Volume 2, Issue 12, December 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

IRJIF IMPACT FACTOR: 3.821

NAIRJC JOURNAL PUBLICATION

North Asian International Research Journal Consortium

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: -North Asian International Research Journal Consortium (NAIRJC) 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815, Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

IRJIF IMPACT FACTOR: 3.821

THE NEW HYBRID TECHNIQUE FOR SECURE DATA TRANSMISSION

PROF.KRISHNA TAYADE [1], MR.BALKRISHNA POKHARKAR [2], MR.SUYOG JAGADALE [3], MR.UMESH RAMANE [4] & MR.NIKHIL YEWANKAR [5]

[12345]**Department of Computer Engineering, Pune University, Pune India**

ABSTRACT

Various encryption algorithms have been developed for processing text documents, images, video, etc. If we are able to collaborate the advantages of the different existing encryption methods, then a new hybrid encryption method can be developed which offers better security and protection. So, in order to accomplish the Hybrid encryption technique, data encryption techniques using a standard Symmetric and Asymmetric three algorithm to achieve better security and high performance i.e. RSA algorithm, RC6 algorithm, AES algorithm are studied, analyzed and their performance is compared. The message is divided into three parts and these three different techniques are applied to these parts and the performance is again analyzed. The application of these three different methods to different parts of the same message along with two keys, namely, segmenting key and encrypting key to provide further authentication and validation is the basis of our paper.

Keywords:- (Encryption, Decryption, RC6 Algorithm, RC6 algorithm basic operations, AES Algorithm, RSA Algorithm)

1. INTRODUCTION

A Computer Network is an interconnected gathering of independent figuring hubs, which utilize a very much characterized, commonly concurred set of guidelines and traditions known as conventions, cooperate with each other genuinely and permit asset sharing ideally in an anticipated and controllable way. Correspondence has a noteworthy effect on today's business. It is sought to discuss information with high security. Security Assaults bargains the security and henceforth different Symmetric and Asymmetric cryptographic calculations have been proposed to accomplish the security administrations such as Authentication, Confidentiality, Integrity, Non-Repudiation and Availability. At present different sorts of cryptographic calculations give high security to data on controlled systems. These calculations are required to give information security what's more, client's legitimacy.

To enhance the quality of these security calculations, a new security convention for on line exchange can be planned utilizing blend of both symmetric and halter kilter cryptographic procedures. This convention gives three cryptographic primitives, for example, trustworthiness, classification and verification. These three primitives can be accomplished with the assistance of Retest Cipher (RC6), RSA calculation and Advance Encryption Standard. That all there calculation utilized for the encryption on single record with making distinctive lump. This new security convention has been intended for better security with trustworthiness utilizing a mix of both symmetric and unbalanced cryptographic strategies.

2. RELATED WORK

Framework having a calculation to encode and unscramble the information base on symmetric key encryption system. The proposed framework is creating good results. In future: the framework can be further enhanced by utilizing variable length key. Framework can be made to encode the information on the premise of Unicode values. It additionally can be enhanced for to unscramble the sentence type of information. so it can be acknowledged universally[1].

A middle of the Software approach which is programming based era of PN arrangement however acts/works intently to equipment. C is a dialect fit of getting to the frameworks memory in bitwise way and it can perform bitwise operations as well. The approach demonstrates that the memory utilized for execution of LFSR is only 2 bytes and 8 bytes for short and long PN succession respectively. Lesser sum memory implies lesser number of memories gets also; lesser number of guideline execution .The estimations demonstrates almost 70%of decrease in guideline on execution, which assistant suggests almost half of less vitality utilization for creating PN arrangement [2].

These framework utilization of how message from sender is encoded utilizing triple DES through Unicode and conceal the encoded picture into a stage picture. On the collector end, extraction calculation is composed in such a way that the procedure isolates the message and picture into two unique substances; at that point peruses the separated message which is in the encoded shape and changes it from the Unicode images to a meaningful shape. The technique is characterized as imperceptible, solid and secured correspondence of information identified with the mixed media picture. Consequently any classified message can be send to any objective without the learning of others through an unsecured correspondence channel. This encoding and disentangling plan of the proposed new strategy is essentially diverse when contrasted with conventional plans [3].

This paper having a creative strategy for information encryption is proposed in light of the arbitrary succession era. The new calculation gives information encryption at two levels and henceforth security against crypto examination is accomplished at generally low computational overhead. The framework has capable key administration and, considerably more essentially, open key cryptography can execute advanced marks in an effective way. Be that as it may, symmetric-key is a type of cryptography in which two gatherings that need to convey can share a typical and mystery key [4].

These paper having utilized as an incited encrypted as a part of programming situations to secure imperative codes and secure transmission in research offices. the abnormal state of security is given by the scrambling designs, client logins, space change and so on the future extent of this application depends the advancement of higher request FFT calculations which relatively increments the conceivable number of scrambling examples for higher security[5].

In these paper Information security has turned into an extremely basic part of present day correspondence frameworks. With the worldwide acknowledgment of the Web as a medium of correspondence, for all intents and purposes each PC on the planet is associated with each other. It has made another hazard for the clients of the computers with a steady risk of being hacked and being casualties of information burglary. In this association information encryption has turned into a vital piece of secure correspondence of the messages. In the present paper we propose another technique for encryption of information in squares utilizing the operations Rotation and Logical XOR [7].

In Secure Electronic Transaction (SET), different encryption calculations are utilized, for example, DES (Data Encryption Standard) and RSA calculation. Information Encryption Standard (DES) is a 56-bit key calculation, which is used to encode online exchanges. This encryption strategy was very little secure and can be effectively broken utilizing advanced programming inserted equipment. In 1993, utilizing an idea of beast compel assault, a DES breaking machine was outlined by a researcher Michael Wiener. In 1996, an incredible researcher Schneider proposed that a parallel machine can be outlined that breaks DES framework inside a second. In this way, for the protected exchange the DES was supplanted by effective and dependable framework as Secure Electronic Transaction (SET) [8].

In these paper which includes brief depiction of RSA and DES cryptography calculations and their current vulnerabilities alongside their countermeasures. Other than this, there is a hypothetical execution investigation furthermore, examinations of symmetric and halter kilter cryptography [9]. In this paper the fundamental Applicant OD investigated is the transmission of twofold strings whose length is in a OD. obscure range, utilizing hearty Fibonacci representations rather than the routine error sensitive logarithmic slope representation. Despite the fact that the previous is asymptotically more than the last mentioned, the previous is really shorter for substantial introductory sections of whole numbers. [10]

3. SYSTEM ARCHITECTURE

System providing following security importance:-

1. Security of data is important.
2. Cryptography is used to secure data.
3. 4 main requirements of cryptography are
4. To maintain
5. Data confidentiality
6. Data integrity
7. Authentication and non-repudiation from unauthenticated users
8. To protect above properties symmetric or asymmetric cryptography is used

In the proposed model three entities exist as:-

1) Data Owner (DO):-

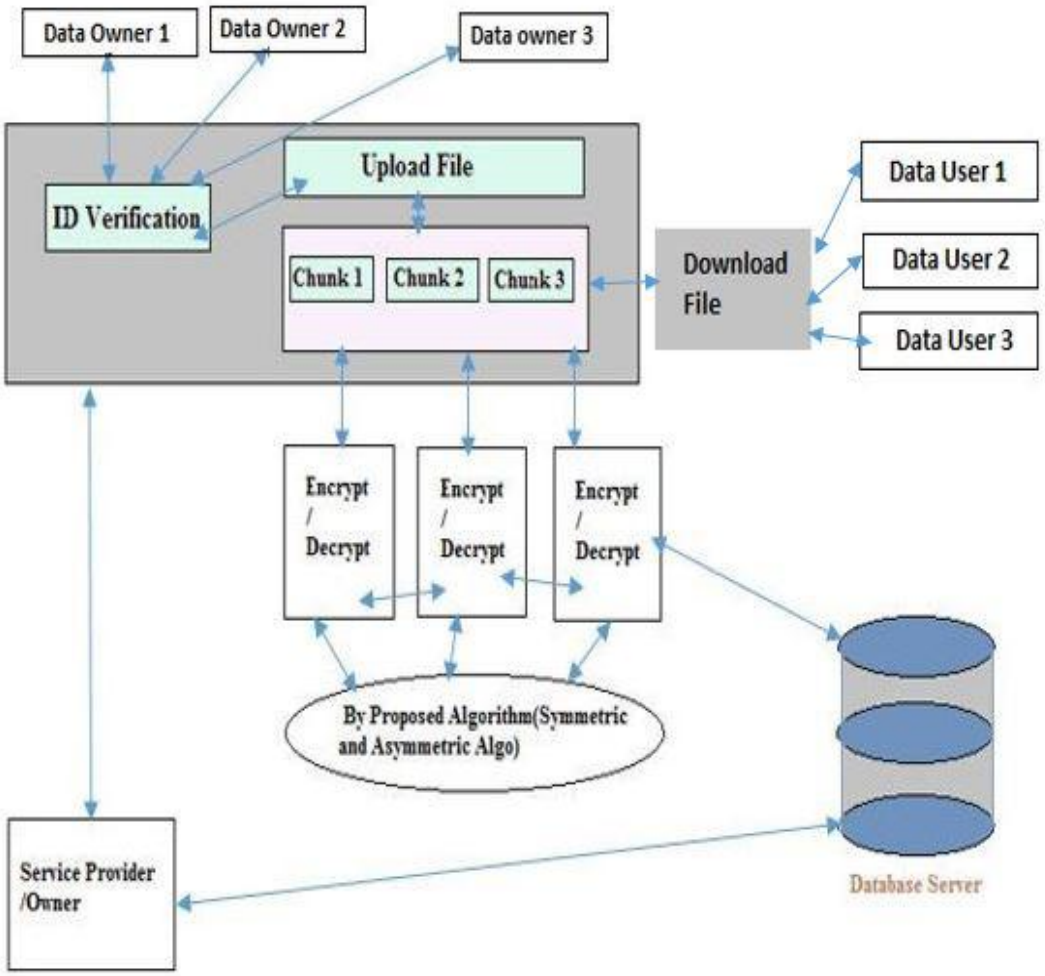
It is the entity which is responsible for generating the data/ files or services to be shared with other users over cloud environment. DO want it data to be secured from unauthorized users and authorized users will be able to access the data from the cloud after the verification done by SP (Service Provider).

2) Cloud Service Provider (CSP):-

It is the cloud server responsible for DO data storage and its delivery to authorized user only. CSP is an un-trusted third party that's why DO encrypt its data before storage on cloud server.

3) Data User (DU) :-

It is the entity which requires the DO file services and gets them from CSP after verification of its authenticity done by CSP. User knows the decryption key for its retrieved data and can get back the original data after decryption. In the proposed model, DO combines the classical techniques i.e. hybrid symmetric and asymmetric encryption for the encryption and decryption of data. Both of these techniques have cipher text in text file form. In this model, DO initially converts the plaintext into its corresponding ASCII value and then perform the encryption using College Short Form Name, Department of Computer Engineering 2015 41 hybrid symmetric and asymmetric algorithm with different part called as chunk. DO also send the key used during the encryption to data user for decryption purpose when they requested. For security or stop misuse of file only data owner having permission edit and delete file from cloud server.



4. PURPOSE AND SCOPE

Project scope contains developing the The New Hybrid Technique For Secure Data.

Transmission using three different cryptographic algorithm i.e.RC6 Algorithm, AS algorithm and RSA Algorithm to useful for performing encryption operations on cloud data. Web and Network applications have seen an enormous development in the last decade. Accordingly episodes of digital assaults and traded off security are expanding. This requires more concentrate on reinforcing and securing our correspondence.

One approach to accomplish this is cryptography. In spite of the fact that a great deal of work has been finished here yet this issue still has extent of change. In this paper we have concentrated on symmetric& uneven cryptography and proposed a novel strategy by consolidating the three most prevalent calculations RC6, RSA and AES to accomplish more security.

5. APPLICATIONS

1) Military Campus
2) College or Organization System.
3) Internet Sharing

6. CONCLUSION

Hybrid encryption technology makes use of three different cryptographic algorithms. Which removes the drawback of use of any single cryptographic algorithm and provide triple security to secret data .It removes the key distribution problem Security systems tends to use a hybrid solution to increase the security and speed of Encrypting documents.

7. ACKNOWLEDGEMENT

We are thankful to our project guide Prof. Krishna Tayade & Prof. Ashvini Jadhav for their support. Also all the staff of Computer Department for coordination.

8. REFERENCES

[1] Udepal Singh and Upasna Garg, An ASCII value based text data encryption System, in International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013, ISSN 2250-3153

[2] Rina Choudhary, An enhancement of code and energy optimization in PN Sequence generation, in International Journal of Engineering and Management Sciences, I.J.E.M.S., VOL.4 (4) Sep2013: 426-429, ISSN 2229-600X

[3] Sharad Kumar Verma and D.B. Ojha , An application of data encryption technique using random number generator, in International Journal of Research Studies in Computing, Volume 1, Number 1, 35-42, April 2012

[4] A. Joseph Raphael and V. Sundaram , Secured Communication through Fibonacci Numbers and Unicode Symbols, in International Journal of Scientific & Engineering Research, Volume 3, Issue 4, April-2012, ISSN 2229-5518

[5] Sudha Rani, T. C. Sarma and K. Satya, Text File Encryption Using FFT Technique in Lab View 8.6, in IJRET: international Journal of Research in Engineering and Technology ISSN: 2319-1163, Volume: 01, Issue 01, April-2012

[6] D. Saran Kumar, CH. Sabetha and A.Chandrasekhar, A Block Cipher Using Rotation and Logical XOR Operations, in IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011, ISSN (Online):1694-0814

[7] Himanshu Gupta and Vinod Kumar Sharma, Role of multiple encryption in secure electronic transaction, in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[8] V. Sundaram and A. Joseph Raphael, Secured CryptoStegano Communication Through Unicode, in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 4,138-143, Aug2011

[9] Alberto Apostolico and Aviezri S. Fraenkel, Robust Transmission of Unbounded Strings Using Fibonacci Representations, in Report Number: 85-545, 1985 Jun-2010

[10] Books by William Stallings Cryptography and network security, sixth edition.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- North Asian International Research Journal Consortium (NAIRJC)
221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com