**IJARCCE** ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12555

# A Method to Achieve Data Security Using RSA Algorithm and Fingerprint

**Ganavi M[1], Suhas S A[2], Chandan Singh[3], Karthik V R[4], Sahana C[5]**

Assistant Prof., Dept. of CS&E, JNNCE, Shivamogga, India[1]

Research Scholar, Dept. of CS&E, JNNCE, Shivamogga, India[2-5]

**Abstract:** In the present world, the data security is the major problem. The data should be secured in such a way that only the sender and the receiver should be able to view the original data. Most of the traditional techniques that are being used today uses the generic functions, random key generators, or algorithms to generate the keys. But the keys generated using the traditional techniques will not be unique to each and every individual. So, the Biometric Cryptosystems can be used to achieve the data security. The Biometrics, such as fingerprints can be used for data security. Since the fingerprints of each and every individual in the world is unique, the keys generated using the fingerprints will be unique. In this work, the fingerprint of the individual is taken as the input to generate the prime numbers using the minutiae points. The generated prime numbers are then given as the input to the RSA algorithm to generate the keys. The generated keys are then used for the encryption and the decryption process**.**

**Keywords:** Fingerprint feature, Minutiae points, RSA algorithm, Cryptography, Data security

## I. INTRODUCTION

Data security refers to the protection of the sensitive information such as personal identification data, medical records, financial information, and other confidential information from the third parties. The data should be secured in such a way that it can be accessed only by the sender and the receiver. In this work, the cryptography based “A method to achieve data security using RSA algorithm and fingerprint” is developed to secure the data from the unauthorized access. Since the biometrics such as fingerprints are unique to each and every individual, the keys generated using the fingerprints will be unique.

## II. RELATED WORKS

Muaad M. Abu-Faraj et al., [1] proposed the method for the comparative analysis of the several fingerprint feature extraction methods such as, K-means Clustering Method, Wavelet Packet Tree Decomposition, LBP Based methods and Fingerprint Minutiae Extraction. According to this paper the Fingerprint Minutiae Extraction and the K-means Clustering Method will provide distinct features for all fingerprint images regardless of the image rotation, but the Wavelet Packet Tree Decomposition and the LBP Based methods are concerned about the image rotations. For the process of fingerprint feature extraction from texture, minutiae points and the frequency spectrum, Yoshinori Koda et al., in [2] have proposed a CNN based method. The minutiae attention module has been introduced in the proposed system to extract the efficient texture features from local areas surrounding the minutiae. For the process of training, the public dataset is used in the proposed system which consists of small number of the fingerprint classes, so the data augmentation technique has been used in the proposed system, which takes into consideration the properties of the fingerprint images and increases the number of fingerprint images during the process of training. For the purpose of fingerprint identification and verification, Samy Bakheet et al., in [3] have proposed an automated minutiae extraction and matching system. The developed framework consists of the several steps, such as, Image Preprocessing, Minutiae Feature Extraction and Minutiae Feature Matching. In the Image Preprocessing step, the quality of the fingerprint image will be improved and the noise present in the image will be removed. The next step is the Minutiae Feature Extraction, in this step the features will be extracted from the improved quality fingerprint image. After the Minutiae Feature Extraction, the next step is the Minutiae Feature matching, in which the feature matching will be performed on the two fingerprint images, namely, test and the template image. A lot of critical data will be shared in the Health Care Systems which need to be secured from the third parties, Sekar M et al., [4] have proposed a technique to improve the efficiency by using the MJ2RSA cryptosystem. In the proposed system, the fingerprint will be taken as the input to generate the prime numbers. The generated prime numbers will be then given as the input to the MJ2RSA cryptography. Since the fingerprints will be unique to each and every individual, the generated keys will be unique. Ranjith Jayapal et al., [5] have proposed a method for increasing the security using the biometrics. In the present world, most of the data will be protected using the passwords, which is not an efficient way to secure the data. In the proposed system, the biometrics will be used to encrypt the messages.

DOI: 10.17148/IJARCCE.2023.12555

In this paper, Veri-Finger 9.0 / MegaMatcher9.0 algorithm is used for the fingerprint minutiae extraction and the matching process. Sayuti Rahman et al., [6] RSA key generator has been developed to generate the keys for the encryption and the decryption process. The fingerprint image will be taken as the input to generate the prime numbers and the generated prime numbers will be given as the input to the RSA algorithm to the generate the public and the private keys, which can be used for the encryption and the decryption of the text message. Sayani Chandra et al., [7] have proposed a method to secure the speech message using the fingerprints of the individual as the input to generate the public and the private keys. From the speech message, the text message will be generated that need to be encrypted for the security purpose. First the noise present in the speech message will be reduced, then the language model will be used to convert the speech message into the text message. Subhas Barman et al., [8] have proposed a method which deals with the generation of the keys from the fingerprints of the individuals. There are several steps included in the proposed system, namely, Template Generation, Key generation and message encryption, Key regeneration and cipher text decryption. Initially, the fingerprint template will be generated and then the keys will be generated using the fingerprint features, which will be used for the encryption and the decryption process. Cynthia Sthembile Ntshangase et al., [9] have proposed a method in which the minutiae points will be transformed into binarized form, from which the keys will be generated which can be used for the verification and the authentication process. The main advantage of the proposed system is that the length of the generated key will be long and also the length of the key will variable, which can be used in the different methods of the cryptography such as the RSA or AES. Ziad Addel AlQadi et al., [10] have proposed a method to detect and count the minutiae in human fingerprint. In this paper, they have introduced the LBP enhancement for the improved minutiae recognition and counting, from which the keys will be generated.

## III. METHODOLOGY

The main objective of the research project is to secure the data from the third parties using the fingerprints of the individual and the RSA algorithm. In this research paper, several methods have been used for the generation of the keys and the encryption and the decryption process.

### A. Fingerprint Image as an input and Extraction of Minutiae points:

In this method, the user will be first asked to select the fingerprint image as an input. The input image will then be loaded using the OpenCV's imread() function and then it will be converted into grayscale. The fingerprint image will be binarized to remove the noise present in the image using the morphological operations, then the topological skeletonization is applied to binarized image to obtain the skeleton image. From the obtained skeleton image, the ridge bifurcations and the endings will be detected and the count of the non-zero pixels in a 3*3 window, which is centered at each pixel. If the count is 2, then the pixel is considered as a bifurcation point, if the count is 1, then the pixel is considered as the ending point. After detecting the minutiae points, the original input image with the detected fingerprint minutiae points will be marked as green circles for the bifurcation points and the ending points will be marked in the red circles.

### B. Generating prime numbers:

In this method, the prime numbers will be generated from the detected minutiae points. Two functions, namely, find_primes( ) and the is_prime( ) are used to generate the nearest prime numbers and to check whether the generated numbers are prime or not.

The find_primes( ) function takes the generated minutiae points as the input and returns the nearest lower and the upper prime numbers. The nearest lower prime number is generated by moving backwards from the n-1 to 2 and checks whether the number is prime or not by using the function is_prime( ), if it is a prime number then it is assigned to 'lower_prime' and then it exits the loop. Then then nearest upper prime number will be generated by moving forwards from n+1 and checks each number by using the function is_prime( ), if the prime number is found, then it will be assigned to 'upper_prime' and then it exits the loop.

The is_prime( ) function will take the number as an input and checks whether the number is prime or not, returns 'True' if the number is prime and returns 'False' if the number is not a prime. If the number is less than 2, then it is not a prime number, so the function returns false. The is_prime( ) function will iterate starting from all the integers from 2 until the square root of the input number (int(n**0.5)+1), checks if each integer divides input integer without remainder. If there is no remainder, then the number is not a prime and returns false, if there is a remainder, then it is a prime number so it will return true.

### C. RSA Algorithm for text and text file:

In this method, the RSA algorithm is used to encrypt and decrypt the text message entered by the user. The generated prime numbers will be given as the input to the RSA algorithm, from which the public and the private keys will be

DOI: 10.17148/IJARCCE.2023.12555

generated based on the prime numbers. Initially, the key pair will be generated based on the two random prime numbers p and q. Then the user input will be taken in the form of text or to select an input file from the storage, and then the user input will be encrypted using the public key. Then encrypted message will be displayed on the console, and then the message will be decrypted using the private key.

### D. RSA Algorithm for image file:

In this method, the image file will be given as the input for the encryption and the decryption process. The input image file can be in the form of JPEG, JPG, TIFF and PNG, which will then be converted into RGB format using the "convert" method. The variables such as row, column, pixels, row1, phi, occ and the primes will be initialized. The Euler's Totient function will be calculated for all numbers ranging from 2 to 1000000 and the result will be stored in phi list. The RSA algorithm will be applied on each pixel of the image to encrypt the input image, then using the decryption key, the input image will be decrypted. The correctness of the decryption will be verified by comparing the last pixel values of both the original and the decrypted image.

## IV. RESULTS

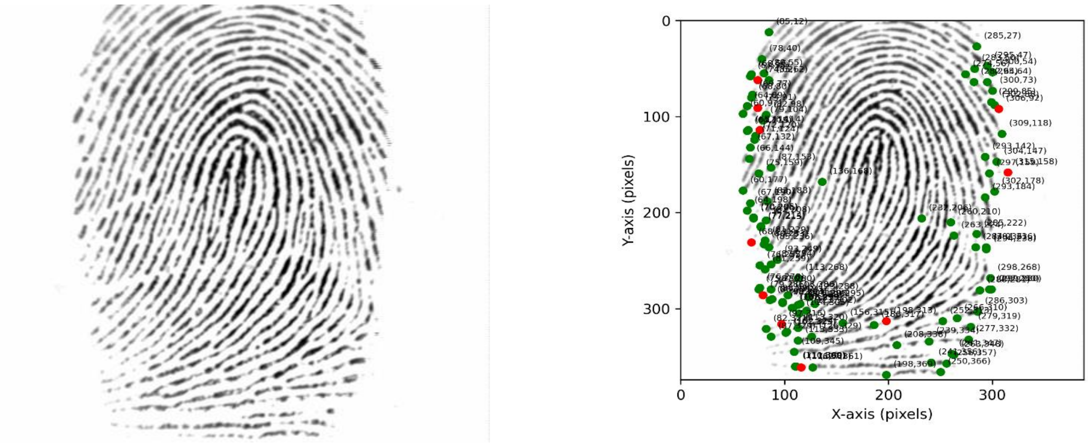
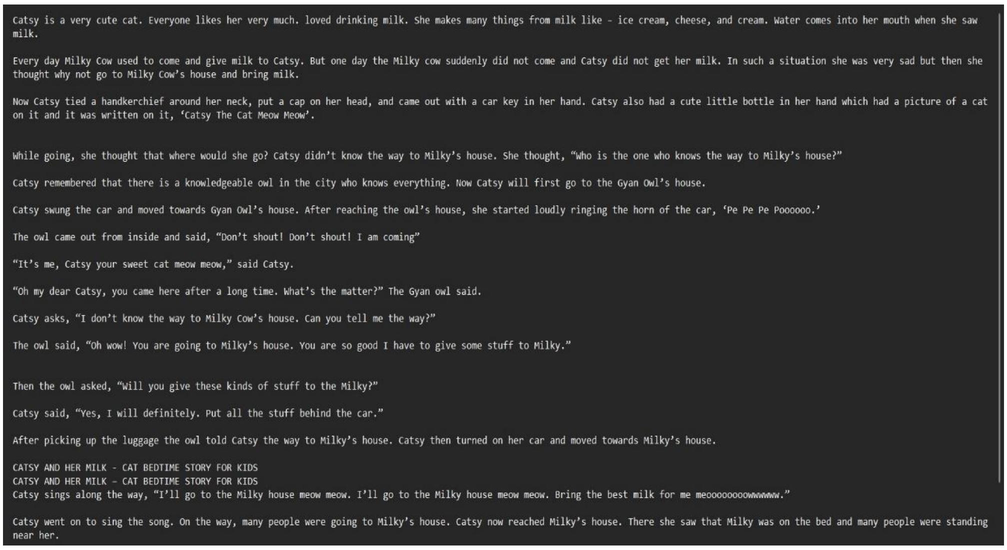


Fig 1: Fingerprint Image with Minutiae Detected Points

The figure 1 shows the fingerprint image with the minutiae detected points. The fingerprint image will be given as the input from which the minutiae points will be detected based on the ridge bifurcations and the ridge endings.



```
Catsy is a very cute cat. Everyone likes her very much. loved drinking milk. She makes many things from milk like - ice cream, cheese, and cream. Water comes into her mouth when she saw
milk.

Every day Milky Cow used to come and give milk to Catsy. But one day the Milky cow suddenly did not come and Catsy did not get her milk. In such a situation she was very sad but then she
thought why not go to Milky Cow's house and bring milk.

Now Catsy tied a handkerchief around her neck, put a cap on her head, and came out with a car key in her hand. Catsy also had a cute little bottle in her hand which had a picture of a cat
on it and it was written on it, 'Catsy The Cat Meow Meow'.


While going, she thought that where would she go? Catsy didn't know the way to Milky's house. She thought, "Who is the one who knows the way to Milky's house?"

Catsy remembered that there is a knowledgeable owl in the city who knows everything. Now Catsy will first go to the Gyan Owl's house.

Catsy swung the car and moved towards Gyan Owl's house. After reaching the owl's house, she started loudly ringing the horn of the car, 'Pe Pe Pe Poooooo.'

The owl came out from inside and said, "Don't shout! Don't shout! I am coming"

"It's me, Catsy your sweet cat meow meow," said Catsy.

"Oh my dear Catsy, you came here after a long time. What's the matter?" The Gyan owl said.

Catsy asks, "I don't know the way to Milky Cow's house. Can you tell me the way?"

The owl said, "Oh wow! You are going to Milky's house. You are so good I have to give some stuff to Milky."


Then the owl asked, "Will you give these kinds of stuff to the Milky?"

Catsy said, "Yes, I will definitely. Put all the stuff behind the car."

After picking up the luggage the owl told Catsy the way to Milky's house. Catsy then turned on her car and moved towards Milky's house.

CATSY AND HER MILK - CAT BEDTIME STORY FOR KIDS
CATSY AND HER MILK - CAT BEDTIME STORY FOR KIDS
Catsy sings along the way, "I'll go to the Milky house meow meow. I'll go to the Milky house meow meow. Bring the best milk for me meooooooowwwwww."

Catsy went on to sing the song. On the way, many people were going to Milky's house. Catsy now reached Milky's house. There she saw that Milky was on the bed and many people were standing
near her.
```

Fig 2: Input Text File

DOI: 10.17148/IJARCCE.2023.12555

The figure 2 shows the text file which is given as the input. Instead of giving the text as the input, here the text file is given as the input for the process of encryption.

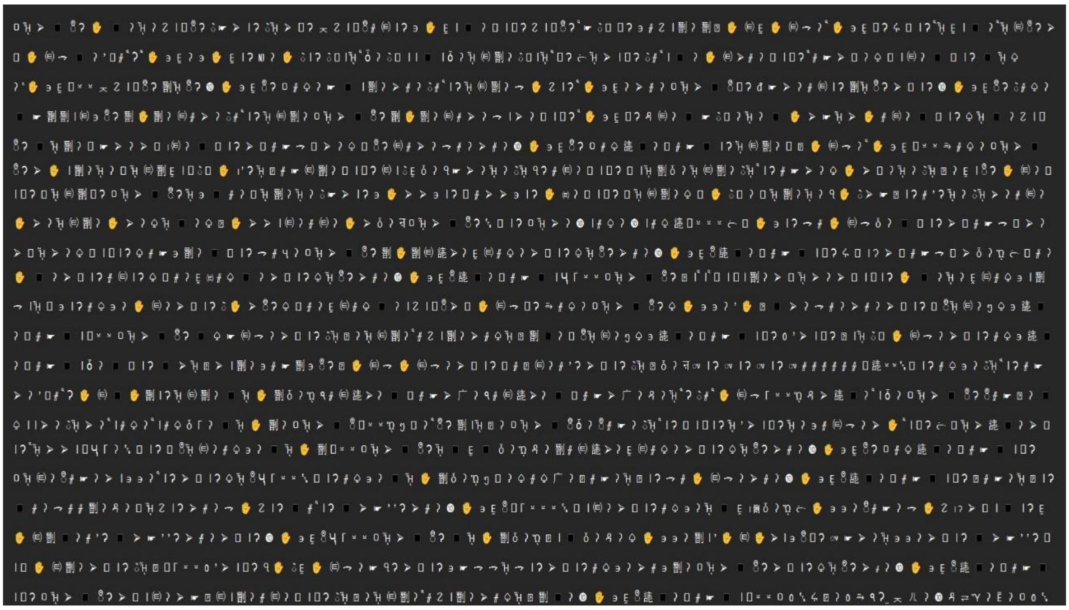


Fig 3: Encrypted text file

The figure 3 shown the encrypted text file. The text file which is given as the input will be encrypted, so that the input text file will be protected from the third parties.

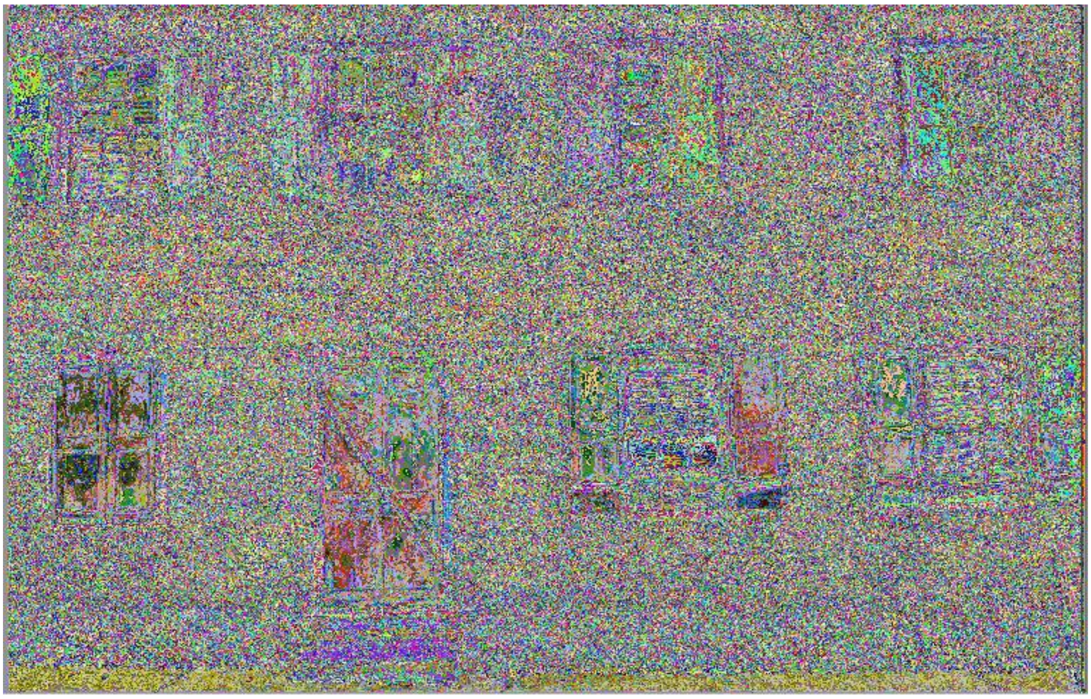


Fig 4: Encrypted Image

The figure 4 shows the Encrypted Image. The image which is given as the input will be encrypted as shown in the figure 4.

DOI: 10.17148/IJARCCE.2023.12555

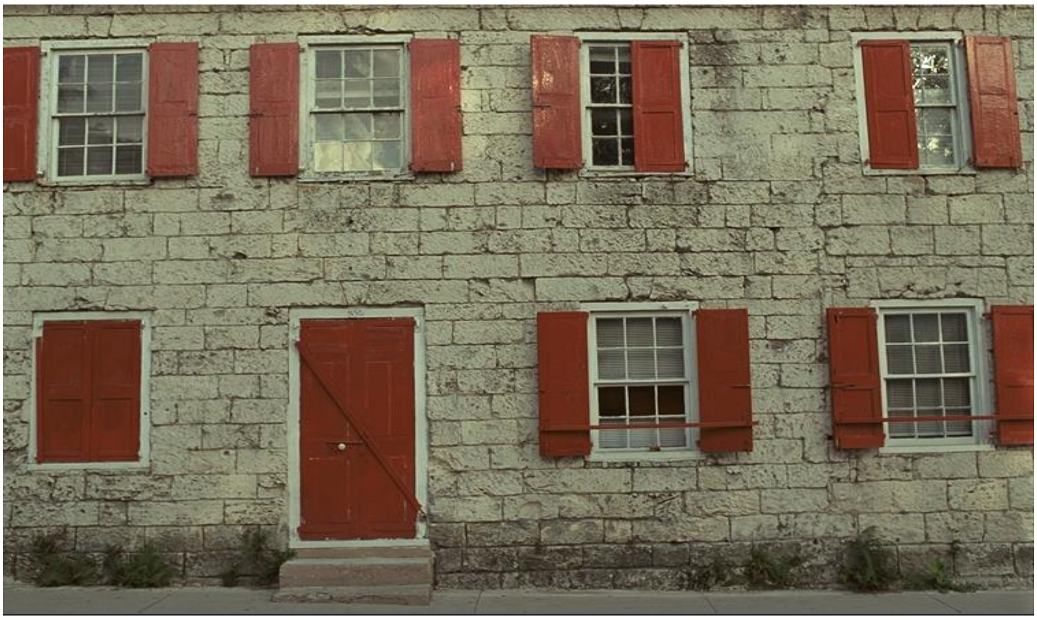


Fig 5: Decrypted Image

The figure 5 shows the decrypted image. The input image which is given as the input will be encrypted, then the encrypted image will be decrypted as shown in the figure 5.

## V. CONCLUSION

From the literature review generation of prime numbers is the challenging task. RSA algorithm is applied in various fields such as banking, IT sectors, Credit/Debit cards. In this project fingerprint data will be used for the generation of prime number and RSA algorithm is used for the encryption of input Text/Image.

## REFERENCES

[1]. Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Khaled Aldebei, "Comparative Analysis of Fingerprint Features Extraction Methods", Journal of Hunan University (Natural Sciences), pp.177-182, Vol. no. 48, Issue No. 12, December 2021.

[2]. Ai Takahashi, Yoshinori Koda, Koichi Ito, Takafumi Aoki, "Fingerprint feature extraction by combining texture, minutiae, and frequency spectrum using multi-task CNN", In 2020 IEEE International Joint Conference on Biometrics (IJCB), pp.1-8. IEEE, 2020.

[3]. Bakheet, Samy, Shtwai Alsubai, Abdullah Alqahtani, and Adel Binbusayyis. "Robust Fingerprint Minutiae Extraction and Matching Based on Improved SIFT Features", Applied Sciences, Vol. no. 12, December 2022.

[4]. K.Sekar and M.Padmavathamma, "Identity and Authentication Using Fingerprint Biometrics MJ2-RSA Cryptosystem in Health Care System", International Journal of Computer Science and Mobile Applications, pp. 14-20, Vol. no. 5, Issue. 12, December 2017.

[5]. Ranjith Jaypal and Pramod Govindan, "Biometric Encryption System for Increased Security", Systematics, cybernetics and informatics, pp. 75-80, Vol. no. 16, YEAR 2018.

[6]. Sayuti Rahman, Indah Triana, Sumi Khairani, Amru Yasir, Siti Sundari, "RSA Key development using fingerprint image on text message", Journal of Physics: Conference Series, Vol. no. 930, August 2017.

[7]. Sayani Chandra, Sayan Paul, Bidyutmala Saha, Sourish Mitra, "Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network", IOSR Journal of Computer Engineering (IOSR-JCE), pg. 16-22, Vol. no. 12, Issue 1, June 2013.

[8]. Subhas Barman, Samiran Chattopadhyay, "Debasis Samanta, Fingerprint Based Symmetric Cryptography", 2014 International Conference on High Performance Computing and Applications, pp. 1-6, Febuary 2015.

[9]. Cynthia Sthembile Ntshangase and Meshack Bafana Shabalala, "Encryption using finger-code generated from fingerprints", 2018 Conference on Information Communications Technology and Society (ICTAS), pg. 1-5, March 2018.

[10]. Ziad Abdel AlQadi, Yousf Eltous, Mohammad Abuzalata, Ghazi M. Qaryouti, "Detecting and Counting Minutiae in Human Fingerprint", Open Science Journal, Vol. no. 5, January 2020