INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 6)
Available online at: www.ijariit.com

Framework for information management through step sequencer

R. Arun Chakravarthy
arunchakravarthy7@gmail.com
KGiSL Institute of Technology, Coimbatore, Tamil Nadu

M. Arun
arunkset@gmail.com
KGiSL Institute of Technology, Coimbatore, Tamil Nadu

N. Kaleeswari
kalees_n2003@yahoo.co.in
Dhaanish Ahmed Institute of Technology, Coimbatore, Tamil Nadu

P. Manivannan
pctmani@gmail.com
Park College of Technology, Coimbatore, Tamil Nadu

D. Prabha
prabha@skcet.ac.in
Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu

ABSTRACT

Data is now commonly stored in digital format because it is the most secure way to store, manage, access and share information across networks. However, there is always a risk that unauthorized users will access data and, in the worst case, that malicious hackers will modify the data. The symmetric cryptosystem is used in the approach proposed. The symmetric cryptosystem is used in the proposed method. Data is divided into two sub-blocks and each block is encrypted to provide enhanced security using three separate secret keys. This deterministic algorithm is implemented using the LabVIEW tool. One of the three keys that diffuses the one other key provided by the information is for misunderstanding. In the proposed solution blocks the main search attacks heavily. There are two separate secret keys used and to improve the robustness of the algorithm, random rotation is applied.

Keywords— *Cryptosystem, Random rotation, Symmetric cryptosystem*

1. INTRODUCTION

Development and advances in this digital world have become so inevitable that all internet-connected devices have made communicating work very easy. The need for security comes as interaction is simpler [1]. It is said that data is secure until it is corrupted. The need for secure communication is the need for the hour as individuals are more concerned about privacy. Security is a decisive factor which plays a major role in today's arena where the information is disclosed having a negative thought on the growth of any pattern [2]. Safety is of greater importance and interest. Recent digital applications require security that is both more reliable and special. Confidential information must be transmitted securely without being scrutinized by malicious people. The protected information is transmitted by unauthorized persons without becoming known [3]. The data breach has emerged as a major factor affecting both small and large businesses. Safety can indeed be maintained by encrypting it and have different encryption methods [4]. The system of cryptography has both the formal and informal keys [5]. Everything depends on the level of software that are concerned with end product.

Within the case of an application which bargains with online shopping can be tended to with a moo level or medium level encryption whereas the money related applications ought to be concerned with more security, encryption like DES calculation is chosen, where the little botch will lead to deadly results [6]. The information isn't implied to be uncovered to all but at times due to inappropriate arrangement or due to human mistakes. The blunder can be maintained a strategic distance from, but still, a more secure way of exchanging data can maintain a strategic distance from information misfortune and at the same time guarantee that information which is in wrong hands isn't influenced since it is ensured by secured encryption [7]. The current scenarios demand that as a client got to secure the private data because it ought to not be abused by the unauthorized individuals [8].

As of now existing strategies are being compromised due to disgraceful arrangement of touchy information [9]. The most goal of cryptography is to supply secrecy by making beyond any doubt that the message is gotten as it were by the planning beneficiary. Cryptography and Steganography are the two primary building squares when it comes to security [10]. More secure transmission is the require of the hour which we bargain in our way of life beginning from online entry where we purchase essential embellishments to online installments which we do are beneath all dangers as possibly destructive assaults are habitually made these days [11]. Labview may be a straightforward graphical representation of calculations in a user-friendly way. The approach of implanted frameworks within the current situation has made the utilization of LABVIEW in a more advanced way. The genuine world is in require of the user-friendly stage where working as require of the hour is the way better security of mystery data utilizing different encryption strategies. Not as it were in information but too in picture as well.

Cipher block chaining is a better technique for image encryption. Documentation using paper has become an outdated technology nowadays people are more concerned with having a centralized database. Cryptography is a method of making information unpredictable by modifying it to ensure secure transfer of sensitive data. When it comes to image encryption, we have randomization of pixel position to make sure that there is shuffling of the data security is one of the major parameters which needs to be preserved be it social information or personal information. Cipher square chaining may be away better procedure for picture encryption. Documentation utilizing paper has ended up an obsolete innovation these days individuals are more concerned with having a centralized database. Cryptography could be strategy of making data erratic by altering it to guarantee secure exchange of sensitive data. When it comes to picture encryption, we have randomization of pixel position to create beyond any doubt that there's rearranging of the information security is one of the major parameters which ought to be protected be it social data or individual data. Vigor of the encryption is obligatory for any application as this proposed strategy guarantees that this characteristic is guaranteed [14]. Besides, the complicated plans of the Advanced Flag Preparing and FPGA plans can be created and executed in this stage in a much easier way [15]. The requirement of the hour is to scramble and descramble the information. By AES cipher unit the plain content is being scrambled or decoded utilizing arbitrary key era [16].

This paper comprises of three areas; to begin with area conversation approximately the crypto framework proposed. Moment segment bargains with the result of the approach, in which comes about and resistivity against the assaults too examined. Proposed strategy is compared with the accessible writing. Third and final segment is the conclusion of the approach.

2. MATERIALS AND METHODS

Any organization should center on security angles which are done by cryptosystem. In which, encryption module gets the plaintext for encryption and the resulting cipher content is put away within the database server. The cipher content can be changed over back to plain content after passing through a decoding module of a cryptosystem which is appeared in figure 1.

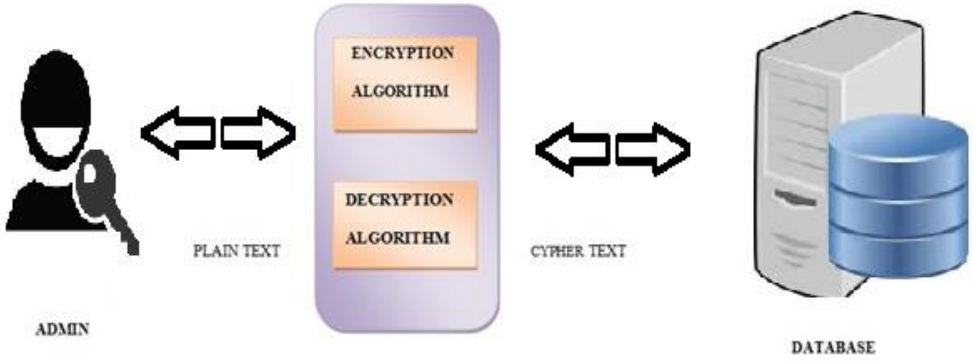


Fig. 1: Date security framework

2.1 Encryption Algorithm

Step 1: Collect data to be stored as plain text (P)
Step 2: Compute math expansion between P (i) and secret key S1, where i →0 to size of P
Step 3: Sum = X
Step 4: Get X1[] and X2[]
Step 5: Compute Z1 [] = X1[] >> p and Z2 []= X1[] >> q, Provided p ≠q
Step 6: Divide as
T = Modulo div (Z1 [], S2)
U = Modulo div (Z2 [], S2)
Step 7: Form Cipher text = Insertion between T and U

In this proposed approach, encryption employments two diverse mystery keys. Key S1 may be a haphazardly chosen expansive prime number and key S2 is huge Armstrong number. Other than mystery keys, a number of turns (p & q as third key) moreover offer assistance to extend the information disarray and dissemination [12]. Decoding takes after the mystery keys and switched calculation.

2.2 Decryption algorithm

Step 1: Reverse the cipher text into binary Z []
Step 2: Decimation Z [] such that Z1[] and Z2[]
Step 3: Create module:
T= Modulo div (Z1 [], S2)
U = Modulo div (Z2 [], S2)
Step 4: Compute Z1 [] = S1[] >> len(S1[]) - p & Z2[]=S2[] >> len of (S2[]) - q,where p ≠ q
Step 5: Z []= Insertion between S1[] & S2[]
Step 6: Plain text=P1-S[i], where i →0 to size of P

3. SIMULATION RESULTS AND DISCUSSION

3.1 File storage phase

The plaintext should be scrambled given to the cryptosystem and the output cipher text is put away within the database. The system is executed in LabVIEW which is made for the encryption calculation, which gets input from the client record. The yield of subVI is composed into the record as cipher content with instrument. The same is appeared in figure 2a and 2b.

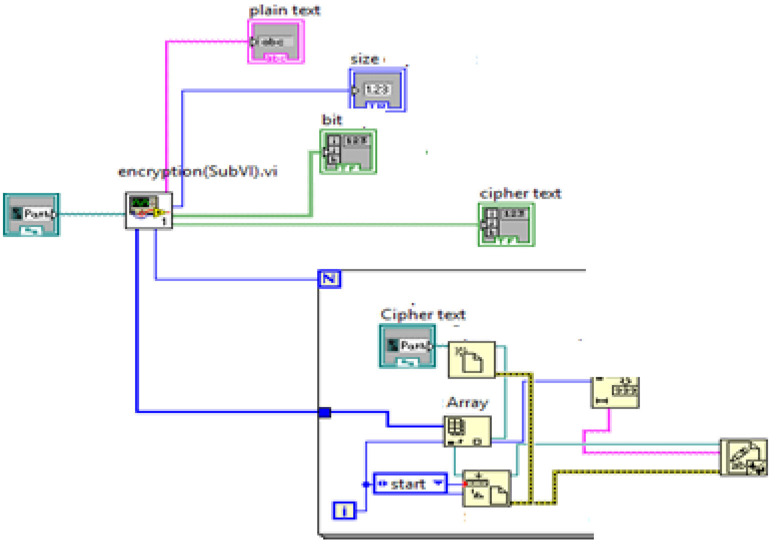


Fig. 2: Encryption Algorithm

3.2 File Retrieval Phase

Within the decoding portion, the cipher content is passed through the cryptosystem where it is decoded back to induce a plain content. Decoding calculation is actualized within the frame of sub VI, which is outlined utilizing LabVIEW in figure 3 portrays the Piece chart and Front board individually.

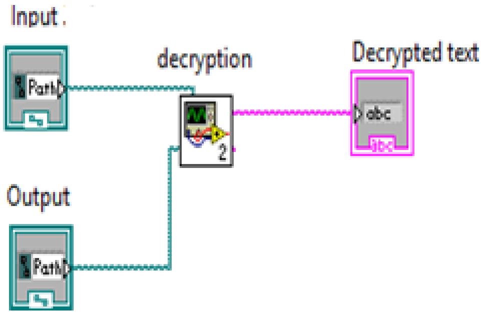
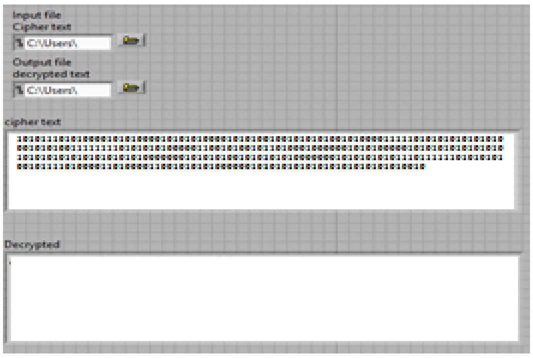


Fig. 3(a): Decryption Algorithm



Input file
Cipher text
C:\Users\

Output file
decrypted text
C:\Users\

cipher text
[illegible]

Decrypted

Fig. 3(b): Panel

3.3 Proposed System for Resistance to threat Algorithm

The proposed approach is highly blocking the key search attack since there are three different keys available. K1 is hard to factorize, K2 is large Armstrong number. There is no relation between K1 & K2. Rotation factors n & m also playing a role of the key. Existing algorithms have an issue on its key space, so they do not resist Brute force attack [5]. Cryptanalytic attacks such as cipher text-only, chosen cipher text are also impossible because the proposed approach is exceedingly blocking the key look assault since there are three diverse keys accessible. K1 is difficult to factorize, K2 is expansive Armstrong number. There's no connection between K1 & K2. Turn variables n & m moreover playing a part of the key. Existing calculations have an issue on its key space, so they don't stand up to Brute constrain assault [5]. Cryptanalytic assaults such as cipher text-only, chosen cipher text are more over inconceivable since through mystery keys as it were recuperation is conceivable. Comparison of proposed strategy with writing is arranged in table 1.

Table 1: Comparison of Algorithms with Proposed Method

Algorithm	Key word Search	Cipher text	Key Size
DES key[5]	No resistance	-	Single key Upto 56 bits
PBE key[9]	No resistance	-	Size of the Message
Proposed method	Resistance	Resistance	3 keys S1 = S2 = 32 bits S3 = Revolving pattern (p,q)

4. CONCLUSION

In this proposed work, the cryptosystem has been viably utilized, so that the unauthenticated get to secret information has been killed by utilizing private keys. There are two diverse mystery keys utilized and arbitrary turn is connected for expanding strength of the calculation. In this way making the information secure as well as improving the efficiency of the method by consolidating the highlights accessible in LABVIEW will offer assistance in maintaining a strategic distance from an information breach and at the same time giving superior efficiency. This approach can be mixed with reconfigurable equipment in future.

5. REFERENCES

[1] Sun, Y., Y. Zhang and G. Zhu, 2014. Data security and privacy in cloud computing. Int. J. Dist. sens. Net. 10(7):190903.

[2] Iyer, S., 2011. Cyber security for the smart grid, Cryptography, and privacy. Int. J. Dig. Mul. Broadcasting.

[3] Abomhara, M., O. O. Khalifa, O. Zakaria, A. A. Zaidan, B. B. Zaidan and H. O. Alanazi, 2010. Suitability of using Symmetric Key to secure Multimedia Data. J. Applied Sci: 1656- 1661.

[4] Bruise Schneier, 2001. Applied cryptography: protocols, Algorithms, and source code in C. 2e, John Wiley &Sons.

[5] Saranya, K., R. Mohanapriya and J. Udhayan, 2014. A Review on Symmetrical key Encryption techniques in cryptography, Int. J .Sci. Eng. Res Technology., 3:539-544.

[6] Najaflou Y., B. Jedari, F. Xia, L.T. Yang and M. S. Obaidat, 2015. Safety challenges and solutions in mobile social networks, IEEE Systems Journal 9:834-854.

[7] Biondi F., T. Given-Wilson and A. Legay, 2016. Attainable unconditional security for shared key cryptosystems, Information Sciences 369:80-99.

[8] N. Chidambaram, P. Raj, K. Thenmozhi, and R. Amirtharajan, 2016. Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique. Int. J. Digit. Multimed. Broadcast. vol.2016.

[9] Juels, A. and T. Ristenpart, 2014. Honey encryption: Encryption beyond the brute-force barrier. IEEE Security., 12:59-62.

[10] Janakiraman, S, R. Amirtharajan, K. Thenmozhi and J. B. B. Rayappan, 2012. Firmware for data security. Res. J. Inform. Technol., 61-72.

[11] Park S. B., 2015. Security requirements for multimedia archives, Advances in Multimedia.

[12] K. Nanthini, D. Prabhakaran, C. Ramkumar, “An Intelligent System for Forest fire detection Using Anisotropic diffusion And Fuzzy C- Means Algorithm”, International Journal of Innovations in Scientific and Engineering Research (IJISER), Vol 2 no 12,pp238-241,2015.

[13] Essick J., 2013. Hands-on introduction to LabVIEW for scientists and engineers. Oxford University Press.

[14] Praveenkumar, P., G. U. Priyanga, K. Thenmozhi, J. B. B. Rayappan and R. Amirtharajan, 2015. Chain of shuffling and chaos.Asian.J.Sci.Res:359-366.

[15] Bossuet,L., L. Grand, V. Gaspar, V. Fischer, G. Gogniat, 2013. Architectures of flexible symmetric key crypto engines-a survey: From hardware coprocessor to multi-crypto- processor system on chip, ACM computing Surveys, 45.

[16] Yaakob, W.F., J. Sampe and N. Kamal, 2017. FPGA implementation of rapid ciphering and high Throughput of smart card memory ciphering system. Asian J. Sci. Res., 10(2):88-96.

[17] Nithye C, et. al. 2018 Framework for data security through virtual instrument – A diffused cipher model International Journal of Pure and Applied Mathematics, Vol 119, No.16, pp. 547-554.