NOVEL ALGORITHM FOR DATA COMMUNICATION USING THREE KEYS AND SHA

Priyanka Agarwal[1], Yogesh Kumar Tiwari[2]
[1]M.Tech Scholar, [2]Assistant professor HOD (ECE specialization in Digital Communication),
[1,2]Chandravati Group of Institutions, Bharatpur.

Abstract: Secure data communication is the primary objective of any of the data communication system. The proposed concept provides the unique concept for the user authentication as well as the communication system. The concept is using the three keys on the basis of the user name , date of birth and email id in the case of the user authentication and the concept of the using these three keys and the combination of the selected picture names with the OTP pattern. The results of security which are achieved are quite promising.

Keywords: Secure communication, Data sending, User Authentication

I. INTRODUCTION

Web personality, in like manner online character or web persona is a social character that an Internet client sets up in online gatherings and locales. It can moreover be considered as a successfully created presentation of oneself. Though a couple of individuals use their certifiable names on the web, some Internet clients like to be puzzling, perceiving themselves by techniques for nom de plumes, reveal fluctuating proportions of before long recognizable information. An online personality may even be constrained by a client's relationship to a particular get-together they are a bit of on the web. Some can even be misdirecting about their character. [1]

In some online settings, including Internet discussions, online visits, and extraordinarily multiplayer online pretending diversions (MMORPGs), clients can address themselves outwardly by picking an image, an image estimated sensible picture. Images are one way clients express their online character. Through cooperation with various clients, a set up online character picks up a reputation, which enables various clients to pick whether the personality is meriting trust. Online characters are connected with clients through confirmation, which generally requires enlistment and marking in. A couple of destinations in like manner use the client's IP convey or following treats to recognize clients. [1]

There are basically two clarifications behind restricting a client to a personality:

- The client personality is a parameter in access control decisions
- The client personality is recorded when logging security-significant events in a survey trail

The central matter is required for the framework to enable granularity in access control. In case we don't have the foggiest idea who the client is we can't know the client's rights, beside single client frameworks. The usage of a character isn't appropriate for physical clients, framework shapes furthermore require access control and ought to be recognized. [1]

II. RELATED WORK

Z. Pan and L. Zhang [1] In this letter, compressive worldly apparition imaging with tumultuous laser is connected to optical encryption with great time-controllable irregular qualities and a moment request time relationship property. The security, attainability, and appropriateness of our strategy are confirmed based on the exploration on the encryption system. The examination proposes the strategy can acquire great recuperation signal, oppose clamor attack, and apply to various types of sign. This procedure can be quickly connected to encryption and media transmission with the benefits of high security, wide pertinence, and high caliber of remade data.

R. Bassous, H. Fu and Y. Zhu[2] In this paper we present and portray every one of the tests and results that are done on "Questionable Multi-Symmetric Cryptography" (AMSC). We contrast AMSC with symmetric and hilter kilter ordinary calculations including AES and RSA. We explain AMSC center strategies in subtleties alongside the trial setup and execution. Moreover, we structure and actualize a constant application as a proof of idea for AMSC. The application utilizes TCP/IP Multicast convention to send numerous messages in a single cipher-text utilizing the AMSC calculation.

A. Sarkar and B. K. Singh [3] Most of the current calculations of key age for symmetric cryptographic utilize a private key having size of 128, 192 or 256 bits. These long keys are hard to recollect, thus, put away in keen card; alter safe token, and so forth or secret word based validation strategy is utilized to control the entrance of cryptographic key. However, these client chose passwords now and again lost or speculated by word reference attacks. In addition, in symmetric cryptography, sender and collector must have a similar mystery key and the key must be verified which prompts another risk of security. As a substitute to this, age of cryptographic key utilizing the biometric characteristics of both sender and collector during the sessions of correspondence can be a conceivable arrangement of the above talked about key administration issue. In any case, the issue with biometrics is that once it gets traded off it can't be reused. As a capable answer for dropping and reissuing biometric format cancelable biometrics has been proposed.

The present work proposed to create 128 piece symmetric key from cancelable unique mark formats of both imparting parties. The present methodology affirms the security of fingerprints by one route change of unique format into cancelable one just as purposes the trouble of key stockpiling and key conveyance as the key isn't sent to the beneficiary and is additionally not spared anyplace.

J. Won, A. Singla and E. Bertino[4] Assured Mission Delivery Network (AMDN) is a collective system to help data gathered logical joint efforts in a multi-cloud condition. Each logical cooperation gathering, called a mission, shows a course of action of standards to manage enrolling and organize resources. Security is a basic bit of the AMDN plan since the rules must be set by affirmed customers and the data created by each mission may be protection delicate. In this paper, we propose a Certificate Less cryptography-based Rule-organization Protocol (CL-RP) for AMDN, which supports approved oversee selections and updates with non-denial. We evaluate CL-RP through demonstrating ground examinations and difference it and other standard shows.

J. H. Jeong, J. O. Kim, T. Y. Kim and J. R. Choi[5] In this paper, autors present a region proficient crypto chip for sharing and choosing the equipment activity of the one open key cipher and three square ciphers (ECC, AES, ARIA, and HIGHT) and reconfigurable crypto chip of an exhibit processor-based cryptography calculation. In light of the proposed processor, we structured an encryption chip that diminished the absolute territory of ECC, AES, ARIA and HIGHT by 21% utilizing 0.18μm CMOS innovation. Likewise, Cryptography Array Processor (CAP) of ECC, AES, ARIA, and HIGHT demonstrates superior at 40Kbps, 1,085 Mbps, 746 Mbps and 175 Mbps individually. The proposed plan of crypto chip demonstrates the reconfigurable adaptability of the encryption calculation and high equipment execution.

III. PROBLEM DEFINITION

The main issue is to develop the more genuine authentication system which will be difficult to crack as well as to develop the secure system for the file transfer.

Proposed Work

The proposed work is developed in the Matlab and the development is made in the two phases,

The first phase of the development is the user registration in which we are creating the user data base who will be allowed to perform the data transfer.

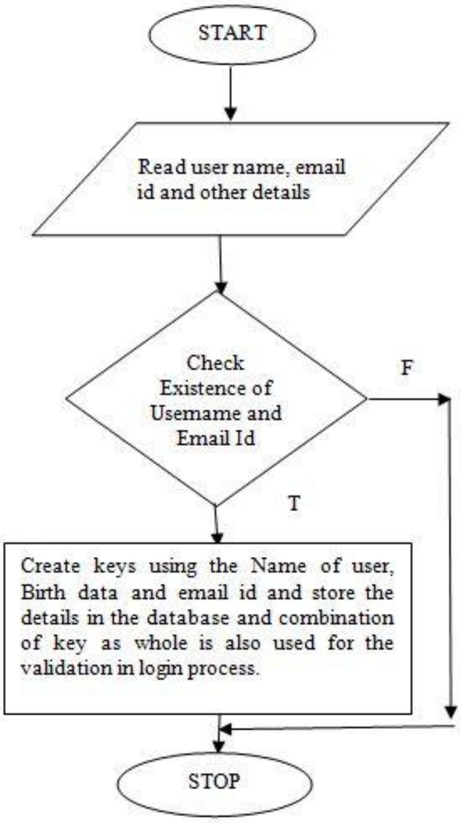

START
Read user name, email id and other details
Check Existence of Username and Email Id
F
T
Create keys using the Name of user, Birth data and email id and store the details in the database and combination of key as whole is also used for the validation in login process.
STOP

Fig 1. User registration

After the user get registered, the next step is the user login. The same credentials will them be user for the accessing of the user access.

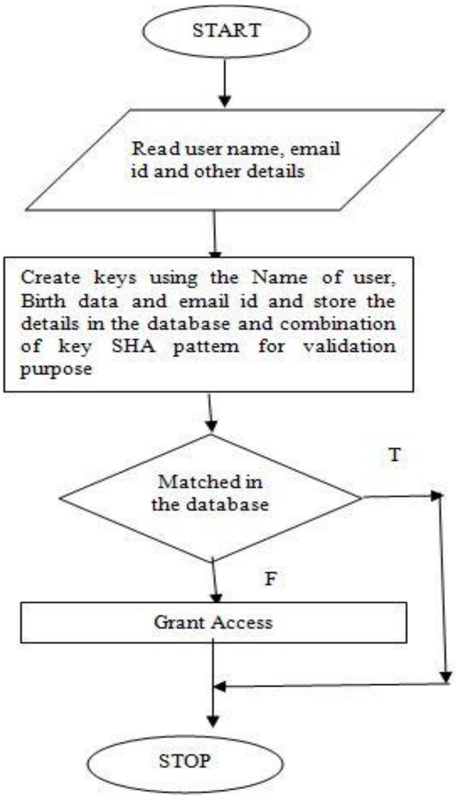
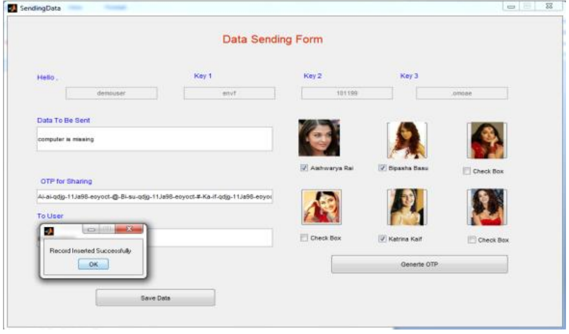

START
Read user name, email id and other details
Create keys using the Name of user, Birth data and email id and store the details in the database and combination of key SHA pattern for validation purpose
Matched in the database
T
F
Grant Access
STOP

Fig 2. User Login

The similar is the concept which is used in the data sending and receiving, in this the users will make use of the Keys which are used in the time of the login or registration , then these are combined with the alphabets combination of the pictures which are checked or selected by the user and also some special character to further improve the strength.



demouser
envf
101199
.omoae

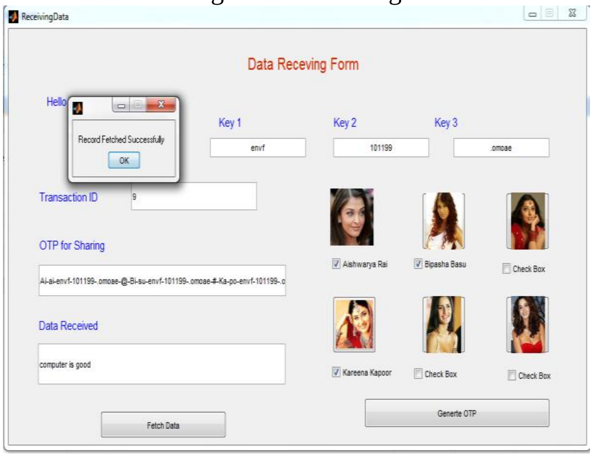
computer is missing

Ai-ai-qdjg-11Ja98-eoyoct-@-Bi-su-qdjg-11Ja98-eoyoct-#-Ka-if-qdjg-11Ja98-eoyo

☑ Aishwarya Rai ☑ Bipasha Basu □ Check Box
□ Check Box ☑ Katrina Kaif □ Check Box

Record Inserted Successfully

Fig 3. Data Sending



Record Fetched Successfully

envf
101199
.omoae

9

Ai-ai-envf-101199-.omoae-@-Bi-su-envf-101199-.omoae-#-Ka-po-envf-101199-.o

computer is good

☑ Aishwarya Rai ☑ Bipasha Basu □ Check Box
☑ Kareena Kapoor □ Check Box □ Check Box

Fig 4. Data Receiving

The data structure which is used for storing the details regarding the data sending and receiving is maintained in the Microsoft Access and the structure which is used for the storage purpose is shown in table 1.

Table 1. Storage structure for Sending /Receiving data

S.No.	Fieldname	Description
1	Fuser	This field is used for storing the user name of the sender
2	Key1	The generated key 1
3	Key2	The generated key 2
4	Key3	The generated key 3
5	Tuser	This field is sued for storing the user name of the receiver
6	Data	It will store the data to be shared
7	OTP	The generated OTP will be stored in this field
8	Tid	It is the auto number field for the transaction id

IV. RESULT ANALYSIS

This section corresponds to the result analysis in which the generated OTP pattern for the login authentication or the data sharing is compared on various tools for the purpose of checking the strength of that OTP. First using the various tools like the password checker, cryptool2 and other online tools , the OTP generated using the base approach is provided as the input to these tools and the result related to the strength of the OTP for the base work or concept is shown in the table 2.

Table 2. Base Work Strength Check

OTP	Website/Tool	Result
ABCDE	Kaspersky Password Checker	Too Short Cracked in 1 Second
ABCDE	www.my1login.com/resources/password-strength-test/	Very Weak Cracked 0 Second
ABCDE	Cryptool2	Entropy 2.322 Strength 16 Very Weak

Then using the various tools like the password checker , cryptool2 and other online tools , the OTP generated using the proposed approach is provided as the input to these tools and the result related to the strength of the OTP for the base work or concept is shown in the table 3.

Table 3. Proposed Work Strength Check

OTP	Website/Tool	Result
Ai-ai-envf-101199-.omoae-@-Bi-su-envf-101199-.omoae-#-Ka-po-envf-101199-.omoae-%-	Kaspersky Password Checker	10000+centuries Extremely Strong
Ai-ai-envf-101199-.omoae-@-Bi-su-envf-101199-.omoae-#-Ka-po-envf-101199-.omoae-%-	www.my1login.com/resources/password-strength-test/	**15 million trillion trillion trillion trillion trillion trillion trillion trillion trillion years Review:** Fantastic, using that password makes you as secure as Fort Knox.
Ai-ai-envf-101199-.omoae-@-Bi-su-envf-101199-.omoae-#-Ka-po-envf-101199-.omoae-%-	Cryptool	Entropy 3.881 Strength 186 Extreme Strong

V. CONCLUSION

In respect of the data security the proposed work is not only better than the base paper work which is taken for the comparison analysis but also it has the strength via which it is much more secure as compare to the existing alternatives.

REFERENCES

[1] Z. Pan and L. Zhang, "Optical cryptography-based temporal ghost imaging with chaotic laser,"IEEE Photon. Technol.Lett., vol. 29, no. 16, pp. 1289–1292, Aug. 2017

[2] Bassous, R. , Mansour, A. , Bassous, R. , Fu, H. , Zhu, Y. and Corser, G. ,"Ambiguous Multi-Symmetric Scheme and Applications. Journal of Information Security", 2017.

[3] Sarkar, A.; Singh, B.K. ,"Cryptographic key generation from cancelable fingerprint templates",

In Proceedings of the 2018 4th International Conference on Recent Advances in Information Technology (RAIT),2018

[4] J. Won, A. Singla, E. Bertino and G. Bollella, "Decentralized Public Key Infrastructure for Internet-of-Things," MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), 2018.

[5] J. H. Jeong, J. O. Kim, T. Y. Kim and J. R. Choi, "Reconfigurable array-based design for flexible cryptography chip architecture," 2017 13th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME), Giardini Naxos, 2017, pp. 345-348.

[6] Hong Deukjo et al. "HIGHT: A new block cipher suitable for low-resource device" International Workshop on Cryptographic Hardware and Embedded Systems 2006.

[7] Daniele. Fronte Annie. Perez "Celator: a multi-algorithm cryptographic co-processor" International Conference on Reconfigurable Computing and FPGAs 2008.

[8] Gokhan. Sayilar Derek. Chiou "Cryptoraptor: High Throughput Reconfigurable Cryptographic Processor" International Conference on Computer-Aided Design (ICCAD) 2014.

[9] Jun-Hong. Chen Ming-Der. Shieh "A High-Performance Unified-Field Reconfigurable Cryptographic Processor" IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS vol. 18 no. 8 pp. 1145-1157 August. 2010.