Novel Hybrid Cryptography for Confidentiality, Integrity, Authentication

Avinash Jain
Dept. of Information Technology,
IET DAVV
Indore (MP) India

V. Kapoor
Dept. of Information Technology,
IET DAVV
Indore (MP) India

ABSTRACT
Information security is more important for data communication in physical or network environment. Sending and receiving data over the internet is easy, fast and cost efficient due to development of information technology. Protected communication is more imperative for data move in the network. That put forward a new technique for hybrid cryptography with message digest and symmetric Algorithm, asymmetric algorithm. This research study proposes hybrid cryptography is a permutation of Message digest and Symmetric Key cryptography algorithm in the form of Digital Envelope. Message Digest is a fingerprint or the summary of a memo or data. Now the proposed system will try to improve the existing problem for integrity, proposed system use the MD5 algorithm. Due to this basis proposed system is capable then existing system. The message is initially encrypted with AES and the symmetric keys of AES are encrypted with RSA then the hybrid of both AES-RSA is embedded with message digest of data. The new results based on grouping of symmetric algorithm and Message digest will approve the effectiveness of the planned concept, and show the huge difference in key space and provide high-level security. This algorithm provides additional security as well as authentication comparing to other existing hybrid algorithm. It guarantees all cryptographic primitives, integrity, confidentiality and authentication. The implementation of the proposed technique is made with the help of JAVA technology and their performance is description with the help of space and time complexity. According to the trial results the proposed technique offers more secure environment and with less computational overheads.

General Terms
Message Digest, Hybrid Encryption, Symmetric Encryption.

Keywords
Message Digest, Symmetric key Encryption Algorithm, Cipher text, Plain text, Asymmetric key Encryption, Hybrid Algorithm

1. INTRODUCTION
The day by day, enlargements in the communication structure anxiety the very high altitude of information security in communication networks [1]. There is a call for cryptographic algorithms because of the exponential enhance in electronic transmit of data in several fields such as, e-commerce, banking, finance, etc. The transmission of information is augmented on the internet so network security is getting very importance. As a result, the confidentiality and the reliability of the information must be protected from unauthorized access [2]. It means their necessity be an explosive development in the field of information protection along with the copyrights of Data or change of Data. Confidentiality, accessibility, and integrity are the three main concepts of information security.

Cryptography is an encryption technique used to translate the readable information into an unreadable form. It is of two type's symmetric and asymmetric key cryptography. In[3] symmetric key cryptography identical key is used for both encryption and decryption while in public key or asymmetric key cryptography dissimilar keys are used for both encryption and decryption i.e. the public key for encryption and private key for decryption or vice versa.

The hybrid cryptosystem is itself a public-key structure, who's public and private keys are the equivalent as in the key encapsulation format.

- A key has encapsulation method which is a public (asymmetric) key or any other type of cryptosystem.
- A data has encapsulation scheme which is a private key cryptosystem.
- A data is also encapsulation with message Digest.

The main purpose of this project is to provide an efficient way to user send or receive the message over a secured channel and ensures the principles of security. Message digest provides the more secure mechanism [9].

As we all know that hash functions play an important role in digital signature schemes. A digital signature is a cryptographic technique that produces the electronic equivalent of a manual signature. This means that a digital signature can prohibit the forging of a message by anybody else but the sender. Symmetric key algorithms [5] are facing a difficulty related to the security of the keys and asymmetric key algorithm facing the difficulty of very slow speed as compare to symmetric key algorithms. Symmetric key algorithms can be used for both large and small message broadcast but asymmetric key algorithms are only well suitable for small message transformation over the internet. Therefore to shrink or overcome the problems of both symmetric and asymmetric key algorithms.

Proposed technique is a manner of encryption and decryption that merge two or more cryptography technique and usually includes a combination of symmetric, asymmetric and message digesting technique to take advantage of the strong suit of each type of cryptography. Mainly there are four security ethics "Confidentiality", "Integrity", "Authentication", and "Non-Repudiation".

2. RELATED WORK
Security plays a vital role while exchanging a large quantity of information from source to destination. Currently,

technology is growing very quickly from the security point of view. Each and every human being wants his communication must be confidential and protected from the access of the illegal users over the internet. Cryptography acts a very important job as security tools. Cryptography is the art of converting the readable information into an unreadable form [4].

Blueprint the innovative security protocol using hybrid encryption technique. The hybrid encryption technique is a combination of both symmetric sand asymmetric cryptographic techniques. It provides all the three cryptographic primitives -- integrity, confidentiality, and authentication. In this proposed design methodology, the new protocol design using Symmetric cipher and public key cryptography (RSA) with hash function [7].

“Ravindra Kumar Gupta, Parvinder Singh” projected technique is a method of encryption that combines two or more cryptography technique and usually includes a combination of symmetric and message digesting system to take help of the strengths of each type of cryptography. In which Symmetric technique fulfills the concept of Confidentiality, it also provide the performance advantage and therefore is the common solution for encrypting and decrypting performance-sensitive data [8.]

The study [11] reported that digital signatures are time-consuming in processing but it can be enhanced by combing it to hash functions that are fast in speed and also recognized as the message digest or deletion codes but another technique called authentication codes is also available to provide message integrity. The benefits to authentication codes are similar as the hash function with the additional characteristic of producing shorter length message. Report the comparison of the digital signature, hash functions and Message Authentication Code (MAC).

For getting security in wireless sensor networks (WSNs), cryptography acts a significant role. In this paper, a new security algorithm using a fusion of both symmetric and asymmetric cryptographic techniques is proposed to suggest high security with minimized key guard. Elliptical Curve Cryptography (ECC) and Advanced Encryption Standard (AES) are shared to make available encryption. XOR-DUAL RSA algorithm is considered for authentication and Message Digest-5 (MD5) for integrity. The results demonstrate that the projected hybrid algorithm gives enhanced performance in terms of computation time, the range of cipher text, and the energy consumption in WSN [12].

In this particular look, the accurate selection of precise encryption scheme matters for desired information exchange to meet improved security objectives. This survey compares fashionable encryption techniques for convinced choice of both key and cryptographic system. In addition, this study introduces two new encryption selection check’s which are neglected in previous studies. Finally, this full survey thrash outs the latest trends and research issues upon cryptographic elements to bring to a close forthcoming requirements related to the cryptographic key, algorithm structure and enhanced privacy especially in transferring the multimedia information[15].

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 [16] to take benefit of the strengths of each type of encryption. Basically, there are four security principles "Confidentiality", "Integrity", "Authentication", and "Non-Repudiation. In which Symmetric Technique do the concept of Confidentiality, it furthermore provides the performance advantage and as a result is a common solution for encrypting and decrypting performance-sensitive data. On the other hand, message digests technique fulfilling the authentication with integrity security principle theory to provide better security for cryptographic [17].

In paper "Meenakshi Shankar and Akshaya" integrates the RSA Algorithm with round-robin priority scheduling proposal in order to extend the level of security and reduce the efficiency of intrusion. It aims at obtaining nominal overhead, better throughput, and privacy. In this technique, the sender uses the RSA algorithm and creates the encrypted messages that are sorted priority-wise and then send [20].

This technique reduces the risk of man-in-middle attacks and timing attacks as the encrypted and decrypted messages are more disorderly based on their right of way. It also reduces the power monitoring attack risk if a very small amount of information is exchanged. It raises the bar on the principles of information security, ensuring more efficiency.

3. PROBLEM DOMAIN

3.1 Objective

In the cryptographic environment, efficiency is more important and means time for encryption and time for decryption in a real time environment. Suppose we are sending large information in a network, time to convert to plain text into cipher text or cipher text to plain text is more important. We are proposed that type hybrid algorithm that can take less time in compares to other present algorithms. We are also providing more security as compare to another algorithm.

3.2 Rationale

The existence of high computing influence processors is the creating diversified condition for symmetric encryption that relies on the small length of the key because distributed computation methods can break small key easily. 56 bits symmetric key of Data Encryption Standard (DES) has already been busted practically by Electronic Frontier Foundation in 1998 within the duration of fewer than 3 days [22].Another problem of symmetric encryption is the key exchange because, without secret and secure key exchange, symmetric encryption becomes unconfident. Origin authentication and cluster based secure information exchange under symmetric approach are the immense issues. It cannot be guaranteed at the time of exchanging secret key, both the received key is not falsely modified by the hacker and it is really sent by the authentic sender from whom we are expecting?

In the light of debate and analysis, it is clear that Public key cryptography is not feasible in case huge data. For asymmetric encryption large key(s) are based on complex factorization where the diversified situation with large factorization is that 663 bits and 911 bits composite number have been practically factorized in 2005 and 2006 respectively. NIST supports the exercise of symmetric encryption scheme DES and AES up to 2030 as mentioned in NIST stranded (SP800-57, 2005a).

4. PROPOSED METHODOLOGY

In existing cryptographic system, the major problem is cannot achieve this property like authentication, confidentiality, integrity, access control, and non-repudiation with not proper efficiency and reliable. In our proposed scheme, we try to ensure all these problems as well as improve our system and reliable. The proposed solution give a way to establish secure communication and it will also help to improve the level of encryption. The system does not require any external system interface for development. The proposed work includes two different major goals to achieve first the secure message on which the data is transmitted and efficiency in a cryptographic manner.

The proposed research is the designing and implementation of a new hybrid cryptosystem. Proposed technique is a manner of encryption that fuses two or more encryption technique and usually includes a combination of symmetric, asymmetric algorithm and message digesting technique.

Hybrid encryption is considered an extremely safe type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of asymmetric encryption scheme. Hybrid encryption is reached through data transmit using unique session or symmetric keys along with symmetrical encryption. The proposed algorithm is more efficient in compare to other algorithm or methods. The proposed algorithm is the combination of the symmetric key algorithm as "AES" with "message digest" than transmit the cipher text, message digest, and key. On the other hand, message digests technique satisfying the authentication as well as integrity security standard concept to offer better security for cryptographic.

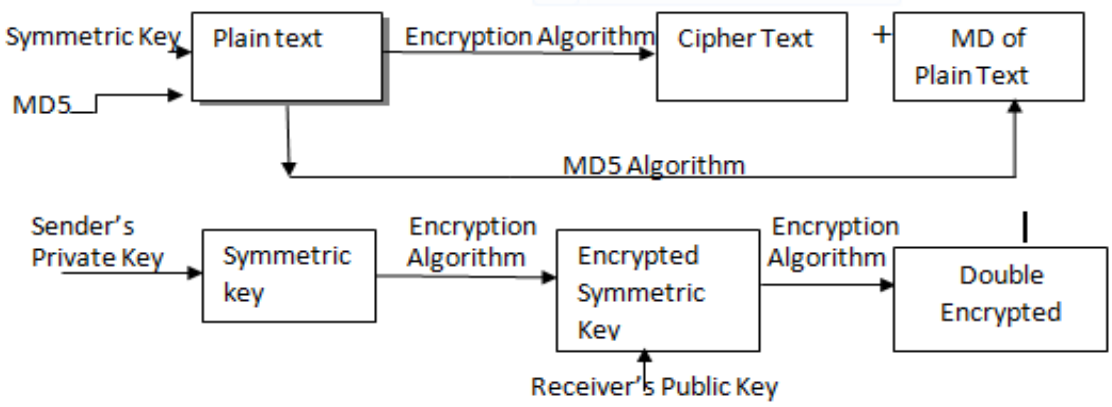

Fig.1 Encryption Process at Sender Site

Encryption Phase by User A

Step 1: Secret key Generation (Sk) with help Symmetric Algorithm

Step2: Calculate the message digest of Message (M) in form of DM.

Step3: That practically encrypted the *M* with Sk by using AES algorithm that returns cipher of plaintext *C.*

Step4: Encryption of Sk with B-PbK *and* APrK by using RSA algorithm which returns Double encrypted key as D*E*Sk.

Step5: Send the final encrypted message (*C* + DESk+*DM)* to *User* B.

Decryption Phase by User B:

On receiving *(*DESk + DM+ C*), User B* applies the following functions.

Step- 1: Decryption of DESk by applying his private key *(B*-PrK*)* and (*A* -Pbk) in order to get original session key *(*Sk*)*

.

Step 2: After that *user B* can decrypt the *C* by applying original Sk and AES algorithm in order to generate plaintext (M).

Step 3: After that User B can compare the old hash value of both DM and MD as sent by User A with the newly created hash values of C. If the hash values are the same it means no false modifications in message.

These steps discuss how normal security goals (confidentiality, origin authenticity, non-repudiation) can be fulfilled by any hybrid cryptosystem scheme. By applying these (ten steps), that practically tested the selected hybrid cryptosystems with a JAVA based tool against all phases including encryption, and decryption, compare of message digest.

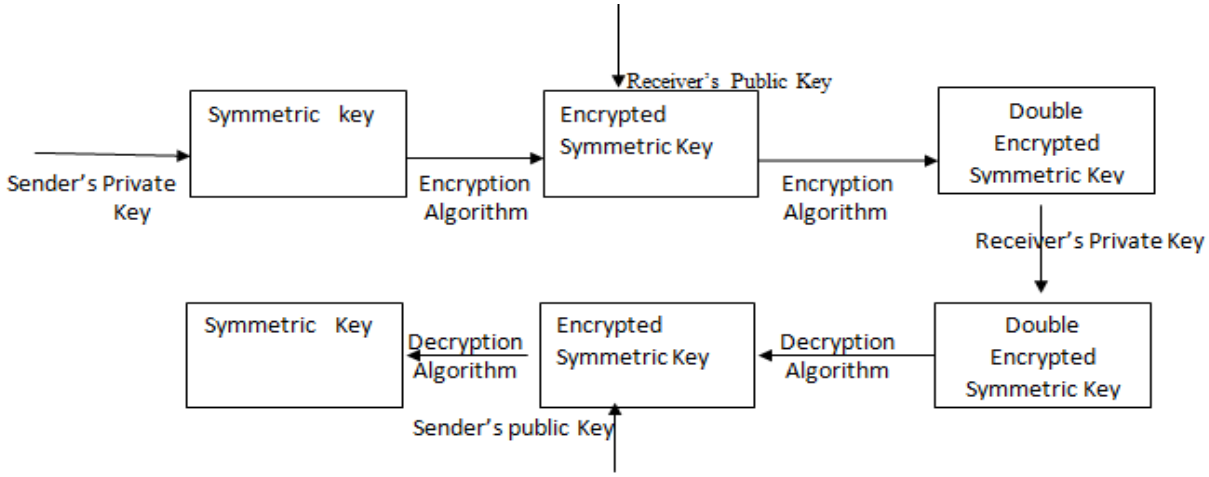

Fig 2: Encryption and Decryption Process of Key

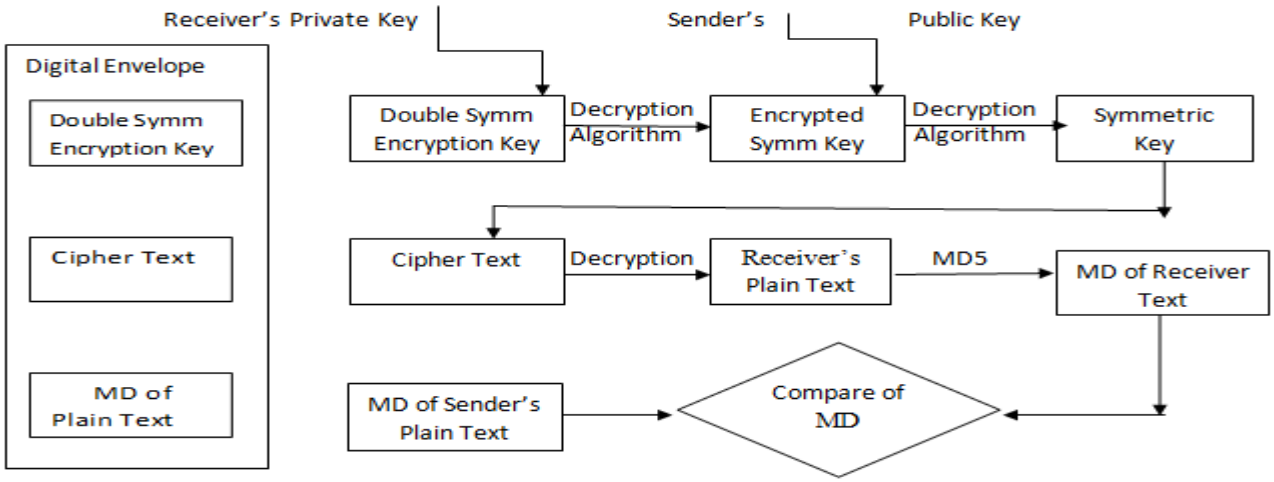

Figure 3: Decryption process of Symmetric key, Cipher Text and Compare of Message Digest

5. RESULTS

The Proposed solution will help to get better performance, encryption/decryption process, and also improve the security of the system. Proposed methodology implemented using java technology for estimation the performance of security system. Security of information over the internet is becoming a major concern. The proposed method is used to hide the information in a way that for any unauthorized person it is hardly accessible and they cannot easily recognize.

This section presents the results of evaluating the effectiveness of the proposed technique that is based on selected parameters like (time and space, processing unit.

Describe output of encryption process. It gives you an idea about the size of the cipher text in bytes. It is shown that algorithm has a largest size of cipher text whereas the other algorithms give a cipher text sizes that are equal or very close to the size of the plain text.

Table 1: Size of cipher Text

Plain Text(Byte)	Cipher Text(Byte)
407	416
813	816
1146	1152
1567	1696
1977	1984

Table 2: Time of encryption

Plain Text(Byte)	Encryption Time(in ms)
407	602
813	640
1146	670
1567	695
1977	702

Table 3: Time of Decryption

Plain Text(Byte)	Decryption Time
407	547
813	562
1146	583
1567	601
1977	624

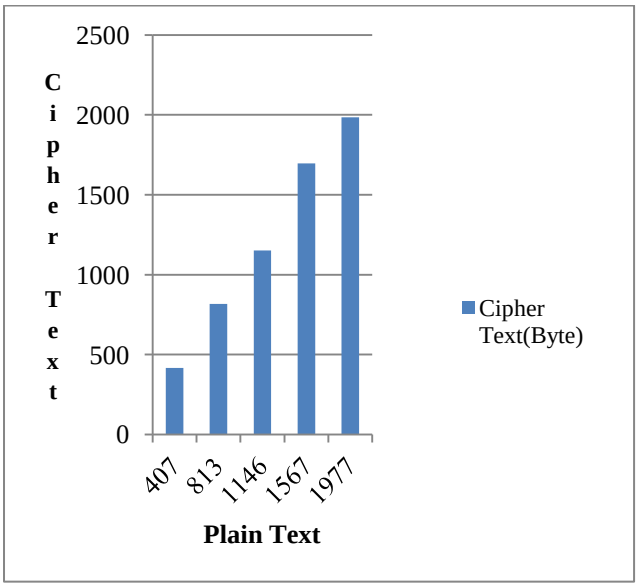

Figure 4: Cipher text size against Plain text

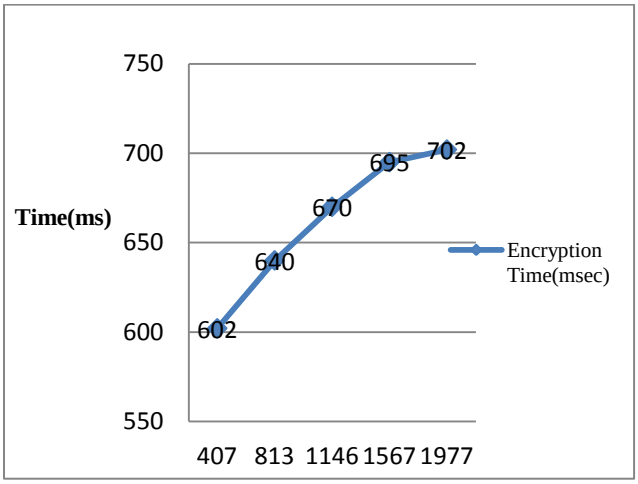

Fig 5: Encryption Time

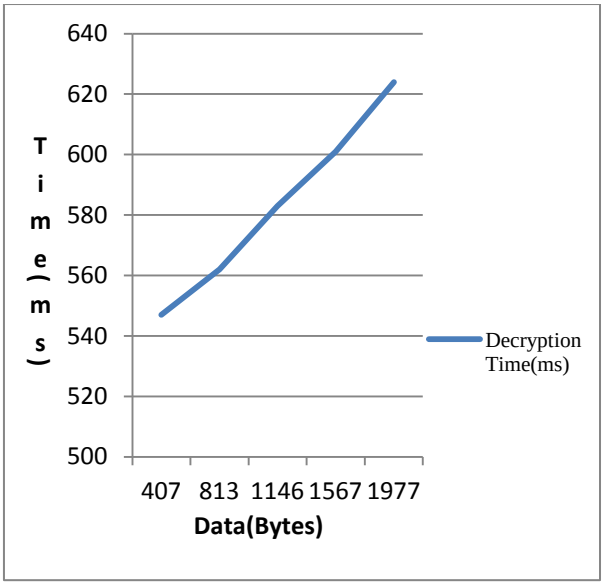

Fig 6: Decryption Time

For an algorithm, it is important to be competent and secure. The efficiency of an algorithm is computed on the basis of time and space complexity. These results come after the implementation of proposed methodology.

6. CONCLUSION

The encryption and decryption of any information cover a secure key, which is used for data encryption or decryption. The result of the proposed research plan shows that processing time is more efficient another algorithm. Thus AES algorithm along with the use of RSA algorithm for key administration will supply an efficient technique to ensure the security of transmitted data. Thus AES algorithm alongside with the use of RSA algorithm for key administration will provide an efficient technique to ensure the security of transmitted data.

A single is used for both encryption and decryption i.e. it has come under secret key cryptographic algorithm. But as public key cryptography is extra secured then secret key cryptography our next task would be to develop and design a public key cryptographic algorithm in a simple manner as it is done in this paper.

7. FUTURE WORKS

The proposed work is an effective technique for securing information in unsecured media. In future, we will put into practice for advance research together with features like authentication, confidentiality, integrity, access control and non-repudiation. More security will produce using all these entire features. This is efficient and suitable in terms of privacy, securely data access and utility of memory.

As a result, the proposed methodology may improve the system that used in real world. It's known that security is the main worried 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. Proposed encryption schemes to maintain the integrity and confidentiality of the data. The number of an existing system involving confidential information at the governmental managerial 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 problem and contributes the following. From the results, it will be analyzed that security of the proposed hybrid concept is very high as compare existing concept. It is already identified that security of the algorithm is text information on performance and security perspectives; second, access control methods use to control right of entry for all parties using the depended on the length of the key that means 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.

8. REFERENCES

[1] William Stallings "Cryptography and Network Security", 3rd Edition, Prentice-Hall Inc., 2005.

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

[3] Atul Kahate "Cryptography and Network Security",3rd Edition McGraw-Hill publication.

[4] Deepak Garg, Seema Verma "Improvement over public Key cryptographic Algorithm" 2009 IEEE International Advance computing conference.

[5] Bhatele, K. Sinhal, A.; Pathak, ." A novel approach to the design of 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.

[6] Rivest, R.L., Robshaw, M.J.B., Sidney, R., & Yin, Y.L (2000a). "The Case for RC6 as the AES PublicCommentURL:http://csrc.nist.gov/CryptoToolkit/aes/round2/comments/20000515-rrivest.pdf.

[7] Ramaraj, E., Karthikeyan, S. and Hemalatha, M. (2009), 'A design of security protocol using hybrid encryption technique', *International Journal of the Computer, the Internet and Management*, Vol. 17, No. 1, pp. 78-86.

[8] Gupta, R.K. and Parvinders, S. (2013), 'A new way to design and implementation of hybrid crypto system for security of the information in public network', *International Journal of Emerging Technology and Advanced Engineering*, Vol. 3, No. 8, pp. 108-115.

[9] Kuppuswamy, P. and Al-Khalidi, S.Q.Y. (2012), 'Implementation of Security through simple symmetric key algorithm based on modulo 37', *International Journal of Computers & Technology*, Vol. 3, No. 2, pp. 335-338.

[10] Kuppuswamy, P. and Al-Khalidi, S.Q.Y. (2014), 'Hybrid Encryption/Decryption Technique Using New Public-Key and Symmetric Key Algorithm' Department of Management Information Systems, College of Commerce, *MIS Review* Vol. 19, No. 2, March (2014), pp. 13.

[11] Kaliski. B. (1993), A Survey of Encryption Standards, *IEEE Micro,* 0272-1732/93/1200- 0074$03.00 1993 IEEE.

[12] Rawya Rizk , Yasmin Alkady "Two-phase hybrid cryptography algorithm for wireless sensor networks" Journal of Electrical Systems and Information Technology 2 (2015) 296–313.

[13] A Hybrid Crypto System based on a new Circle-Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications by "Rasmi P S Asst. Professor Toc H Institute Of Science Technology.

[14] Sitesh Kumar Sinha and Krishna Kumar Pande "A New Way of Design and Implementation of Hybrid Encryption to Protect Confidential Information from Malicious Attack in Network" International Journal of Computer Applications (0975 – 8887).

[15] 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 Conference for Page(s):87 - 92 Print ISBN:978-1-4673-5325-0.

[16] 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 - 765Print ISBN: 978-1-4673-2981-1.

[17] 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.

[18] Amrita Jain, Vivek Kapoor, "Policy for Secure Communication using Hybrid Encryption Algorithm", International Journal of Computer Applications (0975 – 8887), Volume 125 – No.10, September 2015.

[19] Ijaz Ali Shoukat , Kamalrulnizam Abu Bakar1 and Mohsin Iftikhar2 " A Survey about the Latest Trends and Research Issues of Cryptographic Elements" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011 ISSN (Online): 1694-0814.

[20] Meenakshi Shankar and Akshaya. "hybrid cryptographic technique using rsa algorithm and scheduling concepts" International Journal of Network Security & Its Applications (IJNSA)