International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Secure Handshake Hybrid Secured Algorithm for Acceleration-Based Pairing Mechanism in Wrist Worn Devices

V. R. Balaji, Kanimozhi. M, Kanimozhi. N, Kuralarasi. R, Kalieswari. S

Abstract: ***With the large spread of wrist worn smart devices in day-to-day lives, an extensive series of applications are enabled. Securing message conversation between these devices has become a challenging issue, considering the high security necessities and low computation abilities of these wrist worn devices. In this paper, we propose a secure wrist worn smart device coupling arrangement by manipulating the wave indication of the strategies generated by the handshake to barter a trustworthy key between users. To guarantee the safety of key negotiation, a hybrid secured algorithm is further developed. On Comparing with existing algorithms, the planned algorithm evades complicated fault alteration algorithms. In existing work the key generation is small in size so it is easy to detect by the intruder, in order to overcome this issue the RSA algorithm is combined with the AES algorithm, So that the size of the key is increased due to the combined algorithm and therefore robustness of the key is increased compared to the existing method. Investigational results are provided, which prove that the proposed handshake acceleration-based coupling arrangement is strong, safe, and effectual.***

Keywords: Handshake, Secure Device Pairing, AERSA Cryptography, Key Negotiation

I. INTRODUCTION

In current Years, we have observed a creation of the wrist worn smart plans, which has been widely used in people's daily lives. As reported in Canals, global shipments of keen timepieces were about 28.5 million in 2017, and this number will rise to 53 million by 2021. In fact, the number of apps for Apple Timepiece alone has reached 10,000. Rather than being the fixtures for keen handset and pill, wrist tatty smart devices are acting as independent strategies, owing to the improved capability in computation and battery. For instance, the newly launched Apple Timepiece Sequence 4 cannot only screen precise well-being statistics, but also be associated to the cellular webs and in instruction to brand or obtain calls.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
V. R. Balaji, Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India. Email: balajivr@skcet.ac.in
Kani Mozhi. M, Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India. Email: 18epcm004@skcet.ac.in
Kani Mozhi. N, Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India. Email: 18epcm005@skcet.ac.in
Kuralarasi. R, Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India.
Kalieswari. S, Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India.

As additional purposes of wrist tatty keen strategies are discovered, they can allow individuals to conversation commercial cards, group financial records, communal system information, and health data. In this paper, we suggest a handclasp-founded coupling arrangement amid wrist tatty keen devices founded on the observation that, by shaky hands, together wrist worn smart devices conduct similar movement designs.

Precisely, we chief generate a clandestine key from the wrist worn smart devices three-dimensional hastening statistics to assurance the protected statistics transmission. Additionally, owing to the noted three-dimensional hastening statistics are loud, an innovative AERSA hybrid cryptography procedure is planned to safeguard secure, healthy and efficient key negotiation. The rewards of this arrangement are as follows: 1) by way of the accelerometer is armed on greatest of the standard wrist tatty keen devices, it can appropriate greatest strategies deprived of needful any distinct hardware; 2) additional initialization and important pre- allocation are evaded; 3) the produced clandestine important is with great entropy and the key conversation procedure is safe and healthy; and 4) the planned system is exceedingly effectual and climbable. In instant, the chief aids of this daily are drew as shadows.

- We suggest a safe coupling arrangement for wrist tatty keen strategies founded on the handclasp hastening. It safeguards the safety of statistics broadcast amid wrist tatty keen strategies and is accessible, effectual and little-cost. We suggest an innovative AERSA hybrid cryptography procedure, which safeguards the discriminability of our arrangement and produces a clandestine important of great entropy amid strategies, thus assuring the strength of the important cooperation.
- We assess the presentation and safety of our arrangement. The consequences demonstration that by selecting the appropriate parameters, the planned wrist tatty keen strategies coupling arrangement is strong and receipts squat period ingesting. It is talented to battle together the inert outbreak and lively outbreaks.

II. RELATED WORK

Here, we analysis the prevailing works which can be branded in the subsequent three sets. Pairwise expedient coupling procedures. As outdated Communal Important Organization and password are not appropriate for wearable strategies, around numerous standing the whole thing on pairwise scheme coupling which denotes to safe key founding amid two strategies without pre- shared solutions or genuine communal solutions.

Prevailing pairwise expedient coupling procedures can be largely separated hooked on the subsequent three groups. The first one is based on Obtainable- of-Group station and communal important cryptography. In cooperation gatherings' communal keys are tested with OoB stations like humanoid support and bodily stations. For occurrence, adventures operators' known message design to confirm all other's communal keys takes the confusion of communal solutions transfer via OoB stations such as infrared and audial stations as the assurance to transported communal keys over wireless station. While these procedures evade the participation of any reliable third festivity or PKI, they are susceptible to man-in-the-middle (MITM) attack and computationally intensive. The second kind of protocols straight produce or quandary solutions with the topographies mined from ambient surroundings and stations. For example, ambient complete, wireless surroundings, occurrence forms of the wireless station and station sate info are used to produce communal confidences. These procedures resolve the difficulties of the chief group, although they are impractical happening rotten-the-ledge wrist tatty strategies, since they need superior coupling surroundings or essential superior sensors which are not armed on most rotten-the-ledge devices. The latter is the procedures exploiting human-computer interactions (HCI), such as walk, emotion strokes pointer gestures etc. Meanwhile prevailing wearable strategies are armed with consistent instruments, they are applied. Maximum of these etiquettes are dedicated on coupling strategies armed on a solo user, though our investigation is dedicated to strategies coupling among dissimilar operators.

III. SYSTEM MODEL

A. System model

1) We deliberate a scheme where two timepieces with accelerometers are correspondingly tatty on the two dissimilar operators. The message amid the timepieces is concluded wire- less channel. In this scheme, when the two operators jiggle hand with each other, together timepieces twitch to best their individual inertial hastening statistics. Afterward the handclasp, topographies are produced and a task is spread by together timepieces. Then, the related timepieces negotiate with each other to produce a safe and dependable clandestine key. Lastly, a dependable produced in the handclasp by examining the snooped info. For a lively imitation assailant, he copies the in the timepiece tatty by the genuine users.

2) Regulatory and receiving the accelerometer statistics noted by the timepiece.

- Insertion strategies on the time piece worn by the operators or Risk prototypical. We mostly reflect the risk of passive eavesdropping and active mimicry occurrences. An inactive attacker knows the key distribution device and can snoop the packages swapped by all genuine devices.

B. Proposed of AES and RSA hybrid algorithm

Compared to algorithm analysis and previous experiments the AES algorithm is much faster than the RSA algorithm, the AES algorithm is suitable for encrypting the large files or data, while the RSA algorithm is suitable for encrypting small amount of data and can perform digital signature and identity authentication. The RSA algorithm as small number of keys and the key management is convenient, while the AES key distribution is very troublesome. In summary it can encrypt data with AES algorithm, and encode the AES vital with the communal vital of RSA algorithm, so as to achieve the secure distribution of the AES key.

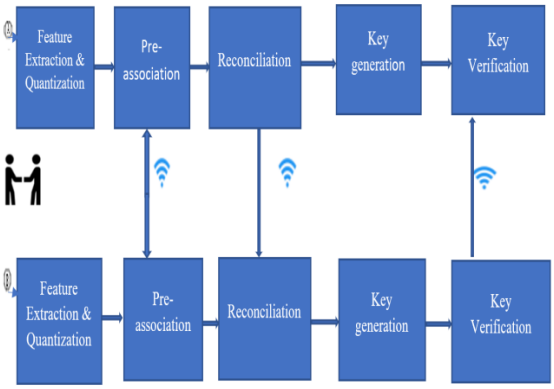


Fig.1 The construction of the proposed Agitation to Communication system

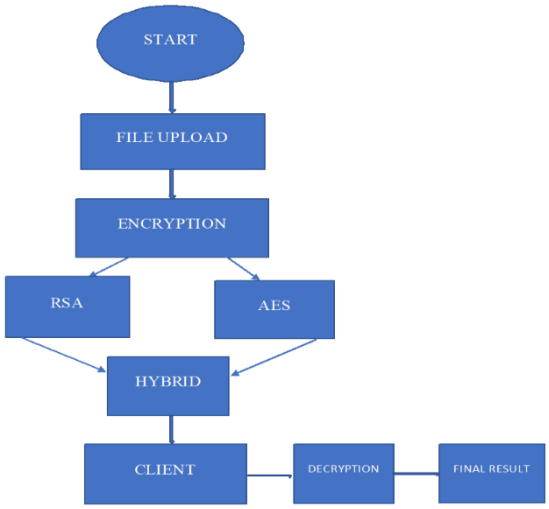


Fig:2 Proposed AES and RSA hybrid algorithm flowchart

C. Article compeers and quantization

- Article indication assortment**:** We undertake that every operator is tiring a smart timepiece furnished with accelerometer sensors. The accelerometer sensors constructed into present rotten-the- ledge keen timepieces usually comprise a 3-axes accelerometer, associated with the tri axial hastening, the hastening greatness is additional vigorous and has extra advantages in key generation and negotiation. We midpoint the hastening greatness *Mag*, and the focused hastening greatness is shown.
- Feature removal**:** Owing to the issues such as casing earthquake and timepiece shake, here are motionless numerous tall- incidence sounds in the gotten indication *ACC*. Acceptable to eradicate the tall-incidence sound that touches the piece removal consequences, we put on a 5Hz squat-permit strainer to the unique indication. Fig.displays the filtered acceleration magnitude, and it can be seen that the nearness is meaningfully increased.

The era of the hastening greatness produced by the combined keen watches is alike. In the previous literature, for the episodic sign, the intermissions of head-to-head mountains which called Inter-Pulse-Interval (IPI) are mostly used. Though, in handshaking situations, the nearness amid IPIs Produced since harmonizing watches is low.

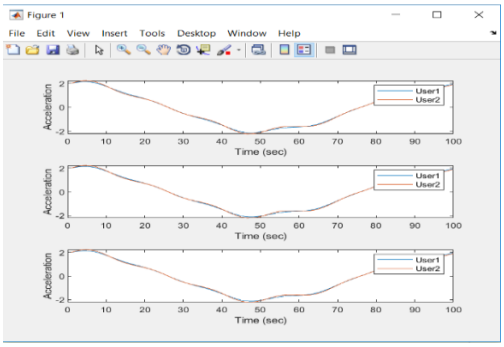


Fig.3 The acceleration of the wrist worn device

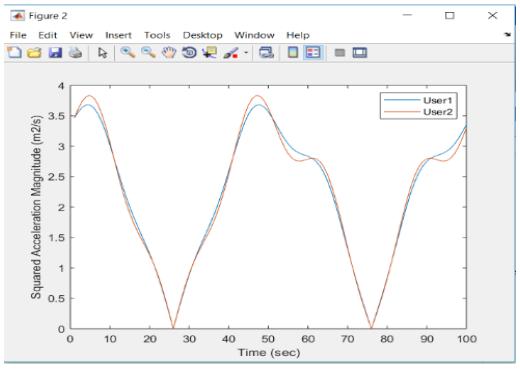


Fig.4 The squared acceleration magnitude

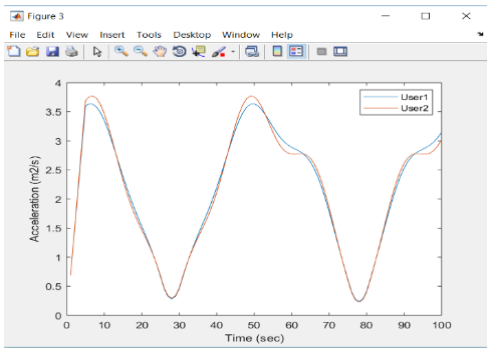


Fig.5 Is the cantered acceleration magnitude

Luckily, we novelty that throughout handclasp, the period once the two flanks produced statistics with nearly nothing hastening greatness is actual close. Consequently, they are appropriate for making topographies for the important group. The clean statistics can be signified by tuples of the procedure t_j, mag_j . Here t_j is the period the jth statistics is logged, mag_j is the hastening greatness of jth data. Meanwhile the statistics we noted are distinct, it is not always possi- ble to income a example whose hastening greatness is precisely zero. In this daily, we become the examples with zero hastening greatness by lined exclamation and income the consistent period as the topographies order $Fr = fr_1,\ldots,fr_k,\ldots,fr_n$, fr_k is signified as equation 3. For the sake of synchronize. we income the consistent period of the chief example with hastening greatness of 0 as the origin.

D. Pre-association

After the topographies are removed and quantized, the wrist-timepiece is successful to connect with its consistent spouse. But in our handclasp act, the operators have not recognized each other beforehand, so their timepieces don't obligate any info about each other, counting the individuality of the additional expedient.

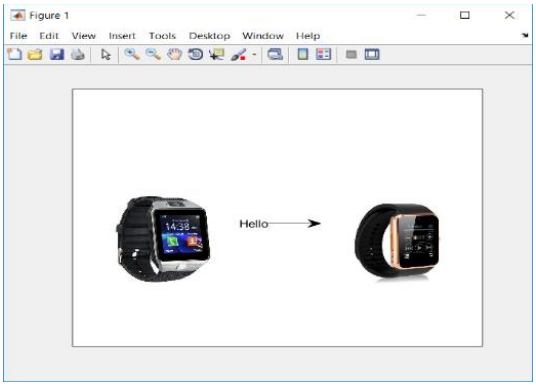


Fig: 6 Pre-association between devices

E. Resolution

Owing to the misrepresentation of the removed statistics produced by device kinds, attainment fault and act changes, etc., smooth by sifting and quantization, the topographies produced from the hastening scales still cannot be precisely the same. To resolve this issue, we further propose an AERSA cryptography algorithm based on the fault alteration device planned. It covers three events: (1) piece reorganization, (2) assistant statistics building, and (3) piece alteration. The chief two events are accomplished by the dispatcher, and the latter process is achieved by the earpiece.

IV. SCHEME ASSESSMENT

We assess the planned arrangement by preforming a sequence of trials. In this segment, we chief assess the disc rim-incapability, which is a significant pointer for assessing the precision of the arrangement. Also, we associate our planned AERSA cryptography procedure with prevailing ones and demonstration that our procedure workings finest for the topographies we removed,

Lastly we associate the planned arrangement with additional standings of competence.

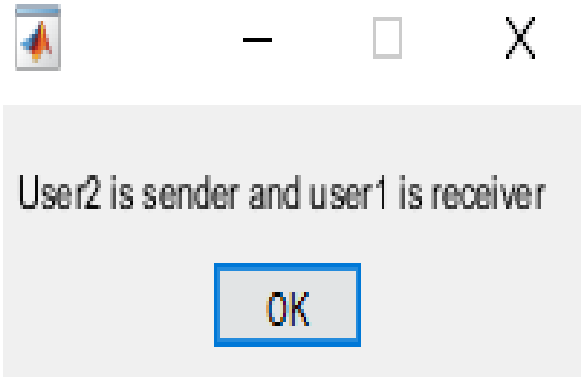


Fig.7 Communication between users

Fig 8:key verification

The influence of the quantization stricture θ and agitation course measurement m when $s = 4$. (a) false acceptance rate below dissimilar θ and m; (b) false rejection rate below dissimilar θ and m; (c) influence on equal error probability, the finest rate can be attained once $\theta = 2$ and $m = 3$

A. Competence

In this unit, we assess the competence of our arrangement in rapports of period ingesting and broadcast above.

As the AERSA arch-founded arrangement includes complex arch group and needs a big quantity of statistics broadcast, we only reflect the BCH code based scheme and Shake-n- Shack. In order to facilitate the comparison of their time ingesting, we pretend our arrangement and additional arrangements on a processor (microchip: Intel(R) Essential (TM) i7-8750H @2.20GHz, RAM: 8G, OS: Windows 10) with MATLAB. We comportment 100 trials for each arrangement and income their regular computational time, the research consequences are shown. In our arrangement, the expedient can be together the dispatcher or the receiver, so we income the customary of the computational period of in cooperation gatherings. As it goes available, meanwhile our arrangement evades complex exact calculation operations, his computational period is fewer than that of the BCH code founded arrangement and Shake-n- Shack. We take the entire scope of the communication as the standards for broadcast above. In our arrangement, we set the amount $n\ of$ examples we composed to be 32, and use the last 4 bits of the piece to make the key. The distance of the produced key is 128 bits and the distance of the assistant statistics is 96 bits. We take the expedient ID and the chance number N used to confirm cleanness to be 160 moments. The chance number No is 8 moments and the time T is 64 bits. Consequently, the entire scope of the communication directed by the dispatcher is 938 bits and the entire scope of the communication directed by the earpiece is 842 bits, which is satisfactory for wrist tatty plans.

Table-I: Computational time (MS) comparison of diverse schemes

Schemes	Computational time (ms)
BCH code-based scheme	1004.2754
Shake-n-Shack	2.0505
Our proposed scheme	0.2209

B. Key unpredictability

To safeguard safety of our arrangement, the clandestine key produced by our arrangement should be accidental. In this effort, we produce the clandestine key by the latter s bits of the topographies, so we examine the chance of bits in the topographies we removed. we can see that the inferior the significant of the bits, the advanced its estimated entropy. From the fifth smallest significant bit, the estimated entropy of the bit has reduced significantly. Consequently, in our succeeding trials, we take the latter four bits of the topographies to produce the key. We assess the entropy of the clandestine key. Our clandestine key is complete up by 0s and 1s, so its entropy differs amid 0 and 1, with 1 suggesting the uppermost likely chance. Entropy is slow in bits. Shows the entropy of the keys produced by 8 collections of helpers. It can be understood that the entropy of the clandestine keys produced by diverse collections are overhead 0.98, representative that the produced solutions are comparatively safe.

Relevance of assistant statistics to safeguard the safety of the scheme, the opponent should not be talented to deduction the clandestine key from the assistant statistics Help data. In Help data, the supplementary info which could disclose the key info is endangered by pi off∗ i . The superior the chance of b pi, the additional safe the secondary info is, so is the produced clandestine key. We examine the estimated entropy of bits at dissimilar locations in fn. For contrast, we compute the estimated entropy of 100 chance bit orders made by MATLAB with the similar strictures in our experimentation, and gotten the regular of their estimated entropy of 0.5241.Shows the estimated entropy of the bits at dissimilar locations of topographies. We can see that usually, the inferior the significant of bits, the advanced the estimated entropy they have, and the estimated entropy of squat significant bits is close to that of arbitrary moment arrangements produced by MATLAB.

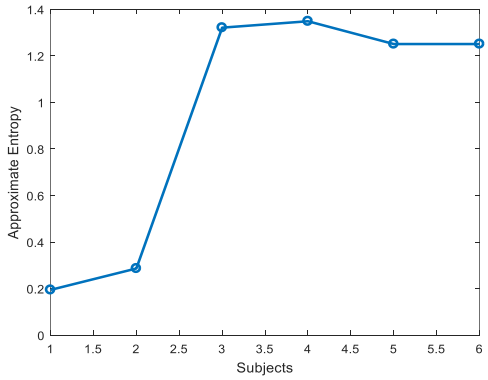


Fig.9 Approximate Entropy

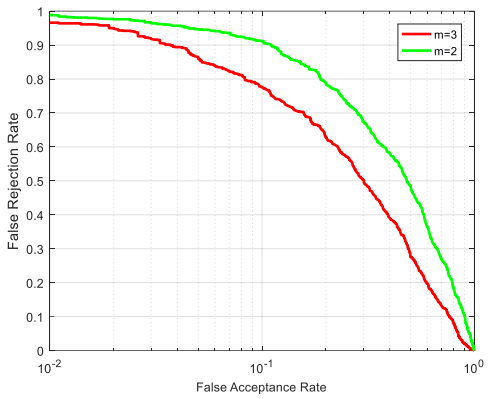


Fig.10 Approximate Rate

C. Huffman Encoding

Huffman Encoding is a procedure for liability statistics density and its methods the rudimentary impression late folder firmness. This helps to encode the data messages at fixed length and uniquely decodable codes.

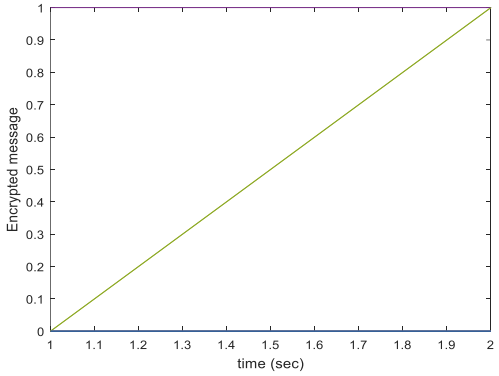


Fig.11 Encrypted message

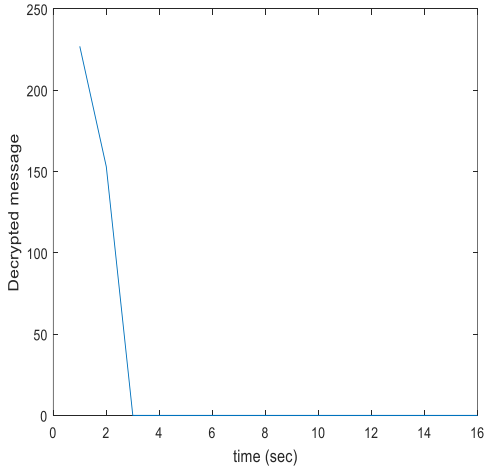


Fig.12 Decrypted message

D. Velocity

The velocity of a wrist worn smart device worn by the user is the degree of alteration of its location with admiration to an edge of orientation, and is a purpose of period. Speed is corresponding to a requirement of a thing's haste and way of gesture.

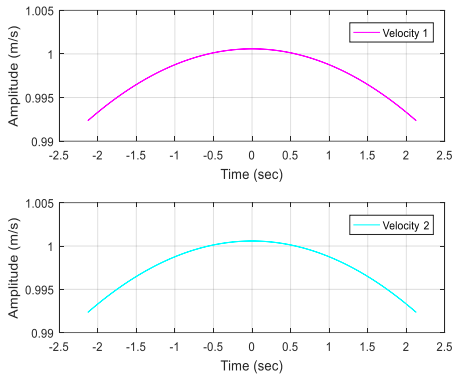


Fig.13 Rapidity of the wrist worn smart device

V. COMPARITIVE ANALYSIS

In existing work the key generation is small in size, so it is easier to detect by intruder. In order to overcome this issue, RSA algorithm is combined with the AES algorithm. The size of the key is increased due to the hybrid algorithm. So the robustness of the key is increased compared to existing method.

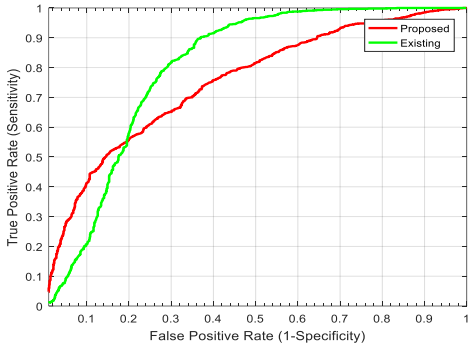


Fig.14 Approximation Rate of proposed method

A. Comparison of different algorithms

On comparison of different algorithms according to their taken and corresponding bit processed, the computational time taken by this algorithm is comparatively low and the efficiency of the system is increased by this process and it as high robustness against attacks.

Table-II: Computational time comparison of different algorithms

ALGORITHM	BIT PROCESSED	TIME TAKEN(SEC)	ROBUSTNESS AGAINST ATTACKS	COMPUTATIONAL TIME(SEC)
BLOWFISH	256	8.5232	LOW	0.6234
RIJNDAEL	128	8.1242	MEDIUM	0.4325
DES	128	8.0233	MEDIUM	0.3789
3 DES	192	7.6921	MEDIUM	0.3682
FUZZY CRYPTOGRAPHY	128	7.5010	MEDIUM	0.2965
AES AND RSA HYBRID	129	7.2991	HIGH	0.2209

B. AES&RSA combined encryption time

The combination of RSA – AES to study their complexities individually on the basis of a very basic parameter that is. More the amount taken to decrypt the encrypted data, more complex & hence, more secure will be the applied cryptography technique.

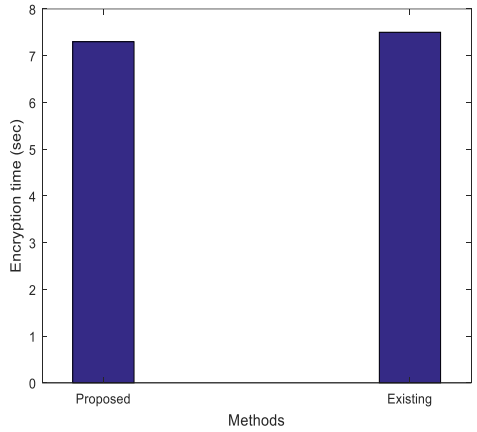


Fig.15 Encryption time taken for proposed method

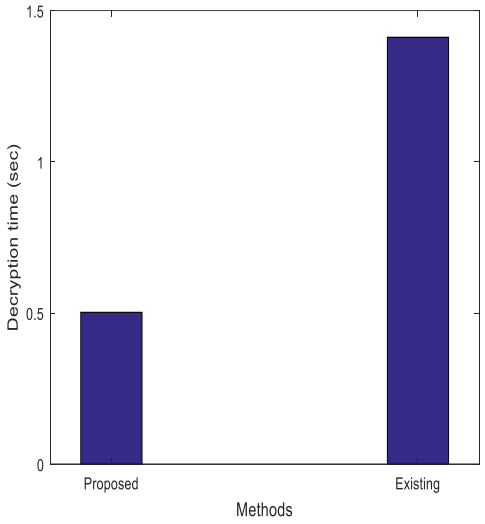
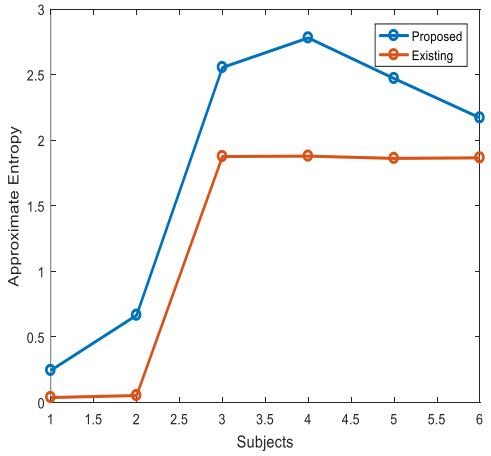


Fig.16 Decryption time taken for proposed method

C. Estimated entropy

In data, an estimated entropy of our technique is cast-off to enumerate the quantity of orderliness and the randomness of variations ended period-sequence statistics.



S

Fig.17 Approximate entropy of our proposed method

Table-III: Approximate entropy of different algorithms

ALGORITHM	ENCODING TIME(SEC)	DECODING TIME(SEC)	APPROXIMATE ENTROPY
Fuzzy Cryptography	7.5010	1.4118	0.2443 0.6653 2.5541 2.7798 2.4700 2.1699
AES and RSA combined Hybrid algorithm	7.2991	0.5022	0.0376 0.0529 1.8754 1.8784 1.8611 1.8653

VI. CONCLUSION

In this paper, we propose a secure handshake hybrid secured algorithm for acceleration- based pairing scheme for wrist worn smart devices. Wide experimentations have established that the key produced by the planned arrangement has tall chance and the key negotiation process is vigorous. In accumulation, the planned arrangement is well-organized as it doesn't include any complex controls. Amir's fault correction device, which is well-organized and vigorous. Wide spread experimentations have established that the key produced by the planned arrangement has tall unpredictability and the key negotiation procedure is vigorous. In adding, the planned arrangement is well-organized as it doesn't include any complex controls. For the forthcoming work, we will advance our system by additional cumulative the piece group amount, margarine the handshake period, growing the span of the produced key, and firming the key safety.

REFERENCES

1. Kyritsis, A. I., Deriaz, M., & Konstantas, D. (2018, September). Considerations for the planning of an activity recognition system using inertial sensors. IEEE Communications Magazine, vol. 55, no. 6, pp. 146–152, 2018.
2. Wei, Z., & Bao, T. (2018, June). Research on a completely unique strategy for automatic activity recognition using wearable device. ACM Computing Surveys (CSUR), vol. 47, no. 1, p. 8, 2018.
3. Weiss, G. M., Timko, J. L., Gallagher, C. M., Yoneda, K., & Schreiber, A. J. (2019, February). Smartwatch-based activity recognition: A machine learning approach. In 2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), vol. 35, no. 1, p. 8, 2019.
4. Lee, K. T., Yoon, H., & Lee, Y. S. (2018, January). Implementation of smartwatch interface using machine learning based motion recognition. In 2018 International Conference on Information Networking (ICOIN), vol. 76, pp. 37–48, 2018.
5. A. Juels and M. Sudan, "A Fuzzy Vault Scheme," Des. Codes Cryptography, vol. 38, no. 2, pp. 237–257, 2017.
6. Balaji, V R & Subramanian, S 2014, 'A Novel Speech Enhancement Approach supported Modified DCT and Improved Pitch Synchronous Analysis', American Journal of Applied Sciences(SciencePub), vol.11, no.1, pp.24-37.
7. Balaji V R 2018, "A Comparison of Compression Sensing Algorithm and DUET algorithm for Advanced DCT based Speech Enhancement System for Vehicular noise", International Journal of Pure and Applied Mathematics,Volume 119 No. 12 2018, 1385-1394.
8. Balaji V R, Sathiya Priya.J 2018 "Enhancement of Speech Signal Using Modified Binary Mask Based Algorithm for Vehicular Noise", Journal of Advanced Research in Dynamical & Control Systems, Vol. 10, 12-Special Issue, 2018

9. V. R. Balaji , C. Thulasi, 2019,"The Study on Revelation of Glaucoma using Structural Features", Indian Journal of Science and Technology, Vol 12(2), DOI: 10.17485/141364
10. Balaji.V.R, Thulasi.C, 2019, "Detection Of Glaucoma In Fundus Image-A Survey", 2nd International Conference on Recent Advances in Engineering and Technology, 8th & 9th Feb.2019 ISBN: 978-93-87862-50-0
11. V.R.Balaji, M.Karpagam, J.Sathiya Priya, July 2019, "Transform Based Speech Enhancement for Auditory Signals Based on Iterative Weiner Filtering" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Iss-2.
12. V. R. Balaji and J. Sathiya Priya, July 2019, "Revelation of Glaucoma Adopting Hybrid Structural and Textural Features", Indian Journal of Science and Technology, Vol 12(27), DOI: 10.17485/ijst/2019/v12i27/146049.
13. V.R.Balaji, J.Sathiya Priya, J.R.Dinesh Kumar, 2019, "FPGA Implementation of Image Acquisition in Marine Environment", International Journal of Oceans and Oceanography ISSN 0973-2667 Volume 13, Number 2 , pp. 293-300.

AUTHORS PROFILE

Dr. V. R. Balaji has completed his Ph.D. from Anna University, Chennai in September 2015. He is currently working as an Associate Professor in the Department of Electronics and Communication Engineering. His area of research includes Speech signal processing, VLSI and Image Processing. He has published various research papers in reputed journals. He is a member of various professional bodies.

Kanimozhi. M, currently pursuing a Master's degree in Engineering in the communication system stream under ECE branch at Sri Krishna College of Engineering and Technology. Have published a paper entitled "Cognitive Technology in Various Applications" in e-journal Volume 7, Issue 1 0n March 2019 in International Journal of Scientific Research & development. Additionally, have presented paper entitled "Application of Selective Region Growing Algorithm in Lung Nodule Segmentation" in 2018th fourth International Conference on Devices, Circuits and Systems (ICDCS) 2018.

Kanimozhi. N, currently pursuing a Master's degree in Engineering in the communication system stream under ECE branch at Sri Krishna College of Engineering and Technology. Have published a paper entitled "A patient Monitoring in Ambulance by using Internet Protocol" in e-journal Volume 7, Issue 1 0n March 2019 and "Animal footprint Identification for safety purpose" in the second International Conference on "Recent Advances in Engineering and Technology-ICRAET 2019" in February 2019.

Kuralarasi. R, currently pursuing a Master's degree in Engineering in the communication system stream under ECE branch at Sri Krishna College of Engineering and Technology. Have published a paper entitled "A patient Monitoring in Ambulance by using Internet Protocol" in e-journal Volume 7, Issue 1 0n March 2019 in International Journal of Scientific Research& development. Additionally, have presented the paper entitled "Animal footprint Identification for safety purpose" in the second International Conference on "Recent Advances in Engineering and Technology-ICRAET 2019" in February 2019.

Kalieswari. S, currently pursuing a Master's degree in Engineering in the communication system stream under ECE branch at Sri Krishna College of Engineering and Technology. Have published a paper entitled "A patient Monitoring in Ambulance by using Internet Protocol"in e-journal Volume7, Issue1 0n March2019 in International Journal of Scientific Research& development. Additionally, have presented the paper entitled "Animal footprint Identification for safety purpose" in the second International Conference on "Recent Advances in Engineering and Technology-ICRAET 2019" in February 2019.