Image Encryption using Jumbling-Salting Algorithm

Mayuresh Vartak, Rishabh Reddy, Prathamesh Churi

Abstract*: With the advent of digital world today, securing images across internet has become an important issue. There exist many image security techniques viz. steganography, encryption, watermarking etc. Image Encryption is one of such fruitful technique which encrypts an image using random secret key and stores the encrypted image on the server. There are many challenges of implementing image encryption algorithms such as higher computational complexity, loss of information during encryption, universality and applicability of algorithm, less scalability etc. Many image encryption algorithms are selective image encryption algorithm which works for specific part of image. It consists of encrypting only a subset of the data. The aim of selective encryption is to reduce the amount of data to encrypt while preserving a sufficient level of security. The selective encryption algorithms have a problem of scalability and data loss. The paper proposes a new algorithm Jumbling-Salting for images. The algorithm was earlier used in encryption passwords, text files, DNS, payment gateway data etc. An application is developed which incorporates the Jumbling salting encryption stategy for images.

***Keywords* : Jumbling, Salting, Algorithm, Images, Encryption**

I. INTRODUCTION

Security is a process, not a product. The well-known proverb to acquaint with that there may be en number of technique that dispense various security techniques nowadays [1], but the certainty is that it cannot independently address all the intent of security for an organization. The majority concern is dealing with relocation of image data security is been followed by technological development where the fulfillment of the data can be cut off to attack so data will have lost intimidating remark to privacy [1][6].

Today is the era of digital world where information processing is automated. Government sectors, healthcare organizations, transport and food industry uses automated processing techniques to handle the data. The data can be anything viz. numeric, binary, sensor-data, images, video, audio etc. elaborating on images, when transmitted via internet, the guarantee of secure transmission is very difficult, since there are number of attacks are possible on images. [2, 4, 5]. It is required to have image security techniques of various images types depending upon the type of importance of the image [2].

Nowadays communication through images provides great addition in multimedia. Sending an image over an unsecured network and providing protection is really a challenge to preserve the data privacy, so securing of image and the data can be done using Encryption method. The field of Information Technology is growing rapidly with the help of internet which resulted in interaction of mass with media in section of communication. In field of army, national security and much more confidential information is being transfer through mode of image Encryption. [7]

Providing a secure protection over an insecure network becomes very challenging for the people to convey image. So basically image needs a strong security check to protect the confidentiality, integrity and authenticity [CIA] [8] of the data from various incoming attacks. There are various methods that are involved in securing the image, one of which is Encryption which transforms the image data into cryptic image with the help of key.

Jumbling Salting (JS) encryption algorithm has two techniques which have one part as jumble block and other is the small thinly distributed amount of code to make it complex which is salt block. The Image in Jumbling block should pass through “addition” ”selection” and “reverse” sub block. [9, 10] In the addition block, the number of characters which are to be added to the native block are created .Selecting characters from the given character set and adding it to the binary matrix is been done in selection block .Character set is been provided with n different character .In reverse block, by running a predefined condition the result generated is been reverse.

In predefined conditions any mathematical proficiency as even, odd, composite number, divisibility etc. Salt selection is constructed on the timestamp of uploading time. The selection of salt is in the format of “mm yyyyddhhssmm” which is prepended to Jumbled string. Brute force can be ceased using randomized algorithm. Due to this reason, randomized algorithm is globally used in cryptography. Jumbling Salting algorithm has randomization at each and every sub process; henceforth we have attained "Randomness in Security".

The problem Statement of the algorithm will be – “Being an important aspect of security, image is an authentication [11] [6] technique which provides the claimant access to system resources. The probability of attacking the image is considerably high.

Revised Manuscript Received on October 31, 2019.
***** Correspondence Author
Mayuresh Vartak *, IT Engineer, ATOS-Syntel Pvt. Ltd. Mumbai, India Email: mayureshvartak18@gmail.com
Rishabh Reddy, School of Engineering and Technology Management, NMIMS University, Mumbai, India. . Email: rishabh3599@gmail.com
Prathamesh Churi, School of Engineering and Technology Management, NMIMS University, Mumbai, India. . Email: Prathamesh.churi@gmail.com

Although image encryption provides solution to prevent many attack shave proven this image encryption technique to be futile. To overcome the problem of securing encrypted image, we have developed Jumbling-Salting technique which will provide additional security to the stored images"

The sections of the paper are as follows. Section II has literature survey studied for proposed image encryption algorithm. In the same section, the existing image encryption techniques are studied. Another subsection has existing work done in Jumbling-Salting algorithms for another formats of the data (such as text, files). Section 3 has block diagram of proposed JS algorithm in images. The section III also has various scenarios implemented in Unified Modeling Languages. Section 4 has implementation part with results. Section 5 concludes our research work.

II. RELATED WORK

There are existing encryption algorithms on images in recent years which are tabulated in table I.

Table 1 : Existing Image Encryption Techniques.

Citation and year	Title	Author	Approach
[12], 2011	Research of Image Encryption Algorithm Base on Chaos Theory	Liu Bo, Liu Na, Li Jianxia, Liang Wei	Using Chaos Theory, chaotic sequence is generated by Logistics Chaos Mapping.
[13], 2000	Image Encryption for secure Internet Multimedia Applications	Philip P. Dang, Paul M. Chau	Using Discrete Wavelet Transform for image compression and block cipher Data Encryption Standard for image encryption is proposed.
[14], 2015	Digital Image Encryption based on Advanced Encryption Standard Usage Mining Using Artificial	Qi Zhang, Qun Ding	Using AES algorithm implemented on MATLAB, performing digital image processing, obtaining the date that can use AES Encryption algorithm & combining both approaches.
[15], 2014	A Review on Various Digital Image Encryption Techniques and Security Criteria	Mohit Kumar, Akshat Aggarwal, Ankit Garg	Survey of diverse image encryption techniques and comparison of discrete image encoding approaches.
[16], 2015	A Fast and Secure Image Encryption Algorithm using Number Theoretic Transforms and Discrete Logarithms	Jeyamala Chandrasekaran, Dr. Thiruvengadam S Jayaraman	Discrete logarithms used for generation of random keys and Number Theoretic Transform (NTT)
[17], 2015	Secure Non Real Image Encryption Algorithm development using Cryptography & Steganography Usage	Mukhedkar, Prajakta Powar, Peter Gaikwad	Using Blowfish algorithm, Image hiding LSB technique is used and bit manipulated. PSNR and MSE are used for measuring the quality of image.

There are some existing Jumbling-Salting algorithms used in text, online transaction details, DNS, text files etc. The details are discussed in table 2.

Table 2 : Research in Jumbling-Salting Algorithm

Citation and year	Paper Title	Authors	Description
[9], 2014	JSH Algorithm: A Password Encryption Technique using Jumbling-Salting-Hashing	Prathamesh Churi, Medha Kalelkar, Bhavin Save	The base paper [9], proposes password encryption algorithm using jumbling salting and hashing process. In [10], the algorithm is implemented and analyzed against four parameters viz. Encryption Time, Decryption Time, Throughput and size of cipher text.
[10], 2015	Jumbling-Salting: An improvised approach for password encryption	Prathamesh Churi, Vaishali Ghate Kranti Ghag	
[18], 2017	JSSecure: A Secured Encryption Strategy for Payment Gateways in E-Commerce	Prathamesh Churi, Ramkrishna Oruganti, Yohan Pavri, Neelansh Prasad	The base paper [18], proposes same algorithm encrypted on payment gateway systems as a replacement of traditional SET protocol. The implementation version of the paper [19], has more improvised version where the process of AES is being eliminated and double encryption through same algorithm is proposed. The results shows better security when JS algorithm is implemented over payment gateway system.
[19], 2018	Improvised E-commerce Transaction Security using JSSecure Algorithm	Prathamesh Churi, Ramkrishna Oruganti, Yohan Pavri, Neelansh Prasad	

[20], 2019	Symmetric Jumbling-Salting Encryption Algorithm for Files	Prathamesh Churi, Udit Bali, Nikhil Udgata	In this paper, the JS algorithm is implemented over text files. The paper represents improvised version in the processes of JS algorithm. The different rounds of same encryption s encrypted.
[21], 2017	DNS encryption using innovative algorithm	Prathamesh Churi, Sanjay Deshmukh	In this paper, JS algorithm is used in encrypting the DNS to improvise the security.

III. JS ALGORITHM FOR IMAGES

A. *Block Diagram for JS Algorithm*

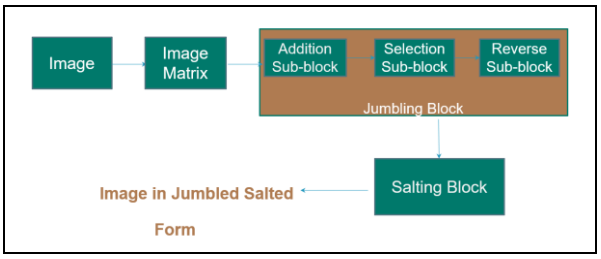

Fig. 1.Block Diagram of JS Algorithm

In figure 1, the block diagram of JS algorithm is given. In the initial Stage, the image is been taken which needs to be encrypted .Then the image is been passed through the Image matrix block. The need of matrix presentation by image is to clear the pixels which in their work use high dimension matrices.

There is a relation between matrices and images. An image is a represented in form of pixel matrix. Each pixel of such image is presented by one matrix element integer from {0,1…255}.The numeric values in pixel presentation are uniformly changed from zero (black pixels) to 255 (white pixels). Color images (with RGB color model) in a computer are presented with three gray-scale images matrices (one for each – red, green and blue – color components).

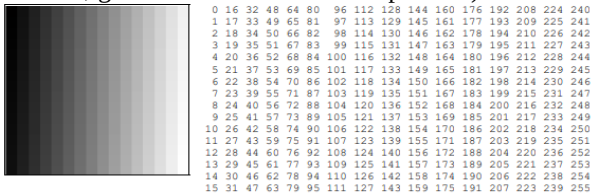

Fig. 2. Sample matrix representation of Images

After the Image matrix is being formed it will then passes through the jumbling salting block.

In this Jumbling salting block, we will provide set of random character and this random character will be placed at each pixel position creating a dummy image of random character pixel which is of same size and will contain same amount of pixels as per the original image pixels.

After getting our random pixel image we will take this two images and will we swap the pixels position with the random pixel image according to its pixel position (same position will be swapped) which will create a shuffled of original pixels the random character that we have provided. These will complete the addition and selection part of Jumbling block. After these we will reverse the pixels of the image using a predefined function .Here we have used the transpose method to reverse the matrix making it more difficult to access.(Any matrix combination can be done).

After providing the set of random character we will add the salting block which will add timestamp value viz. the time at which the image was encrypted and the random pixel image will be send at receiver end to decrypt.

B. *Application Design of JS Algorithm*

Following sequence diagrams in figure 2 and 3 self-explains the role of active user, application and the server (where image is encrypted and decrypted).

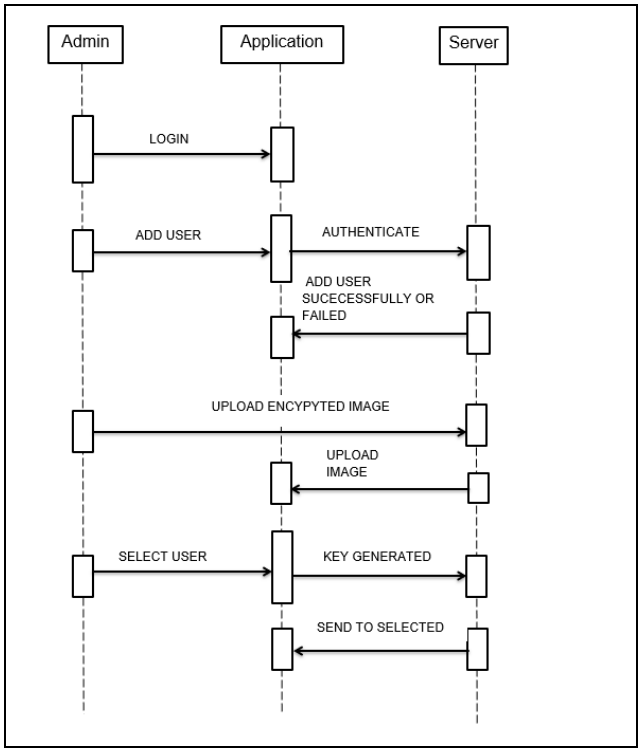

Fig. 3.. Sequence diagram for authenticating valid user and encryption process.

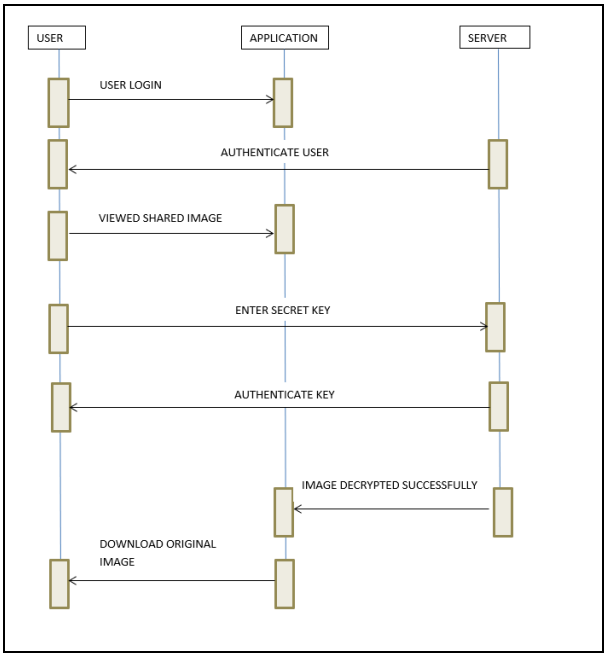

Fig. 4.Sequence diagram for encryption-decryption process

The data flow diagram has drawn below shows how data (Encrypted and Decrypted image) flows into a proposed system.

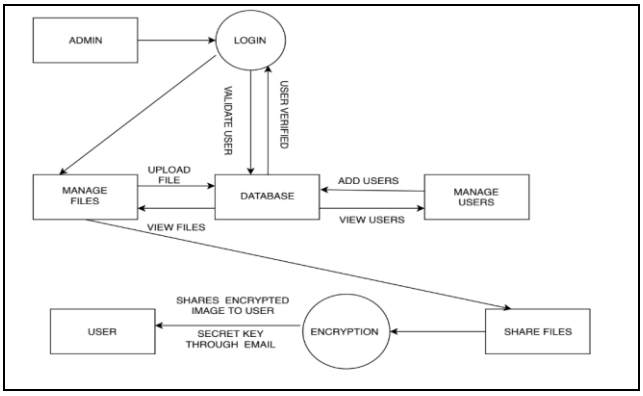

Fig. 5. Data Flow Diagram for Admin

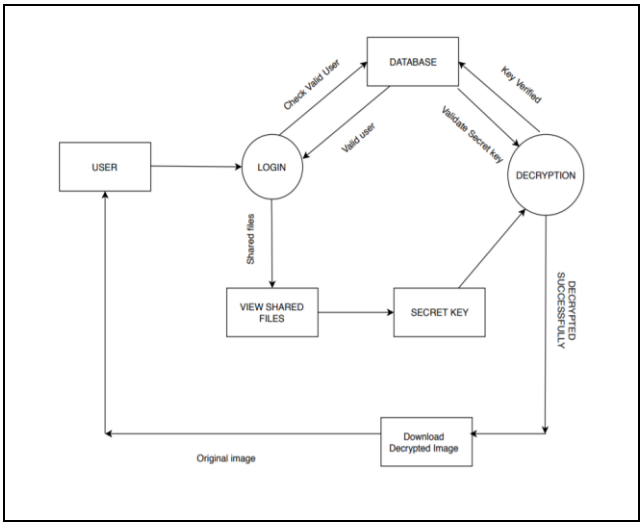

Fig. 6.Data Flow Diagram for User

IV. IMPLEMENTATION

The hardware and software used for the development of the project is tabulated below:

Table 3: Hardware Components for proposed work

Components	Specifications
Screen Resolution	1024x768 display 5400 RPM hard disk
System/Processor	Intel® Core ™ i3-2330M or more than CPU @ 2.20 GHz.
Memory	4 GB of RAM
Hard Disk	500 GB of HDD or higher recommended
Supported Arch	X86 and x64

Table 4: Software Components of Proposed Work.

Components	Specifications
Operating System	Microsoft Windows XP Professional Microsoft Windows Server 2003 Windows Vista Windows 2010 (64-bit)
Database	SQL Server 2008 R2 (64-bit)
Supported Browsers	Microsoft Internet Explorer 8.0 Google chrome Mozilla Firefox
Front End	.NET framework C# language

A. *Results and Discussion:*

- For the implementation purpose, the web application is designed which encrypts and decrypts image using JS algorithm.
- After encrypting an image, It is observed that there is a loss in the resolution of an image.
- The speed of encrypting the image is high such that the image's visual quality is not changed and the image is sent to the desired destination securely.
- For the encryption and decryption phase, JS algorithm is used and implemented in .NET framework using C# programming language.
- The concatenation approach is used in this system in which the image is converted into bytes format and this data is concatenated at the end of the master file. Since this approach is used, there is no change in visual quality of the jumbled image.

Admin Panel:

In this process as shown in Figure 5, the admin first clicks on "Share File" button to share the uploaded image for encryption process.

The admin enters the filename as shown in Figure 6 , which is to be sent to the desired user shows a corresponding unique Share ID is associated with each File ID. As soon as the image file is shared with a particular user, user gets a secret key in his/her email address which is implemented using SMTP protocol.

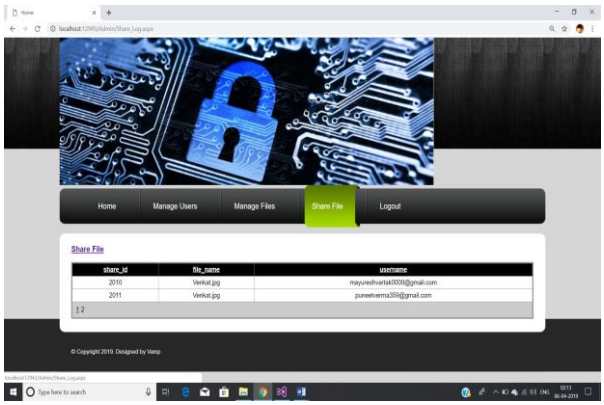

Fig. 7.Screenshot of Admin Share File

Fig. 8.Screenshot of Input Image

User Panel:

In this process as shown in Fig 10 , the user logs in and further clicks on the "Download" option under the "Action" tab to receive the image file as shown in Figure above and enters the secret key which the user had received in his/her email address After the secret key is matched, the user is able to download the encrypted image file into his/her computer system and hence the decryption process comes to an end.

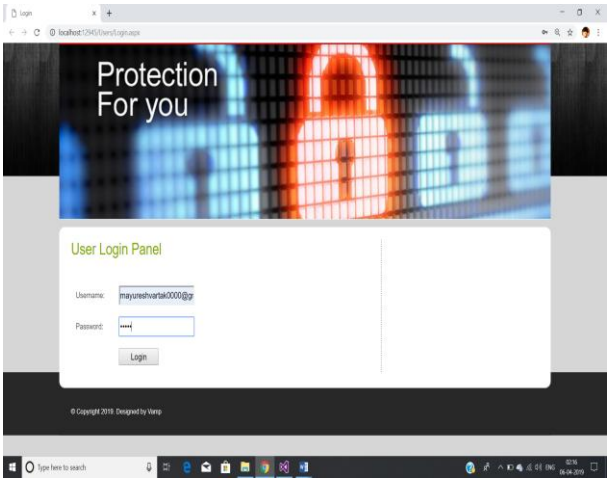

Fig. 9.Screenshot of User panel

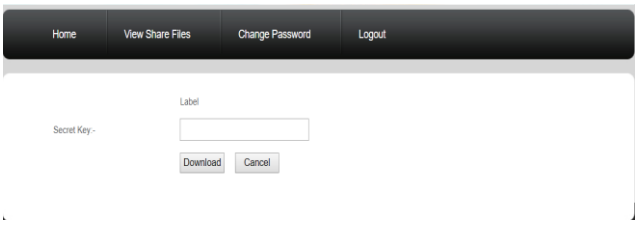

Fig. 10. Screenshot of Selecting Secret Key

Fig. 11. Screenshot of Output Image

V. CONCLUSION

This system puts forward the method that uses the JS algorithm with the key control to encrypt the image. This method incorporates a variety of characteristics, and with a simple design. JS algorithm reduces the probability of decrypting the image. Due to the various randomization techniques, it builds an encrypted image which is almost difficult to decrypt. To decipher this encrypted image is a difficult task. JS algorithm however takes a lot of space and time for both the encryption and decryption which is due to the various randomization techniques but on the other hand this makes the algorithm fully secured. Jumbling Salting algorithm's Encryption is large. The additional overhead of jumbling and salting process increases due to the value of processing time. The encryption and decryption time rises due to the process of randomization.

In future we extend our work in context of comparing our algorithm with existing algorithms. We also want to work upon reducing the time complexity of an algorithm as compared to other image encryption algorithms.

VI. FUTURE WORK

- **Encryption on the World Wide Web**

The world wide web (www) makes extensive use of inline images. There are literally millions of images on various web pages worldwide. It may be possible to develop an application to serve as a web browser to retrieve data embedded in web page images. This "jumbled-web" could operate on top of the existing WWW and be a means of covertly disseminating information.

- **Encryption in printed media**

If the data is embedded in an image, the image printed, then scanned and stored in a file can the embedded image be recovered? This would require a special form of a encryption-decryption mechanism to which could allow for in accuracy in the printing and scanning equipment.

REFERENCES

1. Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons.
2. Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.
3. Reddy, C. S., Sowjanya, C., Praveena, P., & Symmetric, P. S. L. P. A. Key Algorithm Using Randomized Prime Numbers International Journal of Scientific and Research Publications
4. Stallings, W. (2017). *Cryptography and network security: principles and practice* (pp. 92-95). Upper Saddle River:
5. Pfleeger, C. P., & Pfleeger, S. L. (2002). Security in computing. Prentice Hall Professional Technical Reference
6. Kahate, A. (2013). *Cryptography and network security*. Tata McGraw-Hill Education.
7. Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. *Optics communications*, *218*(4-6), 229-234
8. Coatrieux, G., Lecornu, L., Sankur, B., & Roux, C. (2006, August). A review of image watermarking applications in healthcare. In *2006 International Conference of the IEEE Engineering in Medicine and Biology Society* (pp. 4691-4694). IEEE.
9. Churi, P., Kalelkar, M., & Save, B. (2014). JSH Algorithm: A Password Encryption Technique using Jumbling-Salting-Hashing. *International Journal of Computer Applications*, *92*(2).
10. Churi, P. P., Ghate, V., & Ghag, K. (2015, November). Jumbling-Salting: An improvised approach for password encryption. In *2015 International Conference on Science and Technology (TICST)* (pp. 236-242). IEEE
11. Nadeem, A., & Javed, M. Y. (2005, August). A performance comparison of data encryption algorithms. In *2005 international conference on information and communication technologies* (pp. 84-89). IEEE.
12. Bo, L., Na, L., Jianxia, L., & Wei, L. (2011, August). Research of image encryption algorithm base on chaos theory. In *Proceedings of 2011 6th International Forum on Strategic Technology* (Vol. 2, pp. 1096-1098). IEEE.
13. Dang, P. P., & Chau, P. M. (2000). Image encryption for secure internet multimedia applications. *IEEE Transactions on consumer electronics*, *46*(3), 395-403.
14. Zhang, Q., & Ding, Q. (2015, September). Digital image encryption based on advanced encryption standard (aes). In *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)* (pp. 1218-1221). IEEE.
15. Kumar, M., Aggarwal, A., & Garg, A. (2014). A review on various digital image encryption techniques and security criteria. *International Journal of Computer Applications*, *96*(13).
16. Chandrasekaran, J., & Jayaraman, T. S. (2015, February). A fast and secure image encryption algorithm using number theoretic transforms and discrete logarithms. In *2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)* (pp. 1-5). IEEE.
17. Mukhedkar, M., Powar, P., & Gaikwad, P. (2015, December). Secure non real time image encryption algorithm development using cryptography & Steganography. In *2015 Annual IEEE India Conference (INDICON)* (pp. 1-6). IEEE
18. Oruganti, R., Shah, S., Pavri, Y., Prasad, N., & Churi, P. (2017). JSSecure: A Secured Encryption Strategy for Payment Gateways in E-Commerce. Circulation in Computer Science, 2(5), 13-17
19. Prasad, M. N., Oruganti, M. R., Shah, M. S., Pavri, M. Y., & Churi, P. (2018, July). Improvised E-commerce Transaction Security using JSSecure Algorithm. In *2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA)* (pp. 1-7). IEEE
20. Bali, M. U., Udgata, M. N., & Churi, M. P. P. (2018, November). Symmetric Jumbling-Salting Encryption Algorithm for Files. In 2018 Fifth HCT Information Technology Trends (ITT) (pp. 82-86). IEEE.
21. Savla, H., Mohta, V., Parwah, N., Deshmukh, S., & Churi, P. DNS ENCRYPTION USING INNOVATIVE ALGORITHM