International Journal of Computer Trends and Technology (IJCTT) – volume 11 number 1 – May 2014

Evaluation of Common Encryption Algorithm and Scope of Advanced Algorithm for Simulated Wireless Network

Dr. Atul M. Gonsai[1], Lakshadeep M. Raval[2]
[1] Sr. Assistant Professor, Department of Computer Science, Saurashtra University, Rajkot, Gujarat, India
[2] System Administrator, SAL College Engineering, Ahmedabad, Gujarat, India

***Abstract* - Encryption algorithms play a vital role in information security systems. The study discovers the progress of Encryption algorithms in terms of their diversity of applications. Some of the Encryption algorithms have been developed to make transmission and storage of data more secured and confidential. Different levels of securities are offered by different algorithms depending on how difficult is to break them. If it is difficult to recover the plain text in spite of having substantial amount of cipher text then an algorithm is unconditionally secured. This study provides evaluation of eight of the most common encryption algorithms namely: DES, 3DES, AES (Rijndael), Blowfish, RSA, RC2, RC4, and RC6. From our analysis we came to conclusion that the best algorithm is the one which fulfills our need of security and speed. We come with new design of encryption algorithm based on AES or RSA or RC4, various scripts on NS2 or MATLAB or SCILAB, simulation environment of encrypted wireless network based on NS2 or MATLAB or SCILAB. We will implement newly proposed encryption algorithm on simulated environment and also test performance of proposed algorithm on wireless simulated network. We come with design and implement technique to store encrypted data on secondary storage device.**

***Keywords* - Algorithm, cryptography, Cipher, Encryption, Network Security**

I. INTRODUCTION

Cryptography usually referred as "the study of secret", presently is attached to the definition of encryption. Encryption is the process of encoding information with the use of an encryption key in a way that third parties cannot read the encoded information. The encoded information is termed as unreadable ciphertext.

The importance of encrypting data is more pertinent in light of the mushrooming applications and globalization of communication. It is an indispensable for applications like email, electronic transactions, digital cash, and so on.

Data encryption procedure are classified on the type of security keys used for encrypt/decrypt the data. The categories are: Symmetric encryption and Asymmetric encryption techniques.

Symmetric Encryption – Where single key is used.
Asymmetric Encryption – Public Key Cryptography where two keys are used, the key that is known to public is called public key and the key that is familiar only to the user is called private key.

Security mechanisms require specific algorithm or protocol for encryption and decryption purpose, as well as for creating of sub keys to be mapped to plain text for generating cipher text.

Security services and mechanisms can be viewed in the model which is developed by the participants having secret data and protects the data from unauthorized users.

As the security of encrypting models is directly related to the key length, if we increase the key length the more will be the security of the algorithm.

Algorithm is supposed to be safe if the value of the encrypted data is lesser than the cost involved to break an algorithm.

Also it is safe if the amount of data required to break the algorithm is greater than the quantity of data encrypted with a single key.

An algorithm is unconditionally secure if, it is difficult to recover the plain text in spite of having substantial amount of cipher text.

A. The Ways of Conversion of Plain Text

A block cipher processes one block of elements at a time as input and producing an output for every input block. Stream cipher processes element continuously as input and generating output single element at a time, as it goes ahead.

B. The Type of Operations Used For Conversion of Plain Text to Cipher Text

The base of all Encryption algorithms is the two general

principles.

- Substitution: In which every one element in the plain text is mapped to another element.
- Transposition: In which the elements are rearranged in the plain text.

Most of the systems involve multiple stages of substitution and transpositions.

C. The Number of Keys Involve

In the system if the same key used by sender and receiver, it is referred as single key, secret key, symmetric or conventional encryption. In the system if the sender and the receiver each use a different key, it is referred to as two keys, public key or asymmetric encryption.

II. Study Of Some Commonly Used Algorithms

Development in Encryption algorithms is constant to provide the best protection. Here we compared some commonly used algorithms:

A. DES Algorithm

The symmetric algorithm known as the Data Encryption Standard (DES) was considered as main standard for encrypting data. DES encrypts data 64 bits at a time because DES is a 64 bit block cipher.

By researcher [19] it is very necessary for embedded applications to protect important data. The implementations of the DES (data encryption standard) algorithm based on hardware are low cost, flexible and efficient encryption solutions.

B. Triple DES

Today Triple DES increases the key size of DES by using the algorithm thrice in succession with three different keys. To get the combined key size of 168 bits (3 times 56) it is not within the reach of brute-force techniques as utilized by the EFF DES Cracker.

DES could not match up with advancement in technology so it is no longer suitable for security.

As DES was commonly utilized at that time, the rapid result was to launch 3DES which is safe enough for most purposes
While studying [30] it is recommended the use of 3 DES with 3 different keys as it has effective key length of 168 bits. Two-key variation is another variation of 3 DES (K1 and K3 is same) reduces the effectual key size to 112 bits which is not more secure. Two-key 3DES is extensively used in electronic payments industry. The CPU power consumed by 3 DES is three times as more CPU Power as compared to its predecessor which is significant performance hit.

In the form of Triple DES the algorithm is considered to be practically secure, in spite of having theoretical attacks.

C. BLOWFISH Algorithm

Blowfish algorithm was first introduced in 1993. It is a 64-bit block cipher and variable length key. Though this algorithm is widely used in software applications it can also be optimized in hardware applications. None of the attacks are known to be successful against this. As provided by Bruce Schneier one of the world's famous cryptologists and the president of Counterpane Systems. The Blowfish algorithm is one of the most known public domain encryption algorithms

By researcher [28] it was proved in throughput and power consumption in decryption the Blowfish algorithm is the better than other algorithms. The second point observed is that RC6 algorithm requires less time than all algorithms except Blowfish

D. AES Algorithm

While studying [23] Due to AES algorithm's powerful encryption, complicated procedure and its resistance to Brute-force attack it is widely accepted. SubBytes(), ShiftRows(0), MixColumns() functions of an AES round are designed to thwart cryptanalysis via the methods of "confusion" and "diffusion". AddRoundKey() function actually encrypts the data.

By researcher [1] the modifications to AES algorithm are performed on the rounds of the algorithm. These changes made it hard for the attacker to judge a pattern in the algorithm there by enhancing the complexity of the encryption process.

From researcher [2] Cryptography deals with the features of information securities as confidentiality, data integrity, entity authentication, data origin authentication and also it is the study of Mathematical methods for secured communication in the presence of hurdles.

For wired/wireless communication a high speed security algorithm is definitely important and necessary. The symmetric block cipher plays a vital role in the bulk data encryption. Currently advanced encryption standard (AES) is one of the efficient symmetric security algorithms to provide data security.
By researcher [13] the best use of the Advanced Encryption Standard (AES) that can be used as an error correction algorithm with a perspective of reducing the power as a unit of secured wireless communication to correct mistaken errors and its

implementation. The planning of data encryption unit and key schedule unit has been optimized due to their low power AES crypto module and this could be applicable to wireless sensor networks. The detailing of low power design methods used to design low power AES module is also done by them.

By researcher paper [14] an overview of present cryptanalysis research on the AES cryptographic algorithm is done by them. Discussion is done on the impact by each technique to strengthen the algorithm in national security applications. The conclusion in the paper is with an endeavour at a forecast of the beneficial life of AES.

E. RSA Algorithm

One of the well known public key cryptosystems for encryption of blocks of data, key exchange or digital signatures is the Rivest-Shamir-Adleman (RSA) cryptosystem.

The level of speed and security of RSA algorithm is affected by some important parameters. The complexity of decomposing RSA algorithm into its factors increases by increasing the modulus length which plays an important role, due to which the length of private key will increase and so hard to be decrypted without decryption key. The length of encrypted message will comparatively change if the length of message is changes.

While studying [3] when the era of electronic email was awaited to arise that time RSA was introduced. Two important ideas were implemented by it:

- Public-Key Encryption: The person with the correct decryption key can decipher an encrypted message because in RSA algorithm, encryption keys are public, but the decryption keys are not.

- Digital Signatures: It is important for the receiver to verify that transmitted messages are actually originated from the sender (signature), and have not just come from there (authentication). It is done with the sender's decryption key, using the corresponding public encryption key later the signature can be verified by anyone. Therefore the signatures cannot be forged. So, no signer can later refuse having signed the message.

From researcher [4] with some modification, the SRNN (Short Range Natural Number) is same as to RSA algorithm. The security of the cryptosystem is increases by this modification. They have suggested a method for executing a public-key cryptosystem whose security resides in part on the difficulty of factoring big numbers. If the security of their method proved to be sufficient, it can permit secure communications to be setup without the use of envoys to carry keys. They found RSA algorithm with the length of modulus 1024 bits with 512 bits chunk size is finer in speed but some feeble in security .
By researcher paper [17] present a software designed for remote visualization of medical images with data security transfer. This interface is implemented under MATLAB environment. The implementation of the image cryptography system uses the RSA algorithm with 64 bits private key length. More they introduced a comparison study between the obtained performances and those computed with other algorithms such as DES and IDEA.

F. RC2 Algorithm

While studying [31] RC2 is a 64-bit block cipher having a variable key size and using 18 rounds. As a source-heavy feistel network the rounds are arranged, with 16 mixing rounds and 2 interleaved mashing rounds. The 18 rounds are executed using the below mentioned interleaved sequence:

- Perform five mixing rounds.
- Perform one mashing round.
- Perform six mixing rounds.
- Perform one mashing round.
- Perform five mixing rounds.

The key-expansion algorithm is used by RC2 because of which an increase in key size consisting of 64 (16-bit words) is produced depending upon intricate way on each bit of the supplied not consistent length input key. A mixing round has four applications of the "mix-up" transformation. Mashing round is done by adding single 16-bit words of the expanded key.

G. RC4 Algorithm

While studying [6] RC4 algorithm is used in Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), these are encryption protocols often used on wireless routers. It was widely used for its speed and simplicity. For strong encryption typically 16 byte keys are used, but due to export restrictions shorter key lengths are also widely used.

By researcher [7] Analysis based on the result of different variables of the RC4 algorithm were examined. The file size and the implementation time as a function of the encryption key length was examined; this has been stated as security and complexity. The results have been examined and elucidate as mathematical calculations depicting the relationship between the analyzed data and so can be used to speculate any future conduct of the algorithm under different conditions.

While studying [18] after some research on the web to find an interesting cryptographic primitive to implement, they decided to implement RC4 stream cipher as it was most widely used and it is used by important and famous protocols and standards such as SSL, TSL, WEP, as well it was known for its efficiency and simplicity.

H. RC6 Algorithm

While studying [22] the RC6 algorithm is a block cipher that was one of the finalists in the Advanced Encryption Standard (AES) competition. Since RC6 is an evolution of RC5, evolutionary differences will be noted accordingly. The development leading to RC6 has provided a simple cipher providing numerous opinions and enough security in a small package.RC6 consists of three components:

- A key expansion algorithm
- An encryption algorithm
- A decryption algorithm

While studying [20] presents an initial analysis of security offered by RC6 block cipher. Analysis reveals that RC6 is highly resistant to linear and differential cryptanalytic attacks, which are presently two very effective analytical attacks on block ciphers.

III. General Study

By researcher paper [15] provides a beneficial comparison between three well known symmetric key cryptography algorithms: DES, AES, and Blowfish. The performance of algorithms under different settings is the main concern here; the presented comparison takes into consideration performance of the algorithm and the behavior when different data loads are used. These parameters key size, block size, and speed are the base of comparison.

By researcher paper [16] a proposal of a combination of DSA, RSA and MD5 as a hybrid link for wireless devices was made. They had also considered case study for Manet networks so that they could suggest the applications of proposed algorithm.

By researcher paper [21] implements some of the commonly used, Symmetric encryption techniques in MATLAB software i.e. AES and BLOWFISH. The paper compares avalanche effect due to one bit discrepancy in key keeping the plaintext constant, bit discrepancy in plaintext keeping the key constant, memory required for implementation, key length, input block size, output buffer size, simulation time required for messages of different length and number of rounds needed for complete processing.

By researcher [9], to improve security for confidential communication in wireless sensor network, a new byte block cipher algorithm with well defined chaos and Feistel structure has been studied. The cipher algorithm was perceived in the Micaz node, and experiment in wireless sensor network for confidential communication was done successfully. The cipher algorithm needed additional RAM memory 61 bytes and ROM memory 4144 bytes. The cipher algorithm is Feistel structure and nonlinear chaos; it holds the best of the DES, RC6 and SKIPJACK cipher algorithms. The result exhibits that the algorithm is safe at a high level and needs a little memory.

While studying [10], [11] in the world of network security, one faces a number of threats from attackers, from miss configurations of infrastructure or network-enabled devices, or even from simple outages.

By Researcher paper [24] wireless security is indicated by using the common security standards like (802.11 WEP, 802.11i WPA and WPA2) and give the study of six of the well known encryption algorithms for wireless devices on power consumption that is: AES, DES, 3DES, Blowfish, RC2, and RC6. A comparison has been done for those encryption algorithms at different positions for all algorithms such as battery power consumption, divergent sizes of data blocks, dissimilar data types, data transmission through wireless network and lastly encryption/decryption speed.

While studying [25] the RC4 algorithm is used for encryption purposes by the WEP security protocol. RC4 is a stream cipher, a cipher that encrypts each byte of data being sent one byte at a time. Several of the new algorithms have been tested and seem to correct - or at least mitigate - the typical problems associated with the current WEP implementations. As the wireless industry continues to grow, the hope is that wireless networks will eventually be as secure as their modern day wired counterparts.

While studying [26] in the network and internet applications one of the most challenging aspects is security. The idea of selective encryption into the purpose of data protection mechanisms was launched by them. A sender includes proper unpredictability in the process of message encryption by using stochastic algorithm and probabilistic methodology so that other unauthorized junction is unaware of the transmitted messages on the whole and only entrusted receiver can decrypt the cipher text. Without compromising the security of the transmission the computation time and power is reduced by selective encryption algorithm. All messages are not necessary to be encrypted through selective encryption so that the complete data transmission can be seen to be secure entirely. Selective encryption can reduce the processing time and scalability of data transmission is improved.
By researcher paper [30] their evaluation amongst DES, 3DES and AES within nine factors, which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible key at 50 billion second. AES is better than DES and 3DES was proved in the Comparative Study was done between them.

By researcher [31] the comparison of single encryption and multicrypt encryption was done and result was analyzed in the

form of advantages and disadvantages. They selected AES for single type encryption and DES, 3DES, AES & RC2 for Multicrypt encryption scheme. In a selected document single type encryption uses one encryption algorithm while two or more algorithm are used by multicrypt for encryption of the same document. After analysis single encrypt is not so much secure but a speedy process where as multicrypt is more secure but is a time taking process and also needs to remember so many password/Keys and initial vectors. Single type encryption is enough for security of personnel document, while multicrypt is good option to secure important files and documents for corporate and business purpose.

IV. Evaluation Of Selected Encryption Algorithms

By researcher [27]

- Compared to algorithm DES it was found 3DES still has low performance.
- When the results are displayed there is no significant variation either in base 64 encoding or hexadecimal base encoding.
- It is concluded that Blowfish followed by RC6 has superior performance than other common encryption algorithms used from the simulation results.
- In terms of time consumption it was analyzed that RC2 has drawbacks over all other algorithms.
- It was analyzed that AES has superior performance than RC2, DES, and 3DES.
- They also derive the similar result for audio and video files similar to as in text and document.

By researcher paper [28] presents the importance of wireless networks and various threats faced by them. To secure the wireless networks various techniques can be used. In information security systems encryption algorithms play a vital role. On the other hand, those algorithms put CPU load and consume battery fast. This paper provides evaluation of encryption algorithms like AES, DES, 3DES, RC2, Blowfish, and RC6. Blowfish is found to be the finest encryption algorithm when evaluation was conducted for those encryption algorithms.

By researcher paper [29] gives an in-depth study of symmetric key encryption algorithms like RC2, RC4, RC5 and RC6. Among those algorithms the RC6 algorithm utilizes a varied number of bits ranging from 8 to 1024 bits and encrypts data 16 times. That is why it is impossible for a hacker to decrypt it.

Table 1 describes comparative study of selected encryption algorithms from researcher paper [27], [28], [29] & [32]. The algorithms selected are DES, 3DES, AES, Blowfish, RSA, RC6, and RC2.

TABLE I
Comparison of Various Selected Encryption Algorithms

Sr.No.	Algorithm	Block Size (Bits)	Key Size (Bits)	Evaluation
1.	DES	64	56	Insecure block cipher.
2.	3DES	64	112 or 168	Slower than other block cipher
3.	AES	128	256	In terms of time consumption and throughput it has Advantage over DES, 3 DES and RC2.
4.	Blowfish	64	32-448 (128 By Default)	In throughput and power consumption It is better than other algorithms.
5.	RSA	Any byte length	1,024 to 4,096 bit	Some symmetric Encryptions are faster than RSA
6.	RC2	64	8-1024 (64 By Default)	Despite of small key size used performance and throughput are low.
7.	RC4	2,064 (1,684 effective)	40 - 2,048	Very fast stream cipher
8.	RC6	128	128, 192 or 256	Except Blowfish RC6 requires less time than all algorithms.

V. Evaluation On The Basis Of General Point Of View

From our analysis we can derive results that no "best" algorithm; there are only those that meet your needs and those that don't. Your needs are security and speed - choose accordingly. I gave some fairly generic suggestions above.

VI. CONCLUSION

Our study provides evaluation of eight of the most common encryption algorithms namely: DES, 3DES, AES (Rijndael), Blowfish, RSA, RC2, RC4, and RC6. After reviewing about work there is still chance for design and implement encryption algorithm for entirely secured computer networks. We come with design new encryption algorithm based on AES or RSA or RC4 and Implement encryption algorithm on simulated wireless network.

REFERENCES

[1] Priyanka Pimpale, Rohan Rayarikar, Sanket Upadhyay, " *Modifications to AES Algorithm for Complex Encryption*", IJCSNS International Journal of Computer Science and Network Security, Vol.11, No.10, October 2011, pp. 183-186.

[2] Manjesh.K.N, R K Karunavathi, " *Secured High throughput implementation of AES Algorithm*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X , pp. 1193-1198.

[3] Evgeny Milanov, "*The RSA Algorithm*", June 2009. pp. 1-11

[4] Sonal Sharma, Jitendra Singh Yadav, Prashant Sharma, " *Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm*", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 8, ISSN: 2277 128X, August 2012, pp. 134-138.

[5] Rajorshi Biswas, Shibdas Bandyopadhyay, Anirban Banerjee, "Fast *Implementation of the RSA Algorithm Using the GNU MP library*", pp. II-30.1 to II-30.15.

[6] Suk-Hyun Cho, Devin Kaylor, "*RC4 Encryption, Ralph (Eddie) Rise*".

[7] Allam Mousa & Ahmad Hamad, "*Evaluation of the RC4 Algorithm for Data Encryption*", International Journal of Computer Science & Application, Vol.3, No.2, June 2006, pp. 44-56.

[8] Liang Hong a, Wei Chen b, "*Information theory and cryptography based secured communication scheme for cooperative MIMO communication in wireless sensor networks*", www.elsevier.com/locate/adhoc, AdHoc Networks (2013).

[9] Shuai Chen, Xian-Xin Zhong, " *Confidential Communication Through Chaos Encryption in Wireless Sensor Network*", Journal of China University of Mining and Technology, Volume 17, Issue 2, June 2007, pp. 258–261.

[10] Jason Andress, "*Understanding the Fundamentals of Info Sec in Theory and Practice*", the Basics of Information Security, 2011. pp. 115-130.

[11] Chunming Rong, Gansen Zhao, Liang Yan, Erdal Cayirci, Hongbing Cheng, "*Computer and Information Security Handbook (Second Edition)*", 2013, pp. 285–300.

[12] N.W. Lo & Kuo-Hui Yeh, "*Cryptanalysis of two three-party encrypted key exchange protocols*", Computer Standards & Interfaces 31 (2009), pp. 1167-1174.

[13] Supratim Saha, "*Low Power AES Algorithm Implementation for Wireless Communication*", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 8, August - 2013. pp. 29-31.

[14] Alan Kaminsky, Michael Kurdziel, Stanisław Radziszowski, "*An Overview of Cryptanalysis Research for the Advanced Encryption Standard*".

[15] Jawahar Thakur, Nagesh Kumar, "*DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis*", www.ijetae.com , ISSN 2250-2459, Volume 1, Issue 2, December 2011, pp. 6-12.

[16] Khushdeep Kaur, Er.Seema, "*Hybrid Algorithm with DSA, RSA &MD5 Encryption Algorithm for wireless devices*", (IJERA) ISSN: 2248-9622, www.ijera.com Vol. 2, Issue 5, September-October 2012, pp. 914-917.

[17] Samoud Ali, "*RSA algorithm implementation for ciphering medical imaging*", International Journal of Computer and Electronics Research, Volume 1, Issue 2, ISSN: 2278-5795, August 2012, pp. 44-49.

[18] Quentin Galvane Baptiste Uzel, "*Cryptography - RC4 Algorithm*", February 2012.

[19] Cai-hong Liua, Jin-shui Jia, Zi-long Liua, "*Implementation of DES Encryption Arithmetic based on FPGA*", Science Direct, AASRI Procedia 5, 2013, pp. 209 – 213.

[20] Scott Contini, Ronald L. Rivest, M.J.B. Robshaw, Yiqun Lisa Yin, "*The Security of the RC6 Block Cipher*", Version 1.0, August 20, 1998.

[21] Himani Agrawal, "*MATLAB Implementation, Analysis and Comparison of AES and BLOWFISH*", International J. of Multidispl.Research & Advcs. in Engg. (IJMRAE), ISSN 0975-7074, Vol. 2, No. II, July 2010. pp. 283-290.

[22] Morgan Monger, "RC6*: the Simple Cipher*", CS-627-0001: Cryptography, fall 2004.

[23] Eric Conrad, "*Advanced Encryption Standard*"

[24] Diaa Salama, Hatem Abdual Kader, & Mohiy Hadhoud, "*Wireless Network Security Still Has no Clothes*", International Arab Journal of e-Technology, Vol. 2, No. 2, June 2011. pp. 112-123.

[25] Erica Simcoe, Hirsh Goldberg, Mehmet Ucal and Advisor: Dr. Sennur Ulukus, "*An Examination of Security Algorithm Flaws in Wireless Networks* ".

[26] Patil Ganesh G & Madhumita, "*Selective Encryption Algorithm for Wireless Ad-hoc Networks*".

[27] 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, May 2010, pp. 216–222.

[28] Mr. Gurjeevan singh, Mr. Ashwani Singla, Mr. K S Sandha, "*Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System*", International Journal of Multidisciplinary Research, Vol.1, Issue 4, August 2011, ISSN: 2231 780. pp. 143 – 151.

[29] T.Gunasundari, Dr. K.Elangovan, "*A Comparative Survey on Symmetric Key Encryption Algorithms*", International Journal of Computer Science and Mobile Applications, ISSN: 2321-8363, Vol.2, Issue. 2, February-2014, pp. 78-83.

[30] Hamdan.o.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "*New Comparative Study between DES, 3DES and AES within Nine Factors*", Journal of Computing, Volume 2, Issue 3, ISSN 2151-9617, March 2010, pp. 152-157.

[31] Vibha Verma and Mr. Avinash Dhole, "*Analysis of comparison between Single Encryption (Advance Encryption Scheme (AES)) and Multicrypt Encryption Scheme*", International Journal of Scientific and Research Publications, ISSN 2250-3153, Volume 2, Issue 4, April 2012, pp. 1-4.

[32] Lalit Singh, Dr. R. K. Bharti, "*Comparative Performance Analysis of Cryptographic Algorithms*", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN 2277 128X, Volume 3, Issue 11, November 2013, pp. 563-568.