A New Way of Design and Implementation of Hybrid Encryption to Protect Confidential Information from Malicious Attack in Network

Sitesh Kumar Sinha
Professor
AISECT University Bhopal

Mayank Shrivastava
Research Scholar
AISECT University Bhopal

Krishna Kumar Pandey
Assistant Professor, CSE Deptt,
AISECT University Bhopal

ABSTRACT

Because of the defect of only the single data encryption and the use of famous encryption algorithm, which was not improved in traditional methods of the registration process, a combined encryption algorithm is proposed in this paper. That is, the algorithm security is greatly improved, through researching several famous data encryption algorithms, and improving some data encryption algorithms. In this paper, a new hybrid crypto [1, 2, 3] concept is proposed which is the combination of new symmetric and message digesting function (MD-5). Moreover, the security and performance of the proposed technique is calculated and the presented results showing the performance of the proposed technique.

Keyword

Encryption, Decryption, Security, Image, Cryptography, Pixel.

1. PROPOSED WORK

The objective of the proposed work is to design and develop a technique that mediates the user and the operations to achieve security. As known that encryption provides strong security for information at rest. Initially that proposed technique is suitable for small amount of information. The performance and security issues have considered in the proposed work because it all ready known that in real-world scenarios, these are complex issues and experts should be used who understand all available options and the impact for each particular customer environment. This work will prove less query execution times from proposed technique. The objective of proposed work is

- Encrypted information should be in unreadable
- Proposed concept is extending user authentication
- Proposed concept providing security whenever transmitting information from one node to another node because it's important to protect the information whiles it's in transit.
- Proposed concept is the design of a new cryptography algorithm for encryption and decryption at user end on user data.
- The proposed algorithm is based on a symmetric block cipher.
- The performance and strength of proposed algorithm is expected to be better than conventional cryptographic algorithm and highly effective against brute force attack.

From the study of previous researches it is observed several limitations despite the promise it holds. Most of the techniques use one operation which is floating point operation. Due to this operation execution time of the process increased. It has been observed in previous techniques that they are not reliable. Implementation of previous techniques is easy in terms of software but hardware implementation is very complicated due to complex architecture [16]. Due to lots of mathematical operations efficiency of existing algorithms has decreased [1, 2, 3, 4 and 5].

Proposed research is the designing and implementation of a new hybrid crypto system. Proposed technique is a method of encryption that combines two or more encryption technique and usually includes a combination of symmetric and message digesting technique [17] to take benefit of the strengths of each type of encryption. Basically there are four security principles “Confidentiality”, “Integrity”, “Authentication”, and “Non-Repudiation” [18, 19 and 20]. In which Symmetric Technique fulfill the concept of Confidentiality, it also provide the performance advantage and therefore is the common solution for encrypting and decrypting performance-sensitive data. On the other hand, message digests technique fulfilling the authentication as well as integrity security principle concept to provide better security for cryptographic key [21, 22 and 23].

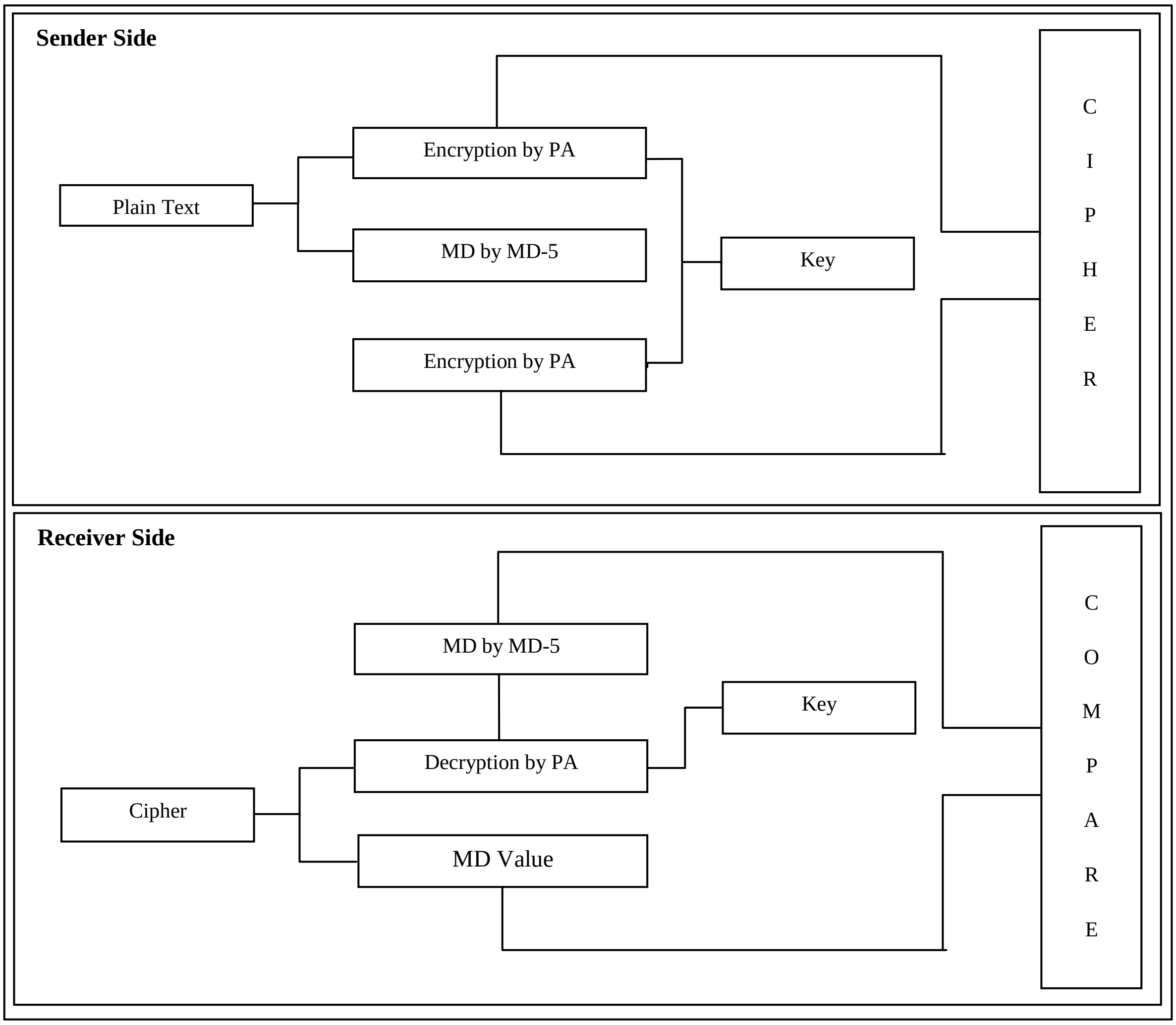

Fig. 1:- Block diagram of Proposed Hybrid crypto system

In the block diagram of proposed hybrid crypto system as show in Fig. 1, plain text encrypted by proposed symmetric encryption algorithm to produced cipher text, then message digesting function is also apply on plain text by using MD-5 [25, 26] to produce message digest of plain text. Now again apply proposed encryption technique on produced message digest text so it will also convert in cipher text. Now combine both Cipher Values (C1 and C2) into one and send to the receiver. At receiver end, separate both cipher (C1 and C2) values and apply proposed decryption algorithm one by one on each cipher value. From first cipher value plain text will get and from second cipher value C2 message digest will get. Then apply message digesting function MD-5[25, 26] on plain text which is produced during decryption to produced message digest. Now finally compare both messages digesting value with each other for changes in message digest. If both message digest are same then plain text securely received otherwise original plain text is tempered by the hacker so drop the whole information. In proposed system including two existing encryption technique and third one is newly design symmetric encryption which is based on block cipher concept and it uses series of logical operation like XOR, Circular Shift (Right, Left) [13, 14, and 15]. It already known that all the selected operation are very simple and very effectively. Due to this reason proposed system is efficient then existing system [6, 7].

Block Diagram of Proposed Encryption/Decryption: To perform encryption approach displace plain text data one by one with its coordinate limits and start performing the encryption process by using logical shift and XOR operation on binary value with key value. Fig. 2 is showing the block diagram of proposed encryption and Fig. 3 is showing the block diagram of proposed decryption. Decryption is just reverse process of encryption.

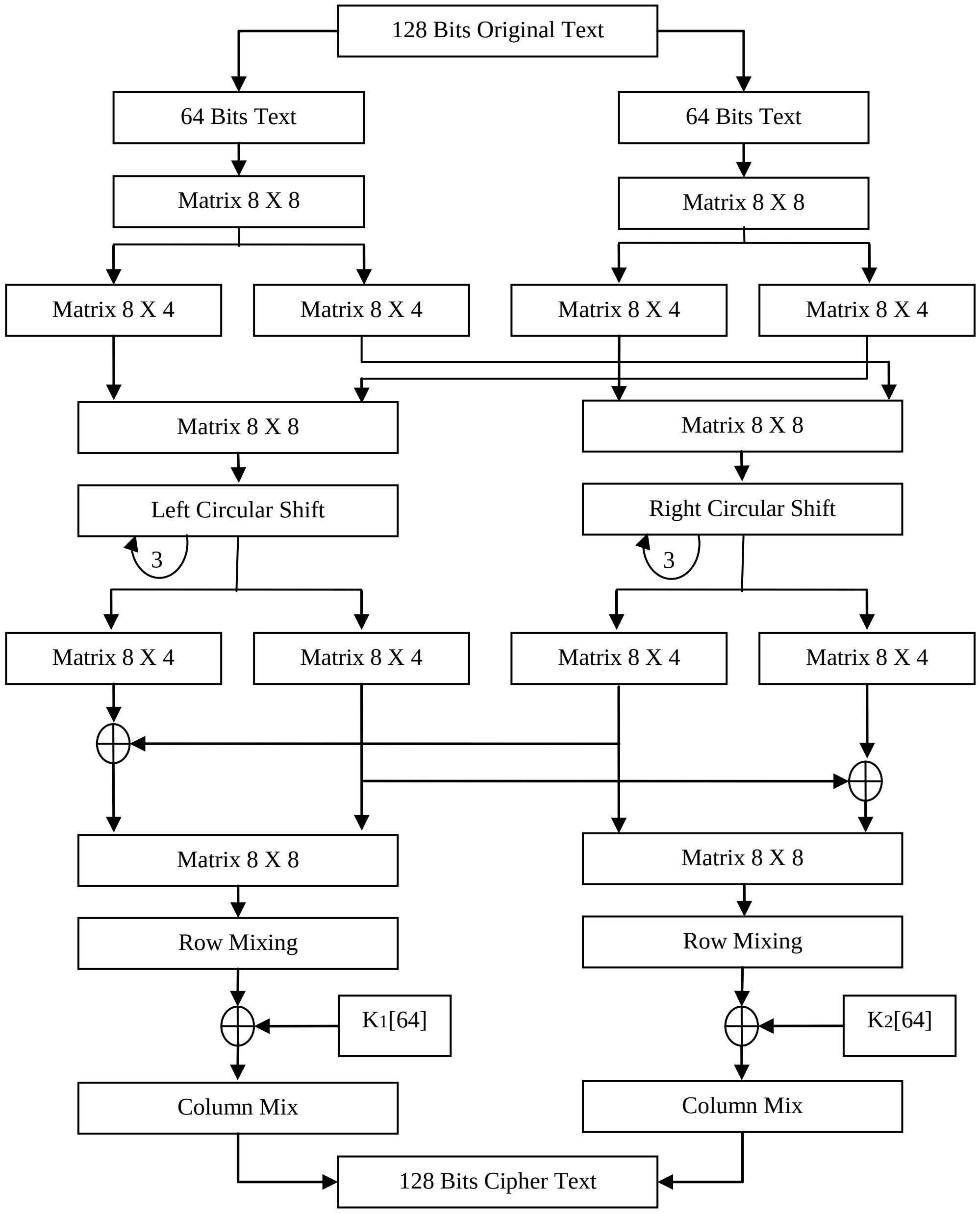

Fig. 2: Block Diagram of Proposed Encryption

Proposed Encryption Algorithm Step:

1. Input S[16] = Plain Text
2. Input K[16] = Key
3. Binary Conversion
   a. BP = Binary (Plain Text)
   b. BP_1 = First 64 Bit (BP)
   c. BP_2 = Last 64 Bit (BP)
4. Apply Matrix on BP_1 and BP_2
   a. Matrix (BP_1 (8 X 8))
   b. Matrix (BP_2 (8 X 8))
5. Dived BP_1 and BP_2
   a. Matrix (BP_{11} (8 X 4)) & Matrix (BP_{12} (8 X 4))
   b. Matrix (BP_{21} (8 X 4)) & Matrix (BP_{22} (8 X 4))
6. Exchange Content of BP_{12} and BP_{22}
7. Combine BP_{11} & BP_{12} and BP_{21} and BP_{22} into Single Matrix
   a. Matrix (BP_1 (8 X 8))
   b. Matrix (BP_2 (8 X 8))
8. Apply Left Circular Shift on Matrix (BP_1 (8 X 8)) and Right Circular Shift on Matrix (BP_2 (8 X 8))
9. Repeat 9 Step 3 times.
10. Dived BP_1 and BP_2
    a. Matrix (BP_{11} (8 X 4)) & Matrix (BP_{12} (8 X 4))
    b. Matrix (BP_{21} (8 X 4)) & Matrix (BP_{22} (8 X 4))
11. Perform XOR
    $BP_{11} = BP_{11} \oplus BP_{21}$
    $BP_{22} = BP_{22} \oplus BP_{12}$

12. Combine BP_{11} & BP_{12} and BP_{21} and BP_{22} into Single Matrix
    a. Matrix (BP_1 (8 X 8))
    b. Matrix (BP_2 (8 X 8))
13. Apply Row Mixing on BP_1 and BP_2
    a. Row_Mix (BP_1)
    b. Row_Mix (BP_2)
14. Perform XOR Between BP_1 and BP_2 with First 64 bits Key (K_1) and last 64 bits Key (K_2)
    $BP_1 = BP1 \oplus K_1$
    $BP_2 = BP_2 \oplus K_2$
15. Apply Column Mixing on BP_1 and BP_2
    a. Column_Mix (BP_1)
    b. Coulmn_Mix (BP_2)
16. Now Combine BP_1 and BP_2
    Cipher Text (CT) = $BP_1 \oplus BP_2$
17. Exit

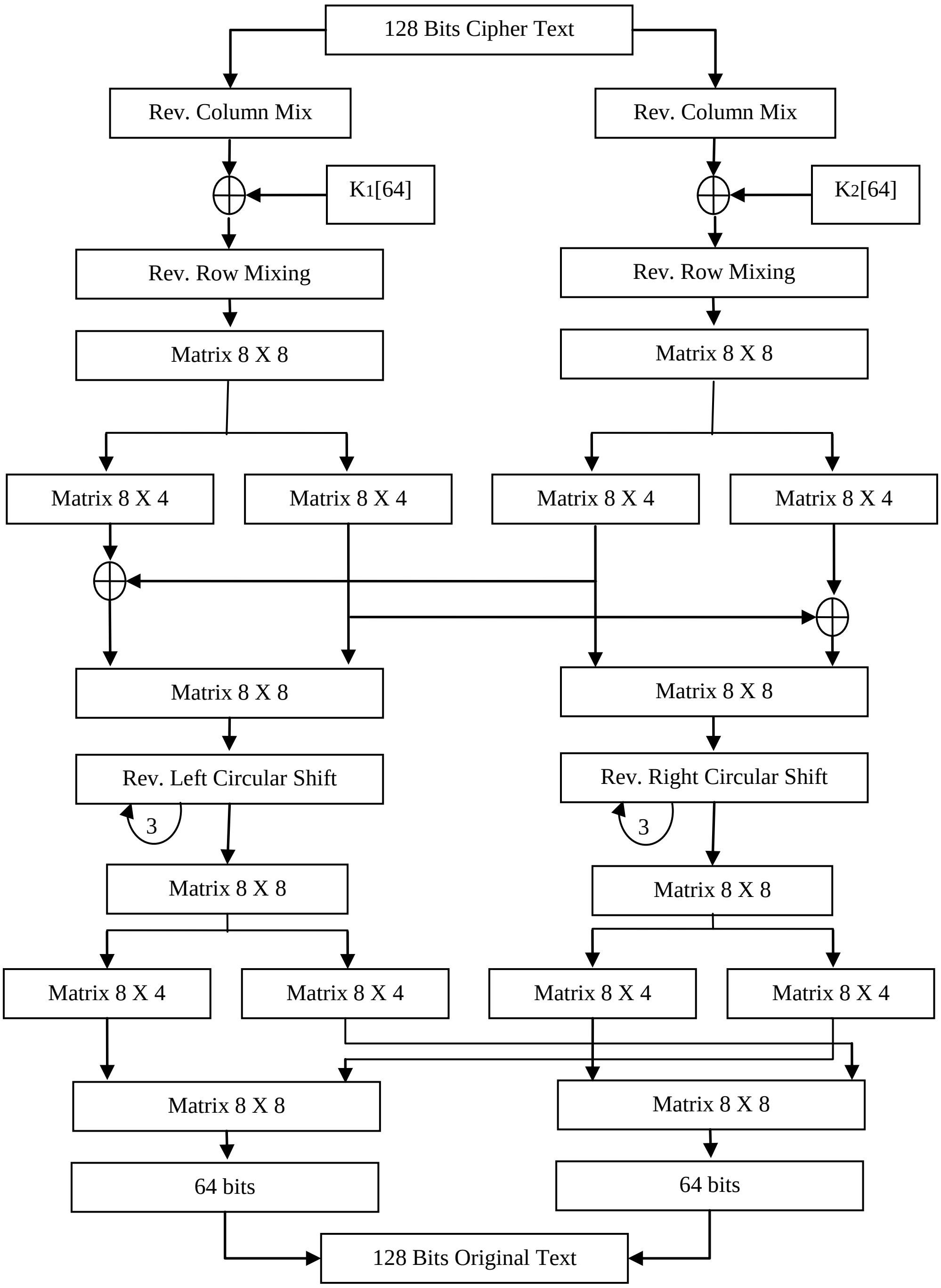

Fig. 3: Block Diagram of Proposed Decryption

Proposed Decryption Algorithm Step:

```
1.  Input C[16] = Cipher Text
2.  Input K[16] = Key
3.  Binary Conversion
        a. BC = Binary (Cipher Text)
        b. $BC_1$ = First 64 Bit (BC)
        c. $BC_2$ = Last 64 Bit (BC)
4.  Apply Reverse Column Mixing on $BC_1$ and $BC_2$
        a. Rev_Column_Mix ($BC_1$)
        b. Rev_Coulmn_Mix ($BC_2$)
5.  Perform XOR  Between $BC_1$ and $BC_2$ with First 64 bits Key ($K_1$) and last 64 bits Key ($K_2$)
        a. $BC_1 = BC_1 \oplus K_1$
        b. $BC_2 = BC_2 \oplus K_2$
6.  Apply Rev Row Mixing on $BC_1$ and $BC_2$
        a. Rev_Row_Mix ($BC_1$)
        b. Rev_Row_Mix ($BC_2$)
7.  Dived $BC_1$ and $BC_2$
        a. Matrix ($BC_{11}$ (8 X 4)) & Matrix ($BC_{12}$ (8 X 4))
        b. Matrix ($BC_{21}$ (8 X 4)) & Matrix ($BC_{22}$ (8 X 4))
8.  Perform XOR
        a. $BC_{11} = BC_{11} \oplus BC_{21}$
        b. $BC_{22} = BC_{22} \oplus BC_{12}$
9.  Combine $BC_{11}$ & $BC_{12}$  and $BC_{21}$ and $BC_{22}$ into Single Matrix
        a. Matrix ($BC_1$ (8 X 8))
        b. Matrix ($BC_2$ (8 X 8))
10. Apply Reverse Left Circular Shift on Matrix ($BC_1$ (8 X 8)) and Reverse  Right Circular Shift on Matrix ($BC_2$ (8 X 8))
11. Repeat 10 Step 3 times.
12. Dived $BC_1$ and $BC_2$
        a. Matrix ($BC_{11}$ (8 X 4)) & Matrix ($BC_{12}$ (8 X 4))
        b. Matrix ($BC_{21}$ (8 X 4)) & Matrix ($BC_{22}$ (8 X 4))
13. Exchange Content of $BC_{12}$ and $B_{22}$
14. Combine $BC_{11}$ & $BC_{12}$  and $BC_{21}$ and $BC_{22}$ into Single Matrix
        a. Matrix ($BC_1$ (8 X 8))
        b. Matrix ($BC_2$ (8 X 8))
15. Now Combine $BC_1$ and $BC_2$
        Plain Text (PT) = $BC_1 \oplus BC_2$
16. Exit
```

Brute force attack: Even if a symmetric cipher [11] is currently unbreakable by exploiting structural weaknesses in its algorithm, it is possible to run through the entire space of keys in what is known as a brute force attack. Since longer symmetric keys require exponentially more work to brute force search, a sufficiently long symmetric key makes this line of attack impractical [12]. With a key of length n bits, there are 2^n possible keys. This number grows very rapidly as n increases. Moore's law suggests that computing power doubles roughly every 18 to 24 months, but even this doubling effect leaves the larger symmetric key lengths currently considered acceptable well out of reach. The large number of operations (2^{128}) required to try all possible 128-bit keys is widely considered to be out of reach for conventional digital computing techniques for the foreseeable future [27]. Security level is the relative strength of an algorithm. An algorithm with a security level of x bits is stronger than one of y bits if x > y. If an algorithm has a security level of x bits, the relative effort it would take to "beat" the algorithm is of the same magnitude of breaking a secure x-bit symmetric key algorithm (without reduction or other attacks). The 128-bit security level is for sensitive information, and the 192-bit level is for information of higher importance [26]. Here proposed algorithm having 128 bits key length so there are 2^{128} possible keys. The larger number of operation (2^{128}) required to try all possible 128-bit keys is widely considered to be out of reach for conventional digital computing techniques for the future [24, 26].

2. RESULT ANALYSIS

During results evolution some parameters are set like execution time means encryption/decryption time, throughput, CPU consumption and memory consumption. Total time during encryption/decryption of the process is known as execution time [8, 9 &10] and throughput is directly depended on execution time which is represent execution speed of whole process. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the total execution time [10].

The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU time is used in the encryption process, the higher is the load of the CPU [8, 9 & 10]. The memory deals with the amount of memory space it takes for the whole process of encryption and decryption [9, 10]. The presented experimental results are showing the performance of the proposed technique. Presented results are environment dependent so they can vary on other environment. Desktop machine has been used to calculate experimental results which have window XP SP-2 operating System, with Intel Pentium Dual Core E2200 2.20 GHz processor and 1 GB of RAM configuration. In the experiments, the system encrypts/decrypt a text/cipher data. There are Four parameters used for calculating by the proposed system one is encryption time/decryption time, second is throughput, third is CPU Consumption and Last is Memory Consumption which is shown in table 1, 2, 3, 4 and 5. The proposed system has run hundred times approximately. In each time, same plaintexts are respectively encrypted by existing system and **"Proposed system"** by copying them. Size of the selected was same in each time. Finally, the outputs of the comparison system are execution time and throughput which is noted in numeric form.

Encryption Time: - "The Proposed Hybrid Crypto System" have been implemented on a number of data files varying types of content and sizes of a wide range. Encryption time of Various Text files comparisons shown in table 1.

Table 1: Encryption Time of Proposed Technique

S.NO	File Size in KB	Proposed Concept
		Execution Time in Millisecond (approx)
1	2	62
2	3	73
3	7	343
4	11	1328

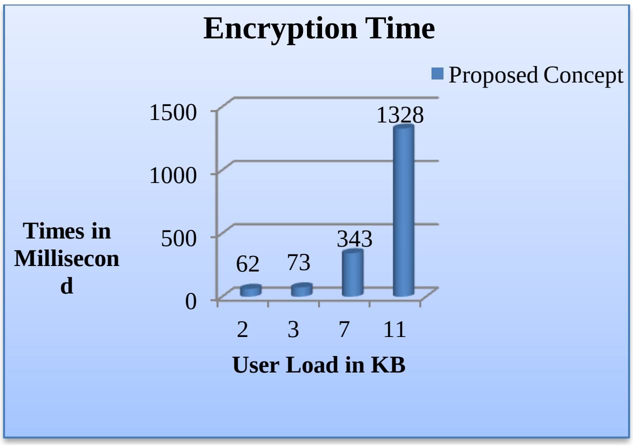

Fig.4: Encryption Time of Proposed Technique

Decryption Time: "The Proposed Hybrid Crypto System" have been implemented on a number of data files varying types of content and sizes of a wide range. Decryption time of Various Text files comparisons shown in table 2

Table 2: Decryption Time of Proposed Technique

S. No.	File Size in KB	Proposed Concept
		Execution Time in Millisecond (approx)
1	2	62
2	3	98
3	7	406
4	11	1343

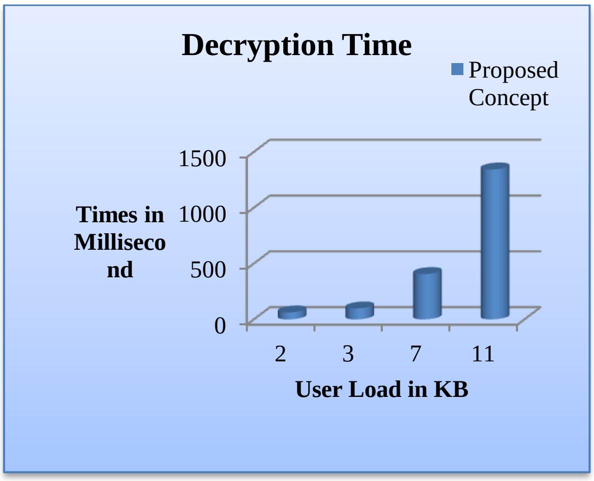

Fig.5: Decryption Time of Proposed Technique

Throughput: Throughput can be calculated by using execution time. It denotes the speed of execution. The throughput of the execution scheme is calculated as in equation (1).

Throughput of Execution = Total Size of plain Text/ Total Execution time (1).

Where Size is measuring in bytes and Execution times are measuring in encryption time and decryption time.

For Example: Here selected file of 2 KB (2048 bytes).

Throughput of the Existing Hybrid Crypto System is

Encryption Throughput = 2048/311
= 6.58

Throughput of Proposed Algorithm

Encryption Throughput = 2048/62
= 33.03

Table 3: Throughput of Proposed Technique

Parameter	File Size in KB	Proposed Concept
Throughput		(Approx)
	2	33.03
	3	42.08
	7	20.89
	11	8.48

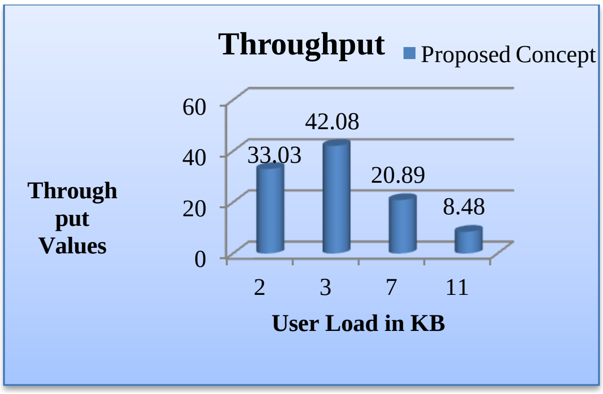

Fig. 6: Throughput of Proposed Technique

CPU Consumption: "The Proposed Hybrid Crypto System" have been implemented on a number of data files varying types of content and sizes of a wide range. CPU utilization 1KB Text files comparisons shown in table 4.

Table 4: CPU Utilization of Proposed Technique

Parameter	File Size in KB	Proposed Concept
CPU		(Approx)
	2	50
	3	50
	7	50
	11	52

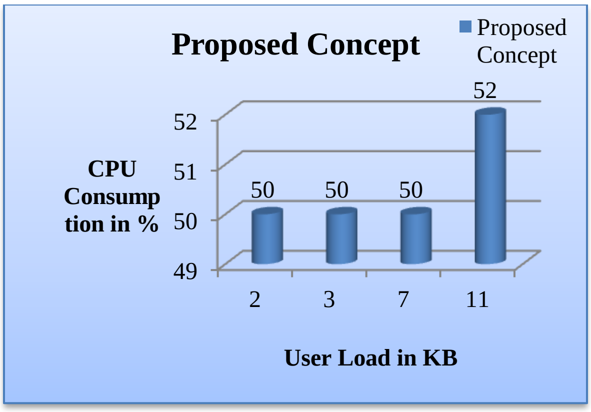

Fig. 7: CPU Consumption of Proposed Technique

Memory Consumption: "The Proposed Hybrid Crypto System" have been implemented on a number of data files varying types of content and sizes of a wide range. Memory Utilization of 1 KB Text files comparisons shown in table 5.

Table 5: Memory Utilization of Proposed Technique

Parameter	File Size in KB	Proposed Concept
RAM		(Approx)
	2	1225
	3	1230
	7	1230
	11	1226

Results Analysis: From the above discussion it can clearly see that the proposed Concept producing good results as compare existing concept which is defined in [1] and hence can be incorporated in the process of encryption of any plain text. Also, I can see that the previous hybrid crypto system have very less efficiency in terms of execution time and hence cannot be used for encryption of larger messages. The proposed hybrid crypto system is good than previous hybrid crypto system as they have higher efficiency. However it is also clear from table 1 to 5 and Fig. 4 to 7 that, by applying proposed concept to the files of different sizes highly security is obtained as compare to different other concept. In execution time, CPU uses and RAM Uses the proposed algorithm have quite good results as compared to different other encryption algorithm. Table 1 showing the encryption time where various file size are producing different time according to size, if 2 kb file are executing through the proposed concept it takes 62 millisecond time to execute at the time of encryption. Similarly at the time of decryption proposed concept is taking 62 milliseconds to decrypt 2KB of file.

3. CONCLUSION

It's known that security is the main concerned over text information where information is stored in bulk. Cryptography is one of the strongest security solutions for confidential information, but developing a cryptosystem must take many factors into consideration. Basically cryptography should be performed in the form of encryption and decryption. This research work examines the various issues of implementing text encryption and makes recommendations. Moreover this works presenting a common relation between three different encryption algorithms and combining to all in one. Proposed encryption schemes to preserve the integrity and confidentiality of the data. The number of existing system involving confidential information at the governmental, organizational and company levels is growing rapidly. Preserving data confidentiality, privacy and integrity in the semi-trusted information context, where the information is shared between many parties, is becoming one of the most challenging issues for such type of community. The proposed work addresses this issue and contributes the following. It proposes a new cryptography algorithm for information security is based on data classification methods. From the results it is analyzed that security of the proposed hybrid concept is very high as compare existing concept. It is already known that security of the algorithm is depended on the length of the key that mean longer key length will always support to good security feature and proposed hybrid concept have used 128 bits key length which is provided too much security for the proposed system. In Future work there are other important research issues related with research: first, improvement to design the best encryption algorithm for text information on performance and security perspectives; second, access control methods use to control access for all parities using the information; and finally indexing and joining between different information. Proposed hybrid concept gives a simple and sequential approach to analysis of different aspects of a secure encryption algorithm. Further development of the hybrid model to accommodate tighter generic security reductions for hybrid encryption is therefore desirable.

4. REFERENCES

[1] Bhatele, K. Sinhal, A.; Pathak," A novel approach to the design of a new hybrid security protocol architecture "Advanced Communication Control and Computing Technologies (ICACCCT), 2012 IEEE International Conference on Page(s): 429 - 433 Print ISBN: 978-1-4673-2045-0

[2] Lili Yu; Zhijuan Wang; Weifeng Wang "The Application of Hybrid Encryption Algorithm in Software Security "Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on Page(s): 762 - 765 Print ISBN: 978-1-4673-2981-1

[3] Mouza Bani Shemaili, Chan Yeob Yeun, Khalid Mubarak, Mohamed Jamal Zemerly "A New Lightweight Hybrid Cryptographic Algorithm for the Internet of Things" Internet Technology and Secured Transactions, 2012 International Conferece for Page(s):87 - 92 Print ISBN: 978-1-4673-5325-0

[4] A Chitra, T Blessin Sheeba "A Hybrid Reconfigurable Cryptographic Processor with RSA and SEA" Recent Trends in Information Technology (ICRTIT), 2012 International Conference on Page(s): 428 - 433 Print ISBN: 978-1-4673-1599-9

[5] Rasmi P S and Dr. Varghese Paul "A Hybrid Crypto System based on a new Circle-Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications" Published in International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011 Proceedings published by International Journal of Computer Applications® (IJCA)

[6] Gaidaa Saeed Mahdi "A Modification of TEA Block Cipher Algorithm for Data Security (MTEA)" published in Eng. & Tech. Vol No 29, No.5. Journal 2011**.**

[7] S. Subasree and N. K. Sakthivel "DESIGN OF A NEW SECURITY PROTOCOL USING HYBRID CRYPTOGRAPHY ALGORITHMS" published in IJRRAS 2 (2), February 2010

[8] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud "Evaluating the Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.213 {219, May 2010

[9] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms" published in 2009 International Conference on Computational Intelligence and Security978-0-7695-3931-7/09 IEEE DOI 10.1109/CIS .2009.81

[10] Majdi Al-qdah & Lin Yi Hui "Simple Encryption/Decryption Application**"** International Journal of Computer Science and Security, Volume (1): Issue (1) 2008

[11] Janakiraman V S, Ganesan R, Gobi M "Hybrid Cryptographic Algorithm for Robust Network Security" ICGST- CNIR, Volume (7), Issue (I), July 2007.

[12] Rivest, R.L., Robshaw, M.J.B., Sidney, R., & Yin, Y.L (2000a). “The Case for RC6 as the AES.”AES Round 2 Public Comments. URL:http://csrc.nist.gov/CryptoToolkit/aes/

round2/comments/ 20000515-rrivest.pdf.

[13] Shimoyama, T., Takeuchi, K., & Hayakawa, J. (2000). “Correlation Attack to the Block Cipher RC5 and the Simplified Variants of RC6.” 3rd AES Conference (AES3). URL: http://csrc.nist.gov/encryption/aes/round2/conf3/papers/36-tshimoyama.pdf.

[14] Rivest, R.L., Robshaw, M.J.B., Sidney, R., & Yin, Y.L (1998b). “The Security of the RC6 Block Cipher.” URL: ftp://ftp.rsasecurity.com/pub/rsalabs/rc6/security.pdf John Gordon “Introduction to Cryptography” 1998

[15] Rivest, R.L (1997). “The RC5 Encryption Algorithm.” URL:http://theory.lcs.mit.edu/%7Erivest/Rivest-rc5rev.pdf.

[16] Kelsey, John; Schneier, Bruce; Wagner, David (1996). "Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES". Lecture Notes in Computer Science 1109: 237–251. Doi: 10.1007/3-540-68697-5_19. http://www.schneier.com/paper-key-schedule.pdf.

[17] Introduction of cryptography by H. Delfs and H. Knebl springer Verlag berlin Heidelberg 2007

[18] William Stallings “Cryptography and Network Security”, 3rd Edition, Prentice-Hall Inc., 2005.

[19] Bruce Shnier “Applied Cryptography Second Edition Protocols. Algorithms, and Source, and Source Code in C”, John Wiley and Sons, Inc., 1996.

[20] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[21] B. Schneier, "Data Guardians," MacWorld, Feb 1993, 145-151.

[22] Dorothy Elizabeth, “Cryptography and Data Security”, Addison-Wesley, 1982.

[23] Menezes A., van Oorschot, P. and Vanstone, S. “Handbook of Applied Cryptography”, CRC Press, 1996.

[24] Stallings, W. “Cryptography and Network Security: Principles and Practice”, Prentice-Hall, USA, Second Edition, 1999.

[25] Henry Beker & Fresd piper, “Cipher System, the protection of communications”, A willey inter-science publication 1982.

[26] El-Mageed, T., Hamdy, N., Amer, F., and Kerisha, Y., “Cipher System and Cryptanalysis Techniques: An overview of the basic principles”. The Egyptian Computer Journal, ISSR, Cairo UNIV, VOL (28), No. 1, 2000.

[27] Schneier, Bruce, “Applied Cryptography. Protocols, Algorithms, and Source Code in C”, New York: Wiley & Sons, 1996.