RESEARCHERID
THOMSON REUTERS

[Soni, 6(6): June 2019] ISSN 2348 – 8034
IDSTM-2019 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

NOVEL APPROACH USING HEART BEAT AND SHA ANALYSIS FOR SECURE MESSAGE TRANSFER

Shailendra Soni[1] & Ritesh Kumar[2]

AP, [1,2]Department of Computer Science Engg, School of Engineering and Technology, Soldha

ABSTRACT

: Data and Information transfer is needed in every moment of the everyday life , it can be as big as transferring the high quality photo or can be a small as transferring the single word online. With the growth of the information technology, the data whether crucial or not is shared online, so with this concept it is required that the proper measures should be taken for its security also. Hacking attacks, intruders are increasing day by day, so the proper concept is required to authenticate the user. In the dissertation, the attempt is made to propose an algorithm to validate the users as well as to transfer the data more securely. The concept of ECG and Heart Beat Charts are used as the unique identity of the user , the process of the message or image transfer is shown in the dissertation . For the both concept the interacting users are required to be validated using the ECGs corresponding to the user. As the ECGs analysis using the Heart Beat Chart is done then the session for the data transfer is considered as the transaction so the transaction id, which is unique for the transaction is generated and the SHA code corresponding to the ECGs reports of the users are generated and stored in the database. The second phase starts with entering that unique transaction id and SHA keys generated in the first phase, after the validation is done, then the image or the message transfer is done by further validating the finger prints.

Keywords: *SHA, ECG Analysis, Data Transfer, Image Transfer.*

I. INTRODUCTION

Biometrics is motorized techniques for recognizing a man or checking the identity of a man in light of a physiological or behavioral trademark. Instances of physiological traits fuse hand or finger pictures, facial characteristics, and iris affirmation. Behavioral properties are qualities that are discovered or picked up. Dynamic stamp confirmation, speaker check, and keystroke stream are instances of behavioral characteristics. Biometric affirmation requires taking a gander at an enrolled or chose biometric test (biometric design or identifier) against an as of late got biometric investigation (for example, a fingerprint found in the midst of a login). In the midst of Enrolment, as showed up in the photograph underneath, an example of the biometric trademark is gotten, arranged by a PC, and set away for later examination. Biometric affirmation can be used as a piece of Identification mode, where the biometric system recognizes a man from the entire chose masses by means of checking a database for a match develop solely in light of the biometric. For example, a whole database can be hoped to check a man has not associated for capability benefits less than two particular names. That is every so often called one-to- numerous coordinating. A system can in like manner be used as a piece of Verification mode, where the biometric system checks a man's attested identity from their effectively chose case. That is likewise called balanced coordinating. In most PC access or system get to circumstances, check mode would be used. A customer enters a record, customer name, or inserts a token, for instance, a splendid card; be that as it may, instead of joining a mystery scratch, a direct touch with a finger or a glance at a camera is adequate to affirm the customer. [1] A biometric is any quantifiable, physical or physiological segment or behavioural trademark that can be used to perceive an individual or to check the ensured identity of a man. Instances of physiological biometrics consolidate fingerprints, hand geometry, the face, the iris, the retina, the venous systems of the hand and even stench.

II. THE BLOWFISH ALGORITHAM

- Consists of a variable number of cycles.
- For applications with somewhat key size, the trade off between the versatile nature of a savage power strike and a differential ambush make countless superfluous. Thus, it should be possible to lessen the quantity of cycles with no loss of security (past that of the diminished key size).

- Uses sub keys that are a confined hash of the key.
- This licenses the usage of long passphrases for the key without bartering security.
- Have no immediate structures that diminish the multifaceted idea of the extensive chase.
- Uses a framework that is anything but difficult to get it. This empowers examination and additions the trust in the algorithm. Before long, this suggests the algorithm will be aFeistel iterated square cipher [4].

III. DIFFIE-HELLMAN PROTOCOL

The Diffie-Hellman tradition is a system for two PC clients to deliver a typical private key with which they would then have the capacity to exchange information over an unstable channel. Allow the clients to be named Alice and Bob. [13]

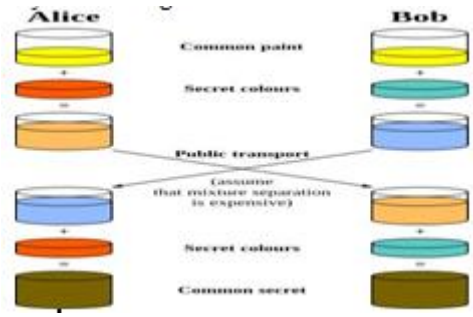

Figure 1. Diffie-Hellman Protocol

III. ECG ANALYSIS

Electrocardiography is the way toward recording the electrical action of the heart over some undefined time frame utilizing anodes set on the skin. These anodes distinguish the minor electrical changes on the skin that emerge from the heart muscle's electrophysiologic example of depolarizing and repolarizing amid every pulse. It is a usually performed cardiology test. In an ordinary 12-lead ECG, ten cathodes are set on the patient's appendages and on the surface of the chest. The general size of the heart's electrical potential is then estimated from twelve distinct edges ("leads") and is recorded over some undefined time frame (typically ten seconds).Along these lines, the general extent and heading of the heart's electrical depolarization is caught at every minute all through the cardiovascular cycle. The diagram of voltage versus time created by this noninvasive medicinal methodology is alluded to as an electrocardiogram. Amid every pulse, a solid heart has a deliberate movement of depolarization that begins with pacemaker cells in the sinoatrial hub, spreads out through the chamber, goes through the atrioventricular hub down into the heap of His and into the Purkinje strands, spreading down and to one side all through the ventricles. This methodical example of depolarization offers ascend to the trademark ECG following. To the prepared clinician, an ECG passes on a lot of information about the structure of the heart and the capacity of its electrical conduction system.

IV. PROPOSED APPROACH

Password strength
Password strength is a measure of the adequacy of a password against theorizing or savage drive strikes. In its regular shape, it checks what number of trials an aggressor who does not have control access to the password would require, overall, to get it proficiently.

Passwords guess validation
Frameworks that use passwords for verification must have some way to deal with check any password entered to get entrance. In the event that the protected passwords are simply secured in a system record or database, an attacker

who increments satisfactory access to the structure will procure all client passwords, giving the aggressor access to all records on the ambushed structure, and maybe unique frameworks where clients use the same or equivalent passwords. One way to deal with reduce this risk is to store only a cryptographic hash of each password instead of the password itself. Standard cryptographic hashes, for instance, the Secure Hash Algorithm (SHA) course of action, are hard to pivot, so an attacker who gets hold of the hash regard can't particularly recover the password.
Entropy as a measure of password strength

It is basic in the PC business to decide password strength to the extent information entropy, estimated in bits, a thought from information theory. As opposed to the amount of hypotheses anticipated that would find the password with sureness, the base-2 logarithm of that number is given, which is the amount of "entropy bits" in a password.

A password with, say, 42 bits of strength figured thusly would be as secure as a string of 42 bits picked haphazardly, say by a sensible coin fling. Put another way, a password with 42 bits of strength would require 242 undertakings to incapacitate every single potential result in the midst of a savage constrain look for.Random passwords

Essential article: Random password generator Random passwords contain a progression of images of demonstrated length taken from some arrangement of images using an irregular assurance get ready in which each image is comparably inclined to be picked.

The images can be one of a kind characters from a character set (e.g., the ASCII character set), syllables proposed to outline pronounceable passwords, or even words from a word list (thusly molding a passphrase).
The strength of arbitrary passwords depends upon the outright entropy of the shrouded number generator; in any
case, these are as often as possible not irregular, but rather rather a pseudo-irregular.
Pixel By Pixel Approach

The base approach of image correlation examination is pixel by pixel approach which is tedious. Coordinating Images According to Coordinates (MIAC) algorithm analyze the two images without concerning their sizes and background.

This algorithm analyzes the different size of images. This algorithm gives an effective correlation result on various outward appearance and changed facial position of a similar individual. In this algorithm, the correlation between two images is finished by each facilitate. The facilitate of the main image is contrasted and the comparing direction of the second image et cetera [13].

1. Steps of MIAC algorithm are:
2. Initially, to start with, we take the two images taken at different position or might be of various sizes.
3. Now get the tallness and width of the two images.
4. Find the littlest image.
5. It thinks about the image pixel by pixel [13].

ISSN 2348 – 8034
Impact Factor- 5.070

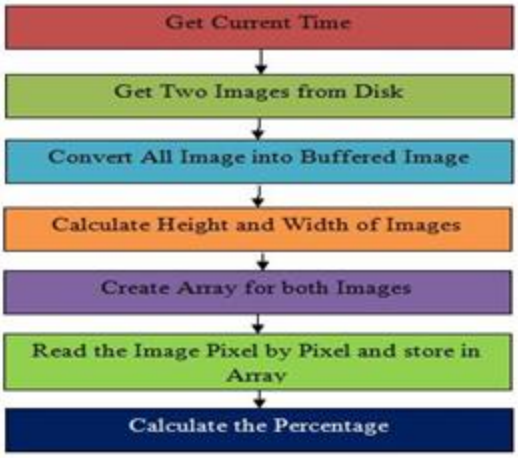

Fig 2 Implementation of MIAC

V. IMPLEMENTATION OF PROPOSED ALGORITHM

Step 1: The DiffMain.java file contains the starting program, and when we start the java file the starting interface will appear where we can choose options.

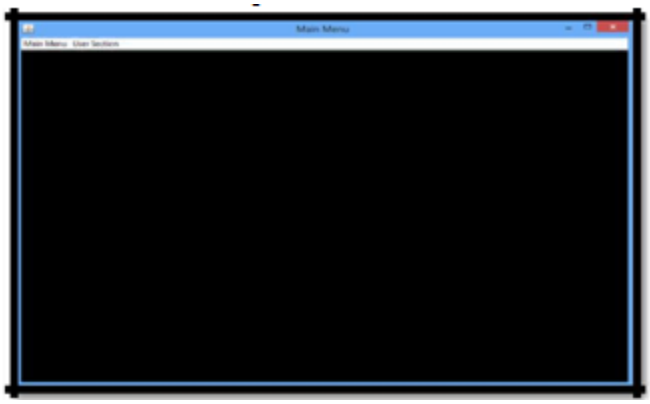

Fig. 3 Starting Interface

Step 2: The first choice is User Validation where we will select the images of the user which will be involved in the message transmission. The sequence of the user image selection is shown below. Figure 4 (a) User 1 ECG Selection and User 1 ECG Graphs. Figure 4(b) User 2 ECG Selection and User 2 ECG Graph.

ISSN 2348 – 8034
Impact Factor- 5.070

Fig. 4 (a) User 1 ECG Selection & User 1 ECG

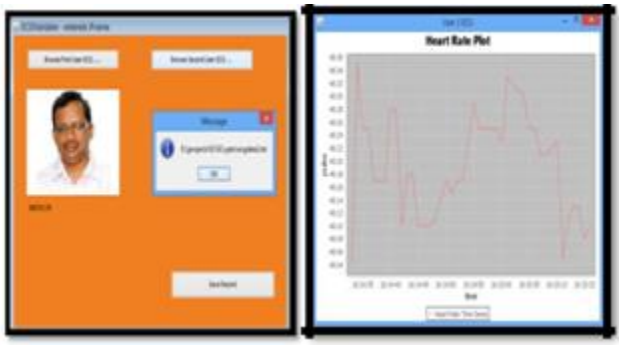

Fig. 4 (b) User 2 Image Selection and User 2 ECG graph

The SHA code corresponding to the ECG is generated in which the ECG file is read and the SHA code which is a 40 characters Hexadecimal value is used and every fifth character of the hexadecimal code is used to generate a 8 characters key corresponding to the keys of the both the users.

Step 3: The information will be stored in the database with the following information. The database which we have used contains the two tables, figdata, and encdata.

1. Figdata table: This table is used for storing the fingerprint of the persons. This table consists of the username, five fingerprint information and ECG file for the person.

2. Encdata table: This table is used for storing the encryption related information; it contains the username, Encryption Keys, and details of the users involved in the data transmission.

Table 1 Figdata table

uname	photo1	photo2	photo3	photo4	photo5	uphoto	ecgfile
amit	1_1.png	1_2.png	1_3.png	1_4.png	1_5.png	user1.jpg	ecgdata1.txt
kapil	2_1.png	2_2.png	2_3.png	2_4.png	2_5.png	user2.jpg	ecgdata2.txt
tinna	4_1.png	4_2.png	4_3.png	4_4.png	4_5.png	user4.jpg	ecgdata4.txt
uma	3_1.png	3_2.png	3_3.png	3_4.png	3_5.png	user3.jpg	ecgdata3.txt

Step 4: In Fig 4.2 shown the registration form which is used for registering the new users , and the data which is saved by the registration form will be stored in the Figdata table shown in table 1.

ISSN 2348 – 8034
Impact Factor- 5.070

Fig. 5 User Registration Form

Table 2 encdata table

uname	photo1	photo2	photo3	photo4	photo5	upphoto	ecgfile
amit	1_1.png	1_2.png	1_3.png	1_4.png	1_5.png	user1.jpg	ecgdata1.txt
kapil	2_1.png	2_2.png	2_3.png	2_4.png	2_5.png	user2.jpg	ecgdata2.txt
tinna	4_1.png	4_2.png	4_3.png	4_4.png	4_5.png	user4.jpg	ecgdata4.txt
uma	3_1.png	3_2.png	3_3.png	3_4.png	3_5.png	user3.jpg	ecgdata3.txt

In Figure 6 the details of the users' interaction the data with the unique transaction key and encryption key will be stored.

Step 5: The next step is the message sending before the step begins the form is selected in which the transaction key and the encryption key is required to be entered by the user, and after that, the users' interaction images will be shown

Fig. 6 Transaction Key and Encryption Key Entry

Step 6: In the Next level, we have to validate the fingerprint, and send the message from user 1 to user 2 using the Diffie – Hellman algorithm. The user one is first required to enter the fingerprint details, and then the fingerprint is validated in the database using the SHA-1 concept, and after that, the user two is required to submit the fingerprint which is again confirmed in the database using the SHA-1 algorithm, and then the Diffie-Hellman algorithm is followed for the message exchange.

ISSN 2348 – 8034
Impact Factor- 5.070

VI. SIMULATION RESULTS

1 Case I: User 1 and User 2 interacting data

In the test case I, the User 1 and User 2 are taken as the test data, and the finger of the user 1 and user 2 are provided as the input and then the pixel by pixel base implementation is carried out on the fingerprints as well as the SHA based proposed implementation is also performed on the fingerprints.

Table 3 shows the time comparison between the two approaches, as from the table 3 we got the information that the time required for the fingerprint comparison using the proposed algorithm is comparatively lesser when compared to the base the pixel by pixel-based implementation.

Table 3Time comparison table for case I

	Pixel By Pixel Approach	Proposed Work
USER 2 AND USER4	401 ms	146 ms

Figure 8 shows the comparison graph between two approaches, using the data which we have obtained in table 5.

ISSN 2348 – 8034
Impact Factor- 5.070

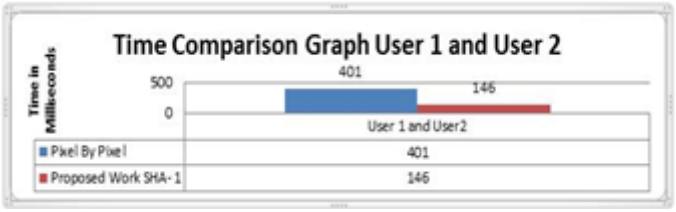

Figure 8 Time comparison graph case I Case II: User 2 and User 4 interacting data

In the test case II, the User 2 and User 4 are taken as the test data, and the finger of the user 2 and user 4 are provided as the input and then the pixel by pixel-based implementation is carried out on the fingerprints as well as the SHA based proposed implementation is also performed on the fingerprints.

The table 4.4shows the time comparison between the two approaches, as from the table 4.4 we got the information that the time required for the fingerprint comparison using the proposed algorithm is comparatively lesser when compared to the base pixel by pixel-based implementation.

Table 4 Time comparison table for case II

	Pixel By Pixel Approach	Proposed Work
USER 1 AND USER2	672 ms	63 ms

The Figure 9 shows the comparison graph between two approaches, using the data which we have obtained in table 4

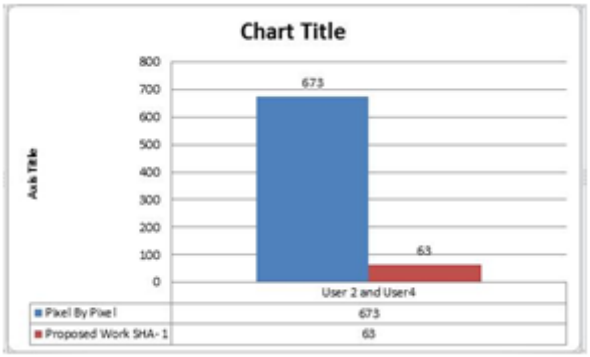

Fig.7 Finger Print Comparison Proposed and Pixel by Pixel

Step 7.The form in Figure 7 presents the pixel by pixel comparison from which shows the base implementation
Fig 9 Time comparison graph case II

VII. TESTING THE STRENGTH OF PROPOSED WORK

We have tested the KEY generated by our proposed implementation using the various tools to check its strength. Below is presented the some of the test analysis presented on the KEY.

ISSN 2348 – 8034
Impact Factor- 5.070

Table 5 test result analysis table

Test Key	Website/Tool	Result
89E7D178B9845423	Password Meter	Very Strong
89E7D178B9845423	Password Checker	Excellent Strength
89E7D178B9845423	Cryptool2	Entropy 3.13 Strength 100 Very Strong

VIII. CONCLUSION AND FUTURE SCOPE

Electronic systems are utilized both in the business world and in addition in our private regular day to day existences. There are different electronic systems and they are utilized for a wide range of purposes. The one thing that every single electronic framework have in like manner is the way that they are utilized to work with information. A solid electronic arrangement of any sort needs satisfactory information security with a specific end goal to work in full working request.

Notwithstanding their size, all organizations are engaged with giving either administrations, products or both to their clients. Organizations of numerous kinds and sizes work with a wide range of sorts of information. Information with respect to the organization's representatives, items, administrations or clients – every last bit of it is data.IT systems saturate about each cutting edge business and is at the core of a large portion of the present exchanges. This being the situation it would appear to be judicious to shield these systems from potential dangers. IT security includes a wide range of procedures which all finish in a sheltered and secure IT framework.

The security of a business' IT systems is central and ought to never be ignored. TheSecurity is the main concern in the transaction, the proposed dissertation make the user of the ECG based analysis in order to increase security be encrypting the photos of a user interacting in the transaction using the SHA based encryption key generated corrosponding to the ECG reports, and the encrypted images are first decrypted at the time of the sending of the message and after the encryption and transaction key validated then the message is further transferred. Using the SHA in the image comparison will speed up the process of image comparison. Thus the security and speed both have enhanced. Thus, we can say that our proposed implementation provides a better way to share the data securely.

In the further studies, we will like to extend our research to use the real-time password like live pictures, video and retina verification concepts for sharing the file to enhance the security in the suggested framework further.

REFERENCE

1. *Gopal D. Dalvi,Dr.D.G.Wakde,"Facial Images Authentication In Visual Cryptography Using Sterilization Algorithm," 2nd International Conference for Convergence in Technology (I2CT),2017.*
2. *Ekta Agrawal,Dr. Parashu Ram Pal,A New and More Authentic Cryptographic Based Approach for Securing Short Message, International Journal of Advanced Research in Computer Science,2017.*
3. *Sarita Kumari,"A Research Paper on Cryptography Encryption and Compression Techniques," International Journal Of Engineering And Computer Science ISSN:2319-7242Volume 6 Issue 4 April 2017.*
4. *Arpit Agrawal, GunjanPatankar,"Design of Hybrid Cryptography Algorithm for Secure Communication," International Research Journal of Engineering and Technology (IRJET),2016.*
5. *Rahman MM, Akter T, RahmanA,"Development of Cryptography-Based Secure Messaging System," J TelecommunSyst Manage,2016.*
6. *Vaibhav Poonia, Dr. Narendra Singh Yadav, "Analysis of modified Blowfish Algorithm in different cases with various parameters," International Journal of Engineering Research and General Science Volume 3, Issue 1,January-February, 2015.*

7. *Snigdha Soni, SandeepPratap Singh,"Secure and Efficient Integrity Algorithm based on Existing SHA Algorithms ,"International Journal of Computer Applications (0975 – 8887) Volume 113 – No. 11, March 2015.*
8. *Saikumarmanku and k. vasanth,"blowfish encryption algorithm for information security," arpn journal of engineering and applied sciences,2015*
9. *DishaShah,"Digital Security Using Cryptographic Message-Digest Algorithm, "International Journal of Advanced Research in Computer Science and Management Studies,"Volume 3, Issue 10, October 2015.*
10. *Snehal Javheri, Rahul Kulkarni,"Secure Data communication and Cryptography based on DNA based Message Encoding," International Journal of Computer Applications (0975 – 8887)Volume 98– No.16, July 2014.*
11. *Maulik P. Chaudhari and Sanjay R. Patel,"A Survey on Cryptography Algorithms,"International Journal of Advanced Research in Computer Science and Management Studies,2014.*
12. *M.S.Durairajan, Dr.R. Saravanan,"Biometrics Based Key Generation using Diffie Hellman Key Exchange for Enhanced Security Mechanism," International Journal of Chem Tech Research, 2014.*
13. *Sangeeta Arora, Lakhan Singh, Aditya Kumar," Comparison of Images using MIAC Algorithm," KIET International Journal of Intelligent Computing and Informatics, Vol.1, Issue1, January 2014.*
14. *Md Asif Mushtaque, Harsh Dhiman, Shahnawaz Hussain," A Hybrid Approach and Implementation of a New*
15. *Encryption Algorithm for Data Security in Cloud Computing," International Journal of Electronic and Electrical Engineering,2014.*
16. *Surbhi Aggarwal, Neha Goyal, Kirti Aggarwal," A review of Comparative Study of MD5 and SHA Security*
17. *Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 104 – No.14, October 2014*