International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

# An Enhanced Cryptographic Algorithm Using Bi-Modal Biometrics

**S.Pavithra, P.Muthukannan, V.Prabhakaran**

***Abstract :*** ***A novel cryptographic algorithm, namely Significant Secure Biometric Key (SSBK) algorithm is proposed.The novel algorithm is compared with the existing cryptographic algorithms like Advanced Encryption Standard (AES), key exchange algorithm like Diffie-Helman and also with Symmetric Random Biometric Key (SRBK) algorithm, and finally we prove the proposed algorithm is superior than existing algorithm based on few parameters. A sample plain text is taken and converted to cipher text and the key from the biometric feature is used for encryption and decryption. In the key generation process, the bi-modal biometrics, namely Ear and Lip features are taken. The concatenated key values obtained from ear and lip can be of minimum 8 bits to the maximum of 1024 bits based on the type of algorithm used.***

***Keywords : Bi-modal biometrics, Ear and lip biometrics, AES, Diffie-Helman, Key generation.***

## I. INTRODUCTION

The development of communication has led in a huge amount of digital data over public shared media. Cryptography provides security for the data over the shared medium. Therefore secure transmission is important. Generally, keys are so long to remember and storing them is unsafe. So we propose a method to generate a cryptographic key using biometrics. These keys are constant throughout person lifetime. Thus, the keys square measure generated directly from biometric knowledge and it's not hold on within the info. Since it creates a lot of complexness to crack or guess the crypto keys, this approach has reduced the complicated sequence of the operation to get a crypto- keys within the ancient cryptography system. [1], [3], [4], [13],[16]

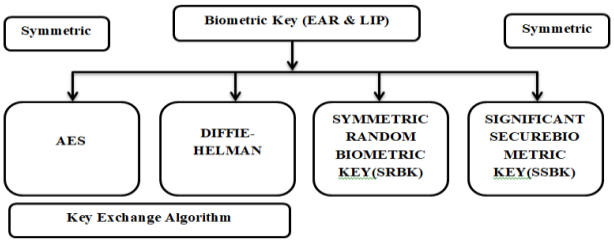



**Fig 1: Key from Ear and Lip applied to various algorithm**

**Manuscript published on 30 September 2019.**
***Correspondence Author(s)**
**S.Pavithra***, Research scholar, Saveetha Institute of Medical And Technical Sciences (SIMATS)
**Dr.P.Muthukannan**, Professor, Saveetha School of Engineeriing, Saveetha Institute of Medical and Technical Sciences
**V.Prabhakaran**, Assistant professor (G-II), Department of Biomedical Engineering, Aarupadai Veedu Institute of Technology



### 1.1. STEPS FOLLOWED FOR KEY GENERATION IN EAR AND LIP BASED BIOMETRICS

a) Input image –A sample image is taken.
b) Converting the image from the RGB form to a GRAY form.
c) Filtering- Various frequency domain filters are applied to analyze the performance of noise removal.
d) Enhancement- The better filtered image is taken for further process such that even tone is maintained Throughout (Tonal regularization)
e) Image reshaping- Adjusting the mean value of the pixel.
f) Extraction- Concentrating on a particular area on the image.(Viz Concha of the Ear)
g) Concatenation- Calculating the gradient using Prewitt's operator.
h) Gradient image-
i) Sorting- Re arranging the pixel value for generating the binary key.
j) Key generation. [10]
k) After performing the above process, the binary value is obtained from Ear and Lip biometric feature. The 8 -bit binary value is shown below:


**Fig 2: Eight bit key from EAR**

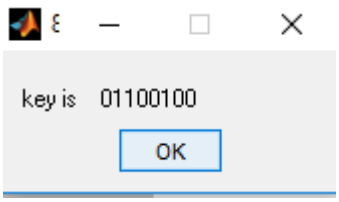



**Fig 3: Eight bit key from LIP**

## II. AES ANALYSIS

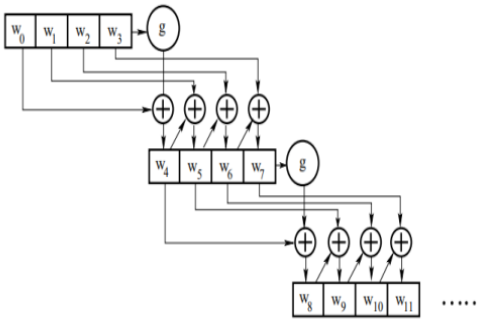
i. AES is based on block cipher with length of 128 bits.[15]
ii. AES takes into account three distinctive key lengths: 128, 192, or 256 bits.[5]
iii. Encryption comprises of 10 rounds of preparing for 128-bit keys, 12 rounds for 192- bit keys, and 14 rounds for 256- bit keys.[6]
iv. Except for the last round for each situation, every other round are indistinguishable [2]

$$\begin{bmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{bmatrix}$$

$$\Downarrow$$

$$\begin{bmatrix} w_0 & w_1 & w_2 & w_3 \end{bmatrix}$$

**Fig 4: Key representation as words in AES [2]**



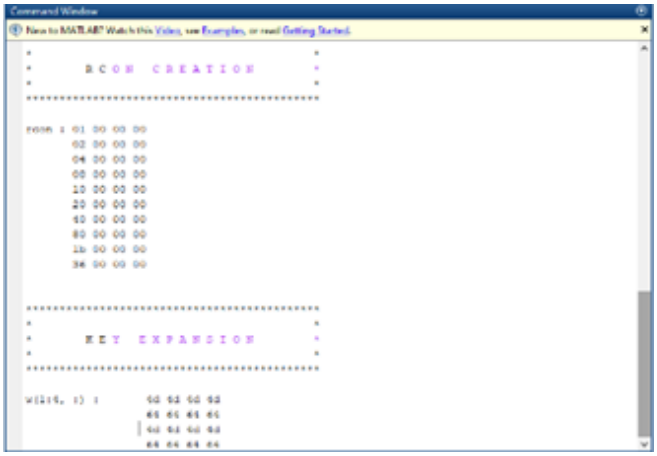




**Fig 6: Concatenated key (Ear and Lip) used in AES for Pre-round**

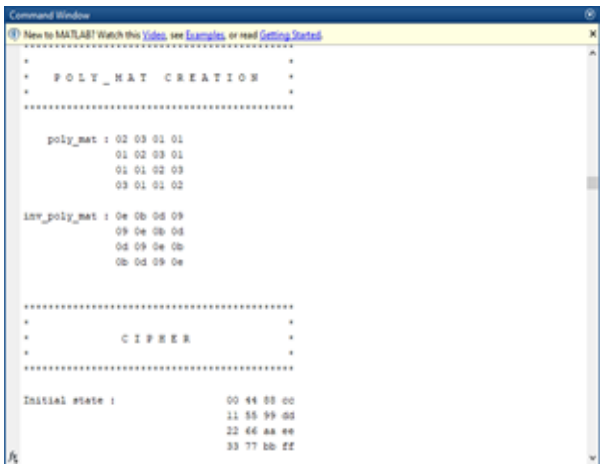



**Fig 7: Sample data taken for encryption**


**Fig 8: The Key at the end of encryption and cipher text**

*Retrieval Number: K18700981119/19©BEIESP*
*DOI: 10.35940/ijitee.K1870.0981119*
*Journal Website: www.ijitee.org*



*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

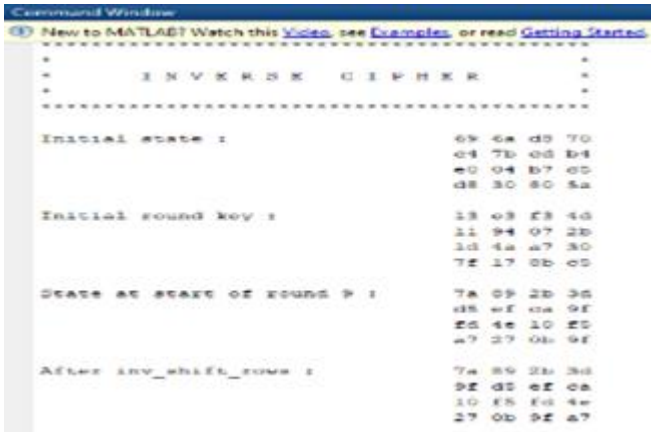



**Fig 9: Decryption process- key and cipher text to plain text conversion**

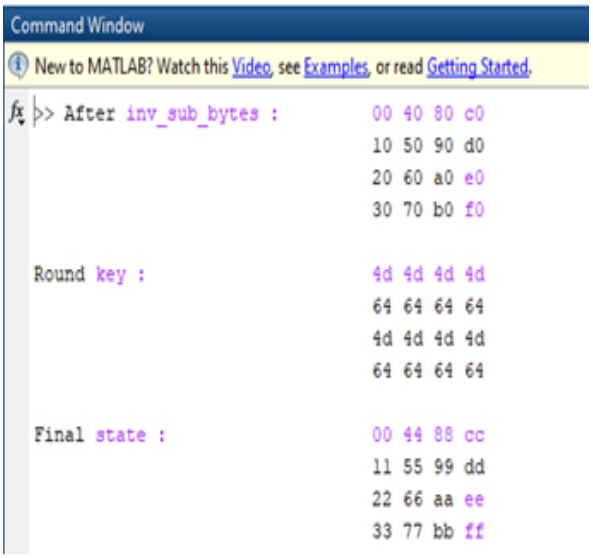



**Fig 10: Final, key and plain text at the end of decryption**

## III. THE BIOMETRIC KEYS IN KEY EXCHANGE ALGORITHM- DIFFIE-HELMAN ALGORITHM

***Step 1***: USER A and USER B selects a random number 11 (q=11)

Select α such that it should be a primitive root of q.

Considering α=2.

***Step 2:*** USER A selected a private key $X_a$ = 9(00001001)- (Ex: KEY OBTAINED FROM EAR FEATURE) and

USER B selected a private key $X_b$ = 5(00000101)- (Ex. KEY OBTAINED FROM LIP FEATURE)

***Step 3***: USER A and USER B computes public values,

USER A: $Y_a = \alpha^{X_a} \bmod q$

=2^9 mod 11

=512 mod 11

**= 6**

USER B: $Y_b = \alpha^{X_b} \bmod q$

=2^5 mod 11

=32 mod 11

**$Y_b$ = 10**

USER A = {PUBLIC KEY, PRIVATE KEY } = {6,9}

USER B = {PUBLIC KEY, PRIVATE KEY} = {10,5}

***Step 4***: USER A and USER B exchange public numbers,

***Step 5:*** USER A receives public key $Y_b$= 10 and

USER B receives public key $Y_a$ = 6

***Step 6***: USER A and USER B compute symmetric keys

USER A: $K = Y_b \wedge (X_a) \bmod q$

= (10) ^ 9 mod 11

=10

USER B: $K = Y_a \wedge (X_b) \bmod q$

= (6) ^ 5 mod 11

=10

***Step 7***: K=10 is the shared secret.

## IV. THE PROPOSED ALGORITHM IS ALSO COMPARED WITH SYMMETRIC RANDOM BIOMETRIC KEY (SRBK) ALGORITHM.

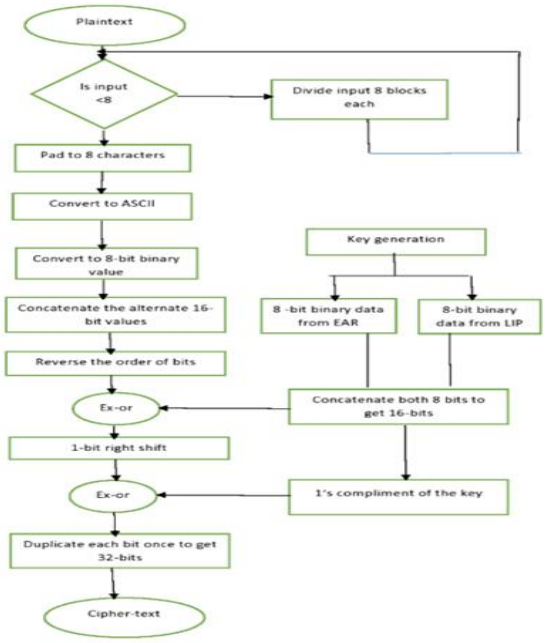



**Fig 11: Encryption flow chart**

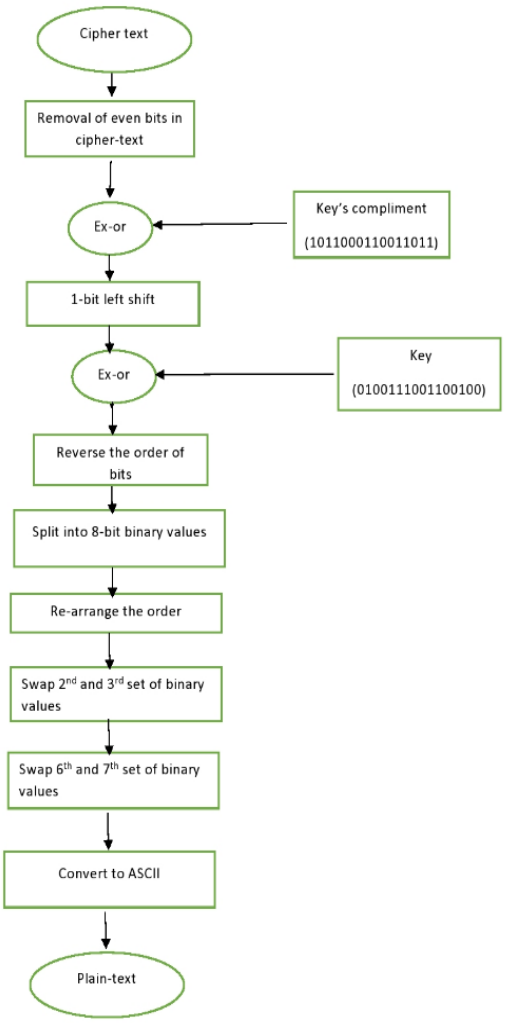



**Fig 12: Decryption flow chart**

## A. SRBK ANALSIS ON VARIOUS PARAMETERS

| MEMORY OCCUPIED | PERCENTAGE |
|---|---|
| SRBK | 9% |

| INPUT FILE SIZE(KB) | 50 | 60 | 100 | 240 | 320 |
|---|---|---|---|---|---|
| ENCRYPTION TIME (MILLISECONDS) | 29 | 56 | 48 | 76 | 88 |
| DECRYPTION TIME (MILLISECONDS) | 22 | 18 | 38 | 46 | 72 |

## V. PROPOSED NOVEL METHOD

## A. SIGNIFICANT -SECURE BIOMETRIC KEY ALGORITHM (SSBK) ENCRYPTION/DECRYPTION OF SSBK

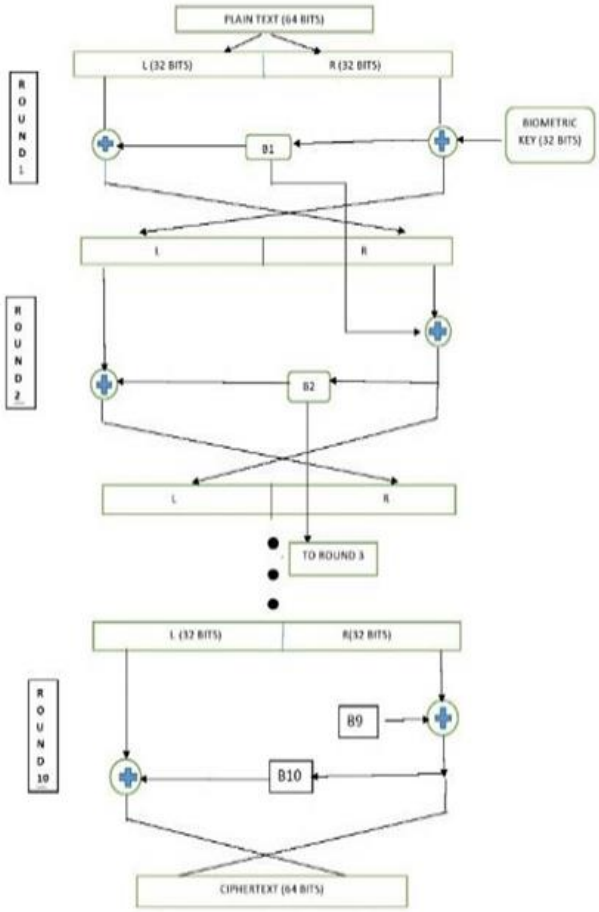



**Fig 13: Diagram of SSBK encryption**

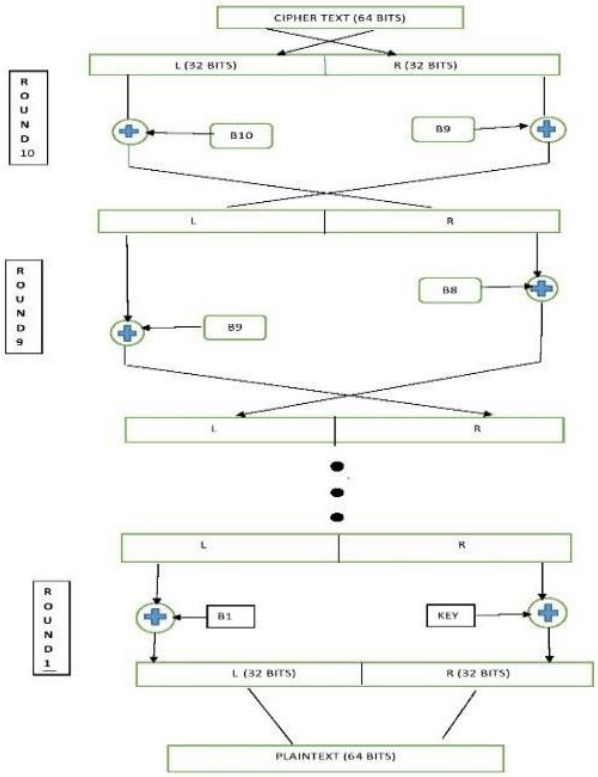



**Fig :14 Diagram of SSBK decryption Workflow of Encryption**

*Retrieval Number: K18700981119/19©BEIESP*
*DOI: 10.35940/ijitee.K1870.0981119*
*Journal Website: www.ijitee.org*



*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

| | LEFT OPERATION | RIGHT OPERATION |
|---|---|---|
| PLAIN TEXT | 1.01001E+63 | |
| ROUND 1 | | |
| | 1.01001E+30 | 1.00001E+31 |
| BIOMETRIC KEY | | 1.00111E+30 |
| OUTPUT | 1.011E+30 | 00001011001101110000101100110111 (BUFFER 1) |
| ROUND 2 | | |
| | 1.011E+27 | 1.011E+30 |
| EX-ORING WITH BUFFER 1 | | 1.011E+27 |
| OUTPUT | 1.011E+30 | 01010011010101010100001101000011 (BUFFER 2) |
| ROUND 3 | | |
| | 1.01001E+30 | 1.011E+30 |
| EX-ORING WITH BUFFER 2 | | 1.01001E+30 |
| OUTPUT | 1.011E+30 | 00001011001101110000101100110111 (BUFFER 3) |
| ROUND 4 | | |
| | 1.011E+27 | 1.011E+30 |
| EX-ORING WITH BUFFER 3 | | 1.011E+27 |
| OUTPUT | 1.011E+30 | 01010011010101010100001101000011 (BUFFER 4) |
| ROUND 5 | | |
| | 1.01001E+30 | 1.011E+30 |
| EX-ORING WITH BUFFER 4 | | 1.01001E+30 |
| OUTPUT | 1.011E+30 | 00001011001101110000101100110111 ( BUFFER 5) |
| ROUND 6 | | |
| | 1.011E+27 | 1.011E+30 |
| EX-ORING WITH BUFFER 5 | | 1.011E+27 |
| OUTPUT | 1.011E+30 | 01010011010101010100001101000011 (BUFFER 6) |
| ROUND 7 | | |
| | 1.01001E+30 | 1.011E+30 |
| EX-ORING WITH BUFFER 6 | | 1.01001E+30 |
| OUTPUT | 1.011E+30 | 00001011001101110000101100110111 (BUFFER 7) |
| ROUND 8 | | |
| | 1.011E+27 | 1.011E+30 |
| EX-ORING WITH BUFFER 7 | | 1.011E+27 |
| OUTPUT | 1.011E+30 | 01010011010101010100000001000011 (BUFFER 8) |
| ROUND 9 | | |
| | 1.01001E+30 | 1.011E+30 |
| EX-ORING WITH BUFFER 8 | | 1.01001E+30 |
| OUTPUT | 1.011E+30 | 00001011001101110000101100110111 (BUFFER 9) |

| ROUND 10 | | |
|---|---|---|
| | 1.011E+27 | 1.011E+30 |
| EX-ORING WITH BUFFER 9 | | 1.011E+27 |
| OUTPUT | 1.011E+30 | 01010011010101010100000001000011 (BUFFER 10) |
| | | |
| CIPHER TEXT | 1.01001E+62 | |

## Workflow of Decryption

| CIPHER TEXT | | 1.01001E+62 |
|---|---|---|
| | LEFT OPERATION | RIGHT OPERATION |
| DIVIDING THE BITS INTO LEFT AND RIGHT BITS | 1.011E+30 | 1.01001E+30 |
| EX-0RING WITH B 10 WITH LEFT AND B9 WITH RIGHT | 1.01001E+30 | 1.011E+27 |
| OUTPUT | 1.011E+27 | 1.011E+30 |
| ROUND 9 | | |
| | 1.011E+30 | 1.011E+27 |
| EX-0RING WITH B9WITH LEFT AND B8 WITH RIGHT | 1.011E+27 | 1.01001E+30 |
| OUTPUT | 1.01001E+30 | 1.011E+30 |
| ROUND 8 | | |
| | 1.011E+30 | 1.01001E+30 |
| EX-0RING WITH B8 WITH LEFT AND B7 WITH RIGHT | 1.01001E+30 | 1.011E+27 |
| OUTPUT | 1.011E+27 | 1.011E+30 |
| ROUND 7 | | |
| | 1.011E+30 | 1.011E+27 |
| EX-0RING WITH B7 WITH LEFT AND B6 WITH RIGHT | 1.011E+27 | 1.01001E+30 |
| OUTPUT | 1.01001E+30 | 1.011E+30 |
| ROUND 6 | | |
| | 1.011E+30 | 1.01001E+30 |
| EX-0RING WITH B6 WITH LEFT AND B5 WITH RIGHT | 1.01001E+30 | 1.011E+27 |
| OUTPUT | 1.011E+27 | 1.011E+30 |
| ROUND 5 | | |
| | 1.011E+30 | 1.011E+27 |
| EX-0RING WITH B5 WITH LEFT AND B4 WITH RIGHT | 1.011E+27 | 1.01001E+30 |

| | | |
|---|---|---|
| OUTPUT | 1.01001E+30 | 1.011E+30 |
| | | ROUND 4 |
| | 1.011E+30 | 1.01001E+30 |
| EX-0RING WITH B4 WITH LEFT AND B3 WITH RIGHT | 1.01001E+30 | 1.011E+27 |
| OUTPUT | 1.011E+27 | 1.011E+30 |
| | | ROUND 3 |
| | 1.011E+30 | 1.011E+27 |
| EX-0RING WITH B3 WITH LEFT AND B2 WITH RIGHT | 1.011E+27 | 1.01001E+30 |
| OUTPUT | 1.01001E+30 | 1.011E+30 |
| | | ROUND 2 |
| | 1.011E+30 | 1.01001E+30 |
| EX-0RING WITH B2 WITH LEFT AND B1 WITH RIGHT | 1.01001E+30 | 1.011E+27 |
| OUTPUT | 1.011E+27 | 1.011E+30 |
| | | ROUND 1 |
| | 1.011E+30 | 1.011E+27 |
| EX-0RING WITH B1 WITH LEFT AND KEY WITH RIGHT | 1.011E+27 | 1.00111E+30 |
| | 1.01001E+30 | 1.00001E+31 |
| PLAIN TEXT | 1.01001E+63 | |

**Features of SSBK Algorithm**

i. The security level is enhanced by the increased number of rounds.
ii. The biometric key is 32- bit in SSBK whereas it is 16 bits in SRBK algorithm.
iii. Each round has internally stored buffer which stores the current value and also fed as an input for the next round.
iv. Throughput of the proposed method is higher than the existing algorithm since the process time for encryption and decryption time is less. (results are discussed in later section)
v. The security is likewise improved by the utilization of biometric keys, as the underlying worth changes which thusly modifies the info esteem for the progressive stages.
vi. This is best known for fast, secure, significant and hence the name Significant-Secure Biometric Key algorithm.

## VI. RESULTS AND DISCUSSIONS

The following comparisons are made to show the proposed method is better in terms of memory, encryption time, decryption time and throughput.

Memory: As shown in fig.13, the SSBK algorithm occupies the least memory next to SRBK algorithm. The other encryption algorithms occupy the successive places in the graph.The encryption time is determined by using encryption algorithm which converts plain text to cipher text. The throughput is determined dependent on the encryption time. It shows the speed of encryption. The throughput of the encryption is the ratio of the total plaintext in bytes encrypted to the encryption time. The process time of the CPU is the time taken to perform a particular dedicated set of calculations. In other words, it highlights the load of CPU. The encryption time is proportional to the load on CPU. Various analysis have been performed using different file size of data. It is observed that the obtained throughput of SSBK outperforms the existing algorithms like AES, DES and RSA.

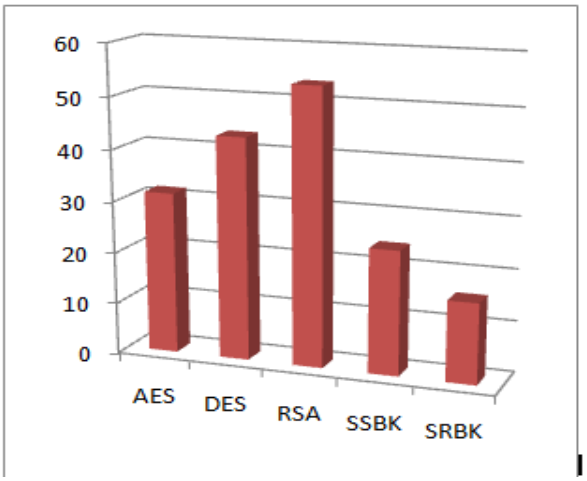



**Fig 15: Memory occupied by various algorithms**

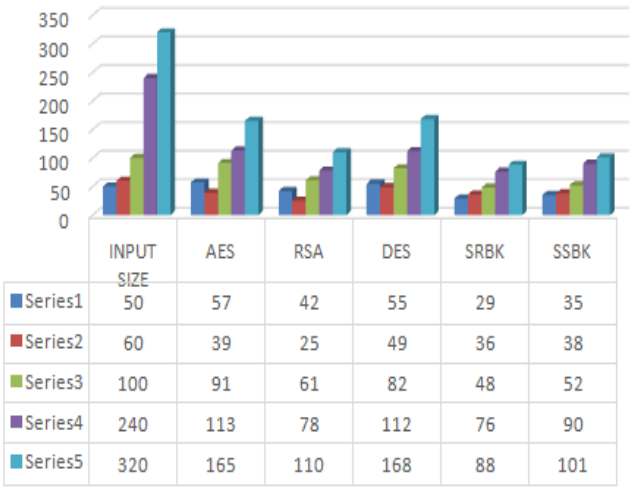
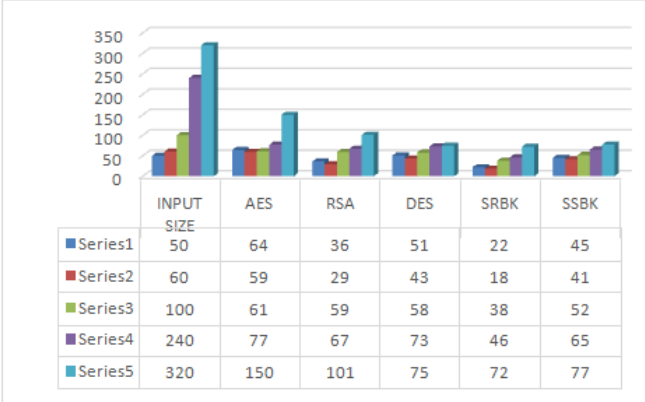
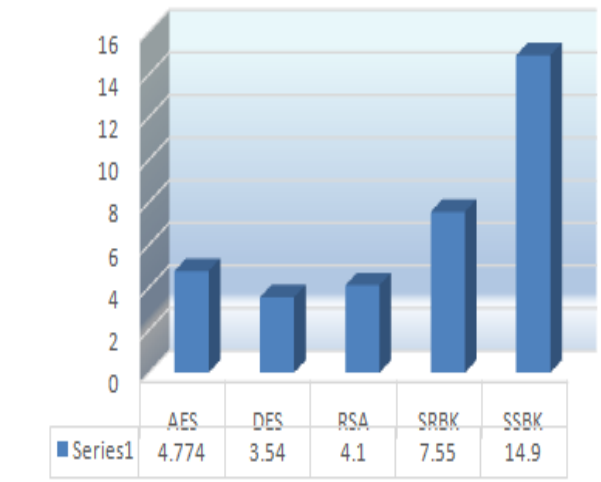



**Fig 16: Input data (Kb) Vs CPU process time-Encryption**




| | INPUT SIZE | AES | RSA | DES | SRBK | SSBK |
|---|---|---|---|---|---|---|
| Series1 | 50 | 64 | 36 | 51 | 22 | 45 |
| Series2 | 60 | 59 | 29 | 43 | 18 | 41 |
| Series3 | 100 | 61 | 59 | 58 | 38 | 52 |
| Series4 | 240 | 77 | 67 | 73 | 46 | 65 |
| Series5 | 320 | 150 | 101 | 75 | 72 | 77 |

**Fig 17: Input data (Kb) Vs CPU process time-Decryption**




| | AES | DES | RSA | SRBK | SSBK |
|---|---|---|---|---|---|
| Series1 | 4.774 | 3.54 | 4.1 | 7.55 | 14.9 |

**Fig 18: Throughput (Mb/sec)- Encryption**


| | AES | DES | RSA | SRBK | SSBK |
|---|---|---|---|---|---|
| Series1 | 6.653 | 5.776 | 5.775 | 7.53 | 17.16 |

**Fig 19: Throughput (Mb/sec)- Decryption**

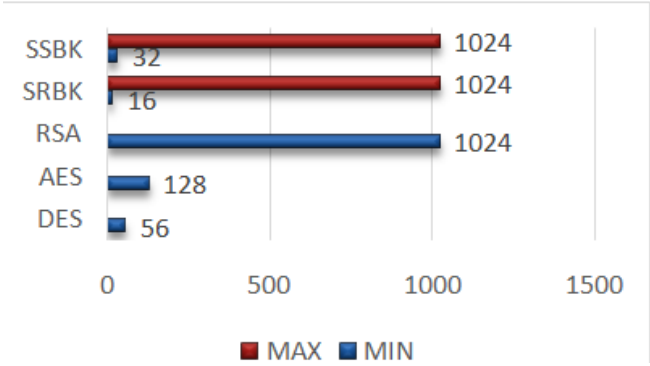



**Fig 20: Various key length comparison**

## VII. CONCLUSION AND FUTURE WORK

Thus the proposed cryptographic algorithm is used for trusted communication between parties, avoiding few disadvantages of other existing algorithms .The proposed algorithm uses 32-bit (SSBK) biometric key which the most important parameter to be noted. Thus the biometric key generation is flexible and can be altered based on the cryptographic algorithm used. The proposed algorithm uses simple operations, thus taking less time for processing and works faster for encryption and decryption which gives high throughput. Finally, it is proved that the proposed algorithm is performing better in terms of memory, encryption and decryption time and also throughput than the other existing algorithms. The biometric key is also generated from EAR and LIP which offer more security for communicating the data. The future work will include testing/simulations on the various biometric features, with multimodal biometric key generations and performing the key on the various file size of text, audio/video data and can concentrate on reducing the encryption/decryption process time and to overcome attack.

## REFERENCES

1. "A Comparative Survey on Symmetric Key Encryption Techniques"- Monika Agrawal, Pradeep Mishra, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, ISSN 0975- 3397,Page no.877-882.
2. "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data" -Ako Muhamad Abdullah- Research gate- Publication Date: June 16, 2017.
3. "A Survey on Cryptography Algorithms" Omar G. Abood, Shawkat K. Guirguis-International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018 495 ISSN 2250-3153.
4. "A Survey on Common Symmetric Encryption Algorithms" Arvind Kumar Sharma and Hitesh Sharma- International Journal of Engineering Research & Technology (IJERT) IJERT ISSN: 2278-0181 Vol. 3 Issue 12, December-2014.
5. "A Survey On Encryption Algorithms Using Modern Techniques" Venkat Prasad.K, S. Magesh,- International Journal of Pure and Applied Mathematics Volume 117 No. 16 2017, 673-678.
6. "A Survey on the Cryptographic Encryption Algorithms" -Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris-(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017.
7. Biometric Authentication: A Review Debnath Bhattacharyya, Rahul Ranjan , Farkhod Alisherov A. , and Minkyu Choi- International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009 13.

8. CHAPTER 6 Performance analysis – ShodhgangaDiffie–Hellman key exchange-https://www.math.brown.edu/~jhs/MathCrypto/SampleSections.pdf "Encryption Algorithms: A Survey"-Swathi S V, IILahari P M, IIIBindu A Thomas-International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)- Vol. 4, Issue 2 (Apr. - Jun. 2016).
9. Formulation of Ear Biometric Key with an Eminent Noise Immune Filter to Provide High Security in Authentication-Ms.S.Pavithra,v,Dr.P.Muthukannan, Mr.V.Prabhakaran, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 07-Special Issue, 2018
10. "Foundations of Computer Security" Lecture 52: Diffie-Hellman Key Exchange Dr. Bill Young Department of Computer Sciences University of Texas at Austin.
11. "Generation of Cryptographic Keys from Personal Biometrics: An Illustration Based on Fingerprints" By Bon K. Sy and Arun P. Kumara Krishnan.
12. Lecture Notes on "Computer and Network Security" by Avi Kak .
13. "Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java", Shraddha Dadhich, International Journal of Computer Trends and Technology (IJCTT) – Volume 35 Number 4 - May 2016.
14. "Performance Analysis of AES, DES and RSA Cryptographic Encryption Algorithms: A Novel Study"- Nitin Arora, Kritika Metha, Km. Anjali, Manisha Bhatt, Km. Aradhana, Krishan Chandra Mishra, Mamta Martolia-International Journal of Electrical Electronics & Computer Science Engineering Volume 3, Issue 3 (June, 2016) | E-ISSN : 2348- 2273 | P-ISSN : 2454-1222.
15. "State of the Art in Biometric Key Binding and Key Generation Schemes"- Abayomi Jegede , Nur Izura Udzir , Azizol Abdullah , Ramlan Mahmod-International Journal of Communication Networks and Information Security (IJCNIS) Vol. 9, No. 3, December 2017.
16. " Survey On Different Type Of Encryption Algorithm's"- Namdev Choure, Prof. Shrikant Dhamdhere-open access international journal of science and engineering-|| Volume 3 || Special Issue 1 || March 2018.


## AUTHORS PROFILE

**Ms.Pavithra.S** specialized in Applied Electronics and has graduated in the field of Electronics and Communication Engineering. Currently doing research at Saveetha Institute of Medical and Technical Sciences. Has 8.2 years of academic experience and has published many research articles in SCOPUS indexed journal and also presented many papers in international conferences. Organized many conferences, workshops and guest lecture in the career timeline.

**Dr.P.Muthukannan** currently working as a Professor and Associate Dean of Examination at Saveetha School of Engineering, SIMATS. His research caliber bandwidth spreads over many areas including Network Security, Image Processing, Embedded Systems, VLSI, Fiber Optics, etc. He has published many research articles in reputed peer reviewed journals. He has received many academic achievements and also reviewer in many indexed journals. He served many academic institutions as a high profile in his career timeline.

**Mr.V.Prabhakaran** is currently working as Assistant Professor (G-II) at Aarupadai Veedu Institute of Technology, VMRF. He has 10 years of teaching and research experience in his career timeline. He has published many research articles in SCOPUS and Thomson Reuters indexed journals, and also presented many papers in conferences. He is dynamic in his research thrust areas which includes Applied Electronic, Robotics, Nanotechnology, Image Processing.