Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.036093
Article

A Secure Method for Data Storage and Transmission in Sustainable Cloud Computing

Muhammad Usman Sana[1,*], Zhanli Li[1], Tayybah Kiren[2], Hannan Bin Liaqat[3], Shahid Naseem[3] and Atif Saeed[4]

[1]College of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an, Shaanxi, 710054, China
[2]Department of Computer Science (RCET Campus), University of Engineering and Technology, Lahore, 39161, Pakistan
[3]Department of Information Sciences, Division of Science & Technology, University of Education, Lahore, 54700, Pakistan
[4]Department of Computer Science, COMSATS University, Islamabad, Lahore, 54700, Pakistan
*Corresponding Author: Muhammad Usman Sana. Email: m.usman@uog.edu.pk

Received: 16 September 2022; Accepted: 06 January 2023

Abstract: Cloud computing is a technology that provides secure storage space for the customer's massive data and gives them the facility to retrieve and transmit their data efficiently through a secure network in which encryption and decryption algorithms are being deployed. In cloud computation, data processing, storage, and transmission can be done through laptops and mobile devices. Data Storing in cloud facilities is expanding each day and data is the most significant asset of clients. The important concern with the transmission of information to the cloud is security because there is no perceivability of the client's data. They have to be dependent on cloud service providers for assurance of the platform's security. Data security and privacy issues reduce the progression of cloud computing and add complexity. Nowadays; most of the data that is stored on cloud servers is in the form of images and photographs, which is a very confidential form of data that requires secured transmission. In this research work, a public key cryptosystem is being implemented to store, retrieve and transmit information in cloud computation through a modified Rivest-Shamir-Adleman (RSA) algorithm for the encryption and decryption of data. The implementation of a modified RSA algorithm results guaranteed the security of data in the cloud environment. To enhance the user data security level, a neural network is used for user authentication and recognition. Moreover; the proposed technique develops the performance of detection as a loss function of the bounding box. The Faster Region-Based Convolutional Neural Network (Faster R-CNN) gets trained on images to identify authorized users with an accuracy of 99.9% on training.

Keywords: Cloud computing; data security; RSA algorithm; Faster R-CNN

1 Introduction

Nowadays, cloud computing is the most rapidly growing technology. It has tremendous advantages as it is faster in processing data, consumes less power, is low in cost, and has ample storage capacity. But despite these advantages, cloud computing faces some challenges regarding user security and privacy. An essential aspect of improving the quality of service is the security of data in cloud computing from cloud service providers [1]. Cloud computing is efficient, more reliable, and easy to use. It provides ample storage to their customers to save their data without having any virus threat. It also provides secure data transmission between different equipment [2]. The availability, confidentiality, and data integrity are significant security concerns associated with cloud computing. Therefore; for the confidentiality of the data, non-repudiation, authorization, and authentication of people who use the data are very important so that the unapproved parties are not able to get or see any confidential data. Preserving data accurately and controlling the network devices and data from legal access is vital to keep the data integrity and to ensure valid and absolute information. Availability of data is a big issue as it is stored in different locations in the cloud. The data availability whenever a client requests and the guarantee of data being available is vital. In the public model of the cloud, authentication is required when the client retrieves their specific data. Authorization is needed to find out whether a particular individual has the authority or not to perform an action on others' data. Non-repudiation; is required to verify that a reliable person cannot withdraw after performing a job [3].

A lot of organizations adopted cloud computing, and hence as a consequence of loads of digital resources, security dilemmas are rising [4,5]. It is predictable recently that security in cloud computing has become a considerable research focus [6–8]. Since the data is susceptible to intruder attacks, the key concern to the consumers is to find a secure cloud platform [9,10].

Numerous solutions have been provided by researchers, and several researchers are still working on them to find out more accurate and efficient solutions. The main objective of this research is to look for a solution by applying the cryptographic technique for achieving data security in the cloud environment. Cryptography is one of the main approaches for the confidential transmission and storage of data in the presence of a third party. Keeping information or data protected by changing the raw data into a configuration that is not easily readable is the technique of cryptography [11]. Algorithms of cryptography with essential management techniques are particularly hopeful methods to achieve security and privacy in cloud computing [12,13]. When transferred and stored, data must be encrypted constantly. If properly implemented this approach, data will never be easily understandable even if a different occupier can access the data. To keep non-repudiation and authentication from unauthorized persons, data integrity and confidentiality are the foremost necessities of cryptography.

The concept of cryptography is centered on two standard terms: encryption and decryption. The process of conversion of data recognized using plain text aimed at an unreadable configuration, identified as ciphertext, is encryption. Ciphertext cannot be understood by unauthorized persons. Converting data again into its previous form or making the understanding of encrypted information so it can be understood or read by authorized persons is termed decryption [14,15]. For information security, there are numerous encryption algorithms extensively employed. For example, Amazon Simple Storage Service (Amazon S3), 256-bit Advanced Encryption Standard (AES) is one of the most capable encryption algorithms. There are three types of cryptography algorithms: symmetric algorithms, hashing, and asymmetric algorithms. Symmetric key cryptography is also known as the "Secret Key Encryption Algorithm" for encoding and decoding the private key [16].

In asymmetric key cryptography, symmetric for encoding and decoding, double exclusive keys are applied. The public key on the network is available to anyone. To encode data, the public key gets employed. Data can only be decoded by the only private key. In keeping data secure, the private key is set aside secret. The benefit of applying asymmetric key encryption is that it offers an improved distribution of scalability and key compared to symmetric systems. Some standard Asymmetric Key

Algorithms are Diffie-Hellman, Elliptic Curve Cryptography (ECC), El Gamal, Digital Signature Algorithm (DSA), and RSA: 1, one of the initial asymmetric cryptosystems RSA. In the cryptosystem, RSA is still the most used and employed. It is named after the three researchers who made this system Ron Rivest, Len Adleman, and Adi Shamir. It includes two keys, a private and a public key. Information twisted with a public key can get translated only, with a private key. With its private key engraving, a separate message, that's recognized as a digital signature in this verification procedure. The server represents the authentication of the public key. Afterward that using the public key server verifies then the digital signature is returned to the user [17].

Kumar et al. [18] proposed an efficient technique in a virtual environment related to the storage of cloud data focusing on problems and suggested techniques by using a public key cryptosystem to offer data security and storage in the cloud by using the modified RSA algorithm concept to offer improved security in the cloud for data storage.

In terms of storage as well as computational complexities and solving these complexities in clouds. Ambika et al. [19] proposed the SKT-RSA technique based on the Secure Key Transmission (SKT). There proposed technique is a distribution scheme of cluster keys that is tree based. And they also proposed the distribution of keys between the end user and certified authority. Gupta et al. [20] study proposed RSA and Blowfish as two individual cryptographic calculations and examined the effect on speed and security, how they work, and when these two algorithms combine to form one hybrid algorithm after suitable modification. In terms of encryption and decryption time, their study presented a comparative analysis of hybrid algorithms and individual algorithms. Dhamodaran et al. [21] modified RSA, as on large blocks, RSA is largely byte-parallel and is computationally intensive. In a distributed environment System will perform parallel the encoding and decoding process and in terms of execution time, the performance analysis confirms progress and maintains security.

In the cloud, to resolve the confidentiality trouble in transmitting sensitive data, the n-RSA encryption algorithm for a multi-level security model is proposed [22]. A security valuation is conducted by the power cloud security center of the data to decide the security level. According to the security level of the data, then, for the n-RSA algorithm, select the suitable prime number. A proposed method for power clouds is investigated with advantages and disadvantages. The safe transmission of power cloud data is shown in experimental results, and the proposed method can efficiently develop flexibility and security. For securing the cloud, [23] proposed an innovative algorithm combining the RSA algorithm and Ciphertext Policy-Identity Attribute-Based Encryption (CP-IDABE). The performance of the RSA-CP-IDABE algorithm for varying data sizes based on the time it takes for encryption, decryption, and execution is evaluated. Matched with the existing algorithms, the results achieved by the proposed method show higher efficiency.

Seth et al. [24] proposed an integrating encryption technique in the cloud for secure data storage. The proposed method ensures secure and safe data transmission in the cloud using different data fragmentation techniques and double encryption methods. Jiang et al. [25] proposed a model by using Faster R-CNN for the detection of faces. By using a dataset of WIDER face, they train a face detection model in Faster R-CNN, and proposed a model of face detection in another work that is centered on the evolutionary Haar filter [26] set. There are 159,424 faces and 12,880 images in training. They described experimented images of the WIDER dataset. By using deep learning, the authors presented a new face detection system, and attain advanced recognition performance on the benchmark evaluation by a distinguished Face Detection Data Set and Benchmark (FDDB). Specifically, Sun et al. [27]

developed the modern Faster R-CNN system by uniting several approaches, including model pre-training, hard negative mining, feature concatenation, proper calibration of key parameters, and multi-scale training. Consequently, the suggested scheme gained advanced face detection performance, and with regards to Receiver Operating Characteristic (ROC) curves on the FDDB benchmark evaluation, was graded as one of the best models.

Based on Faster R-CNN, Wu et al. [28] proposed a Different Scale Face Detector (DSFD), the novel network, while performing a Faster R-CNN in real-time, can advance the accuracy of face detection. A multi-task effective region proposal network joined to attain the human face Region of Interest (ROI), Region Proposal Network (RPN) with improving face detection is developed. An anchor is consistently formed on the top feature while setting the ROI as a limit, mapped by the multi-task RPN. And the anchor shared with the facial signs is mined with a human face scheme. The authors proposed a Fast R-CNN network, which is parallel-type. The schemes are allotted to three parallel Fast R-CNN networks according to the different percentages of the images they cover. A range of approaches is presented in the face detection network, comprising feature concatenation, feature pyramid, and multi-task learning. Related to advanced face detection approaches, for example, HyperFace, UnitBox, and FastCNN, on standard benchmarks comprising Annotated Faces in the Wild (AFW), FDDB, WIDER FACE, and PASCAL face, the proposed DSFD technique attains good performance.

Faster R-CNN, in object detection applications, is a common technique. Based on Faster R-CNN, an improved model Face R-CNN is proposed in which a facial feature enhancement technique related to the attention process is used. Syntax-guided network (SG-NET) combined with Face R-CNN to unite the produced image with the unique convolutional features that in the feature map improve the concentration on the area of the face and in the case of large-scale obstruction, can efficiently attain face detection. Through the analysis by testing and training Face R-CNN on the dataset of Wider Face, the experimental results show that the improved model has a further noticeable recognition outcome on blocking faces, and is greater than the Faster R-CNN accuracy rate average is 3.5% [29].

To recognize candidate face frames that are to be detected with partial occlusion. The Non-Maximum Suppression (NMS) technique based on Faster R-CNN practices a strict threshold. In multifaceted scenes with fractional obstruction of the face and irregular lighting, the occurrence of mislaid and incorrect face detection is likely to happen. To solve this issue, Yan et al. [30] suggested a novel face detection technique through CNN to extract facial features, and the Region Proposal Network (RPN) detected and generated a considerable amount of face candidate frames; by linear weighting technique, the hard threshold of NMS is enhanced, and by the linearly weighted NMS face candidate frame is selected. On the FDDB dataset, comparison experiment results show, the newly proposed face detection method has high detection robustness, and accuracy, and under partial occlusion and uneven lighting, can efficiently avoid missed detection and wrong detection of abundant faces.

In cloud infrastructure, when a user sends the data, it is first transferred to the cloud server side, and after encryption, data is sent to the receiver. Data owners have no access or control over the data once they send it, and can’t monitor and check the security status. All the problems related to user data security are handled or controlled at the cloud server. Data-centric security is an approach in which users have the authority to control data and check the security aspects when the data is at the server end. The driving force behind modifying the RSA in the proposed research is the secured and safe transmission of data through a secured transmission of key. Also, the appropriate authentication technique is required as this is missing in previous research. In previous research for encryption and decryption, RSA Algorithm is used, in which the N key is the product of two prime numbers which can be identified, and someone can easily hack the entire system without any difficulty by knowing the private key.

The main objectives of this research are:

- To enhance the security level of data that is stored on the cloud server.
- To develop a more advanced algorithm for encryption and decryption.
- A face recognition method based on Faster R-CNN was suggested to ensure that only the authorized person can access the keys.

2 Proposed Methodology

2.1 RSA Algorithm

Three famous mathematicians discovered the RSA algorithm for data encryption and decryption named, Ronald Rivest, Adi Shamir, and Leonard Adleman in, 1978. How efficiently an RSA algorithm works to secure the user data relies on the complexity of the mathematical function, the more complex the function means that it is difficult to guess or solve by any other person. To give access authorized users to send or receive information via the cloud RSA Algorithm is being implemented and through this technique, data is not retrieved by any attacker or authorized person. When a user saves their data on the cloud, it first gets encrypted, and then saved on the cloud. When the user requires data that is being stored on a cloud, first, it sends a request for data retrieval to the cloud provider, and then after proper identification and authorization of user data is sent to the specified user. In the RSA algorithm, each message is converted into integers. RSA works on public and private keys. A private Key is only familiar to the authorized user and it is used to decrypt the data which is first encrypted by the cloud provider.

The whole process consists of three steps which are:

1. Key Generation:

Calculate the product of any two random numbers as

$v = a \times b$

Euler function

$\varphi\,(n) = (a - 1)\,(b - 1)$

Now take any number named e to estimate $(e, \varphi\,(v)) = 1$, and $1 < e < \varphi(n)$.

$d = e\,(-1)\ mod\varphi\,(n)$

$\varphi(v)$ multiplication inverse is named d, which also satisfies the following equation.

$e \times d = 1\,mod\varphi(v)$

The keys (*E, n*) are public, while the keys (*D, n*) are private.

2. Encryption

M information is encrypted by the correspondent by using the following equation where C is encrypted ciphertext.

$C = Memod\,(n)$

3. Decryption

Cipher C has been decrypted by the receiver, who receives the information.

$M = Cdmod\,(n)$

RSA Algorithm is the most popular algorithm for the encryption and decryption of data in a more secure way. RSA helps in the identification of service providers and authentication over insecure mediums of communication, and it's challenging to hack the system and retrieve other persons' information. RSA encryption cracking is as challenging as huge numbers factoring [31,32]. The RSA algorithm comprises three steps:

1. To generate a public and private key
2. Encryption
3. Decryption

Two prime numbers, modular multiplicative inverses that are generated randomly, are selected as w and x.

Calculate $n = w * x$

Calculate $f\,(n) = (w - 1)(x - 1)$

Choose number e, $e < f\,(n)$.

Calculate D, such that $module1\ (modf\,(n))$ and $e < f\,(n)$.

Private key $= \{D, n\}$

Public key $= \{E, n\}$

Cipher text $C =$ message E mod n

Plain text $P =$ cipher text D mod n

We divide the platform into three steps

1. Public key1 + plaintext → ciphertext1
2. Public key2 + ciphertext1 → ciphertext 2
3. Private key + ciphertext1 → plain text

2.2 Modified RSA Algorithm

We propose a modified RSA Algorithm in which it is not easy to crack the system and get access to other users' private data. Previously for encryption and decryption, RSA Algorithm is used, and the N key, is the product of two prime numbers which can effortlessly be identified, and someone can easily hack the entire system by knowing the private key.

The following are the steps of a modified RSA System.

1. $n1 = p \times q$
2. $n2 = r \times s$
3. $N = n1 * n2$
4. $\varphi(N) = (p - 1) * (q - 1) * (r - 1) * (s - 1)$
5. $E = E1 * E2$
6. After the calculation of E, we get two encryptions and one decryption key by just dividing the key by $E1$ and $E2$.

Fig. 1 presents a flow chart demonstration of the improved RSA algorithm. To calculate n and *mod* $\varphi(N)$ four different prime numbers $p^*q^*r^*s$ are taken as the input of the random number (a, b) is carefully chosen from the range $1 < e < f\varphi(n)$ as the exponent of the public key. To utilize as the exponent of the private key multiplicative inverse modularity of the random numbers (w, x) is considered. Encryption and decryption are completed using those exponents of the public and private keys.

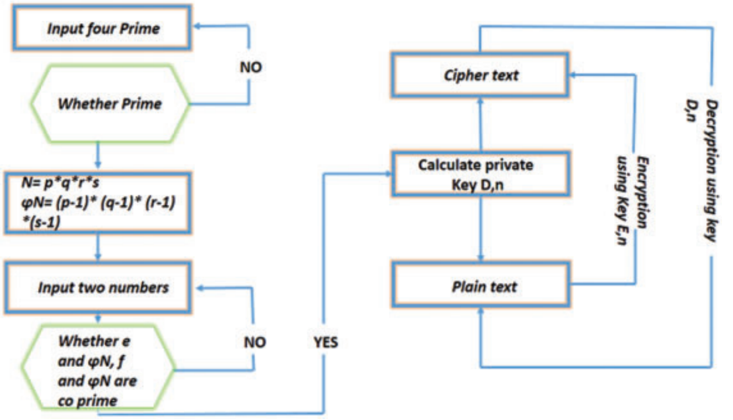


Figure 1: Flow chart demonstration of modified RSA algorithm

3 Results and Discussion

In the modified RSA model, instead of two prime numbers, we have used four that are p, q, r, and s. E, f, and N are used to generate a public key where f is chosen randomly, and D, g, and N are used to generate the private key in which g is randomly generated. In the previous RSA algorithm as N is the most complex number, and in this proposed model, if a person (hacker) knows the N value, then they cannot trace the private key and public key because he cannot estimate the values of four prime numbers [33–36]. RSA keys are usually 1024 or 2048 bits long. However, researchers consider that against all attacks, 1024-bit keys are no longer wholly protected. That is why the minimum key length of 2048 bits are used by some industries and the government.

Key size: 2048. Prime number *p, q, r, s* secret keys are given below.

P: J6NnsfaTBJoNcTE9MgyYssdAeuJI8oUjPgBWMS81w5jl/lqvqJLJcXF85zWha2RTllCsTnC9
U4E4Ut/NokJRJBxx0D+YbF2JbhdwcBAhk9LeVn1aXLgPeKT247tIJo+EtHuaOm+hovqKT
bbuxSsutZVBXQ4/F/bBQIs+gTlyxvqzUwGsngFodRRTC+kA+DbH3zL1+IU2pjkfWi0o4Hv
my6/mKsdgK8Pk5SudGkk+kQkVOA9/Z9RqXlxJlQLHnvQkPMsFqadhH5hlWgZx+VdJoO5
KqxIzSvXi54d3LtUI5rt2Xqv0Kqp+JoOlj7zP1DfMjX6EZGRvod36Us/+zrfK+g==.

Q: b4lOQvVlOJids16GO6HEV7fvRFAfxy62hs3A134h1eOC4uqPIzxXvdGLbhVxgjGVtn24QN
14/aGeFiMoJR3ds0u+07Zscxu8o9m3ZVRjqRsH4efm0Zci7oGz17yAXez1iY2AFpkPXZiZo/
WitNpwXY3VI7BmjNxaTG4+x+UOXhVSUvMnfaquIlwT62SYwxSXRe80gKbEV0Fs8M3+
UmVGQnoERuux+93XM9UI7+ZCfchQMhgjS1D2/cOl9alczDBipztL81jughU9OvSVl3LbpJ
MOdSXQfdWs4n1sfuPjncb9VqrmG3P5rgGZmoKAwltuIWjoqY59IH8EOfViivBXOw==.

R: NpM1vC4NZokOJSeNkvdlhyGhfkpak7v1nYWan6/P6U+iAK/fLXKBY25pk9T54pLqUF7
FNk/igHwjVtnNfPGXCGpIo6nAPrAC+gWEwui5r0vuUesEddAsh+0Ab+YqnVjci51Ew+FP
Bl+oNhf7t70N8DtoRvG1D2MP9ekP0KsoiUXGlqsRHsuvEPz7177FedVS/HFKdakwJGrWpT
xY1btn7VoWsDsGZHo3YdPEJVI+YYFzpD/acwzkOAXqYWIgDrqTjU3WznGii9kcw4nmsE
hGuq4ndaLBYB4WOOnnlvEOSthz4b446WzwZQc3hQHXwphyi7vM3OKUVu+EU4Tyz/X1A
Q==.
S: c4wWaEhdA1Qei+fizmE6+cew/45Xqc0ScBDHUAVnjKMygG7plT69aJt/1Jw6z4AhpSL89F
pFG82PoRN6vTradQcse93yj64Byl5EMLGNac/hdXVpSbkKeLoJdF83Qvfuq+PJbIUhvMGLT
LC/kDt0Mq0eRLGt/Ze6nbe0oiulAeUHzqBJcYoiroXFgjBiZJy++2Ga/KSf9RdbkqHXFFYXi
mfkVOaVMK3ccG2Ggkaz+lpoHGWuV1ffISJ0GfuV5HuFS+df+Qrhf5RDN3VILwcJ4lgH6T
oaZpZqM1JytP4MrsdtdB/ppFE/Ejn8dvrCAihkKMjf8hvkI7QBEAKP6Nlvag==.

Table 1 presents the proposed key size as 2048 and time needed for encryption is 0.331, and the time required for decryption is 0.321 compared to other key sizes previously used. The function φ (n) analyzes the number of elements in the specified dataset. Similarly, key sizes 2048 and 1024 with the same number of elements show less.

Table 1: Encryption and decryption time for different key sizes as compared to the proposed key

Key size (bits)	Number of elements	Encryption time (ms)	Decryption time (ms)
2048 (proposed)	512	0.331	0.321
2048	512	0.476	0.11
1024	512	0.66	0.7
1024	128	0.0078	0.0076

In Fig. 2 the comparison of encryption and decryption time of the proposed modified RSA the RSA previously used is given. The results recognized that to maintain equilibrium between security and speed, the optimal or best key size is 2048 bits as compared to the remaining key size values, and it is visible that the time required for encrypting or decrypting is improved than the previous RSA models with a similar number of elements. Allowing factorization of 1024 and 2048-bit keys exploit likely because of poor entropy presented by a usual mathematical arrangement of the prime factors that also result in the revealing of keys with this usual structure.

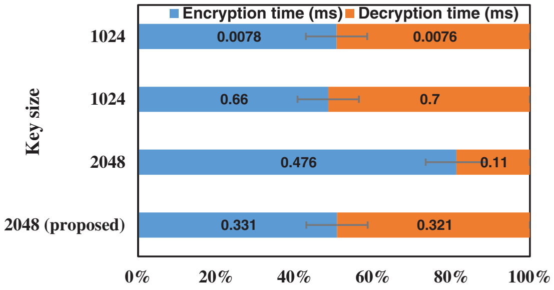


Figure 2: Comparison of proposed RSA key size encryption and decryption time with previous RSA

4 Region-Based Convolutional Neural Network

For more security of data, a trained neural network is implemented to first recognize the person by capturing their image through the camera and then to identify whether it is an authorized person or not by comparing their image with the images placed in the neural network database.

4.1 *Faster R-CNN for Face Detection*

For face recognition, we have implemented Faster R-CNN for the recognition and identification of users or clients to ensure that only the authorized person will be able to retrieve or send data through a cloud environment, as shown in Fig. 3 Faster R-CNN has two main elements [37–39]. The first one is an RPN that is a fully connected network, generating regional proposals that are additionally used as input. The second one is a Fast R-CNN detector which classifies every ROI [40]. As an input, the features of an image are taken from an RPN that produces rectangular object proposals in the form of a set, and each proposal has the object's score. To create region proposals directly in the network, the Faster R-CNN indicator enhances an RPN. The RPN utilizes anchor boxes for the detection of the object. In the network, making regional proposals are better and faster in regulating the data.

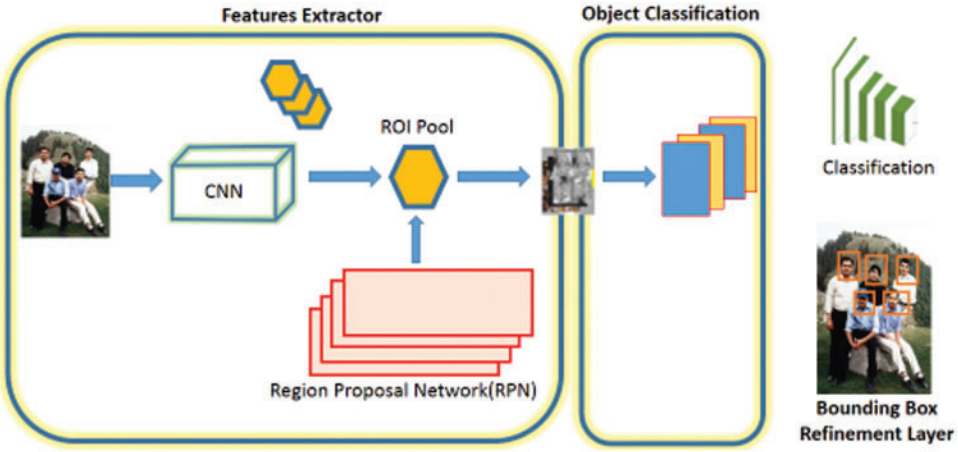


Figure 3: For object classification and detection framework of Faster R-CNN

In the RPN structure, from the convulsion layer, the input of RPN is a feature map. There are two data flows, the upper flow categorizes the boxes with negative or positive labels, and the lower flow analyses the compensation of regression in the bounding box. At that time, both of the flows combined with a fully connected layer to produce and filter appropriate proposals. To produce region proposals, we mapped a tiny sliding window that is the output of the recent pooled convolution layer on the map of convolution features. For a Faster R-CNN detector, a set of regional proposals is provided as input. Every proposal is distributed and provided a feature map of fixed dimension among an ROI pooling layer and, mapped these features into a vector feature by Fully Connected Layers (FCLs). In the classification process, these vector features are the inputs of the box classification layer (CLs) and box regression layer (Reg). In the Faster R-CNN model, the softmax classifier is used.

4.2 Extraction Features

The main part of Faster R-CNN that is presented is extracted. For this difficulty, deep features are used. To extract the features, Visual Geometry Group (VGG) 16 architecture is used to train a net dataset on an image. For human feature detection, a Faster R-CNN is used, as shown in Fig. 4.

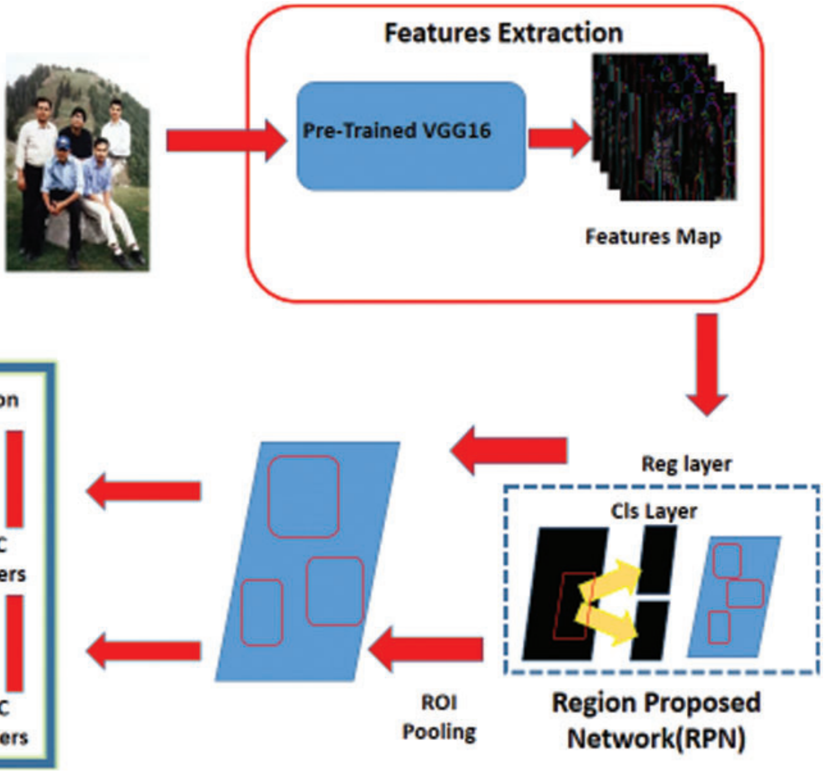


Figure 4: Faster R-CNN for feature extraction

The network architecture of VGG16 layers is described below in Fig. 5. VGG16 network has three fully connected layers and 15 convolution layers. At the end of the network, one softmax layer is present. Sixty-four (64) filters are present in the first two layers of convolutions, 128 filters have been used in the 3rd, and 4th layers of convoluted, 256 filters have been used for 5th, and 6th layers of convolution, and 512 filters have been used in the last five convolutions layers. Three layers that are fully connected have 4096, 4096, and 2622 neurons correspondingly. Maximum pooling of 2 × 2 is practical in every block.

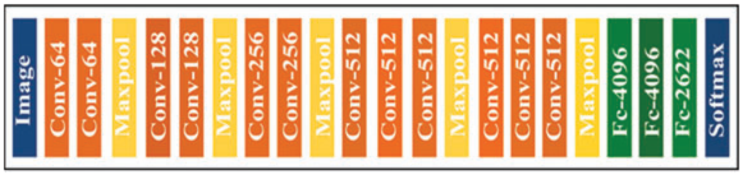


Figure 5: VGG16 Network architecture

4.3 *Region of Interest Pooling*

The regions have uninformed sizes proposed by the RPN. An ROI pooling layer is used to make them constant, which receives the regions projected by the RPN, and other confrontations make them of a similar size. ROI pooling layer sends the proposal to the following fully connected layer after pooling them into the same size if their size is different for the classification of face and regression of position adjustment. In short, the key goal of ROI pooling is to provide fully connected layers to the fixed-length output. The ROI pooling functionality is enlightened in Fig. 6.

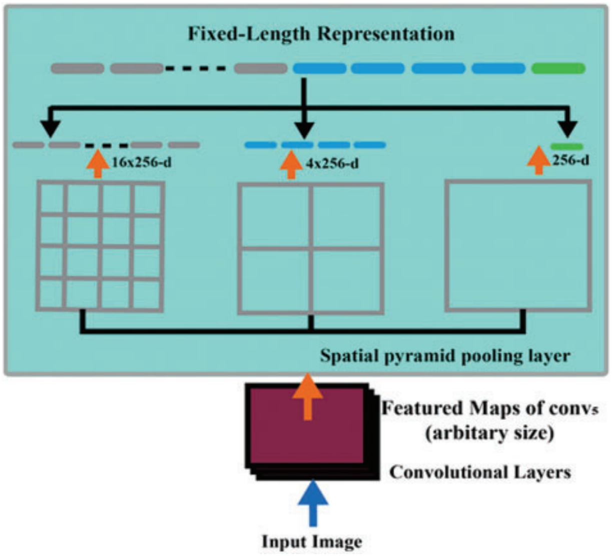


Figure 6: ROI pooling module of Faster R-CNN for face detection and feature extraction

4.4 *Classification and Bounding Box Regressor*

The key determination of a bounding box Regressor is to advance once the object has been classified and managed for the bounding box through support vector machine SVM or softmax classifier. Whether or not the object does not correctly fit inside a bounding box that is generated, through the classifier adjusts the four offset values of the bounding box at that time the bounding box regressor is employed to adjust that object accurately within a created bounding box. For classification, commonly, Softmax and Support Vector Machine (SVM) is applied to detect and classify multiple objects within an image using the bounding box, and Faster R-CNN represents high accuracy results. ROI pooling is used by the fully connected layers, and the permanent length of the output is formed. In fully connected layers, there are two pipelines. The first one is to predict the class present in the ROI box of the object, and the other one is to predict the object's region of interest.

$$\text{Classification Layer Loss} = \text{Bounding Box Regressor Loss} + \text{Classification Loss}$$

The recognition flow is shown in Fig. 6. Though the complete recognition procedure remains unaffected, based on R-CNN the subsequent developments have been made: 1) To unite the images into the fixed size, it is no longer required by capturing and standardizing processes before, in an attempt to resolve the trouble of image misrepresentation and the loss of information initiated by regularization processes; 2) Utilizing spatial pyramid pooling layer substitute the pooling layer of the preceding convolution layer. Thus, spatial pyramid pooling has the following benefits: 1) Spatial pyramid pooling progression images of arbitrary aspect ratio, by significant scalable pooling layer, and arbitrary scale, make fixed size output, and through multi-scale enhance the robustness of the extracted features; 2) The recurrent counting of convolution layer is effectually resolved and overall efficiency is improved Since directly from the complete feature mapping the features of entire nominee regions are extracted.

In a pre-trained network, the convolution layers in the RPN are tracked by a 3 × 3 CNN layer. This communicates in the input image to map a receptive field or large spatial window (e.g., 228 × 228 for VGG16) at a center stride vector to a low-dimensional feature (e.g., 16 for VGG16). For regression and classification branches, two 1 × 1 convolutional layers are at that time included in all spatial windows. To distribute with altered scales and aspect ratios of objects, the RPN anchors are presented. We devise to look out of the RPN modules as they share convolutional layers for the complete arrangement. In the convolutional maps, an anchor is on every descending location in the middle of every spatial window. Every anchor is related to an aspect ratio and with a scale. After the default situation, we utilize three aspect ratios (1:1, 1:2, and 2:1) and three scales (256-d, $4 * 256$d, and $16 * 256$d pixels) and, at every location leading to $k = 9$ anchors. Compared to an anchor, every proposal is parameterized. Thus, we have at maximum conceivable offers for a map size of the convolutional feature. The similar features of every sliding location are utilized to regress k proposals, as an alternative of extracting training, a single regressor, sets of features, and using Stochastic Gradient Descent (SGD) training of the RPN must be completed in an end-to-end approach for both regression and classification purpose.

4.5 Training of the Model

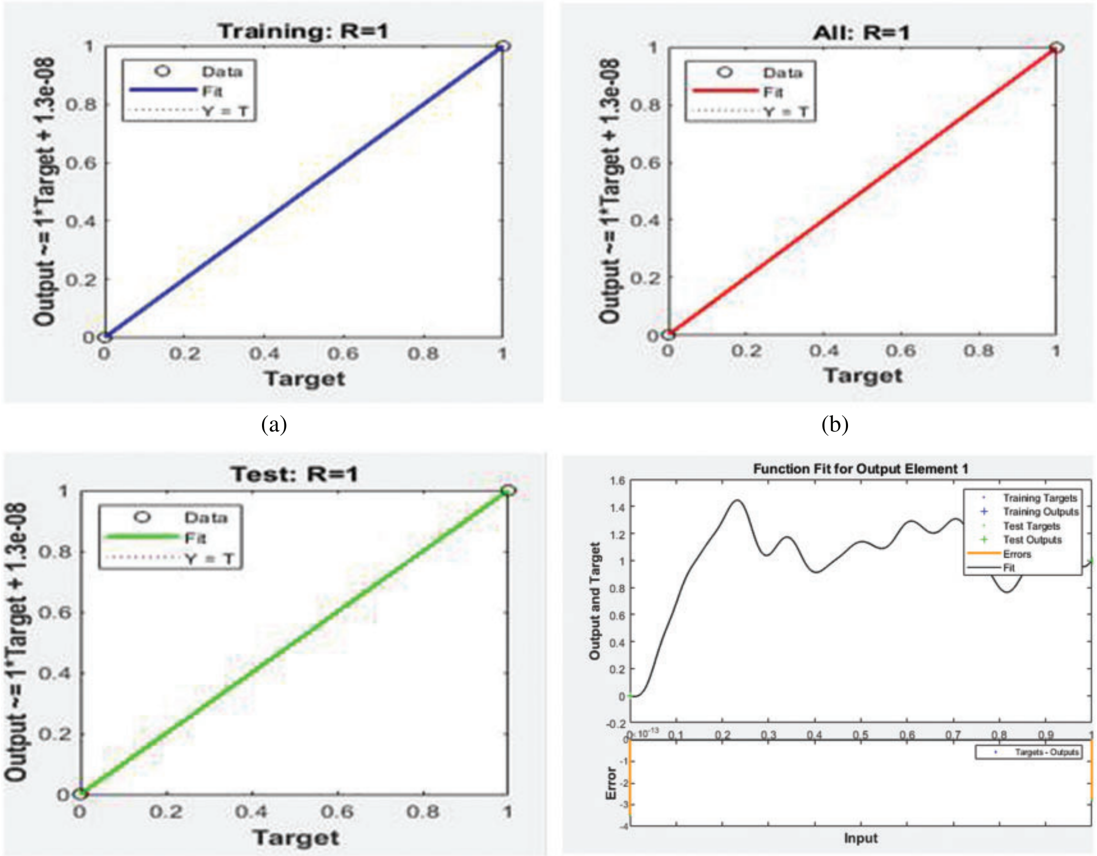
We take an image base dataset from https://www.kaggle.com/dataturks/face-detection-in-images and generate results in MATLAB of how accurate results or matching occurs for user data when a client wants to access data by face recognition method. The proposed model hyperparameters with values are shown in Table 2.

Table 2: Hyperparameters of the model

Hyperparameters	Value/Name
Batch sizes	1
Max_Proposals	300
Localization_loss_weight	1.0
Momentum optimizer value	0.9
Max eval	10
Kernal_size	2
Score_Converter	Softmax
Learning rate	0.0002
NUM-steps	60000
Num_examples	899
PSNR	35–40
Loss function	MSE

For the duration of the training, the total loss begins at 2.413 and then progressively declines as the number of training steps rises at 50–60 k steps, ending in a loss of 0.390–0.104. For regression, the commonly used loss function is in Mean Squared Error (MSE). The squared changes between predicted and true values are the loss in the mean managed data. MSE is complex to outliers and specified instances with similar input feature standards, and their mean target value is optimal prediction. Peak Signal-to-Noise Ratio (PSNR) calculates in decibels between two images. This ratio is utilized as a measurement of quality between the compressed and the original image, which improved the feature of the compressed image that developed the PSNR. The PSNR and MSE are utilized to compare the quality of compression of the image PSNR signify the amount of the peak error. The lower the value of MSE, the lower the error.

The batch size is one, and the learning rate is in the range of 0.002 to 0.0002, as shown in Figs. 7a–7c. Fig. 7d shows the performance evaluation of the dataset by training on the proposed neural network. For learning the algorithm, Stochastic Gradient Descent is used. To complete the Linux Ubuntu, the training acquired 5 h and 55 min on 16.04 virtual machines.



(a)

(b)

(c)

(d)

Figure 7: Result of the dataset using neural network on cloud (a) Validation result (b) Training plot result (c) Training evolution result (d) Performance evaluation result

As shown in Fig. 8, on the training dataset, the Faster R-CNN model fits 99%. We are assured from the result of training that the proposed model in the testing dataset would fit above 90%.

The significant aspects of the proposed Faster R-CNN, compared to previous techniques are shown in Table 3.

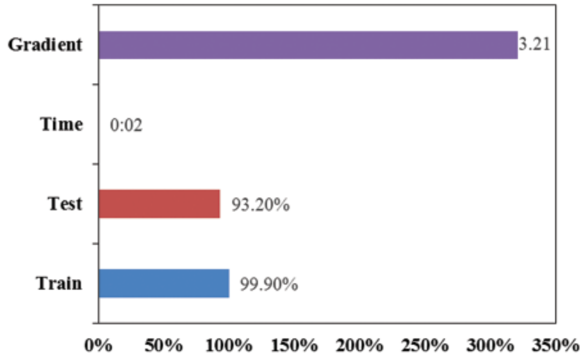


Figure 8: Training and testing accuracy

Table 3: The distinctive characterization comparison of CNN object detectors with proposed Faster R-CNN

Detector	Accuracy in training	Per image prediction time	Description
CNN [41]	99.6	_	It faces high computations as it predicts numerous regions
R-CNN [42]	99%	40–50 s	Slow detection process, although less time is required for training
Fast R-CNN [43]	98.5%	2 s	Allow adapted region proposals
Proposed faster R-CNN	99.9%	0.02 s	Do not allow adapted region proposals. Near to real-time detection performance

5 Conclusion

RSA Algorithm plays a vital role to secure and save data and information efficiently in a sustainable cloud environment. It's a modern, and well-developed method to secure medical data. The RSA Algorithm method works far better than other data security algorithms. In our technique, we use a neural network for user identification and authentication and after the user, proper recognition RSA algorithm technique is implemented for data transmission and retrieval. RSA protects, unauthorized users, and if the attacker intentionally or willingly gets access to cloud data, it does not have the authority to decrypt it and extract information from it. Data protection in the cloud depends on how strong and efficient its encryption and decryption technique is.

This modified version of the RSA Algorithm is far better than the previously implemented RSA Algorithm for secure data storage and transmission. Only the authorized user has the authority to retrieve or get information from the cloud, and if someone hacked the system, then they cannot decrypt the data. Through the implementation of a modified RSA algorithm, we claim and guarantee the security of data in the cloud environment. For more security, we also implemented a trained neural network for person recognition. The Faster R-CNN gets trained on images to identify authorized users with an accuracy of 99.9% on training and 93% on testing. Future research focuses on the implementation of the RSA cryptography algorithm efficiently and reliably with Artificial Neural Network (ANN) technique. Additionally, improve the accuracy of training with low-resolution images in face detection.

Funding Statement: This work is supported by the Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2019JM-348).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. E. Kafhali, I. E. Meir and M. Hanini, “Security threats, defense mechanisms, challenges, and future directions in cloud computing,” *Archives of Computational Methods in Engineering*, vol. 29, no. 1, pp. 223–246, 2022.

[2] S. Shahrin, A. Rosli, M. H. J. A. Hadi and H. Awang, “A theoretical framework of the secure environment of virtual reality application in tertiary tvet education using blockchain technology,” *Journal of Contemporary Social Science and Education Studies*, vol. 1, no. 1, pp. 39–46, 2021.

[3] M. N. Birje, P. S. Challagidad, R. Goudar and M. T. Tapale, “Cloud computing review: Concepts, technology, challenges and security,” *International Journal of Cloud Computing*, vol. 6, no. 1, pp. 32–57, 2017.

[4] P. Srivastava and R. Khan, “A review paper on cloud computing,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 6, pp. 17–20, 2018.

[5] I. M. Khalil, A. Khreishah and M. Azeem, “Cloud computing security: A survey,” *Computers*, vol. 3, no. 1, pp. 1–35, 2014.

[6] K. -K. R. Choo, J. D. Ferrer and L. Zhang, “Cloud cryptography: Theory, practice and future research directions,” *Future Generation Computer System*, vol. 62, no. C, pp. 51–53, 2016.

[7] P. Samarati, S. D. C. D. Vimercati, S. Murugesan and I. Bojanova, *Cloud Security: Issues and Concerns*. Chichester, England: John Wiley & Sons, pp. 1–14, 2016.

[8] M. U. Sana and Z. Li, “Efficiency aware scheduling techniques in cloud computing: A descriptive literature review,” *PeerJ Computer Science*, vol. 7, no. 24, pp. e509, 2021.

[9] H. Wang, S. Wu, M. Chen and W. Wang, “Security protection between users and the mobile media cloud,” *IEEE Communications Magazine*, vol. 52, no. 3, pp. 73–79, 2014.

[10] K. Hashizume, D. G. Rosado, E. F. Medina and E. B. Fernandez, “An analysis of security issues for cloud computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013.

[11] D. R. Stinson and M. B. Paterson, *Cryptography: Theory and Practice*, 4th ed., NewYork, USA: Chapman and Hall/CRC Press, pp. 1–14, 2018.

[12] M. K. Neha, “Enhanced security using a hybrid encryption algorithm,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 7, pp. 13001–13007, 2016.

[13] N. Chintawar, S. Gajare, S. Fatak, S. Shinde and G. Virkar, “Enhancing cloud data security using elliptic curve cryptography,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 3, pp. 1–4, 2016.

[14] B. Qin, H. Wang, Q. Wu, J. Liu and J. Domingo-Ferrer, “Simultaneous authentication and secrecy in identity-based data upload to cloud,” *Cluster Computing*, vol. 16, no. 4, pp. 845–859, 2013.

[15] M. U. Sana, Z. Li, F. Javaid, H. B. Liaqat and M. U. Ali, “Enhanced security in cloud computing using neural network and encryption,” *IEEE Access*, vol. 9, pp. 145785–145799, 2021.

[16] H. Delfs and H. Knebl, “Symmetric-key cryptography,” in *Introduction to Cryptography*, 3rd ed., Berlin, Heidelberg: Springer, pp. 11–48, 2015.

[17] V. Agarwal, A. K. Kaushal and L. Chouhan, "A survey on cloud computing security issues and cryptographic techniques," in *Social Networking and Computational Intelligence*, vol. 100. Singapore: Springer, pp. 119–134, 2020.

[18] Y. K. Kumar and R. M. Shafi, "An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 530, 2020.

[19] S. Ambika, S. Rajakumar and A. Anakath, "A novel RSA algorithm for secured key transmission in a centralized cloud environment," *International Journal of Communication Systems*, vol. 33, no. 5, pp. e4280, 2020.

[20] A. Gupta, S. Gupta and N. Yadav, "Enhancement of security using B-RSA algorithm," in *Inventive Communication and Computational Technologies*, vol. 89. Singapore: Springer, pp. 439–450, 2020.

[21] M. Dhamodaran, E. Punarselvam, S. D. Varshan, P. D. Kumar, C. Saravanan *et al.,* "Security and privacy of sensitive data in cloud computing using RSA," *International Journal of Scientific Research in Science and Technology*, vol. 8, no. 2, pp. 657–661, 2021.

[22] Y. Wang, Q. Ma, L. Li, T. Guan, Y. Geng *et al.,* "An encryption method of power cloud data based on n-RSA," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, vol. 211. Singapore: Springer, pp. 416–423, 2021.

[23] S. Chandel, G. Yang and S. Chakravarty, "RSA-CP-IDABE: A secure framework for multi-user and multi-owner cloud environment," *Information-An International Interdisciplinary Journal*, vol. 11, no. 8, pp. 382, 2020.

[24] B. Seth, S. Dalal, V. Jaglan, D. N. Le, S. Mohan *et al.,* "Integrating encryption techniques for secure data storage in the cloud," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 4, pp. e4108, 2022.

[25] H. Jiang and E. Learned-Miller, "Face detection with the faster R-CNN," in *12th IEEE Int. Conf. on Automatic Face & Gesture Recognition*, Washington, DC, USA, pp. 650–657, 2017.

[26] M. Besnassi, N. Neggaz and A. Benyettou, "Face detection based on evolutionary Haar filter," *Pattern Analysis and Applications*, vol. 23, no. 1, pp. 309–330, 2020.

[27] X. Sun, P. Wu and S. C. Hi, "Face detection using deep learning: An improved faster RCNN approach," *Neurocomputing*, vol. 299, no. 2, pp. 42–50, 2018.

[28] W. Wu, Y. Yin, X. Wang and D. Xu, "Face detection with different scales based on faster R-CNN," *IEEE Transactions on Cybernetics*, vol. 49, no. 11, pp. 4017–4028, 2019.

[29] L. Hai and H. Guo, "Face detection with improved face R-CNN training method," in *3rd Int. Conf. on Control and Computer Vision*, Macau China, pp. 22–25, 2020.

[30] H. Yan, X. Wang, Y. Liu, Y. Zhang and H. Li, "A new face detection method based on faster R-CNN," *Journal of Physics: Conference Series*, vol. 1754, no. 1, pp. 012209, 2021.

[31] A. V. N. Krishna, "A randomized cloud library security environment," in *Cloud Security: Concepts, Methodologies, Tools, and Applications*, Hershey, PA, USA: IGI Global, pp. 1087–1107, 2019.

[32] R. Biswas, S. Bandyopadhyay and A. Banerjee, "A fast implementation of the RSA algorithm using the GNU MP library," in *National Workshop on Cryptography*, IIIT-Calcutta, India, pp. 1–15, 2003.

[33] S. Sharma, P. Sharma and R. S. Dhakar, "RSA algorithm using modified subset sum cryptosystem," in *2nd Int. Conf. on Computer and Communication Technology*, Allahabad (UP), India, pp. 457–461, 2011.

[34] A. Mouse, "Sensitivity of changing the RSA parameters on the complexity and performance of the algorithm," *Journal of Applied Sciences*, vol. 5, no. 1, pp. 60–63, 2005.

[35] M. A. Islam, M. A. Islam, N. Islam and B. Shabnam, "A modified and secured RSA public key cryptosystem based on n prime numbers," *Journal of Computer and Communications*, vol. 6, no. 3, pp. 78–90, 2018.

[36] M. Thangavel, P. Varalakshmi, M. Murrali and K. Nithya, "An enhanced and secured RSA key generation scheme (ESRKGS)," *Journal of Information Security and Applications*, vol. 20, no. 1, pp. 3–10, 2015.

[37] S. Wan and S. Goudas, "Faster R-CNN for multi-class fruit detection using a robotic vision system," *Computer Networks*, vol. 168, no. 12, pp. 107036, 2020.

[38] W. Yang, Z. Li, C. Wang and J. Li, "A multi-task Faster R-CNN method for 3D vehicle detection based on a single image," *Applied Soft Computing*, vol. 95, no. 2, pp. 106533, 2020.

[39] M. Arman, M. Hasan, F. Sadia, A. K. Shakir, K. Sarker *et al.,* "Detection and classification of road damage using R-CNN and faster R-CNN: A deep learning approach," in *Int. Conf. on Cyber Security and Computer Science*, Dhaka, Bangladesh, pp. 730–741, 2020.

[40] Z. Huang, S. Watanabe, Y. Fujita, P. García, Y. Shao *et al.,* "Speaker diarization with region proposal network," in *Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Barcelona, Spain, pp. 6514–6518, 2020.

[41] R. Chauhan, K. K. Ghanshala and R. C. Joshi, "Convolutional neural network (CNN) for image detection and recognition," in *First Int. Conf. on Secure Cyber Computing and Communication (ICSCCC)*, Jalandhar, India, pp. 278–282, 2018.

[42] A. Saranya, K. Kottursamy, A. A. AlZubi and A. K. Bashir, "Analyzing fibrous tissue pattern in fibrous dysplasia bone images using deep R-CNN networks for segmentation," *Soft Computing*, vol. 26, no. 16, pp. 7519–7533, 2022.

[43] S. C. Hsu, C. L. Huang and C. H. Chuang, "Vehicle detection using simplified, fast R-CNN," in *Int. Workshop on Advanced Image Technology (IWAIT)*, Chiang Mai, Thailand, pp. 1–3, 2018.