2D IMAGE SCALING AND CROPPING FOR SECURE DATA SHARING ON CLOUD INFRASTRUCTURE

Namrata D. Ghuse, Kalyani J. Patil

Abstract—Cloud computing is term where large number of systems are connected together that provide dynamically scalable infrastructure for various applications storing all sort of data. It is an emerging technology where the services like platform as a service, software as a service and infrastructure as a service are provided. A new business module defines a structure where the outsourcing of image storage and its processing is done. This processing increases the size of the images up to an remarkable extent. The current system that is 2Dcrypt technique, is based on the modified paillier cryptosystem. In this system cropping and scaling operations are performed without knowing the content of the image. In other words, this system considers the tile of pixels for encryption, unlike other image encryption methods considering each pixel individually. Another limitation of the existing system is data redundancy. This limitation proves to be dominant and affects the performance of the current system. The proposed system enables cloud data center to perform operations such as scaling and cropping over encrypted image by using Shamir Secrete algorithm. This algorithm provides Token for security purpose which can be used for a specific time period. Such use of tokens helps in reducing the limitations of the existing system up to an significant level.

Index Terms—Cropping, Encrypted Scaling, Hidden Image Processing, Image Outsourcing and Paillier Cryptosystem.

I. INTRODUCTION

Cloud computing is the technology that provides different services to the users and these services are made available to the users as per their demand. Users have to pay for the ser-vices depending upon the usage that is pay as you use model. Cloud is fundamentally a bunch of thing PCs composed to-gether in same or distinctive geological regions, cooperating to serve different customers with different need and workload on re-journey preface with the help of virtualization. Circulated processing implies con-trolling, orchestrating, and getting to the gear and programming resources remotely. We can access the data or services from anywhere at any time. Many cloud storage services are available such as Box,DropBox, SkyDrive, Sug-arsync for individual and small to medium business. The confidentiality of outsourced image is protected by using the nave approach. The image is encrypted before it is stored in the cloud. The system has a problem that it is not possibleto perform basic operations on pictures, such as zooming and trimming.

To save secrecy, operations are performed over encoded pictures. 2Dcrypt procedure concentrate on powerful scaling and editing operations on scrambled pictures. These tech-nology can be used to implement scaling and resizing of image, which can be applied on large image. By using this technique no data contained in the pictures can be spilled to the cloud servers, and in the meantime, clients can completely misuse the cloud display. 2DCrypt is a cloud-based multi-customer picture scaling and editing system and it relies upon Pailliercryptosystem[1]. The calculation over encoded information is carried out homomorphic encryption. The right now accessible completely homomorphic encryption plot [10] is not calculation partner down to earth. Along these lines, fractional homomorphic encryption plots, those supporting certain operations over scrambled information, are commonly utilized for useful arrangements. In light of fractional homo-morphicShamirs mystery sharing [21], two principle look into works perform picture scaling and trimming operations in the scrambled space [6], [2].

These methodologies experience the ill effects of two prin-ciple: (I) for each picture, n shares are made and transferred to the cloud, which increment the measure of capacity required and additionally the preparing power and (ii) this approach is not collusion resistant: if k data centers collude then the original image can be retrieved. The utilization of cryptosys-tem for concealing pictures is a very much examined range. Various methodologies, including however are not constrained to, Open Key Cryptosystem (PKC) [11], watermarking [9], Shamirs mystery sharing [15] and confusion based encryption [12], is used to secure images. To permit cloud data centers to perform operations on the scrambled picture, halfway ho-momorphic cryptosystem based solutions have been proposed [4][3]. A fractional homomorphic cryptosystem solely offers either expansion or augmentation operations. Paillier [17], Shamirs mystery sharing [21] are among in part homomorphic

cryptosystem that help expansion. The Paillier cryptosystem is homomorphic to augmentations and scalar increases [13]

and can be changed to an intermediary encryption scheme [13], [5].

A. Objectives

To provide the protection to an image by generating a token.

To improves the efficiency of the system by avoiding the data duplication on cloud.

II. LITERATURE SURVEY

ManoranjanMohanty, Muhammad RizwanAsghar, and Giovanni Russello [1] used some techniques such as, 2DCrypt, Paillier, Tiling, Shamirs secret sharing, Homomorphic Encryption Scheme. Using Pailier technique, scaling and cropping operation is done on encrypted data. To overcome space efficient issues, the system uses tiling scheme.

Mrs. JadhavRohini, Prof. S. A. Kahate [2] used Paillier cryptosystem, Public Key Cryptosystem (PKC), watermarking, Shamirs secret sharing chaosbased encryption. Watermarking is the major applications in image data hiding. Watermarking use cover multimedia to conceal the secret data.

Wenjun Lu1, Avinash L. Varna [4] Used Additive Homomorphic Encryption, Fully Homomorphic Encryption, Secure Min-Hash Secure Inverted Index. It keeps up the inquiry precision of plaintext highlights and offers randomized encryption with the goal that the server can't get separate between encoded includes specifically. It is exceptionally proficient and requires least client inclusion. The hunt precision and condentiality security offered by include/record randomization are near that of homomorphic encryption scheme.

Rohini, B. S. Kurhe [5] uses Shamirs secret sharing, Paillier-based cryptosystem, Public Key Cryptosystem Watermarking schemes. These all techniques are is to security images. Using Pailier scheme, scaling and cropping operation is done on encrypted data. To overcome space efficient issues, the system uses tiling scheme.

KshitijKansal, ManoranjanMohanty, and Pradeep K. Atrey [3] has proposed wavelet-based compresse image scheme is highly secure and has acceptable computational and data overheads.

GulCalikli [8] describes the number of active users on social network is increases day by day as the use of OSN has grown, privacy violation due to in appropriate sharing of information on social sites the privacy of user has been violated.

. JadhavRohini, Prof.S. A. Kahate [7] used 2Dcrypt technique. 2Dcrypt technique divides in to two scheme such as pallier and Tile level. Using Pailier scheme, scaling and cropping operation is done on encrypted data. To overcome space efficient issues, the system uses tiling scheme.

Scale-invariant feature transform PPSIFT scheme is described by [11]. Privacy-preserving Scale-invariant feature transform is secure against ciphertext as well as plaintext attack. This scheme has been solved the most challenging problem, i.e., homomorphic comparison.

Searchable symmetric encryption order-preserving symmetric encryption schemes is implemented in [12]. In this paper, the problem of secure ranked keyword search over encrypted cloud data is solved. This paper gives as-strong-aspossible security guarantee compared to previous SSE schemes.

Muhammad RizwanAsghar [13] used multi-user encrypted search scheme. This method work on multiple users encrypted search method on encrypted database. SQL support encrypted queries. When data is stored on cloud gives access control perform administrative actions. There is no need of redistribution of keys or re-encryption of data. There is a method to protect sensitive user data.

A. Comparative Study

In this section we will study overall comparison between existing system and proposed system. In previous systems there are some drawbacks let us discuss one by one. In this paper this drawback are remove.

Studying previous papers in that the private keys are share to third party for accessing the data. But the third party use these keys multiple times. So that data has no privacy at all. Any time user can access this private data or he can use our private data for wrong way. These drawback remove in this paper.

In previous papers there were duplicate data can be occur. So that efficiency of the system can be less. And the system can work slowly. In that system more space can be required. But in this paper improving the efficiency of the system by avoiding the data duplicating on cloud.

III. SYSTEM ARCHITECTURE

A. Problem Statement

To develop a system that protect the sensitive data while en-abling outsourced im-age services. The system enables cloud data center to perform operations such as scaling and cropping over encrypted image security providing as token that is One Time Password (OTP). The system increases performance of various applications and reduce storage space by using tiling scheme.

B. System Overview

The main goal of this system is to performing scaling and cropping operation over encrypted images by using 2Dcrypt technique. The 2Dcrypt techniques including two schemes such as Paillier Cryptosystem and Tilling scheme. In the exist-ing system the data duplication is created, to overcome these drawback the proposed system use Shamir Secret algorithm.

Figure 1 shows the architecture of 2DCrypt. 2DCrypt technique is a cloud-based multi-client picture scaling and editing framework. This technique depends on Paillier cryptosystem. The storing and processing of image is outsourced to the third party cloud provider by using this

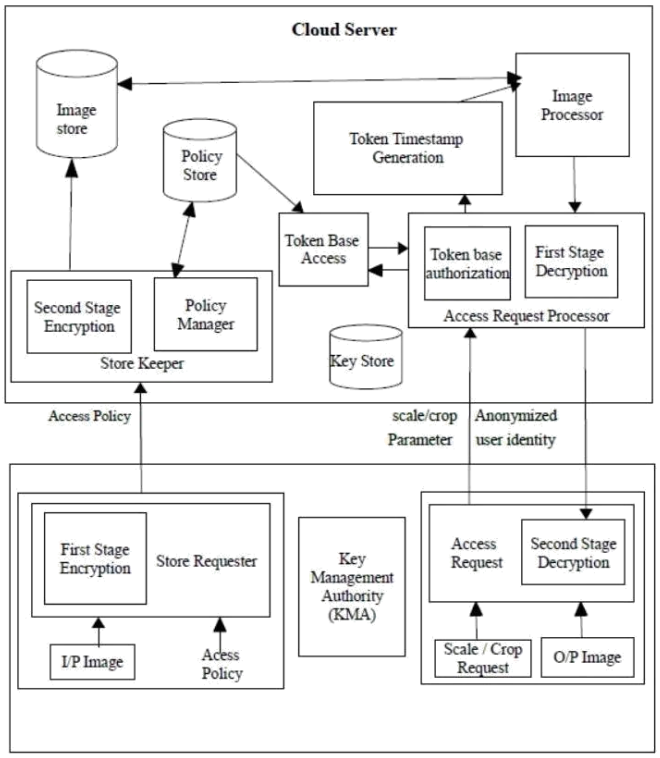

Fig. 1. Architecture of System

entity. It could be an individual or an association, for example, a hospital center. In the last case, a few clients can go about as an Image Outsources. Cloud Server is the part of infrastructure provided by a cloud service provider. It stores encrypted images and access policies used to regulate access to the images. It separate an asked for picture from its picture store after consummation of approval.

C. Working

2DCrypt technique is based on Paillier cryptosystem. In this technique, for each user that is an Image Outsourcer or Image User, the KMA creates two keys combines by arbitrarily part the ace mystery enter into two sections: the client side key sent to the client and the server side key conveyed to the server. The Image Outsourcer stores a picture and its entrance approaches in the cloud server. The Vendor isolates the picture into various tiles and performs per tile encryption. At the Cloud Server-end, the Vendor plays out the second round of encryption using the server-side key co responding to the customer, and stores the mixed picture in a image store. A Picture Outsourcer is responsible for watching out for security and insurance concerns joined to picture outsourcing. The Picture Outsourcer encodes the photo before sending it to the cloud server cultivate. The Picture Outsourcer can store new pictures on a cloud server, revive and modify existing ones, and regulate get the opportunity to control courses of action to guide access to the photos set away on the cloud server. Cloud Server is the piece of framework gave by a cloud specialist co-op, for putting away and handling pictures.

It stores encoded pictures and access approaches used to direct access to the pictures. It stores encoded pictures and access approaches used to manage access to the pictures. In the wake of making approval checks, it recovers an asked for picture from its picture store. In the event that the passage request satisfies get to approaches, it scales and moreover trims pictures scrambledly, that is without unraveling them Picture Client is endorsed by the Picture Outsourcer to get to the requested picture set away in an encoded shape on the Cloud Server. A picture client can issue either read demand or process ask for relying upon approval.

Key Management Authority generates keys. It generates a client and server key pair for each user, be it an Image Outsourcer or Image User. The client and the server side keys are securely transmitted to the user and the cloud Server, respectively. The user- side key send to the user and the server-side key send to the server. In Token Time stamp Generation, the system generate an token that means one time password used to security purpose for a specific time period. In Token base Authorization, unique token is given to particular user for security purpose. If the token get match then and then user can access or update or modify the data. The asked for picture is recovered from the Image Store and the Image Processor performs scaling or editing on the scrambled picture. At the point when the scaling or trimming activities are finished, the picture is sent to the Access Request Processor. The Access Request Processor plays out the first round of encryption on the prepared picture utilizing the key relating to the Image User and sends the picture to the Access Requester module.

IV. METHODOLOGY

A. Algorithm

The algorithm used for proposed framework is as follows: Key Generation Algorithm, Shamir Secret Sharing Algorithm, Hash Key Algorithm.

1) Key Generation Algorithm: In cryptography, encryption is the way toward encoding a message or data such that exclusive approved gatherings can get to it and the individuals who are not approved can't. In an encryption conspire, the proposed data or message, alluded to as plaintext, is scrambled utilizing an encryption calculation a figure producing ciphertext that must be perused if decoded. An encryption plot ordinarily utilizes a pseudo irregular encryption key created by a calculation.

Step 1: The KMA runs the initialization algorithm in order to generate public parameters Params and a master secret key set MSK. It takes as input a security parameter k and generates two prime numbers p and q of bit-length k. It computes n = pq.

Step 2: KeyGen(M SK, i). The KMA runs the key generation algorithm to generate keying material for users in the system. For each user i, this algorithm generates two key sets K U i and K S i by choosing a random x i1 from [1, n 2 /2]. Then it calculates x i2 = x xi1 , and transmit.

The server adds K S i to the Key Store as follows: K S K S K S i .

Step 3: ClientEnc(D, K U i). A user i runs the data encryption algorithm to encrypt the data D using her key K U i . To encrypt the data D Z n , the user client chooses e 1 , e 2), a random r [1, n/4].
Step 4: ServerReEnc(E i (D), K S i).
The server re-encrypts the user encrypted data E i (D)= (e 1 , e 2).It retrieves the key K S i corresponding to the user i and computes the reencryptedciphertext E(D) = (e 1 , e 2). Step 5: ServerSum(E(D 1), E(D 2)). Given two encrypted val- ues E(D 1) = (e 11 , e 12) (where e 11 = g r 1 and e 12 = g r 1 x .(1 + D 1 n) and E(D 2) = (e 21 , e 22) (where e 21 =g r 2 and e 22 = g r 2 x .(1 + D 2 n)), the server calculates the encrypted sum E(D 1 + D 2) = (e 1 , e 2).

2) Shamir Secret Sharing Algorithm: Secret sharing isa strategy for securing delicate information, for example, cryptographic keys. It is utilized to disperse a mystery incentive to various parts shares that must be consolidated together to get to the first esteem. Mystery sharing is utilized as a part of present day cryptography to bring down the dangers related with bargained information. he first mystery sharing plans were proposed by Shamir and Blakley.
Definition: Let s and t be two values and [s] = [s 1 ,...,sn] and [t] = [t1 ,...,tn] be their shares. A secret sharing scheme is (Ł , Ł) - homomorphic if shares [(s 1 Ł t) ,...,(sn Ł t)] uniquely determine the value s Ł t
Data : Input file S to share.
Result: Three Shares S1,S2,S3 of same size as the original file.
Choose a field Zp where p= 257.

while not at end of the input file do
s =read byte(S) // read a byte or pixel if s == 0 then s = 256

end
a = sp 13 //find cube root of s
r =random(257) // random number between 0-256
s1 =r a mod p // s1 is the share1 pixel
if s 1 == 256 then s1 = 0
end

s2 =r2 a mod p // s2 is the share2 pixel if s2 == 256 then s2 = 0 end
s3 = r4 a mod p // s3 is the share3 pixel if s3 == 256 then

s3 = 0
end
end

3) Hash Key Algorithm: A hash work is a scientificcapacity that changes over a numerical information value into another compacted numerical value. The contribution to the hash work is of subjective length however yield is dependably of settled length. Hash work use for the secret word.

The Secure Hash Algorithms are a family of cryptographic hash functions. It works by changing the information utilizing a hash work: a calculation that comprises of bitwise activities, measured increases, and pressure capacities. The hash work at that point creates a xed estimate string that looks not at all like the first. These calculations are intended to be one way works, implying that once they are changed into their individual hash esteems, its essentially difficult to change them over into the first information. A couple of calculations of intrigue are SHA-1, SHA-2, and SHA-5, each of which was progressively composed with progressively more grounded encryption in light of programmer assaults. SHA-0, for in-position, is currently out of date due to the broadly uncovered vulnerabilities.A regular utilization of SHA is to scrambling passwords, as the server side just needs to monitor specic clients hash esteem, as opposed to the real watchword. Figure shows hash function diagram.

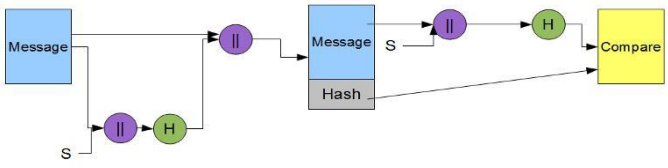

Fig. 2. Basic Hash Function

V. PROBLEM FORMULATION

A. Mathematical Model

Let system S can be dened as, S=I,O,K,P,Eo,Ev, Scale,Crop
I=Set of Input images I=I1,I2,I3,....,In
O=Set of Output images O=O1,O2,O3,....On
k=Set of user/server keys
K=(Uk1,Uk2,...Ukn)(Sk1,Sk2....Skn)
E0= Set of image outsources Encryption Images
E0=E01, E02.....E0n
n=Number of Images
Es= Set of image Encryption on cloud server
Es=ES1, ES2,....Esn

scale= Scale Parameters Crop=Set of cropping Parameters
Function f1- function f1 generate user side and server side Encryption key
f1()- (Uk1,Uk2,...Ukn)(Sk1,Sk2....Skn) (UK,SK)
function f2- function f2 read Imge from image outsources and perform per tile encryption.
f2(I)- I1,I2,I3,....,In-(E(I1)Uk1, E(I2) Uk2) E0
function f3- function f3 generate Image specic Access Policy
f3(I)- (I1,I2,I3,....,In)- (P1,P2,P3,...PN) p

f4- This function read Encrypted outsources Image data and perform server side encryption.

f4(E0)- (E(I1)Uk1, E(I2) Uk2)Sk1 E(E(I2)Uk2)Sk2 ES
function f5- This function read Image Scaling / Cropping parameters and per-form operations
f5(Scale, Crop)- (ES (I),Scale, Crop)- (O1,O2,O3,....On) 0
function f6- This function apply server-user key on output and decrypt Image
f6(Sk,0)-((O1)Sk1 (O2)Sk2)- (EI1,EI2)

function f7- This function apply user key on decrypted Image to get back normal Image
f7(EI1,Uk)- (E(I1)Uk1, E(I2) Uk2.....) I
I= set of output scale/ crop Image.

VI. CONCLUSION

The system discusses various techniques for providing im-age security in cloud. In our research, we have proposed the use of 2D crypt technique for performing various operation such as scaling, cropping etc over encrypted images. The system identied the problem area where there is need to nd solution with different methodology with different features. In this report, we have described the challenges of scaling and cropping over encrypted image by using Shamir Secret algo-rithm and this algorithm provides token for security purpose and also avoid the data duplication.

ACKNOWLEDGMENT

I would sincerely like to thank our Head of Department Prof. (Dr.) Amol D. Potgantwar, Computer Engineering, and Professor Namrata D. Ghuse, Department of Computer En-gineering, SITRC, Nashik for their guidance, encouragement and the interest shown in this project by timely suggestions in this work. His expert suggestions and scholarly feedback had greatly enhanced the effectiveness of this work.

REFERENCES

[1] ManoranjanMohanty, Muhammad RizwanAsghar and Giovanni Rus-sello, 2DCrypt: Image Scaling and Cropping in Encrypted Domains, IEEE Transaction on Information Forensics and Security, 2016.
[2] Mrs. JadhavRohini 1, Prof. S. A. Kahate, A Survey on: A ModiedPaillier Cryptosystem-Based Image Scaling and Cropping Scheme, IJARIIE, 2016.
[3] K. Kansal, M. Mohanty, and P. K. Atrey, Scaling and cropping of wavelet-based compressed images in hidden domain, International Conference on Multimedia Modeling, vol. 8935, pp. 430441, 2015.
[4] J. Yuan, S. Yu, and L. Guo, SEISA: Secure and efcient encrypted image search with access control, in IEEE Conference on Computer Communications, pp. 20832091, 2015
[5] W. Lu, A. L. Varna, and M. Wu, Condentiality preserving image search: A comparative study between homomorphic encryption and distance-preserving randomization, IEEE Access, vol. 2, pp. 125141, February 2014.
[6] JadhavRohini, B. S. Kurhe, Two Dimensional Cryptography Using Modied Pallier Cryptosystem, International Journal of Innovative Re-search in Computer and Communication Engineering, May 2017.
[7] Mrs. JadhavRohini, Prof.S.A.Kahate, Image Scaling and Cropping Scheme using Two Dimensional Cryptography, International Journal of Research in Advent Technology (IJRAT), February 2017.
[8] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signa-tures and public-key cryptosystems, Communications of the ACM, vol. 21, pp. 120126, February 2016.
[9] Jiawei Yuan*, Shucheng Yu*, LinkeGuoy, SEISA: Secure and Efcient Encrypted Image Search With Access Control, IEEE Conference on Computer Communications (INFOCOM), 2015.
[10] M. Mohanty, W. T. Ooi, and P. K. Atrey, Scale me, crop me, know me not: supporting scaling and cropping in secret image sharing, in Proceedings of the 2013 IEEE International Conference on Multimedia Expo, San Jose, USA, 2013.
[11] Chao-Yung Hsu, Chun-hien Lu, and SooChang Pei, Fellow, Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT, IEEE, NOVEMBER 2012.
[12] Cong Wang, Ning Cao, Jin Li, KuiRen, and Wenjing Lou, Secure Ranked Keyword Search over Encrypted Cloud Data, International Con-ference on Distributed Computing Systems, 2010.
[13] Muhammad RizwanAsghar, Supporting Complex Queries and Ac-cess Policies for Multiuser Encrypted Databases, CCSW13, November 8, 2013.
[14] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, Image feature extraction in encrypted domain with privacy preserving SIFT, IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 45934607, 2012.
[15] M. Naehrig, K. Lauter, and V. Vaikuntanathan, Can homomorphic encryption be practical? in Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, pp. 113124, 2011.
[16] Sun, A blind digital watermarking for color medical images based on PCA, in Proceedings of the IEEE International Conference on Wireless Communications, Networking and Information Security, Beijing, China, pp. 421427, August 2010.
[17] C. Gentry, A fully homomorphic encryption scheme, Ph.D. dissertation, Stan-ford University, Stanford, USA, 2009.
[18] T. Bianchi, A. Piva, and M. Barni, Encrypted domain DCT based on homomorphic cryptosystems, EURASIP Journal on Multimedia and Information Security, vol. 2009, pp. 1:11:12, January 2009.
[19] N. K. Pareek, V. Patidar, and K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, vol. 24, pp. 926 934, September 2006.
[20] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, Improved proxy reencryption schemes with applications to secure distributed storage, ACM Transactions on Information and System Security, vol. 9, pp. 130, February 2006.
[21] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, Public key encryption with keyword search, in Advances in Cryptology Eurocrypt, pp. 506522, 2004.
[22] C.-C. Thien and J.-C. Lin, Secret image sharing, Computers and Graphics, vol. 26, pp. 765770, October 2002.
[23] D. X. Song, D. Wagner, and A. Perrig, Practical techniques for searches on encrypted data, in IEEE Symposium on Security and Privacy, pp. 4455, 2000.
[24] P. Paillier, Public key cryptosystems based on composite degree residu-osity classes, in Advances in Cryptology EUROCRYPTx, vol. 1592, pp. 223238, 1999.
[25] J. Benaloh and D. Tuinstra, Receipt-free secret-ballot elections (Ex-tended Abstract), in Proceedings of the Twenty-sixth Annual ACM Symposium on Theory of Computing, pp. 544553, 1994.
[26] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in Advances in Cryptology, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, vol. 196, pp. 1018, 1985.
[27] Goldwasser and S. Micali, Probabilistic encryption, Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270299, 1984.
[28] A. Shamir, How to share a secret, Communications of the ACM, vol. 22, pp. 612613, November 1979.

Namrata D. Ghuse, Assistant Prof, SITRC, Nashik
Kalyani J. Patil, PG Student, SITRC, Nashik,