L)V-$ 1 using the aid of the original eigenvectors and the function f's evaluated Eigen values. This approach is used to compare plain scalar s and cipher text matrix C, as opposed to direct matrix function dependent on computations. Any of these two methods may enable nonlinear binary operations between two cipher text pieces of data. However, in DL, such a procedure is entirely disregarded. The implementation of the sigmoid function under the MORE encryption technique is shown in Algorithm 1.

Algorithm 1. Sigmoid Function Under MORE Encryption Method Implementation.

```
Input: Ciphertext C ∈ $R^{2×2}$
Output:Ciphertext R ∈ $R^{2×2}$
function Sigmoid(C) \\ Utilizing direct matrix process
    $R \leftarrow I_2 \times (I_2 + MatrixExp(- C))^{-1}$ \\$I_2$ indicates identity matrix
    return R
end function
function Sigmoid(C) \\ Utilizing eigen decomposition
    $L, V \longleftarrow$ Eigen Decomposition(− C)
    $L_f \longleftarrow Diag(Exp(L))$
    $C_{exp} \longleftarrow V\times L_f\times V^{-1}$
    $R \longleftarrow I_2 \times (I_2 + C_{exp}) - 1$
    return R
End
```

Starting with these techniques, Algorithm 1 demonstrates how the two proposed approaches may be used to construct the function $f(x) = (1/(1 + e- x))$ specified on $x \in$ R, under MORE conditions, provided any ciphertext $C \in R^{2\times2}$. The logistic sigmoid function is a nonlinear function that is usually employed in neural networks, as will be discussed in the following sections.

3.4. Privacy Feed Forward-Designed Alexnet Convolutional Neural Network (FF-ACNN)

To maintain differentially security in FF-ACNN, the authors of this paper present a differentially privacy subspace approximations that uses an adjusted bias approach. This technique is given the name DPSaab. The concept of contributions may, broadly speaking, be broken down into two primary categories. First, the DPSaab algorithm was designed so that differentiated privacy could be maintained in FF-ACNN. Second, it was shown that the DPSaab method meets the notion of different datasets, and tests were carried out using the benchmark dataset MNIST in order to validate the efficacy of the suggested approach.

3.4.1. Differential Privacy

In recent years, differential privacy has emerged as a popular and frequently utilized method for providing stringent levels of privacy protection in the context of machine learning and deep learning. The following is a list of some fundamental definitions:

Definition 1 ($\in$ −Differential Privacy [29]). Given the presence of two nearby datasets D and D', They were dissimilar in just one tuple across the whole set. Regarding the method M, whose value range is represented by Range (M). In the event that algorithm M generates arbitrary outcomes R ($R \in Range(M)$) on datasets D and D' satisfied:

$$P_r[M(D) = R] \le e^{\epsilon} P_r[M(D') = R] \qquad (5)$$

If this condition is met, we may say that the method M fulfils $\in$ differential privacy, where $\in$ denotes the number of privacy resources. It regulates the quantity of noise that is introduced into M, and the greater the ratio of noise to privacy resources, the more effective the algorithm M is at protecting users' personal information.

Definition 2. Given a query function $f : D \rightarrow R^d$ on any neighbouring databases that start with D and D', When it comes to sensitivities, the variable f is as follows:

$$GS_f = \max_{D,D'} \|f(D) - f(D')\| \qquad (6)$$

where $\|.\|$denotes $L1$ or $L2$ norm. The term "sensitivity" describes the largest possible modification to the outcomes of a query that involves just one record.

The major Laplace and exponentially mechanisms used in the algorithm M implementation of differential privacy security are within the practical issues. Laplace mechanism and L1 norm sensitivity will be used in this study.

Definition 3: Using query method with provided database D $f : D \to R^d$ and its sensitivity GS_f. The random noise is added $Y \sim Lap(\frac{GS_f}{\in})$ *to* the query function $f(D)$, the random algorithm $M(D) = f(D) + Y$ provides ∈-differential privacy protection.

The target item must often be protected in real-world circumstances by combining many privacy security strategies. Sequencing composing and simultaneous composing are the two primary subtypes of the differentiated security combining techniques now in use. To provide differentiated security protections in this work, take advantage of sequence composition's characteristics.

3.4.2. Feedforward-designed alexnet convolutional neural network (FF-ACNN)

Backpropagation (BP) and optimization methods are not needed for the model's parameter training (SGD). The preceding layer's statistical data forms the foundation of the whole network, and the next layer's parameters are collected in a single pass. The FF-ACNN training technique is more useful than the BP training method because the network complexity under the FF design is lower than the BP algorithm.

With FF-ACNN, the model is trained in a single epoch using a data-centric strategy, as opposed to BP-ACNN, which takes many epochs to achieve model convergence. Be aware that FF-ACNN is made up of two cascaded models, as illustrated in Fig. 3:

1) Building convolutional and mixing layers using subdomain modelling is covered in Module 1.

2) The Module2 of least squared regression involves creating completely linked layers (LSR). The multistage Saab transform is used to create the convolutional layer.

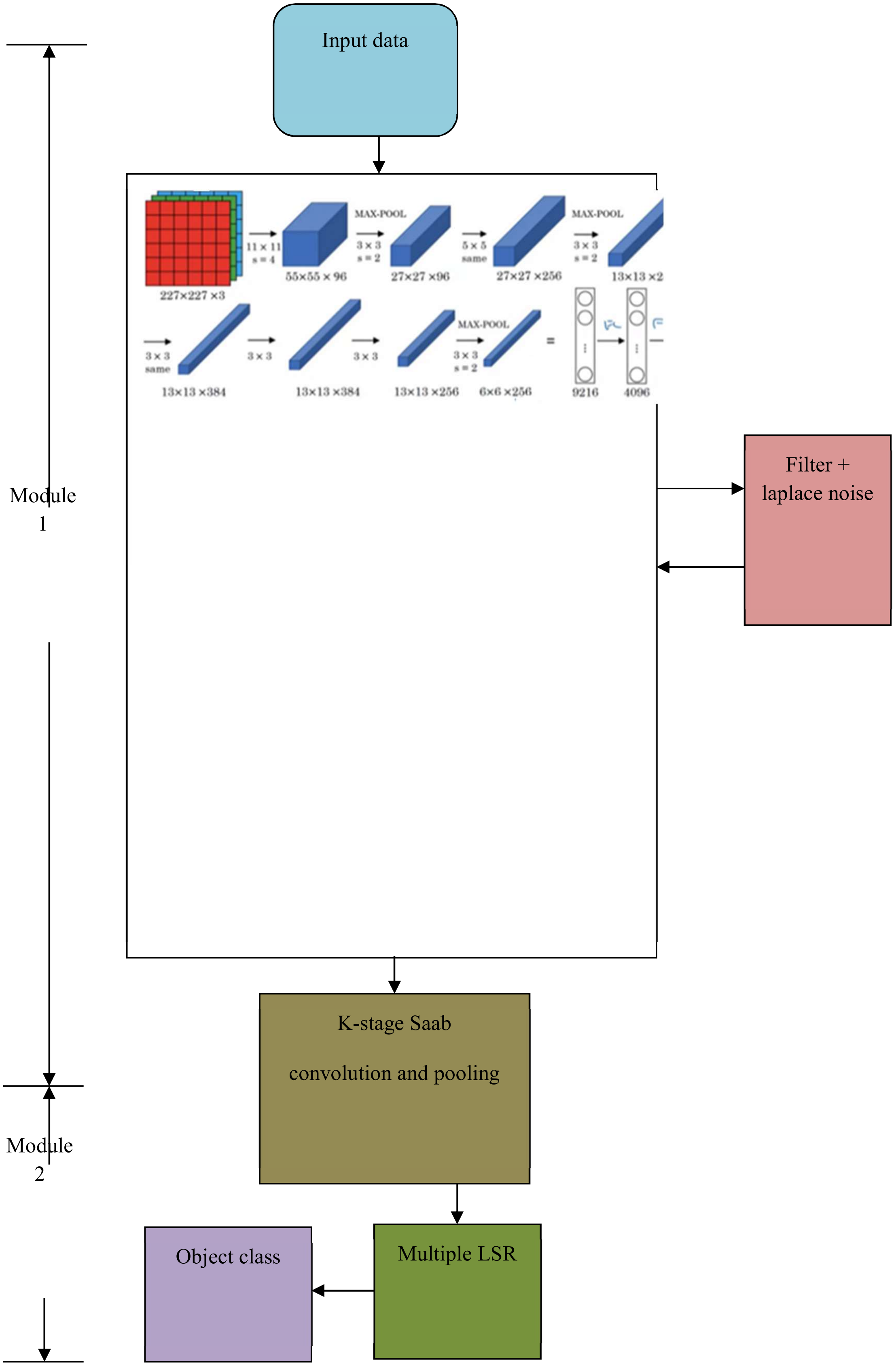
Input data
227×227 ×3
11 × 11
s = 4
55×55 × 96
MAX-POOL
3 × 3
s = 2
27×27 ×96
5 × 5
same
27×27 ×256
MAX-POOL
3 × 3
s = 2
13×13 ×2
3 × 3
same
13×13 ×384
3 × 3
13×13 ×384
3 × 3
13×13 ×256
MAX-POOL
3 × 3
s = 2
6×6 ×256
=
9216
4096
Filter +
laplace noise
Module
1
K-stage Saab
convolution and pooling
Module
2
Multiple LSR
Object class

Fig. 3. The FF-ACNN is shown in an example. Alexnet's convolutional layer is built using the blue block, the fully connected layer is built using the purple block, and the DPsaab technique is built using the red block.

It can determine the parameters of the convolutional layer and to solve the model's symbol ambiguity issue, delete symbols. the FF-input ACNN's is *X* = (*x*0, *x*1, . . . , *xN*−1)*T* the one-stage Saab transformation of dimension N may be obtained as follows.

$$y_k = \sum_{n=0}^{N-1} \omega_{k,n} x_n + b_k = \omega_k^T X + b_k, \qquad k = 0,1, \dots \dots, K-1 \qquad (7)$$

where k is the order in which the filters are applied, ω*k* is filters and *bk* is a phrase used to describe prejudice *k*th Saab filter. When *k* = 0, the DC filter's calculating technique is

$$\omega_0 = \frac{1}{\sqrt{N}} (1, \dots .1)^T \qquad (8)$$

where N is the number of different traits. Projecting the input feature X onto the DC filter, whose calculation is as follows, will give you the DC element *XDC* = √ 1 *N N n*=0 *Xn*. We are able to get this result as a result of the orthogonal connection that exists among the DC element and the AC element *XAC* = *X* − *XDC*. To get *AC* filters ω*k* (*k* = 0, · · · , *K*−1), In order to deconstruct the AC components, the PCA technique is utilized, and then the first (K - 1) eigenvectors are chosen to serve as AC filters. When everything is said and done, the ultimate one-stage Saab transform filters are produced by merging the DC filter with the AC filters. During this time, we can establish the bias rule. vector *bk* ≥ max*x* |*x*| (*k* = 0, . . . , *K*−1) for the purpose of substituting non-linear activating types like as *Relu, Sigmod, Tanh,* etc. The networks very challenging to analyze because to the fact that they.

Multiple rectified linear LSR are cascaded to create the fully-connected layer in module 2. Assumed to be Kin and Kout for an FC layer's input and output parameters, accordingly. To get the parameters of the FC layer, it is necessary to first create an equation system to reverse-solve the variables of the FC layer using the K-means technique to cluster input features of dimensions Kin into Kout groups.

3.4.3. Privacy risks of FF-ACNN

In FF-ACNN, the recurrent layer's settings are set using the Saab transform, as is well known. Figure 1: The input picture for the FF-ACNN is a dimension (*Cin*, *Hin*,*Win*) produces a dimension-based result (*Cout*−1, *Hout*−1,*Wout*−1) after the one-stage Saab conversion. A set of linear equations may then be used to represent the modification of the convolutional.

$$\sum \omega_1 \odot \left(C_{in}, H_{in,} W_{in}\right) = \left(1, H_{out-1}, W_{out-1}\right) \qquad (9)$$

$$\sum \omega_{C_{out}} \odot \left(C_{in}, H_{in,} W_{in}\right) = \left(C_{out-1}, H_{out-1}, W_{out-1}\right) \qquad (10)$$

where ω is element-wised components and is the variables of the convolutional level. If and only if output dimension is considered from the standpoint of linear algebra, $(C_{out-1}, H_{out-1}, W_{out-1})$ is larger than the dimensions that were supplied $(C_{in}, H_{in,} W_{in})$, the Eq. (5) has a special solution. Use the MNIST grayscale database as an instance. The picture input size for FF-ACNN is (32, 32, 1), the first convolution layer's number is 6, the size is (5, 5), and the stride is 1. The result reaction with the dimensions (28,28,6) is produced after the convent in the one-stage Saab transformation. Make sure the input image's size is less than the output response's size. Consequently, in the event that the adversary is successful in destroying the Saab transformation, the variable as well as the output reaction of the convolution layer may be controlled, and the incoming picture may be manipulated $\left(C_{in}, H_{in,} W_{in}\right)$ would be made public.

The MNIST database and the Fashion-MNIST database were each placed via a two-stage Saab transition so that confidentiality dangers could be verified. Following this, the output reaction that was produced because once the transition was used, along with the variables that were ascertained by the two-stage Saab transition, to resemble the previous input data through the linear equation domain that was described earlier.

3.4.4. *DPSaab Algorithm*

The DPSaab approach is shown by the block in red in Fig. 1. And make sure that the final model parameters are in agreement with the concept of distinct datasets before you add the Laplace noise to the filter in the one-stage Saab transformation. In principle, you could preserve the trained information by adding the same magnitude of Laplace noise to filter in order to do so, but doing so would have an impact on the usefulness of the model. As a result, several components of the one-stage Saab transformation provide distinctive contributions to the final response output. The DPSaab method, which allocates privacy resources to filters based on a ratio of eigenvalues, is going to be proposed in this paper. When it comes to filters with higher eigenvalues, more privacy resources are allotted. This results in a reduction in the amount of noise that is produced, and vice versa.

Step 1: First calculate the filter $\omega_0 = \frac{1}{\sqrt{N}}(1,\cdot\cdot\cdot,1)^T$. Taking Into Account the Description 2, set $\Delta\omega_0 = \omega_0$ and privacy resources is $\in_1$. The filter ω_0 a perturbation is introduced in the one-stage Saab transform.

$$\varpi_0 = \omega_0 + Lap\left(\frac{\Delta\omega_0}{\epsilon_1}\right) \qquad (11)$$

where $\omega_0$is the perturbed filter.

Step 2: dividing the database D into separate halves to get *X_{AC}*, After that, to get the filtering ω_k and Eigen values λ_k $(k = 1,\cdot\cdot\cdot,K - 1)$.

Step 3: The worldwide sensitivities levels of the filtering are defined in Specification 2 as ω_k $(k = 1,\cdot\cdot\cdot,K - 1)$ is determined as

$$\Delta\omega = \Delta\omega 1, \Delta\omega 2, \dots\dots, \Delta\omega_{k-1} \qquad (12)$$

$$= \max\{\omega_k\}_{k\epsilon[1,K-1]} - \min\{\omega_k\}_{k\epsilon[1,K-1]} \qquad (13)$$

the filters were then given a dose of Laplace noise ω_k $(k = 1,\cdot\cdot\cdot,K - 1)$. The filters' related eigenvectors are ranked from greatest to lowest in accordance with the underlying mathematical theory, *i.e.*, $\lambda_1 > \lambda_2 > \cdots \lambda_{K-1}$. The significance of the related eigenvalue increases with increasing eigenvectors. Consequently, provide a method for allocating private assets that takes the ratio of eigenvector into account α_k. The k-th convolutional processor's calculating method for its security assets ω_k is

$$\alpha_k = \frac{\lambda_k}{\sum_{k=1}^{K-1}\lambda_k} s.t. \epsilon_k = \alpha_k * \epsilon_2 \qquad (14)$$

Every filtering, as per specification 3, ω_k $(k = 1,\cdot\cdot\cdot,K - 1)$ As a result of the Saab conversion's single phase,

$$\varpi_k = \omega_k + lap\left(\frac{\Delta\omega}{\epsilon_k}\right),\ k = 1, \dots\dots. K - 1 \qquad (15)$$

where ω_k is the distorted filtering.

Step 4: Combine the criteria finally ω_k and ω_0 One-stage transformation filtering are needed that receive this differentiated confidentiality.

$$\bigcup_{k=0}^{K-1}\varpi_k = \bigcup_{k=0}^{K-1}\varpi_k \cup \varpi_0 \qquad (16)$$

With respect to classifier, confidentiality security, and small-sample training, the DPSaab method is quite useful.

4. Results and Discussion

The relative correctness of the categorization methods, or the proportion of properly labelled digit pictures, serves as the standard statistic utilized to evaluate a classifier's effectiveness on the MNIST database. This was to be anticipated since the classifiers selected to evaluate the accuracy of the calculations used to preserve confidentiality in a standard HE issue rather than to resolve the challenge of digits' identification.

Table 2. Security Strength

File size (bits)	MPC	HE	MORE-DL	FF-ACNN
100	82.76	85.43	89.12	91.67
200	84.72	87.28	90.68	93.15
300	86.09	88.15	92.56	94.79

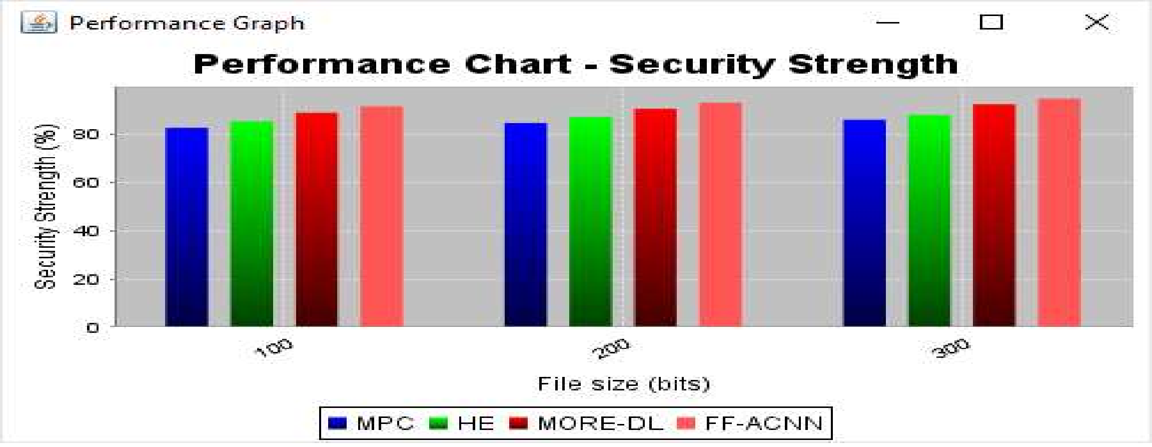

Figure .4. Performance Evaluation Of The Suggested FF-Security ACNN's Strength In Comparison To Current Techniques

The figure 4. illustrate the performance comparison of security strength between the proposed and existing methods. In accordance with the ratio of the associated eigenvector, the DPSaab method adds Laplace noise to the one-stage transform's filtering. Inversely, filtering having lower distortion were applied to those having higher eigenvector. By introducing a filter with the identical amount of Laplace distortion as that produced with the one-stage Saab translation, the DPSaab algorithm safeguards the confidentiality of modeling results. Based on the findings, it can be concluded that the suggested DPSaab method offers the highest level of safety for the MNIST database categorization issue.

Table 3. Detection Accuracy

File size (bits)	MPC	HE	MORE-DL	FF-ACNN
100	82.55	85.29	87.15	89.64
200	84.76	87.43	89.76	91.53
300	91.87	93.57	94.34	95.06

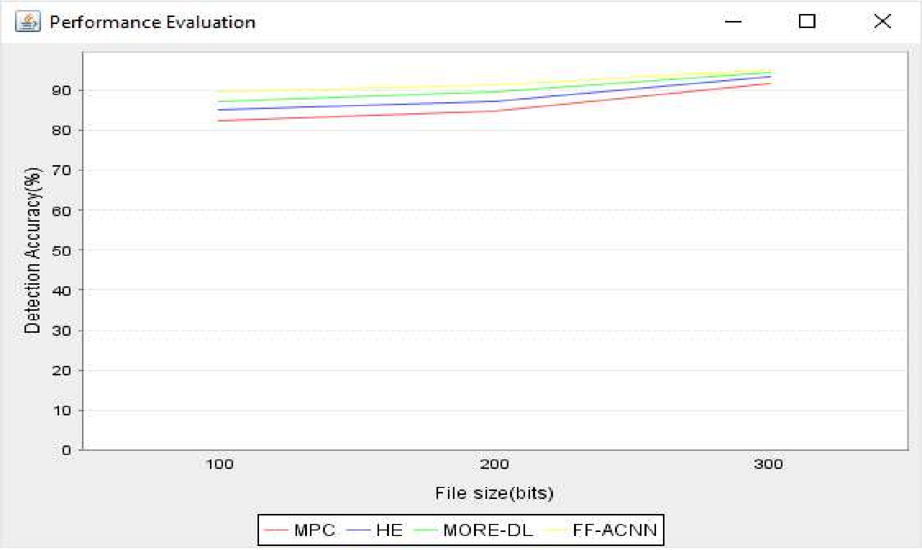

Figure .5. Performance Comparison Of Detection Accuracy Between The Proposed FF-ACNN And Existing Methods

Figure 5 compares the effectiveness of the suggested and current approaches in terms of detecting efficiency. The first layer of the convolutional kernel in the MNIST grayscale database has a layer count of 6, a size of (5, 5), a stride of 1, and an images input size of (32, 32, 1). The result reaction with the dimensions (28,28,6) is obtained after the combination procedure has been completed in the one-stage Saab transformation. The dimensions of the answer that is produced has a higher value than the dimensions of the picture that is being used as input. As a consequence of the findings, it has been shown beyond a reasonable doubt that the suggested approach offers a higher level of reliability rate than the methods currently in use.

Table 4. Run Time

File size (bits)	MPC	HE	MORE-DL	FF-ACNN
100	0.68	0.61	0.57	0.53
200	0.77	0.72	0.69	0.65
300	0.85	0.80	0.76	0.71

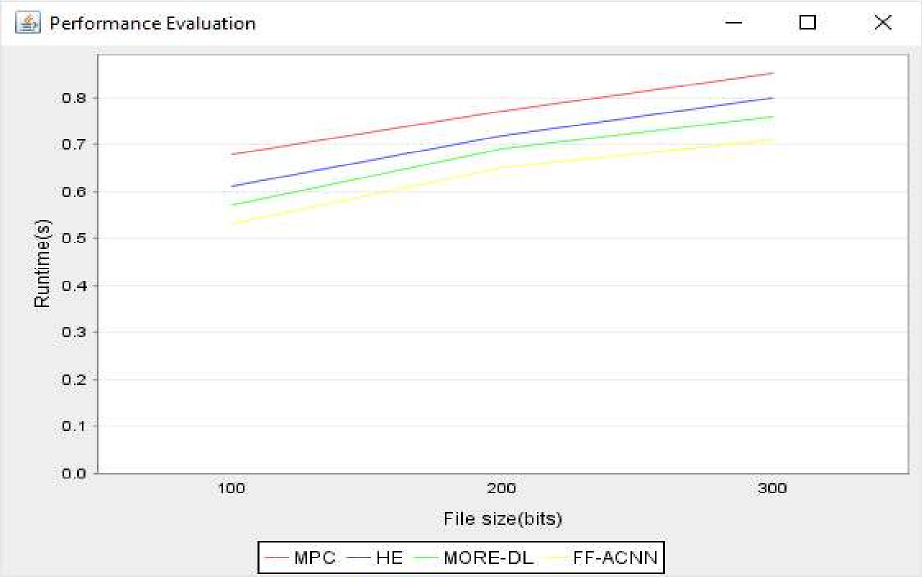

Figure .6. Runtime Comparison Between The Proposed FF-ACNN And Existing Methods

A comprehensive analysis of how long it takes every of these methods to complete is shown in the figure. 6. In order to check for potential data protection risks, we first placed the MNIST and Fashion-MNIST databases each via a two-stage Saab conversion, and after which we utilize the result that is produced after the transition in conjunction with the variables that are ascertained by the two-stage Saab transition in order to estimate the initial input data using the linear equation component described earlier.

5. CONCLUSION

The training data in FF-ACNN were suggested to be protected by a DPSaab as part of this research endeavour. The Min-Max normalization technique is used to begin the process of data normalization here. The privacy leakage issue caused by the Saab transform in FF-CNN should then be analysed and verified. The DPSaab method, which allocates privacy resources to filters based on the ratio of eigenvalues which is proposed in this paper. When it comes to filters that have greater eigenvectors, a higher portion of the private resources is allotted. This results in lower noise being supplied, and the opposite is true when it comes to filtering with smaller eigenvector. Utilize the proportion of eigenvector as a means of allocating the private assets in accordance with the contributions of the filter to the outcome reply of the Saab transform. Verify that the DPSaab algorithm has excellent value from a variety of perspectives, including its capacity to preserve users' confidentiality, its categorization correctness, and its couple training capability. In FF - CNN's Alexnet, distinguished anonymity is maintained via the DPSaab technique. The DPSaab method, which shows the concept of differentiated secrecy, is used to test the effectiveness of the proposed strategy on the MINST identifying database. To improve the effectiveness of the proposed methodology, other optimisation techniques can be used in the future.

REFERENCES

[1] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. J., “A review of machine learning algorithms for cloud computing security”, *Electronics*, *9*(9),(2020) 1379.

[2] Heilig, L., & Voß, S, “Decision analytics for cloud computing: a classification and literature review”, *Bridging Data and Decisions*, 2014, pp:1-26.

[3] Yang, H., & Tate, M, “A descriptive literature review and classification of cloud computing research”. *Communications of the Association for Information Systems*, *31*(1), 2012.

[4] Liu, K., & Boehm, J., “Classification of big point cloud data using cloud computing”, *ISPRS-International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *40*, 2015, pp.553-557.

[5] Khalil, I. M., Khreishah, A., Bouktif, S., & Ahmad, A., “Security concerns in cloud computing”, In *2013 10th International Conference on Information Technology: New Generations, 2013,* pp. 411-416, IEEE.

[6] Waqas, A., Yusof, Z. M., & Shah, A., “ A security-based survey and classification of Cloud Architectures, State of Art and Future Directions”, In *2013 International Conference on Advanced Computer Science Applications and Technologies, 2013,* pp. 284-289, IEEE.

[7] Yang, H., & Tate, M., “A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems*, 2012, *31*(1), 2.

[8] Liu, Y., Sun, Y. L., Ryoo, J., Rizvi, S., & Vasilakos, A. V., “A survey of security and privacy challenges in cloud computing: solutions and future directions”, *Journal of Computing Science and Engineering*, *9*(3), 2015, pp. 119-133.

[9] Masdari, M., & Khoshnevis, A., “A survey and classification of the workload forecasting methods in cloud computing”, *Cluster Computing*, *23*(4), 2020, pp. 2399-2424.

[10] Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P., “State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment”, In *Proceedings of the international conference on advances in computing, communications and informatics* 2012, pp. 470-476.

[11] P. Patro, K. Kumar, G. Suresh Kumar et al., “Similarity and wavelet transform based data partitioning and parameter learning for fuzzy neural network”, *Journal of King saud computer and information sciences*, Volume 34, Issue 6, Part B, 2022, pp. 3424-3432, ISSN 1319-1578, 2022.

[12] Islam, T., Manivannan, D., & Zeadally, S., “A classification and characterization of security threats in cloud computing”, *International Journal of Next-Generation Computing*, 2016, pp.01-17.

[13] Rahulamathavan, Y., Phan, R. C. W., Veluru, S., Cumanan, K., & Rajarajan, M., “Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud”, *IEEE Transactions on Dependable and Secure Computing*, *11*(5), 2013, pp. 467-479.

[14] Ding, W., Yan, Z., & Deng, R. H. ,“Encrypted data processing with homomorphic re-encryption”, *Information Sciences*, *409*, 2017, pp. 35-55.

[15] Li, P., Li, J., Huang, Z., Li, T., Gao, C. Z., Yiu, S. M., & Chen, K., “Multi-key privacy-preserving deep learning in cloud computing”, *Future Generation Computer Systems*, *74*, 2017, pp. 76-85.

[16] P. Patro, K. Kumar, & G. Suresh Kumar. Neuro Fuzzy System with Hybrid Ant Colony Particle Swarm Optimization (HASO) and Robust Activation, *Jour of Adv Research in Dynamical & Control Systems*, Vol. 12, 2020, 03-Special Issue pp. 741-750.

[17] Zhou, L., Wang, H., & Wang, W., “Parallel implementation of classification algorithms based on cloud computing environment. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, *10*(5), 2012, pp. 1087-1092.

[18] Wang, C., Wang, A., Xu, J., Wang, Q., & Zhou, F., “Outsourced privacy-preserving decision tree classification service over encrypted data”, *Journal of Information Security and Applications*, *53*, 2020, pp. 102517.

[19] P. Patro, K. Kumar, & G. Suresh Kumar, “Optimized Hybridization of Ant Colony Optimization and Genetic Algorithm (HACOGA) Based IC-FNN Classifier for Abalone”, *Journal of Computational and Theoretical Nanoscience* Vol. 17, 2020, pp.2756–2764.

[20] Kaur, M., & Mahajan, M. (2013). Using encryption algorithms to enhance the data security in cloud computing. *International Journal of Communication*, *1*(02), 2013.

[21] Pancholi, V. R., & Patel, B. P., “Enhancement of cloud computing security with secure data storage using AES”, *International Journal for Innovative Research in Science and Technology*, *2*(9), 2016, pp. 18-21.

[22] Du, J., & Bian, F., “A privacy-preserving and efficient k-nearest neighbor query and classification scheme based on k-dimensional tree for outsourced data”, *IEEE Access*, *8*, 2020, pp. 69333-69345.

[23] Faheem Gul, Aaqib Amin, Suhail Ashraf, " Enhancement of Cloud Computing Security with Secure Data Storage using AES", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.7, July- 2017, pg. 27-32.

[24] Gupta, U., Saluja, M. S., & Tiwari, M. T., “ Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms”, *International Journal of Recent Research Aspects*, *5*(1), 2018, pp. 55-61.

[25] Mewada, S., Shrivastava, A., Sharma, P., Purohit, N., & Gautam, S. S., “Performance analysis of encryption algorithm in cloud computing. *International Journal of Computer Sciences and Engineering*, *3*, 2015, pp. 83-89.

[26] http://yann.lecun.com/exdb/mnist/.

[27] Pinto, P., “Introducing the min-max algorithm. *Submited to the AI Depot article contest*,2020, pp. 1-10.

[28] Gupta, C. P., & Sharma, I., “A fully homomorphic encryption scheme with symmetric keys with application to private data processing in clouds”, In *2013 Fourth International Conference on the Network of the Future (NoF), 2013,* pp. 1-4. IEEE.

[29] C. Dwork, F. McSherry, K. Nissim, and A. D. Smith, “Calibrating noise to sensitivity in private data analysis,” in *Theory of Cryptography, Third Theory of Cryptography Conference*, 2006, pp. 265–284.

[30] K. J. Muhammed and K. A. Gbolagade, "Enhanced MORE Algorithm for Fully Homomorphic Encryption Based on Secret Information Moduli Set," 2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2019, pp. 469-473, doi: 10.1109/IEEM44572.2019.8978501.