Abstract— a model, in which user can

Abstract— Securing data is major issue in this digital world. Biometric identification suffers a lot ofproblems such as storage of user’s template, leakage of privacy data of userand the major main problems is security problems . It is simple to provide asecurity from the external hackers but the major problem is to provide thesecurity for the data from internal hackers . The proposed system is to protectthe encrypted data to the internal hackers in the Cloud services.

Keywords— Cloud Computing, Cryptography, Security, Finger-print.

I. Introduction Security is the one of the keyissues that interrupts the growth of cloud. Cloud Computing is an advancesprototype of distributed computing. 79% of all internet users have stored datain online. The data stored in cloud may be a sensitive data. There are securityissues in the storing data in the cloud. We propose a model with the biometriccryptography on the client side.

This can reduce the security issues in the cloud. According to the recent cloud security alliance report, insider attacks are theone of the biggest thread in cloud computing 1. Cloud service providers protect theircustomer data only from the external attackers but they cannot protect the datafrom inside attackers. Here we introduce a model, in which user can encrypttheir data on client side. So the encrypted data is send to the cloud, furtherencryption may be or may not be done at cloud. Now, the data is protected fromboth internal and external attackers. The data encrypted by the public key onlyencrypts the use of private key and contrary. There are also various asymmetricencryption algorithms such as RSA, which have shown good performance directlyon encryption and handling and the ability to withstand attacks6.

II. Literature SurveyThe existing system in thebiometric encryption does not provide the security about the encrypted data tothe internal hackers. In the existingsystem work, all the encrypted data are stored directly to the cloud withoutany security. Thus the unsecured encrypted data can be easily stealing theuser’s privacy easily. Thus the internal hackers steal the user’s privacywithout any authentication of the corresponding user. The major problem in theexisting system is that they cannot give any kind of solutions to the securitythreat from the internal users.

Fingerprint features are used most of times. Efforts were made to separate the uniqueness of these biometric features andcreate a unique key 2. In finger print, the integrated set of ridge endingsand backorders creates minutiae. These minutiae can be of different types. Finally, a 256-bit secured encryption key is created in many biometric templates.

Similarly, the fingerprint image was used to create the keys as in 3, 7. RSAalgorithm is efficient because it is difficult to enumerate all bit of RSA module, if some one want toenumerate all 1024 bit he/she would need 5. 95×10211 years.

III.

Pre-RequisticsThe pre-defined techniques and information used in RSAand Fingerprint combination of key generation algorithm is given below. 1. Fingerprint Extraction and ArrayGeneration: The features listed below for each pre-processed imageare extracted, and feature integration features are stored in an array. · Ridge ending points· Ridge bifurcationpoints· Isolated points· Crossover points2. Terms of Array: ME: Minutiae point array for Ridge Endings. MB: Minutiae point array for Ridge Bifurcations. MI: Minutiae point array for Isolated Points. MCP: Minutiae point array for Crossover Points.

3. Advantage or Standard of Fingerprint:§ Easily distinctionbetween the valid user and other, because fingerprint is unique.§ Fingerprint isresistance to ageing.

§ No fingerprint arealike , even identical twins have their own fingerprint. 4. Image Acquisition and Preprocessing: Imageare resized to 255x255px and following algorithms are described in 2, 5, 7, 8, 9.

· Histogram Equalization : Histogram Equalization enhancesthecontrast of the fingerprint imagesat the place where the ridges are not very important. The basic idea here is tofind gray levels based on the probability distribution of input gray size. Itthe intensity of image is transformed given by the equation. Sk= T(rk)=? Pr (rj)= ? nj /n forj= 1.. k.

where Sk is theintensity value in the processed image, rk is the intensity value in theinput image.· Noise Removal: Median filter, Weiner or Gaborfilter areused to remove noise in the fingerprint image. Thiseliminates the noise in the image and removes the rated noise to get a clearimage.

· Binarization: In this phase the gray scale imageisconverted into binary image. Binariztionis done by considering mean of all neighboring pixels around the each pixel. Ifthe intensity of the pixel is greaterthan mean value then that pixel is assigned to value 1 otherwise 0. It reduces the complex fingerprintrecognition to a point pattern matching problem.

· Thinning: This operation is to get the finalimage witha width of single pixel. Theresultant image is the skeleton structure of the image.

IV. Proposed SystemThe proposed system of thebiometric encryption is provide security to the internal hackers of the cloud. So the original data has highly secured with the help of the user'sfingerprint. First the user's data can be encrypted with their correspondinguser's fingerprint identification. Next that the encrypted data is send to theCloud via Internet . Thus the internet having the external hackers their try tohack that user's data.

But the user datahas been protected already with the corresponding user's fingerprint. Then theencrypted data is then sent to the cloud encryption . In the cloud, encryptionis done in the already encrypted data for the second time. This cloudencryption is only providing security to the external hackers.

But in thecloud, there will be internal attackers to steal their user contents. Internetattackers only decrypt the cloud encryption but still there is user endencryption is present. So the proposed system is to provide very high securityto the user's data, without the authentication (fingerprint) of legitimate userno one cannot decrypt the original or encrypted data. 1.

DATA FLOW DIAGRAM: FIG. 1: DATA FLOW DIAGRAM This flowdiagram shows the flow of system and explain how system is work? User want tostore his/her data in cloud, he/she must encrypt the data using thefingerprint. Here the scanner scan the fingerprint and preprocessing offingerprint image is done. By collecting minutiae, Ridge ending point, Ridge bifurcationpoints, Isolated points, Crossover point in a Common Array. Using this array, Encryption and Decryption keys are found using the RSA algorithm. Encryption isdone on the user data.

Similarly decryption is also done using this key whichis generated by the fingerprint. Thusthe user data is secure from the both internal and external attackers. 2. MODULES: There are threemodules in this system.

They are · Fingerprint KeyGeneration· Encryption of userdata· Decryption of userdataEach of the modules is explainedbelow. i. FingerprintKey Generation: In this module, encryption keyis generated using fingerprint and RSA algorithm6. FA= RE+ RB+ RIP+ RCP, where FA is an array which holds the RE, RB, RIP, RCP.

Shuffling of individual feature array : For allthe FA arrays, apply the algorithm as stated:§ Create a Array R of size equalto selected FA Array.§ Calculate seed value S as: S= next_prime(Sx)*next_prime(Sy); § For j= 0 to (size_of_FA-1), Use arandom number generator with seed value ‘ S’. Rj= random_number(S).§ For i= 0 to (size_of_FA-1), do CalculateTX and TY as: TX= xval_FAi*RiTY= yval_FAi*R(size_of_R)-i.

Calculate Ri = (TX+TY) mod S. § Merge all R arrays to create anew array FR.§ Remove all duplicate elementsfrom FR.

Creating KEY generation Array: Create a key array K, of Size of1024For i= 1 to 1023¨ Select a elementrandomly from FR array and check if it is present in K array.¨ If the selectedvalue presented in K array then skip the element , Else, insert selectedelement in K array. Final key Generation: Create an array FK(Fingerprintkey) of size 1024 .

For i= 0 to 1023¨ FKi= Kimod2¨ Consider the valuesin array as bits and the array index as bits position and convert it into hexvalues Thisflow diagram show how the key is generated by the fingerprint. RSA Key Generation: From the array FK, the key pair for RSA Encryption andDecryption generated are as follows: 1) Create two empty arrays FKP andFKQ of size 512. 2) Insert values of FK from index0 TO 511 in FKP and 512 to 1023 into FKQ. 3) Convert these array values todecimal values FKPD and FKQD by considering the values in arrays as bits and the array indexes as bitsposition. 4) Calculate p and q as: p= next_prime(FKPD). q = next_prime(FKQD). 5) Calculate n= p*q.

6) Calculate (n) = (p-1)(q-1). 7) For i= 255 to 1023Calculate Temp= FKi+512*2 +FKi+511*2 +…..

+FKi+1*21 +FKi*20 . Calculate e= next_prime(Temp). If (e

The above generated keys (e, n), (d, n) can now be used forRSA encryption and decryption respectively. ii. Encryption of user data: Before taking backup into cloud, the user data file (itcan be any form like text , picture , video , graphics) aregoing to encrypt with fingerprint through a mobile application. Thisapplication generate the key using he fingerprint of user who want backup theirfiles in cloud . The generated key is given as input to encryption algorithm. This encryption algorithm takes the key which is generated from fingerprintscanner as input.

This encryption algorithm encrypts the data into some otherform. Output of the algorithm produces a data which cannot be understood byanyone. These output files are collectively stored under a folder and the datain the folder is send to the cloud in name of backup. Thisflow diagram show how the encryption is done on user data. Input of this moduleis fingerprint image after performing preprocessing stages.

Output of this moduleis data file which is not understandable, i. e. encrypted data. iii. Decryption of user data: Input is given as Data which isalready encrypted byuser Fingerprint key is retrieved from cloud . Output isgiven produced as user data. The data which is retrieved from cloud is storedin a folder, decryption is done using the fingerprint of the legitimate user.

Here attackers or some other person want to decrypt the data decryption is doneby using attacker fingerprint, but original data is still encrypted. In eitherway output is generated but only the valid user obtains the original data whathe/she encrypted. Mathematical key which is generated cannot be stolen byattackers.

Thisflow diagram show how the decryption is done on data which is retrieved fromcloud . Input of this module is already encrypted data by this system. Outputof this module is data file, i. e. user data.

CONCLUSION Thispaper describes a method for securing the user data from the external as wellas internal attackers by generating the key from fingerprint using RSAalgorithm. Privacy of user is highly protected in cloud. The FK array can beused as large random number for various cryptographic algorithms which needlarge random keys.

futureenhancement This system is implemented on smart phones to secure thedata which is stored in it.

It can beimplemented where the user need highsecurity