An Application of Information Security through Hybrid Approach in Cryptography Technique

Ankur Patney
M.Tech. Research Scholar, CSE Dept
SIRT, Bhopal, M.P., India
ankurpatney@gmail.com

Yogadhar Pandey
Prof. in CSE Department
SIRT, Bhopal, M.P., India
anilpandey45@gmail.com

Dr. Rajiv Srivastava
Prof. in CSE Department
SIRT, Bhopal, M.P., India
drrajiv_sri@yahoo.com

Abstract— **Networks like internet applications are growing very high, so the needs to secure such type of applications are increased. Encryption techniques play an important role in information systems for security. On the other end, those technique which consume a significant amount of computing resources such as execution time, memory, and CPU utilization This paper presents a proposed model as a name given improved encryption algorithm (IEA)for encryption and decryption by which we can secure text information. The newly design encryption model is presented in this paper which is the combination of three different encryption technique. With help of proposed technique of encryption and decryption source stream or plain text, target stream or encrypted text will be generated and decrypted text will be gotten on the applying the reverse process. Expected results will be conduct for IEA technique at different settings like different data blocks size, different data types, different value of key and finally encryption/decryption time. Expected experimental results are given to demonstrate the effectiveness of proposed encryption technique.**

Keywords – **Symmetric key, Asymmetric key, Encryption, Decryption, Network Security**

INTRODUCTION

In cryptography [14], encryption is the process of converting readable information into unreadable information; it has been used to protect information for centuries, only company and individual's user with an extraordinary need for protection. During 1970s, encryption technique included as strong security of secretive government organization into the public domain, and is now employed in protecting widely-used systems, like Internet, mobile telephone networks and bank automatic teller machines. Encryption can be used to protect information, but some other techniques are still needed to make security, particularly to verify the message authenticity and integrity; for example, a message authentication code (MAC) or digital signatures. Figure 1 is showing a simple encryption and decryption process.

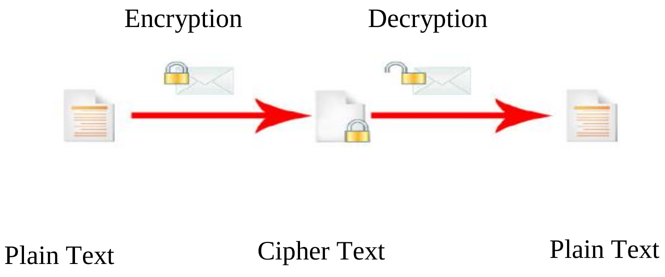

Figure 1: Simple Encryption/Decryption Process

In cryptography, to encrypt or decrypt data from one format to another it is required a key value. To shift five characters right in the alphabet to decode a message, In the case of the Cesar Cipher, this is the key knowledge. In modern encryption technique, file information is needed to encrypt or decrypt information and this can be done by two modern technique like public key encryption which use public key, and it is available to anyone, another is private key, which is used by the owner of the key pair only. If we want to send a message to the key owner, we must encrypt it using the public key. At the time of receiving message owner must decrypt it using his private key. On the other hand in symmetric encryption, it uses only single key which must be kept secret, but this can be shared with others those will be exchanging messages with the key owner [14].

Private Key Encryption: In symmetric encryption or private Key encryption only single key will be used for encryption and decryption of the information. The advantages of the technique are fast in execution due to single key is used for both ends of the encryption chain. Proper key security management is the primary concern at the time using private key encryption [16].

Public Key Encryption: In asymmetric encryption or public key encryption, is solving most perceived problem of the private key encryption is key exchanging between users. In this technique pair of keys used, as a public and as a private key. To privately communicate with the other user the public key is distributed to everyone. That user has the private key, which is paired to the public key. In this, private key will never shared between users where public key is widely available. Asymmetric key encryption is slower as compared to private key encryption because of multiple key distribution of managing between users [16].

Private vs. Public Key: Private Key encryption and public key encryption are alternate name of symmetric encryption and asymmetric encryption, respectively. Asymmetric encryption uses the two different keys to encrypt and decrypt information separately, while symmetric encryption only uses one key to encrypt information and decrypt information. Private key provide higher speed during encryption/decryption and public key solved key exchange problem so that a new technique come in the cryptography field know as hybrid cryptography.

Hybrid cryptography: Hybrid cryptography is a technique using multiple ciphers of different types together, each to its best advantage. A hybrid cryptosystem can be constructed using any two separate cryptosystems one is a key has encapsulation scheme which is a public-key cryptosystem and another is a data has encapsulation scheme which is a symmetric-key cryptosystem.

The hybrid cryptosystem is itself a public-key system, who's public and private keys are the same as in the key encapsulation scheme. Note that for very long messages the bulk of the work in encryption/decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt/decrypt a short key value. For example to encrypt a message addressed to user-1 in a hybrid technique, user-2 does the following:

1. Obtains user-1 public key.
2. Generates a fresh symmetric key
3. Encrypts the message using the symmetric key.
4. Encrypt the symmetric key using user-1 public key. Send both of these encryptions to user-1.

   To decrypt this hybrid cipher text, user-1 does the following:

1. User-1 uses her private key to decrypt the symmetric key.
2. User-1 uses this symmetric key to decrypt the message.

This Paper is dividing in four sections. Section- I, presenting basic introduction about cryptography technique like symmetric, asymmetric and hybrid cryptography, Section-II, presenting literature review on previous research in this era. Section-III, presenting proposed model and section IV presenting expected outcome, conclusion and references.

II. LITERATURE SURVEY

In this section is going to be present study of some previous hybrid cryptosystem. In [1] simply the gathering of recent developments in the field of Hybrid cryptography and its application in the designing of a hybrid security protocol for online transaction based on Hybrid cryptography. A new security protocol for on-line transaction can be designed using combination of both symmetric and asymmetric cryptographic techniques known as Hybrid cryptography. This protocol serves three very important cryptographic primitives-integrity, confidentiality and authentication. Each of the so called cryptographic primitive is provided or fulfilled by the particular symmetric or asymmetric cryptographic techniques. The symmetric cryptographic algorithms are fast as compared to asymmetric cryptographic algorithms, so when both symmetric and asymmetric algorithms are used in tandem or together in a proper way, then the result is very encouraging in terms of providing high security with fast speed. In [1] we have analyzed that a new security protocol for On-line transaction has presented and its importance is very much evident from the fact that Communication has a major impact on today's business. It is desired to communicate data with high security and in less amount of time. At present, various types of cryptographic algorithms provide high security to information on controlled networks. These algorithms are required to provide data security and users authenticity. A Hybrid security protocol has been designed for better security using a combination of both symmetric and asymmetric cryptographic algorithms. 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 suggested in [2]. That is, the algorithm security is greatly improved, through researching several famous data encryption algorithms, and improving some data encryption algorithms and arranging encryption algorithms in some order. Finally, the combined encryption algorithm is successfully made by using the initial encryption algorithm, Micro Genard encryption algorithm and the famous Base64 encryption algorithm. That is, in accordance with the order of the initial encryption algorithm, the improved Micro Genard encryption algorithm and the famous Base64 encryption algorithm, the user's information is gradually encrypted, and the algorithm security is greatly enhanced. Besides, to video surveillance software system for instance, which is widely used in the field of the traffic security management, the combined encryption algorithm is completely validated, and its security is very high. The internet world is continuous revolutions from the World Wide Web and the mobile Internet to the Internet of Things (IoT). IoT is the new world for connecting the object space in the real world with the virtual space in the computer world. Radio Frequency Identification (RFID) and Wireless Sensors (WS) are technologies that can be used to create the loT world. This increases the needs of these technologies in our daily life. However, there is a main drawback within these technologies which is to provide the low computation devices. Such a drawback limits the capabilities of RFID and WS. These technologies can hold a very sensitive data that may be related to the physical world such as the names or places of people. Thus, exposing this data can lead to security breach issues and researchers tried to come up with different security solutions with low computation. However, adding security to such low computation devices is a great challenge as they need a suitable lightweight cipher that is able to fit their properties. In [3] addresses some of the available lightweight ciphers, compares between them and comes up with a new algorithm that can fit low computation devices. A computer network is any set of computing nodes which has the ability of exchanging data by interacting with each other meaningfully, allowing resource sharing in a proper manner. The collection of computers is interconnected by communication channels, which need to be secure for better information exchange. This field of networking consists of specialist area of network security adopted by network administrator to prevent and monitor unauthorized access, modification and denial of computer network [4]. To combat the growing problem, security professionals are in search of better protection. Security Attacks compromises the security and hence various Symmetric and Asymmetric cryptographic algorithms have been proposed to achieve the security service in the proper manner, such as Authentication, Confidentiality, Integrity, Non-Repudiation and Availability. These algorithms are required to provide data security and users authenticity. To improve the strength of these security algorithms, a new security algorithm can be designed using combination of both symmetric and asymmetric cryptographic techniques [4]. This algorithm provides three cryptographic primitives such as integrity, confidentiality and authentication. This can be achieved by the combinatorial effect of Elliptic Curve Cryptography implemented by ECDH and ECDSA, Dual RSA and Hash algorithm implemented by Message Digest 5. In [5] we have observed that there is introduces a new secret data communication system that employs the usage of two state-of-the art cryptographic algorithms (RSA with asymmetric keys and AES with symmetric key) together with steganography. The joining of these three techniques builds a robust steganography-based communication system capable of withstanding multiple types of attacks, detection and reverse engineering. suggested system was designed in a way that offers a solution to the major flaws presented in other steganographic communication systems The secret data is encrypted using AES with a strong key prior to being embedded using a steganographic algorithm. The key used for the data encryption uses a combination between a random generated sequence and a hash of the cover image's color information that remains untouched throughout the entire embedding process. The secret data and the key used for encryption both pass multiple levels of security checks that assure the integrity, authenticity and security, making this a reliable communication channel for sensitive data. While all encryption stages assure that the secret data becomes obsolete without the proper decryption perquisites (keys), the steganographic algorithm introduces an additional level of security: stealth. Advanced Encryption Standard (AES) and Elliptic Curve Cryptosystems (ECC) are the two most commonly used symmetric and asymmetric encryption algorithms. In [6] we have analyzes there are two algorithm has been designed both the AES algorithm and the ECC algorithm. Combining with the characteristics of the AES and ECC, a mixed email encryption system is designed, which can solve the problem such as password system speed and security, which can't efficiently realize the information, data encryption, signature and identity verification. And the hybrid encryption is applied into the email system to enhance the network security of information transmission. In [7] author has presented and developed hybrid cryptosystem for information security over public network. We have already known that a computer network is an interconnected group of autonomous computing nodes, which use a well defined, mutually agreed set of rules and conventions known as protocols, interact with one-another meaningfully and allow resource sharing preferably in a predictable and controllable manner. Here they have concentrate on how they can over come security attack to communicate data between sender and receiver with high security. Security Attacks compromises the security and hence various Symmetric and Asymmetric cryptographic algorithms have been proposed to achieve the security services such as Authentication, Confidentiality, Integrity, Non-Repudiation and Availability. At present, various types of cryptographic algorithms are exists for secured information over networks. To improve the strength of these security algorithms, authors have designed a new security protocol for on line transaction using combination of both symmetric and asymmetric cryptographic techniques. This protocol provides three cryptographic primitives such as integrity, confidentiality and authentication. These three primitives can be achieved with the help of Elliptic Curve Cryptography, Dual-RSA algorithm and Message Digest MD5. That is it uses Elliptic Curve Cryptography for encryption, Dual-RSA algorithm for authentication and MD-5 for integrity. This new security protocol has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.

In [8] they have combined both symmetric and asymmetric encryption techniques where the plain text is encrypted using the AES algorithm. The AES key which is used to encrypt the data by ECC which is also an asymmetric cryptography. The cipher text of the message and the cipher text of the key are then sent to the receiver. To ensure integrity of the data that is transmitted, the data is subjected to MD5 hash algorithm. The message digest obtained by this process is also encrypted using ECC technique.

Issue in Existing System: From the study of above mentioned research we have observed that there are several limitations despite the promise it holds. These are described following. Previous research performed several floating point operations which demands sufficient amount of precision from the sender and receiver processor. This is the time consuming process. Reliability is another factor to observe quality of the algorithm and from the observation of the previous research that previous algorithm has not too much reliable. As we know that reliability can be increased with some modification in symmetric cryptography and to avoid complex mathematical operation. Many algorithms have used floating point calculation and round off operation limits the size of the block to encode. In practical simulation it worked perfectly for 32 bit block size. But increasing the block size may be subject to round off error. Previous algorithms will be more appropriate for software implementation whereas hardware implementation can be quite tedious and tricky - which contrasts to traditional symmetric key algorithms. Due to lots of mathematical operation efficiency of previous technique has degreed. We have already known that to calculate square function, multiplication function and angle function too much efficiency is required. In Existing hybrid cryptosystem in above mentioned research have very high and finally complex structure of previous algorithm which is the causes of high complexity.

Sending sensitive messages and files over the Internet is very dangerous. If I need to send sensitive information over the Internet I should encrypt it first. With Encryption and Decryption I can safely send sensitive messages and files. Need to safely store sensitive information on our computer? Encryption and Decryption works with both text information and files. Just select what I want to encrypt, and Encryption and Decryption helps I keep documents, private information and files in a confidential way**.** Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, I need to ensure information security and safety. Furthermore point is following.

- Need to send secure?
- Need to protect sensitive data stored on our computer?
- Need to decrease encryption/decryption time”
- Need to increase efficiency?

III. PROPOSED WORK

Proposed research is the designing of a new Hybrid cryptography concept. Proposed concept is a method of encryption that combines three encryption techniques to take benefit of the strengths of each type of encryption. Symmetric encryption has the performance advantage and therefore is the common solution for encrypting and decrypting performance-sensitive data. In figure 1.1, showing simple block diagram of proposed hybrid Cryptography Concept. In this original text will pass as an input to first encryption technique which is define in [2] will produced first cipher text, this cipher text will pass as an input to second proposed encryption technique as a name given improved encryption algorithm (IEA) which will produced second cipher text, this cipher text will pass as an input to third encryption technique which is define in [2] will produced final cipher text. At another end final cipher text will pass as an input to third decryption technique this will produced cipher text toward original text, this cipher text will pass as an input to second proposed decryption technique which will produce cipher text and at last this cipher text will pass as an input to first decryption technique to produced original text. In proposed work 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). It already known that all the selected operation are very simple and very effectively. Due to this reason proposed system is secure and efficient.

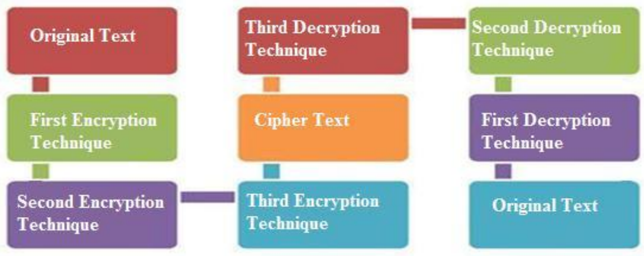
Original Text
First Encryption Technique
Second Encryption Technique
Third Encryption Technique
Cipher Text
Third Decryption Technique
Second Decryption Technique
First Decryption Technique
Original Text

Figure 1:- Block diagram of Proposed Hybrid cryptosystem

Proposed hybrid model has number of characteristic which is following:

- **Adaptability and Availability:** The proposed hybrid model will be efficiently implementable in hardware as well as on general purpose large, medium and small sized processors (for e.g. microprocessors, microcontrollers and smart cards respectively).
- **Correctness and consistency:** The specification of proposed model will be correct. The specification, proposed software will be consistent.
- **Portability:** The proposed software will be in Dot Net programming language (and will execute on any system with Dot Net compiler has been ported to). The portability of other software implementations will depend on portability of choice of programming language.
- **Performance:** To be able to implement proposed model special purpose hardware with the goal to decreasing memory requirements and execution time, special consideration should be given to possible (and alternative) simplifications of proposed hybrid model.

IV. EXPECTED OUTCOME AND CONCLUSION

It is already known that Execution time, CPU Consumption and throughput and many other parameters are very important for any type of encryption/decryption algorithm. These parameters decided to the performance of any algorithm in this era. The execution time is the time that an encryption algorithm takes to produce a cipher text from a plaintext. Execution time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the execution time. 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. Proposed hybrid model will be evaluated on above mention parameter and expected results are shown in table 1-3. Expected results based on performance of selected parameters are shown in this. One more thing is Key length which plays an important role during encryption/decryption so proposed encryption technique supposed 128 bits key length will used during encryption/decryption. The expected experimental results show the effectiveness of the proposed model in terms of execution time, CPU Consumption, and Throughput.

Table 1: Expected Execution Time of Proposed Hybrid Encryption Technique

S. No.	File Size (In KB)	File Type	IEA
Throughput (Approximately)			
1	2	TXT	High
2	4	TXT	High
3	6	TXT	High
4	8	TXT	High
5	10	TXT	High

Table 2: Expected throughput of Proposed Hybrid Encryption Technique

S. No.	File Size (In KB)	File Type	IEA
CPU Uses (Approximately)			
1	2	TXT	Low
2	4	TXT	Low
3	6	TXT	Low
4	8	TXT	Low
5	10	TXT	Low

Table 3: Expected CPU Consumption of Proposed Hybrid Encryption Technique

From table 1 it analyzed that execution time of the proposed hybrid encryption technique is very low due to its simplicity and use very common and strong operation, similarly table 2 and table 3 producing good results for proposed hybrid model for CPU consumption and throughput. Due to low response time of proposed hybrid encryption technique CPU consumption will also low and maximum number of information can be encrypt/decrypt during a period which is the cause of good throughput.

V. CONCLUSION

With discuss the security analysis of the proposed hybrid encryption technique including some important ones like the complexity of time, CPU consumption, and throughput. With the rising demand of the encryption strength, most governments have not satisfied with the current several hybrids cryptographic algorithms now, they continuous research on the new hybrid cryptographic algorithms. However, it is a difficult problem to evaluate the specific algorithm, they must consider many factors: security, the features of algorithm, the complexity of time and other parameters, etc, so research on the time-consuming of algorithm is one of the important respect. The results also indirectly reflect the motivation of developing hybrid cryptographic algorithms.

VI. REFERENCE

S. No.	File Size (In KB)	File Type	IEA
Execution Time (Approximately)			
1	2	TXT	Low
2	4	TXT	Low
3	6	TXT	Low
4	8	TXT	Low
5	10	TXT	Low

[1] Kirtiraj Bhatele, Prof. Amit Sinhal and Prof. Mayank Pathak "A Novel Approach to the Design of a New Hybrid Security Protocol Architecture" 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)

[2] Lili Yu, Zhijuan Wang and Weifeng Wang "The Application of Hybrid Encryption Algorithm in Software Security" 2012 Fourth International Conference on Computational Intelligence and Communication Networks

[3] Mouza Bani Shemaili, Chan Yeob Yeun, Khalid Mubarak, Mohamed Jamal Zemerly "A New Lightweight Hybrid Cryptographic Algorithm for The Internet of Things" 2012 IEEE The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)

[4] Manali J Dubal, Mahesh T R, and Pinaki A Ghosh "Design Of New Security Algorithm Using Hybrid Cryptography Architecture" 2012 IEEE

[5] Septimiu Fabian Mare, Mircea Vladutiu and Lucian Prodan "Secret data communication system using Steganography, AES and RSA" 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME)

[6] Chen JunLi. Qing Dinghu. Yu Haifeng. Zhang Hao. MeiJuan Nie. "Email Encryption System Based On Hybrid AES And ECC"

[7] S. Subasree and N. K. Sakthivel "Design of a New Security Protocol using Hybrid Cryptography Algorithm" published in IJRRAS 2 February 2010

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

[9] Jinbiao Hou "Research on Database Security of E-Commerce Based on Hybrid Encryption" 2009 International Symposium

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

[11] 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)

[12] Jinbiao Hou "Research on Database Security of E-Commerce Based on Hybrid Encryption" 2009 International Symposium

[13] "A New Symmetric Key Encryption Algorithm based on 2d geometry"- 2009 International Conference on Electronic Computer Technology.

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

[15] JJ Quisquarter and Couvreur." Fast decipherment Algorithm for RSA public key crypto system", electronic Letters Vol435, 1989

[16] Elliptic curve cryptography http://en.wikipedia.org/wiki/Elliptic Curve Cryptography

[17] Dus and Gupta, Planar geometry (2nd edition)

[18]The Discrete Logarithm Problem (http: //www.cs.toronto.edu/~cvs/dlog/) Cipher text-Only Attack, http://www.javvin.com/networksecurity/CiphertextOnlyAttack.html)

[19] Known-plaintext attack (http://www.tech- faq.com/knownplaintext-attack.shtml)

[20] RSA (http://en.wikipedia.org/wiki/chinese RSA.html)

[21] RSA (http://en.wikipedia.org/wiki/chineseRemainder.html