SECURE CANCELABLE BIOMETRIC BASED GROUP KEY GENERATION SCHEME USING HOMOMORPHIC ENCRYPTION

[1]Kimee Joshi, [2]Payal Chaudhari
[1]PG Scholar, [2]Lecturer
[11]Department of computer engineering,
[1] LDRP-Institute of technology and Research, Gandhinagar, India.

Abstract: In the traditional cryptography, key is generated randomly and it is very difficult to remember, hence, stored in smart card, tamper-resistant token, etc. or password based authentication method is used to control the access of cryptographic key. But these user selected key sometimes lost or guessed by dictionary attacks. Therefore biometric keys are proving to be better alternative to these non-memorable passwords. But the problem with biometrics is that once it gets compromised it cannot be reused. As a proficient solution for this problem, cancelable biometrics has been proposed. Cancelable biometric refers to the intentional distortion of biometric feature. In this paper,we present a cancelable biometrics based group key generation. The Proposed algorithm facilitates to update the key when the number of members are added in or revoked from group.We aim to use Homomorphic encryption for group key generation.

***Keywords*- Biometric, Symmetric cryptography, cryptographic key generation, cancelable template, Minutia extraction, Group Key Generation**

I. INTRODUCTION

Security is the most important aspect in the field of internet and network application. It is an essential task to secure information over the network. Cryptography is a useful mechanism to secure the information.

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being.[1] In other words, Biometric system is a method of extracting unique human identity feature and verification of this identity for reliable user authentication.[2]

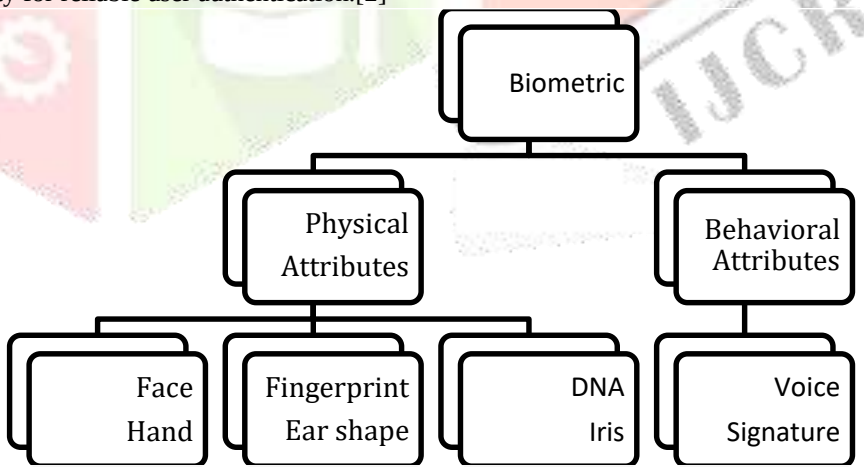

Figure 1: Classification of Biometric

Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. [3] This is a method of enhancing the security and privacy of biometric authentication. Example, Instead of enrolling with a true finger (or other biometric), the fingerprint is intentionally distorted in a repeatable manner and this new print is used. If, for some reason, the old fingerprint is stolen then a new fingerprint can be issued by simply changing the parameters of the distortion process.

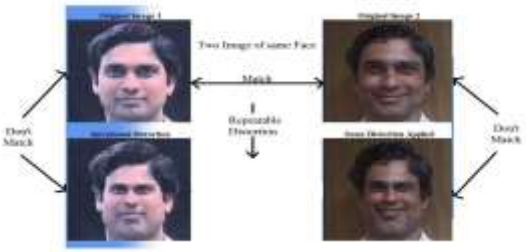

Figure 2: An Example-Cancelable Biometric [4]

II. RELATED WORK

There are existing schemes which provide cancelable or non cancelable biometric based key generation.

In [2] Indu et al proposed a scheme for generating biometric key using traditional algorithms like MD5 and SHA.Two cryptographic keys of size 128 bits and 512 bits are generated using Hash Function.The key generated by algorithms are compared on two factors like entropy and key space.SHA-12 approach can be used to generate more secure biometric key than MD5 Algorithm.

In [5] Arpita et al.proposed a scheme for generating a cryptographic key that is non invertible and tracing any user's fingerprint from the cryptographic key is not feasible. so this approach is free from the identity threat. An approach is to generate and share cryptographic key from the fingerprint features (minutiae points) of sender and receiver. Both sender and receiver generate cancelable template from their own fingerprint and share it with each other. From both cancelable templates, a combine template is generated and finally the symmetric cryptographic key is generated from the combine template.

In [6] Gaurangkumar et al. Proposed a scheme for generating biometric cryptography key from the fingerprints captured from different scanners with different quality of image. Using this fingerprint, they extract the minutiae points as a feature vector and generate a biometric based cryptographic key. Using this biometric-based cryptographic key,they encrypt the user's data. To decrypt the message, capture the biometric fingerprint (i.e. fingerprint data) of the user and generate a biometric-based cryptographic key from the fingerprint.

In [7]Subhas el al proposed an option to revoke cryptographic key.If the key is compromised by the attacker,he is not able to know about the finginerprint data from the key.If the biometric data becomes compromised by a third party,he is not able to generate the same key from the fingerprint.This approach involves mainly three subsections, namely, Feature extraction, template generation and key generation.

In [8] Aditi et al propose an effective scheme that has zero False Acceptance Rate and 15% False Rejection Rate over the different data set. First stable minutiae points extracted for the generation of secure key, secured one way functions are used. From this scheme, it is possible to generate a random key of size 512 bits, whose every bit is a function of the entire set of stable features, which can be compressed to 128 bits (requirement of AES).

In [9] Padma et al have presented a new cancelable biometric template generation algorithm using random projection and transformation based feature extraction and selection. Using cancelable biometric template achieved performance is better than the original template.

OUR CONTRIBUTION

All these existing scheme have provided cancelable or Non-cancelable biometric key generation. All of them have presented the key generation for two party communication.None of them have addressed multiparty key generation. In our current work we address this issues. Our proposed scheme facilities a group key generation from cancelable biometric template.The Scheme also supports dynamic group size.

III. PROPOSED METHOD

In this present work an approach is proposed to generate and share cryptographic key from the fingerprint features (minutiae points) of multiple user. All Users generate cancelable template from their own fingerprint and Encrypt it with group owner's public key to share it with Group Owner. After receiving Encrypted cancelable template Group Owner apply additive homomorphic encryption and generate combine Encrypted cancelable templates and finally the cryptographic key is generated from the template. An overview of the approach is shown in Figure 3

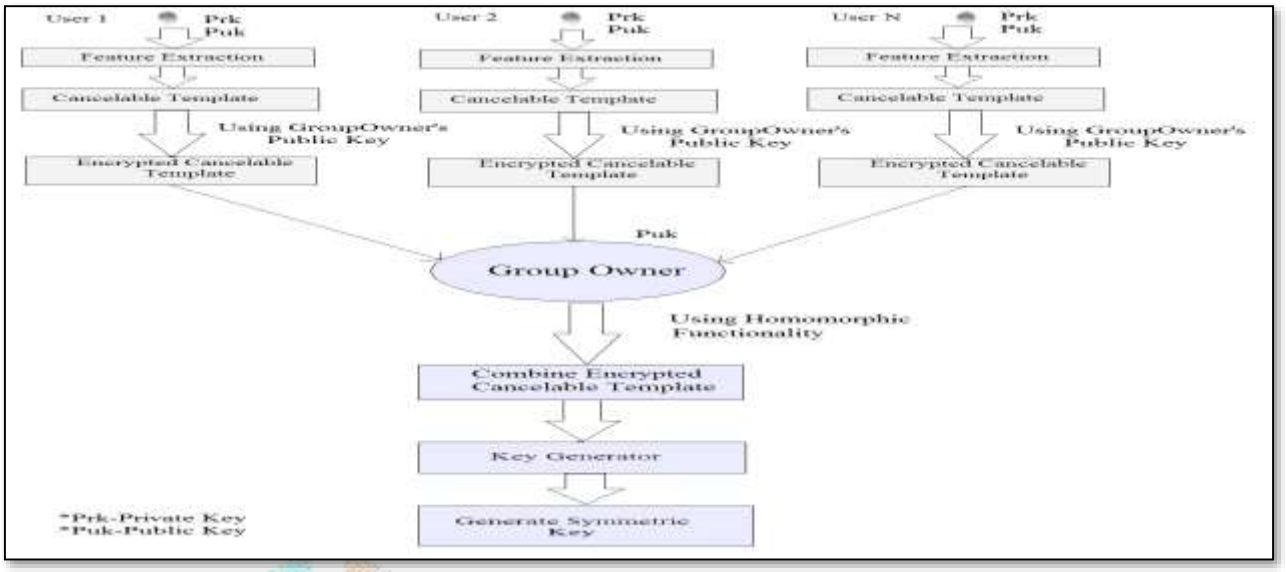

Figure 3: Proposed System Model (a)

Once Group Key is generated and if another user wants to join Group. The whole process of encryption is not repeated for new user. Directly add the user's Encrypted cancelable template with combine If a revocation occurs then,revoked user's template is removed. Encrypted Cancelable template as shown in figure4.

3.1 The Different tasks involved in this approach are discussed in the following:

1. Generation of private and public key
2. Feature Extraction from Fingerprint
3. Cancelable Template Generation
4. Encryption of Cancelable Template & Share
5. Apply Additive Homomorphic Encrytion on Template & Key Generation
6. Share the Key

3.1.1 Generation of private and public key

Public Key & Private key of each user is generated by using any efficient public key encryption algorithm such as RSA(Rivest-Shamir-Adleman)

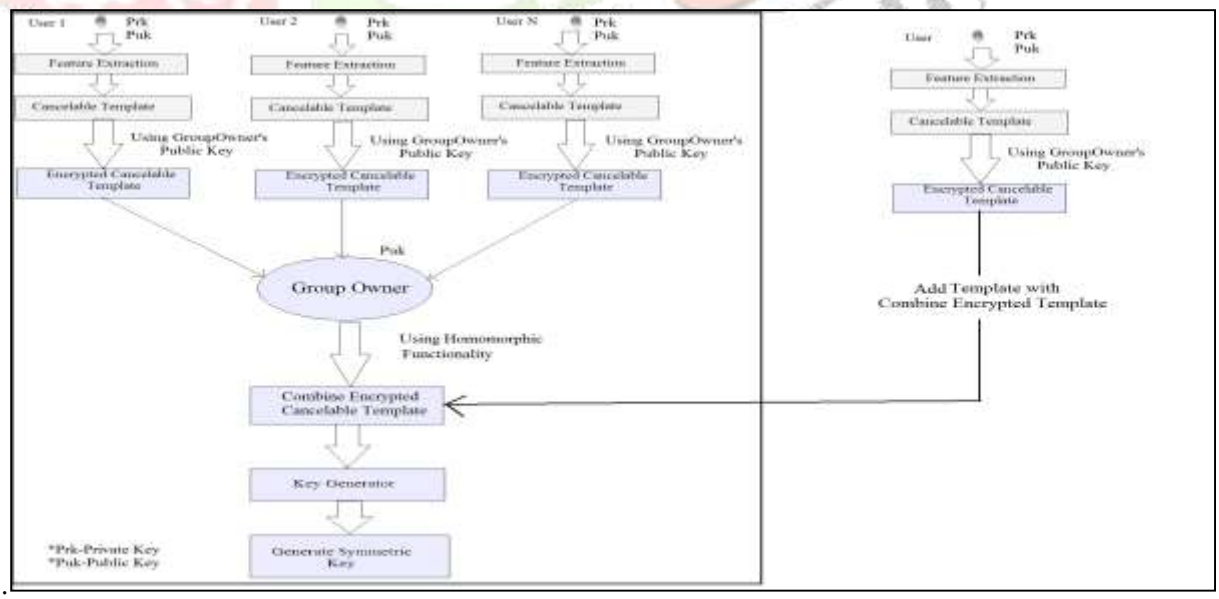

Figure 4: Proposed System Model (b)

3.1.2 Feature Extraction from Fingerprint of User[5]

In this approach minutia points are extracted from the given fingerprint image of sender and receiver. The steps involved in minutia extraction are as follows:

a) Image Binarization:-

Image Binarization convert grayscale image into binary image.One can choose a threshold value and choose all the pixels above that value as white and below that value as black. This process is one of the simplest for Binarization.

b) Thinning:-

Thinning plays a important role.Thinning is used to remove selected image from binary sources and is particularly used for skeletonization. All lines will be reduced to a single pixel thickness. It reduces amount of data to be processed and Reduce time.

c) Minutiae Extraction:-

Minutiae points are extracted from the fingerprint image. Bifurcations, ridge ending and other features are found in this method. This algorithm returns (x, y) as a minutiae point where (x, y) denote(x, y)-coordinate value. Figure Shows minutiae point. These values are stored in two vectors (X, Y). Vector Vx contains x-coordinate values and vector Vy contains y-coordinate values of minutiae points.

Vx = [xi], where i=1 to n

Vy = [yi], where i=1 to n

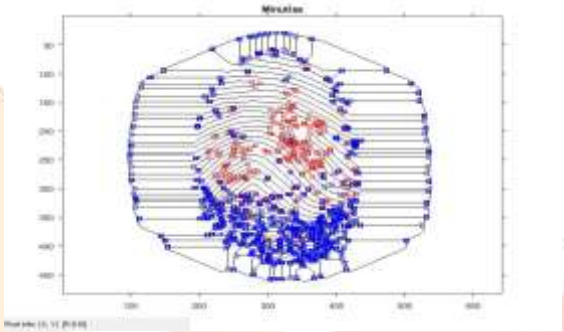

Figure 5: Minutiae Points

Fox example, assume that 8 minutiae points are extracted. Let the points be (280,113), (289,115) ,(284,120), (327,111), (332,104),(358,91), (360,86), (352,81)

Then X and Y are:

X:	280	289	284	327	332	358	360	352
	1	2	3	4	5	6	7	8
Y:	113	115	120	111	104	91	86	81
	1	2	3	4	5	6	7	8

Figure 6: X and Y coordinate values

3.1.3 Cancelable Template Generation

In this step the fingerprint template of the user is transformed into non-invertible forms, called cancelable template. This is because if the original biometric data is compromised, the biometric traits will be useless. So, it is required to convert the irrevocable biometric data into revocable one before it is use in cryptography. The process is as follows: From the X and Y arrays generated in previous step, a template is created.The template array is of 128 elements. For generating this template, following steps are followed:

3.1.3.1 Create lookup table

A 128-element array of unsigned integers is created. Each element of the array will contain integer values from 1 to 2n. Let the array be R.

3.1.3.2 Fill the lookup table

Each element of the 128-element lookup table is assigned a random integer between 1 and 2n.

3.1.3.3. Create template array

A new 128-element array (T) of signed 8-bit integers is created.

3.1.3.4. Fill the template array

The template array is assigned values from X and Y arrays using the lookup table R.

The algorithm for generating cancelable template is as follows:

Algorithm 1:

Input:-
1. X : X is an array of x-coordinates of all minutiae points
2. Y : Y is an array of y-coordinates of all minutiae points
3. n : n is the number of minutiae points
The minutiae points are (X[i], Y[i])
Output:-
T : T is an array of 128 element
Procedure TRANSFORM-TEMPLATE (X, Y, n)

```
//create an array of 128 random integers in the range [1,2n]
R = new Array(128)
for i = 1 : 128
R[i] = random(1, 2n)
end for

//create an array of 128 element  to store the  transformed template
T = new Array(128)

//populate the template array
for i = 1 to 128
if R[i] <= n
T[i] = ( X[R[i]] mod 256 ) - 128
else
T[i] = ( Y[R[i] - n] mod 256 ) -128
end if
end for
return T
End Procedure TRANSFORM-TEMPLATE
```

3.1.4 Encryption of Cancelable Template & Share

Once Cancelable Template is generated, User Encrypt the own Cancelable Template using Group Owner's Public Key. For Encryption RSA Algorithm is used.

3.1.5 Apply Additive Homomorphic Encrytion on Template & Key Generation

Let the encrypted templates be T1,T2,T3,.....,Tn of 128-element arrays. A new template is created is created by using Additive Homomorphic Encryption.

Logical converts `integer` into an array of logical values. Any nonzero element of `array` is converted to logical `1` (`true`) and zeros are converted to logical `0` (`false`).

Algorithm 2:

Input:-
$T1....T_N$: An array of 128 size
Output:-
K: 128-bit integer (Symmetric key)

Procedure GENERATE-SYMMETRIC KEY ($T1..T_N$)

```
//Add the templates
 T = T1+T2+T3+.....+T_N

   //generate 128-bit key
       K= logical(mod(T,2))

      End Procedure GENERATE-SYMMETRIC-KEY
```

Once Group Key is generated and if another user wants to join Group. The whole process of encryption is not repeated for new user. Directly add the user's Encrypted cancelable template with combine Encrypted Cancelable template.

Algorithm 3:

Input:-
T: A Combine Encrypted Cancelable template of 128 size
Output:-

K: 128-bit integer (Symmetric key)
Procedure GENERATE-SYMMETRIC KEY (T,T_N)

//Add the templates
New T = $T+T_N$

//generate 128-bit key
K= logical(mod(New T,2))

//Revocation Of User
New T= T-Tx(If X user is revocke)

End Procedure GENERATE-SYMMETRIC-KEY

3.1.6 Share Key

Once Symmetric Group Key is generated Group Owner Sends the Key to all user using any encryption algorithm

IV. EXPERIMENTS

4.1 Database:

In this work publicly available fingerprint database FVC 2002 DB1 is used to generate cryptographic key.

4.2 Experimental Setup:

This work is implemented with intel®Core™ i3 processor with 1.70GHZ clock speed in MATLAB17a running with Windows10OS

4.3 Experimental Results:

For this Example, Four different fingerprint images are taken as an input fingerprint of user. The minutia points or features are extracted from the fingerprint images. By applying Algorithm 1 mentioned above on the extracted minutia points the generated cancelable template values for user is as follows –

Cancelable template of User1 (T1) : 111 106 66 -33 -126 -54 -61 8 -5 -79 -79 -53 -5 24 -56 -60 89 -22 -117 -86 -57 -19 -33 -64 -24 11 -36 30 -45 -19 35 2 -5 24 25 -19 19 -48 121 -71 -64 -60 -33 -54 121 90 -42 -47 34 -45 34 26 11 -34 66 -2 -17 26 98 103 -67 -64 -5 -64 -17 36 -7 76 7 -3 93 -7 -15 85 27 93 76 -66 105 27 87 -13 -8 16 -60 -36 -64 36 -57 114 -87 106 -87 104 -67 117 72 -15 11 8 -17 14 -34 -118 103 111 -104 -2 72 90 89 91 94 25 114 34 104 19 87 -82 41 -87 14 93 16 17 93 30

Encrypted Cancelable template of User1 : 114 349 349 349 315 349 330 282 315 282 282 315 22 102 102 315 22 349 271 282 315 22 297 239 315 22 282 349 315 57 315 22 297 315 22 200 250 315 22 200 250 315 22 297 102 315 22 297 315 271 239 315 22 297 282 315 22 282 330 315 57 250 315 22 271 271 315 22 349 349 200 315 22 57 282 315 22 297 200 315 22 349 250 315 22 102 102 315 22 282 239 315 22 271 239 315 349 349 315 22 102 282 315 102 330 315 22 239 297 315 22 349 250 315 102 297 315 271 315 22 297 315 271 239 315 271 297 315

Cancelable template of User2 (T2) : 98 -11 -10 -67 -50 -93 -60 -123 -61 30 -89 -93 124 106 104 114 113 104 3 54 -89 -1 -63 -60 97 124 -30 30 80 -14 -114 -124 -77 -100 -127 -16 -89 -15 -77 19 80 -49 16 -89 24 -6 -89 19 119 116 14 -93 95 -56 -50 92 -83 -33 -63 20 -83 76 -49 -111 -58 24 110 -21 -37 113 -21 -6 -124 24 -76 42 -6 24 -38 116 54 76 -120 -100 -36 92 -124 -52 25 80 -56 -12 -110 -10 -37 5 -69 -38 -30 110 20 -47 19 -6 104 102 -89 -16 -63 0 93 124 -58 -16 -114 116 0 103 -93 -111 51 106 109 -39 -16 -69 -127 -58

Encrypted Cancelable template of User2 : 344 304 341 261 68 197 197 261 68 197 193 261 68 384 215 261 68 40 193 261 68 304 204 261 68 384 193 261 68 197 426 204 261 68 384 197 261 204 193 261 68 341 304 261 68 304 204 261 197 426 48 261 197 193 384 261 197 193 48 261 197 197 48 261 197 197 204 261 197 193 48 261 204 261 40 48 261 68 341 304 261 68 197 261 68 384 204 261 68 384 193 261 304 215 261 197 426 48 261 68 204 193 261 204 193 261 341 193 261 68 197 48 261 68 197 197 48 261 68 197 426 48 261 68 215 215 261 68

Cancelable template of User3 (T3) : 83 124 -28 60 -7 -106 111 -98 5 -29 29 79 5 -113 -108 83 -48 23 -28 116 58 29 95 -98 56 -73 -16 23 -70 108 124 58 109 -105 -41 123 17 95 108 -44 9 -35 -98 1 -109 56 -112 -100 123 -94 -88 91 -43 2 -53 -72 119 -124 119 -38 98 -51 12 73 114 5 116 -12 -60 60 -125 -106 31 -35 -55 -65 -78 120 -44 -103 -35 -108 -78 -7 123 -6 -87 37 17 -12 -122 -10 104 -105 9 -117 9 59 102 -26 -7 108 -16 -38 -43 -103 -22 -73 -78 46 -12 120 12 -73 103 -3 -103 -96 -58 -51 -110 -39 -33 -83 -65 -19 2 -33

Encrypted Cancelable template of User3 : 148 23 255 230 400 458 358 230 243 458 23 230 384 75 230 243 319 230 243 400 75 384 230 400 400 400 230 243 63 23 230 212 230 243 458 63 230 458 63 230 319 63 230 212 230 243 400 400 255 230 243 400 75 23 230 23 255 230 243 358 23 230 458 255

230 243 458 23 230 400 400 384 230 212 23 230 458 63 230 63 212 230 243 63 23 230 212 384 230 243 319 255 230 243 400 384 230 458 255 230 243 319 75 230 400 75 23 230 400 458 358 230 212 23 230 400 75 63 230 243 400 75 212 230 243 358 400 230

Cancelable template of User4 (T4): 18 -113 43 76 61 -81 108 110 87 -33 -90 22 -69 86 21 -34 -81 6 -10 -30 -52 -6 -17 -101 -67 108 -63 -123 53 2 89 114 -34 -63 2 -34 -89 -55 75 -41 110 -41 -30 -100 -107 -35 -55 -63 -55 72 -41 -16 1 50 -6 -55 108 -114 124 76 -108 -6 -68 87 92 68 -61 21 -99 -64 89 -61 104 -109 -90 -39 14 87 30 24 50 -89 -30 65 -49 64 -58 60 -109 -33 61 -108 120 -45 -33 -101 64 26 68 123 76 87 -86 -55 21 -120 -45 89 124 -61 -34 2 122 122 45 60 123 108 -89 -113 92 14 76 26 -36 -34 -94 14

Encrypted Cancelable template of User4: 89 505 56 466 577 505 505 390 466 383 390 466 499 587 466 587 505 466 577 56 505 466 505 167 56 466 505 505 167 466 56 499 466 577 390 390 466 577 57 167 466 69 69 466 577 587 57 466 56 587 466 69 505 466 577 390 383 466 577 56 505 466 587 466 577 505 167 466 577 390 167 466 577 393 69 466 577 587 466 577 505 499 466 577 505 167 505 466 577 587 499 466 505 167 56 466 577 587 390 466 577 505 69 390 466 393 390 466 69 466 56 57 466 505 505 383 466 577 390 383 466 577 587 390 466 69 466 577

After Encryption of cancelable template the addition operation is performed.The Vaule of combine encrypted cancelable template T is as follows:

Combine Encrypted cancelable template (T) : 695 1181 1001 1306 1360 1509 1390 1163 1092 1320 888 1272 973 1148 1013 1406 914 1085 1284 999 963 1176 1236 1067 839 1272 1210 1358 613 743 1027 937 1254 1203 1254 850 1207 1554 335 858 1103 788 625 1236 977 1449 683 1424 823 1514 996 1045 799 979 1473 989 857 1171 1198 990 782 1143 1408 1004 1275 1216 1144 772 1353 1332 815 1426 1033 923 414 1059 1318 1015 1237 1259 1000 1146 1156 1216 618 883 1023 1426 897 1496 1250 1297 1061 896 956 1362 1582 1442 1221 786 1126 1299 720 926 1389 1044 776 1128 1027 1307 633 684 1189 911 1034 1277 904 1172 1003 845 1589 1015 1331 927 1239 913 1424 1190

By applying Logical Operation 128 bit key is generated.

Key : 1 1 1 0 0 1 0 1 0 0 0 0 1 0 1 0 0 1 0 1 1 0 0 1 1 0 0 0 1 1 1 0 1 0 0 1 0 1 0 1 0 1 0 1 1 1 0 1 0 0 1 1 1 1 1 1 1 0 0 0 1 0 0 1 0 0 0 1 0 1 0 1 1 0 1 0 1 1 1 0 0 0 0 0 1 1 0 1 0 0 1 1 0 0 0 0 0 1 0 0 1 0 0 1 0 0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 1 1 1 1 1 0 0

4.4 Performance Comparison with Existing approach

We Compare our work with the existing work of [5]. In [5],they have generated Symmetric cryptographic key from the cancelable fingerprint template of sender and receiver. The comparison of this approach and our proposed approach is shown in Table 1

Table 1: Performance Comparison With Existing Approach

	Existing Approach	**Proposed Approach**
No Of User	2	10
Key	Symmetric Key	Symmetric Key
Key Size	128 Bit	128 Bit
Key Operation	Concat	Addition

Performance analysis of the proposed approach is shown in Figure 7.It is observed that as we increase the number of user it increases the time.

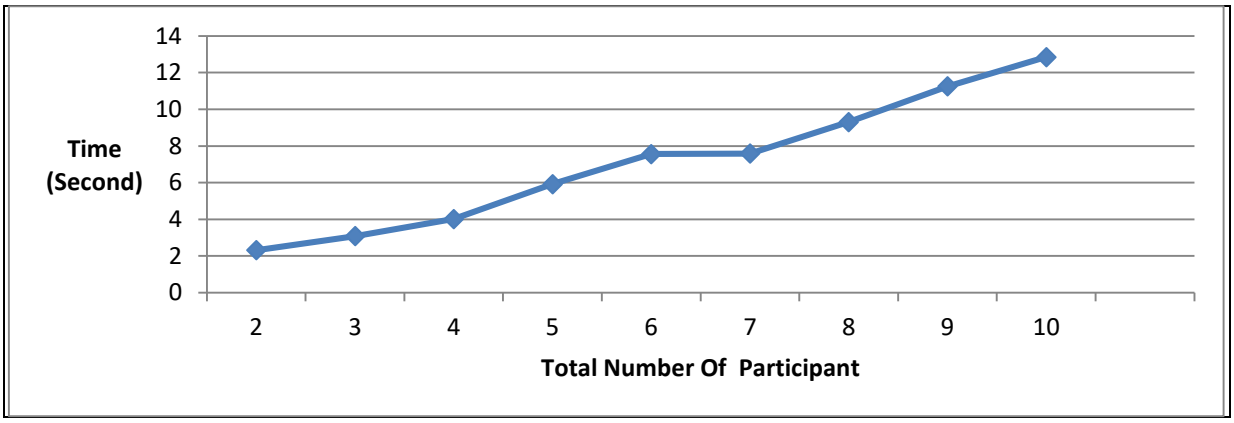

Figure 7: Performance analysis of Proposed Approach

V. SECURITY ANALYSIS

In this approach, the encrypted cancelable template are transmitted over an insecure channel and hence they can be considered as public. Here both cancelable templates are hidden with the help of encryption. Thus, the attacker will not be able to extract cancelable templates. For example when the user sends its cancelable template to the group owner using group owner's public key. The Group Owner after receiving the encrypted template decrypt it with its private key. So without the knowledge of the private key it is impossible for an attacker to get the cancelable template. In this proposed approach, User does not share their original fingerprint images or raw fingerprint features. They share the non-invertible cancelable templates of their fingerprints. The cancelable transformation used in our approach, is a one way transformation and there is no inverse transformation is possible. The cryptographic key is non-invertible and tracing any candidate fingerprint from the cryptographic key is not feasible. So the approach is free from fingerprint identity threat. The key can be generated by an attacker only when all cancelable templates are compromised. It is very difficult to compromise the all cancelable templates as they are transmitted over network after encoding. Whenever a cryptographic key is required to be updated, a new cancelable template is generated by changing the parameter of algorithm applied for generation of cancelable template. Every new cancelable template generates a new cryptographic key.[5]

VI. CONCLUSION

In traditional cryptographic approach, maintaining security of large key is important.The cryptographic keys are not linked with user, thus difficult to remember.This present work proposed an approach where the cryptographic key is generated using cancelable template of the user and generate group key .This Scheme also Support a dynamic group size.

References

[1] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar," Biometric Encryption" McGraw-Hill, (1999)

[2] Indu Verma, Sanjay Jain ,"Biometric based Key-Generation System for Multimedia Data Security"IEEE,2016

[3]https://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=1914

[4]http://www.scholarpedia.org/article/Cancelable_biometrics

[5]Arpita Sarkar, Binod Kr Singh "Cancelable Biometric Based Key Generation for Symmetric Cryptography" International Conference on Inventive Communication and Computational Technologies (ICICCT 2017) IEEE, 2017

[6] Gaurangkumar Panchal, Debasis Samanta "Comparable Features and Same Cryptography Key Generation using Biometric Fingerprint Image " International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB16) IEEE,2016

[7]Subhas Barman,Debasis Samanta, Samiran chattopadhyay "Revocable Key Generation From Irrevocable Biometric Data for Symmetric Cryptography"IEEE,2015

[8] Aditi Bhatega,Kapil Sharma,"Secure Cancelable Fingerprint key Generation"IEEE,2014

[9]Padma Polash Paul,Marina Gavrilova" Multimodal Cancelable Biometrics" Int. Conf. on Cognitive Informatics & Cognitive Computing (ICCI*CC'12),IEEE,2012