Grid Based Data Communication and Acknowledgment

[1]Rukhshar Bano,[2]Shanti Prakash Gehlot
[1]M.Tech Research Scholar,[2]Head of Department
[1,2]Department of Computer Science , Sobhasaria Engineering College Sikar

Abstract: In any of the communication related to data, we require that data should be transferred securely and without being manipulated. Security of data is of utmost importance in the data communication. Seeing, the importance of the data security we are proposing the secure data communication system with the mutual authentication using the concept of the grid placement of the image with the association of the ASCII values in the gird position to form the pattern and the concept of the session token in used for the communication between the two users with involvement of the photos the users has chosen at the time of the registration and hash algorithms for the formation of the pattern involving the hash sequence. Together with the last the hank shake concept of the token deletion after the integrity validation of the data is also done in order to guarantee the proper delivery of data. Such types of communication systems are very useful when transferring some secure data or information, in organization like Banking Sector, when the authentication of users and secure communication is very important.

IndexTerms – *Data Security, Data Communication , Grid Password.*

I. INTRODUCTION

Data security is a major issue for businesses and organizations today. Ensuring that your data is secure is becoming more important every day and vital to business operations. A report from (Computer Discount Warehouse) showed that data loss has emerged as the top cyber security challenge that medium and large businesses are now facing. Data loss damages organizations in a large variety of ways and is expensive, with estimated costs around USD (United States Dollars) 200 per record breached; an average of USD6.8 million per total breach. A number of high-profile breaches outline this concern. However, some of this information not intended to leave the system. The unauthorized access of this data could lead to numerous problems for the larger corporation or even the personal home user. Having your bank account points of interest stolen is similarly as harming as the system overseer who ransacked for the customer data in their database [1].

There has been a gigantic accentuation on data security starting late, largely in view of the web. There are various choices for securing your data from programming answers for equipment systems. Web identity (IID), likewise online identity or web persona is a social identity that an Internet user builds up in online groups and sites. It considered as an effectively built introduction of oneself. Albeit a few people utilize their genuine names on the web, some Internet users like to be mysterious, identifying themselves by methods for nom de plumes, uncover changing measures of actually identifiable data. An online identity controlled by a user's relationship to a specific social gathering, to which they are a piece of on the web. Some can even be misleading about their identity. In some online settings, including Internet gatherings, online visits, and hugely multiplayer online pretending recreations (MMORPGs), users can speak to themselves outwardly by picking a symbol, a symbol measured realistic picture. Symbols are one way users express their online identity. Through communication with different users, a built up online identity gains a notoriety, which empowers different users to choose whether the identity is deserving of trust. Online personalities related with users through validation, which ordinarily requires enrollment and signing in. A few sites additionally utilize the user's IP deliver or following treats to identify users.[2]

There are two purposes behind restricting a user to an identity:

- The user identity is a parameter in get to control choices
- The user identity is recorded when logging security-pertinent occasions in an audit trail

The first point is required for the system to enable granularity in access control. If we do not know who the user is we can't know the user's rights, except for single user systems. The use of an identity is not only relevant for physical users' system processes also require access control and need to be identify the user accessing the system.

The second point enables the system to associate logged events to identities. Since this thesis is primarily concerned with security, security events are most important, but logging system [2] events has a much wider usage than mere security. Logging system events can help in locating configuration and functional errors and is critical for system maintenance. Another field in which logging plays a central role is in the construction of customer debit.

The use of a digital identity representing the physical user is, as outlined above, critical for security processes like authentication. When the system has authenticated the identity, access control handles the privileges associated with that identity.[2]

II. LITERATURE SURVEY

R. K. Ibrahim, et. Al [3] The SHA-2 hash function is used in many fields of security system such as digital signature, tamper detection, password protection and so on. SHA-2 is very important algorithm for integrity and authentication realization, SHA-2 is a one way algorithm to produce hash code of any message with 256 random hash bits (that's according to the version of SHA-2), which cannot be reversible, this property makes the hash function in general susceptible to breaking, and also the limitation of number of bits makes a probability of collision incidence. So, the hash code's merged with a kind of cryptography which is the stream cipher. The stream cipher mode of operation named Output Feedback (OFB) method combined with SHA-2 256 algorithm to produce encrypted hash code that can be reversible to achieve confidentiality. Implementation and simulation results of OFB based on SHA-

2 256 algorithm obtained in LabVIEW project shows simplicity in modelling hash function algorithm generating hash codes encrypted by OFB method.

A. S. Eissa, et. Al [4] The Secure Hash Algorithm 3 (SHA-3) is a crypto-graphic hash function widely used in most security applications. The execution of the SHA-3 function is computationally intensive on lightweight embedded RISC processors. In this work, authors advance a SHA-3 Instruction Set Extension (ISE) to improve its performance on a 32-bit MIPS processor. Two ISE approaches are proposed, namely native datapath and coprocessor-based ISEs. The ISE is developed with the aid of Codasip Studio, and the extended processor is implemented and benchmarked on a Xilinx Virtex-6-XC6VLX75t FPGA.

Sachin Malhotra and Munesh C. Trivedi [5] The proposed model makes sure about the system from the notable and habitually happened assaults (pantomime, adjusts steering data, dark gap). In this work, two degrees of validation have been utilized, first level for bounce to-jump confirmation (MD5 algorithm has been utilized for verification code formation) and second level for start to finish verification (SHA1 algorithm has for confirmation code formation).

Anjali Somwanshiet. Al 2017 [6]textual secret key's most typically used authentication system for anchoring these applications. Authentication schemes area unit helpless against totally different varieties of attacks. The projected system provides declare the attacks specially, 'Keystroke Logging', 'Shoulder Surfing' and 'Copy Login Pages'. The system enhances login security part. The system includes of 6X6 framework of twenty-six letters so as and ten digits to enter the key phrase. Whereas achievement within the system the shopper has to be compelled to offer his non-public key which can be used whereas coming into the key phrase into the framework. The non-public key of the shopper can ne'er be used anywhere therefore there aren't any odds of obtaining the key word bust.

III. PROPOSED WORK

3.1 User Registration

In the user management we have the management of the users, including the user enrollment and the user login.
The unique way of authenticating the user includes the following concepts ,

a. Image as Password :
   - ✓ In the image as password , we will ask user to select and image and for that image we will store the Hash Pattern for the validation of that the user select the same image as the time of the login also.
   - ✓ Secondly, we use the image click concept , on the image we store the clicks of the user , so the number or the count of the click is stored and that will be used for the validation of the user.

b. Grid for formation of password :
   - ✓ In the grid concept , we take the image from the user and organize the segments or the parts of the images pieces in the grid blocks and this grid blocks will form the organization as follows ,
   - ✓ Suppose the Image which we choose is of airplane and divide it in the 8 parts and place in grid , the user has only to place the elements in the grid and have to remember the position where the parts are placed in the grid for the login purpose also.

2. Data Exchange:
The data is exchanged in between the two users and for the exchange purpose the session is maintained and first the token is generated with the unique slot number and the process of generation of the token is ,

a. Generation of MD5 hash of the user 1 photo.
b. Generation of MD5 hash of the user 2 photo
c. Extraction of first 15 characters of hash of both users
d. Generation of the Random 10 numbers and contacting all to form the token

The generation of SHA-512 hash for the data which is to be exchanged.
The receiver provides the session token and unique slot number to access the data and integrity of the data received is verified by checking the Hash of the message sent with the message received.

3. Data Acknowledgement:
After successful interpretation of data receiver will delete the token and client will verify the acknowledgement, by validating the absence of the token. (It is for the particular time limit as after the allotted time for the transfer, the token will get deleted automatically).

IV. IMPLEMENTATION

The implementation of the proposed work is performed in VS 2010 and SQL Server 2008

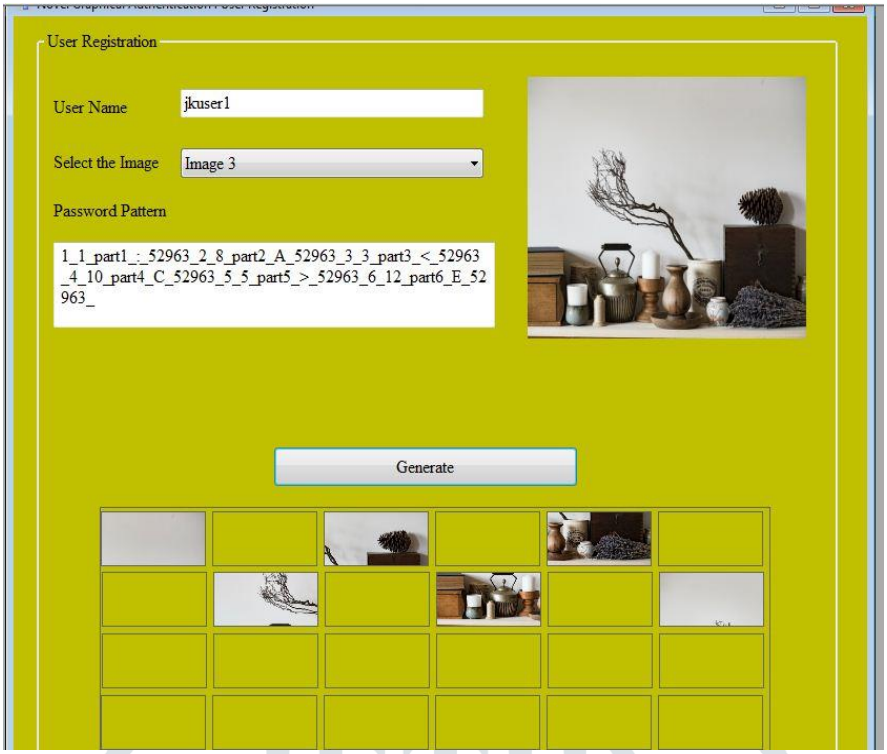

Fig 1 User Registration

The fig 1 shows the client enlistment structure, where the client enrollment measure is appeared in which the client name is needed to be entered by the client. At that point the client needs to choose the picture name from the combo box, as the client select the picture from the combo box, the picture is shown and it is sectioned into the size parts which we can put in any area present in the network. At that point, we need to tap on the Generate catch to produce the secret key and after that , we need to save the record in the information base.

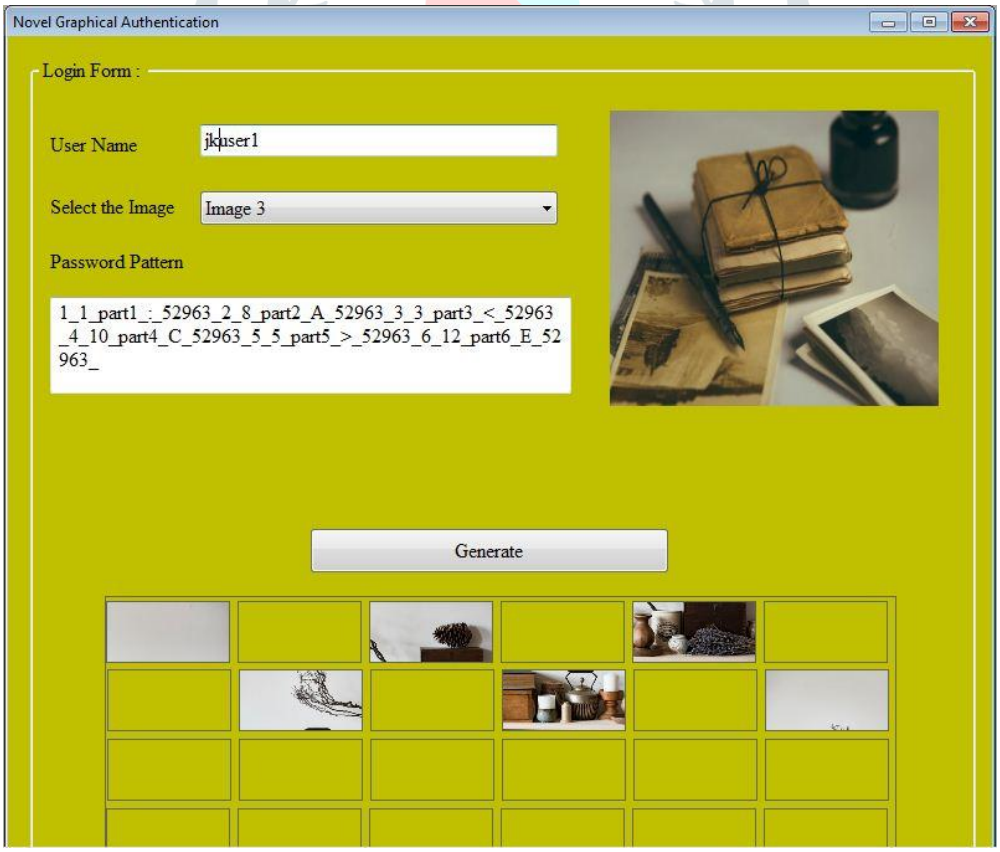

Fig 2 User 1 Login Process

In the login interaction likewise, a similar idea is needed to be rehashed which is appeared in the client enlistment measure. Here the picture which is chosen by the client, the hash of that picture is created utilizing the SHA 512 and is checked with the hash which is put away comparing to that client. At that point the client needs to situate the picture sections into the network and produce the example, that design additionally coordinated in the information base record of that client. On the off chance that both the approvals are fruitful, the entrance is conceded.

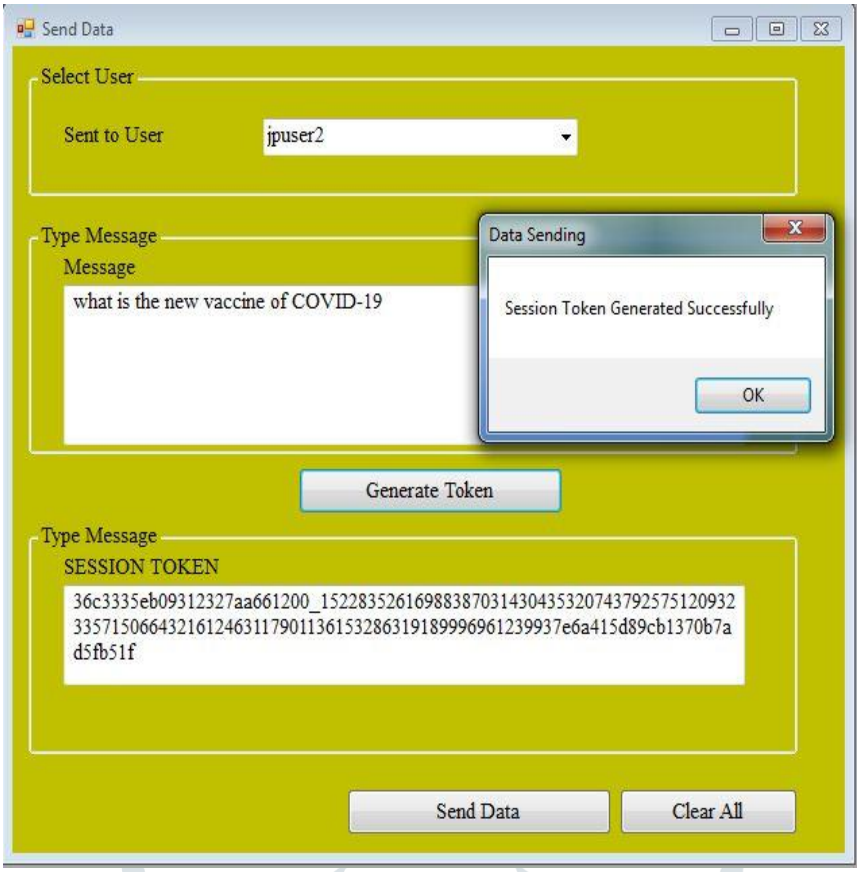

Fig 3 Sending Data to Receiver

The fig 3, shows the information sending structure , in which we need to initially choose the name of the beneficiary , at that point need to type the message and after that we need to create the meeting token which will be legitimate for the information correspondence . At the point when the client send the information , the SHA 512 hash for the message is additionally produced , which will be utilized for the approval reason at the collector end.

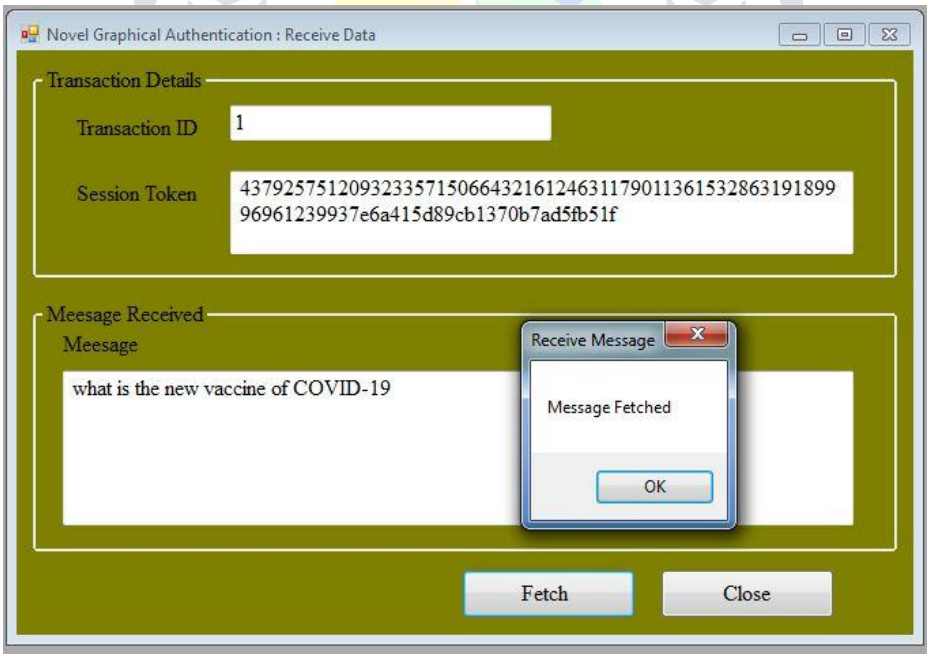

Fig 4 Fetch Message

The fig 4 shows the get message structure , where the exchange id and meeting token and after the approval, everything being equal, and checking the trustworthiness of the message , the message is show to the collector.

V. `RESULT ANALYSIS

As per the Base Paper "Symmetric Key Based Authentication Mechanism for Secure Communication in MANETs" by Sachin Malhotra and Munesh C. Trivedi

Testing the strength of the Session Keys

Base: 8192-df55da268244ca76670-924645b3e345a600bda7

Proposed: 36c3335eb09312327aa661200_11522835261651831281_e6a415d89cb1370b7ad5fb51f

5.1 Tool 1: How Secure My Password (Website Ref: https://password.blue/test.html)

The following is a secret word meter that tests entropy utilizing zxcvbn by Dropbox. It tests for word reference words, leet-talk, unmistakable examples, and different heuristics to give an informed supposition at what the entropy could be.

In the event that you are sticking passwords from the generator, you will see differences. This analyzer is a visually impaired entropy surmise. It doesn't have a clue about the arrangement of components your secret word is from, nor can it say whether an arbitrary capacity was utilized. In this way, the speculation might be higher or lower than what you realize that it will generally be.

.Table 1 Security Strength Comparison 1

	Base Key Score	Proposed Key Score
Entropy	146 bits	232 bits
Length	45	73

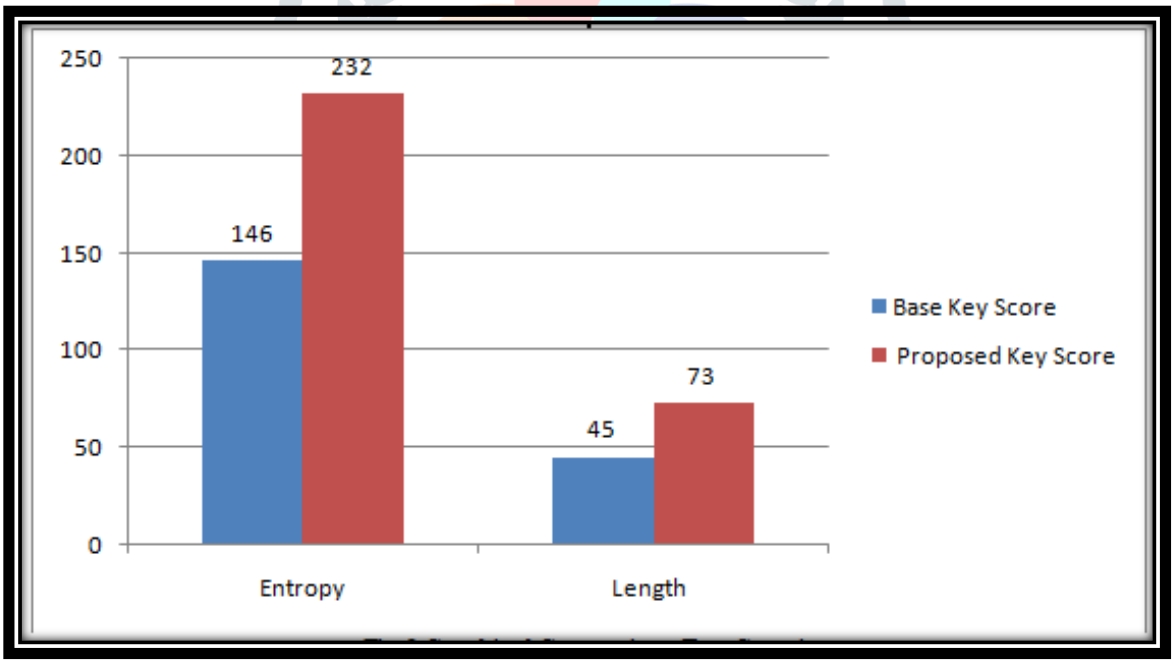

Fig 5 Graphical Comparison Test Case 1

5.2 Tool 2: Runkim Test (Site Reference: http://rumkin.com/tools/password/passchk.php)

The Runkin tool also test the password strength and calculates the entropy together with determining the length of the string..

Table 2 Security Strength Comparison 2

	Base Key Score	Proposed Key Score
Entropy	181.3 bits	287 bits

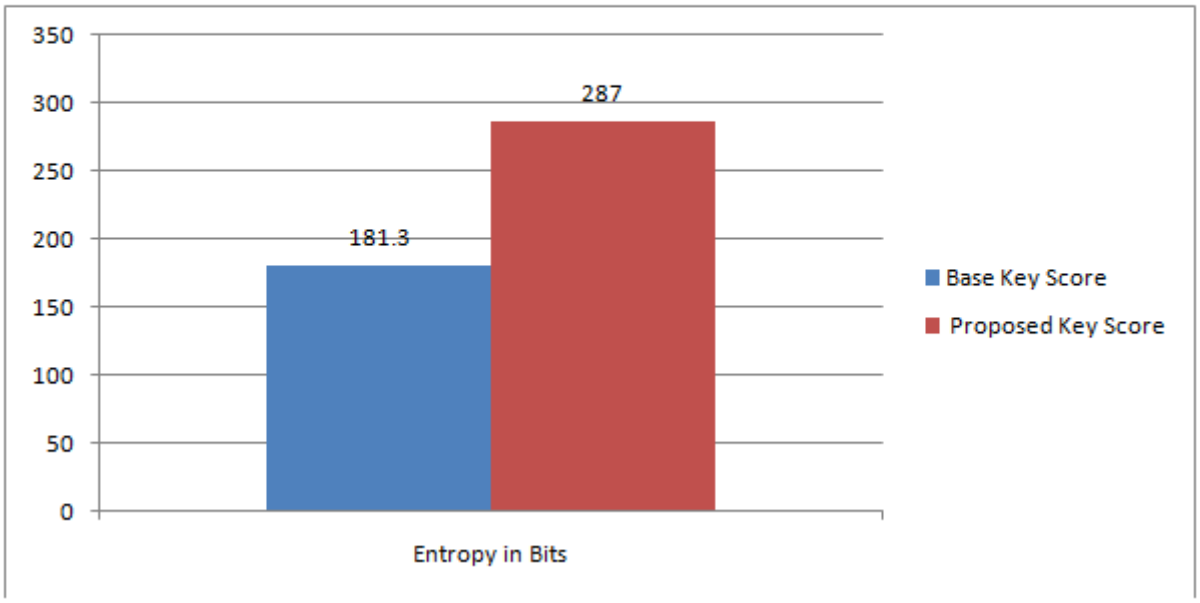

Fig 6. Graphical Comparison Test Case 2

5.3 Tool 3: Cryptool

CrypTool is an open-source venture. The primary outcome is the free e-learning programming CrypTool showing cryptographic and cryptanalytic ideas. As indicated by "Hakin9", CrypTool is worldwide the most across the board e-learning programming in the field of cryptology.

Table 3 Security Strength Comparison 3

	Base Key Score	Proposed Key Score
Entropy	2.41 value	3.807 value

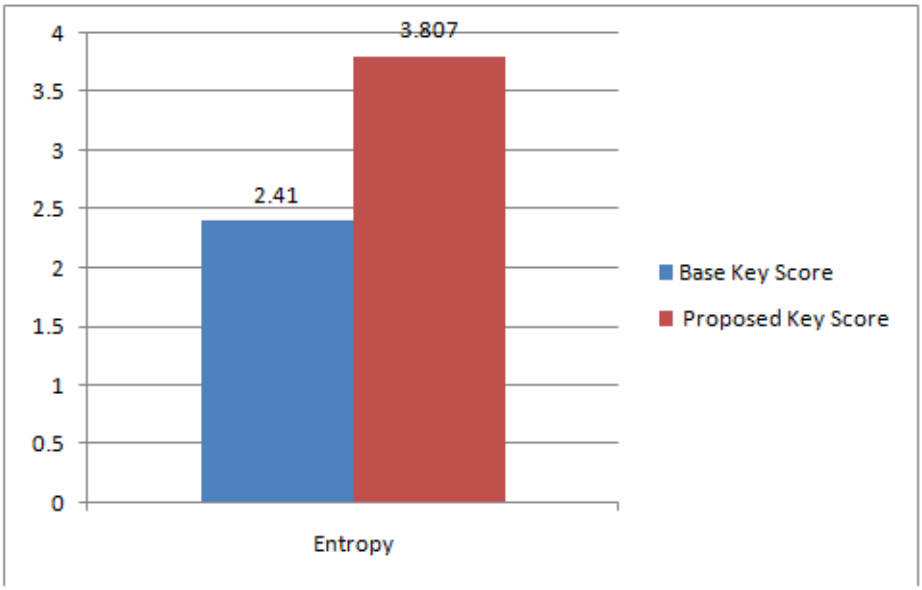

Fig 7 Graphical Comparison Test Case 3

VI. CONCLUSION

Discussing the data with the data security is must in each exchange. With the expansion of the innovation, data hazards are additionally expanding. Seeing, the significance of the data security we are proposing the protected data correspondence system with the shared validation utilizing the idea of the network situation of the picture with the relationship of the ASCII esteems in the brace position to shape the example and the idea of the meeting token in utilized for the correspondence between the two clients with contribution of the photographs the clients has picked at the hour of the enlistment and hash calculations for the arrangement of the example including the hash succession. Along with the last the hank shake idea of the symbolic erasure after the trustworthiness approval of the data is likewise done so as to ensure the best possible conveyance of data.

REFERENCES

1. S. Pandey, R. Motwani, P. Nayyar and C. Bakhtiani, "Multiple access point grid based password scheme for enhanced online security," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, 2013, pp. 144-148.
2. S. Agrawal, A. Z. Ansari and M. S. Umar, "Multimedia graphical grid based text password authentication: For advanced users," 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), Hyderabad, 2016, pp. 1-5.
3. Manishaben Jaiswal "GAME DEVELOPMENT PRINCIPLE, ARCHITECTURE AND METHODOLOGY", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.3, Issue 5, page no.267-270, May-2016, DOI Member: 10.6084/m9.jetir.JETIR1912034 Available at: http://www.jetir.org/view?paper=JETIR1912034
4. AJ. Kadhim, Raaed K. Ibrahim, Ali SH. Alkhalid,"Implementation of Secure Hash Algorithm Sha-2 256 by using Labview ",Proceedings of 2015 International Conference on Image Processing, Production and Computer Science (ICIPCS'2015) ,Istanbul (Turkey), June 3-4, 2015 pp. 112-119.
5. A. S. Eissa, M. A. Elmohr, M. A. Saleh, K. E. Ahmed and M. M. Farag, "SHA-3 Instruction Set Extension for A 32-bit RISC processor architecture," 2016 IEEE 27th International Conference on Application-specific Systems, Architectures and Processors (ASAP), London, 2016, pp. 233-234.
6. Sachin Malhotra and Munesh C. Trivedi,"Symmetric Key Based AuthenticationMechanism for Secure Communicationin MANETs",Spinger ,2018
7. Manishaben Jaiswal, "COMPUTER VIRUSES: PRINCIPLES OF EXERTION, OCCURRENCE AND AWARENESS ", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 4, pp.648-651, December 2017, http://doi.one/10.1729/Journal.23273 Available at http://www.ijcrt.org/viewfull.php?&p_id=IJCRT1133396
8. Anjali Somwanshi, Devika Karmalkar, Sachi Agrawal, Poonam Nanaware,Mrs. Geetanjali Sharma ,"Dynamic Grid Based Authentication With Improved Security",International Journal of Advances in Scientific Research and Engineering (ijasre),2017
9. Manishaben Jaiswal "Big Data concept and imposts in business" International Journal of Advanced and Innovative Research (IJAIR) ISSN: 2278-7844, volume-7, Issue- 4, April 2018 available at: http://ijairjournal.in/Ijair_T18.pdf
10. A. Agarwal and S. J. Singh, "Mask IDs based asymmetric session key exchange," 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC), Chirala, 2017, pp. 418-422.
11. A. Carreto, M. A. Diaz and B. Carvajal, "Developing an implementation model and Architecture Standard Digital ID," 2016 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa, 2016, pp. 1-6.
12. Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen and L. Fang, "Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol With Extended Security Model," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1382-1392, June 2017.
13. K. Lin, L. Yuan and G. Qu, "SecureGo: A Hardware-Software Co-Protection against Identity Theft in Online Transaction," 2007 ECSIS Symposium on Bio-inspired, Learning, and Intelligent Systems for Security (BLISS 2007), Edinburgh, 2007, pp. 59-64.
14. Manishaben Jaiswal " SOFTWARE QUALITY TESTING " International Journal of Informative & Futuristic Research (IJIFR) , ISSN: 2347-1697 , Volume 6, issue -2 , pp. 114-119 ,October-2018 Available at: http://ijifr.com/pdfsave/23-12-2019214IJIFR-V6-E2-23%20%20OCTOBER%202018%20a2%20files%20mergeda.pdf
15. H. Al Housani, JoonsangBaek and Chan YeobYeun, "Survey on certificateless public key cryptography," 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, 2011, pp. 53-58.
16. H. Wang, D. He and S. Tang, "Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165-1176, June 2016.
17. M. Sarvabhatla and C. S. Vorugunti, "A secure and robust dynamic ID-based mutual authentication scheme with smart card using elliptic curve cryptography," 2015 Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA), Bengaluru, 2015, pp. 75-79.
18. Z. Gao, S. H. S. Huang and W. Ding, "Cryptanalysis of three dynamic ID-based remote user authentication schemes using smart cards," 2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS), Chongqing, 2016, pp. 44-52.

.