ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Design and Implementation of a Hybrid Database Encryption Model

Moses Okechukwu Onyesolu., Nwachukwu Chigozie Nnabugwu,

Department of Computer Science, Faculty of Physical Sciences, Nnamdi Azikiwe University, Awka, Nigeria

ABSTRACT:Development and management of good database system as well as providing security control for the database has always been a major issue in this digital age. Various encryption techniques has previously been developed to provide security to users. However, a number of these encryption algorithms are weak or have bottlenecks thereby putting the security of data stored in the database in question. In this research, we designed a new hybrid database encryption model that improves the security of the database. The new hybrid encryption algorithm combines the features of the Advanced Encryption Algorithm (AES) and the RSA algorithm for encryption of the database to provide integrity, authentication and key distribution. Additionally, Secure Hashing Algorithm (SHA512) and salting technique is used to enhance the security of the stored passwords. The results from the analysis demonstrate that proposed model offers a highly secure approach that provides users and organization with data confidentiality and integrity.

KEYWORDS:Ciphertext, encryption, decryption, symmetric encryption, asymmetric encryption, hashing and salting, authentication, hybrid encryption, encryption key.

I. INTRODUCTION

Security is one of the most important aspects in computing. In data transfer, security must be considered as one of the methods implemented to ensure secure data transfer. Data transfer simply refers to transferring information from a location or host to another host, or server. To have a secure data transfer, few methods can be applied, and one of them is encryption of data. Data security cannot be achieved without considering its management. Database management system maintains the integrity and confidentiality of data hence the need for strengthening data security is growing. One of the necessities for securing databases is to encrypt the information stored inside them. Considering the importance of data in organization, it is absolutely essential to secure the data present in the database.

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [1]. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage. The main goal of cryptography is keeping data secured from unauthorized attackers. The reverse of data encryption is data decryption.

Encryption is a process of transforming information that usually are plaintext using an algorithm (known as cipher) to make it unreadable to anyone except those who have the special knowledge known as the key [2]. The output from the process is known as cipher text. In the reverse, the process is called decryption to make the information readable. Encryption can be referred to as the process of transforming information in such a way that an unauthorized third party cannot read it; a trusted person can decrypt the data and access it in its original form though. There are a lot of popular encryption/decryption methods, but the key to security is not just the proprietary algorithm. Encryption of data mostly has to do with the robustness of encryption methods, achievement of security constraints and processing speed related issues. The actual problem occurs at the time of exchanging encrypted data and key(s) via insecure remote communication channels [3]. In evaluating technology solution for data security, an effective data protection solution

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

must be able to ensure end-to-end security, reliability, integrity and confidentiality throughout the data exchange process and provide management visibility over the process through integrated application level security.

There are a lot of encryption techniques that have been in existence over the years each with its bottlenecks. These encryption techniques have different algorithms which help to determine how the system converts the plaintext into ciphertext and decrypts it back to plaintext. Some of these encryption standards includes Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Rivest –Shamir-Adleman (RSA), Blowfish, Twofish, Digital Signature Algorithm (DSA), Elliptic Curve Cryptography (ECC) to mention but a few. In this work, a review of some these encryption standards will help determine a better way of concatenating/combining them to produce a more efficient model.

II. REVIEW OF RELATED WORKS

Previous works by other scholars and researchers were reviewed. An overview of these related works by various authors on hybrid encryption security algorithms are stated:

Arshad et al. [4] developed a new affine block cipher named Enhanced Affine Block Cipher Technique for database encryption. This helped improve the weakness of the original affine cipher. The new encoding schema developed was also beneficial in protecting user password.Jhanwar and Barua[5] came up with a hybrid public-key encryption scheme which is provably secure against adaptive chosen ciphertext attack. The scheme was constructed using Kurosawa-Desmedt paradigm. The security of the scheme is based on the Decisional Bilinear Diffie-Hellman problem.Wi[6] designed a protocol for encryption of information on a web which makes it secure and hard to decrypt. This model used the substitution cipher in which each letter in the plaintext is replaced by some fixed number of position down the alphabet. This method is named after Julius Caesar who used this method to communicate with his generals. The result from this project is a data which is encrypted and decrypted to its readable form.

Kuppuswamy andChandrasekar[7] came up with a new algorithm, which was based on linear block cipher. The concept of the algorithm was based on modular 37 (alphabets and numerals) whereas existing algorithms are based only on modular 26 (only alphabets). They named it New Linear Block Cipher (NLBC) as it was linear based algorithm. Thakur et al. [8] provides a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behaviour and the performance of the algorithm when different data sizes are used. The comparison is made on the basis of these parameters: speed, block size, and key size. Jignesh,Rajesh and Vikas[9] presented an improved Hybrid AES-DES algorithm as means of strengthening the current AES architecture. The hybrid model gives a better non linearity to the plain AES and as it is merged with DES there is better diffusion hence the possibility of an algebraic attack on the hybrid model is reduced.

Pratap[10] provided a fair comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. Comparison was made on the basis of these parameters: rounds block size, key size, encryption/decryption time and CPU process time in the form of throughput and power consumption. These results show that blowfish is more suitable than AES.Mateescu and Vladescu[11] came up with the hybrid approach of system security for small and medium enterprises by combining two different cryptography techniques which are Digital Signature algorithm and the RSA algorithm.Kuppuswamy and Al-Khalidi[12] carried out further research on hybrid encryption. The result of their research was a hybrid encryption algorithm using Block cipher and symmetric key which provides a more secure and convenient technique for secure data transmission for all kind application.Singh and Kaur [13] developed a hybrid approach for encrypting data on cloud to prevent DoS attacks. The new system was introduced to encrypt and decrypt the data before sending on cloud by using the two different techniques and was beneficial for simple data transfer and storing the data on a cloud.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Onyesolu and Ogwara[14] designed a hybrid encryption system that combines two symmetric encryption algorithms which were 3DES and AES together with hatching and salting techniques. The new hybrid system proved to be a more secure system in keeping out attacks on information stored in the database.Rani and Kaur [15] discussed about cryptography AES and Elgamal and proposed a hybrid algorithm using AES and Elgamal algorithms. The new hybrid cryptographic technique was designed to decrease encryption and decryption time and increase throughput. The Cryptographic algorithms play a very important role in network security.

Summary and Deductions from Reviewed Works

Security is very important feature for any technology. Using any technology will not be worth it if it is not secure. In this research work, a hybrid technique is designed using two different algorithms to provide for the security of data on the higher level. This technique is beneficial in simple data transfer and data accessing. Some experimental analysis has been done on the basis of performance, execution time, response time and the CPU performance in VM telemetry view. Concluding all the different parameters the response time is fair and performance of the new technique is higher than the other two individual techniques and it is providing the higher security to the data. Since the drawback faced in the already existing hybrid is the execution time. The time taken to execute the whole process is a bit higher than that of the other three techniques though it's fair enough. But if any technology is secured then some compromises can also be done.

III. METHODOLOGY

The methodology adopted for this work is the Object Oriented Analysis and Design methodology (OOADM) with Prototyping. OOADM involves studying an existing system from the perspective of objects. Similar objects are grouped as classes and their characteristics are handled as properties while their behaviours are treated as the actions or methods within the same bundle of object. We employ the use of classes and objects to demonstrate the process of implementing the hybrid encryption process of securing data stored in the database, in order to enhance the security of information against unauthorized user's access to the database.The goal of OOADM is to improve system quality and productivity of systems analysis and design by making it more usable

In this work, we propose a hybrid encryption model that includes the features of two existing encryption algorithm which include Rijndael-Advanced Encryption Standard (AES) and RSA. In addition to this is Secure Hash Algorithm (SHA512) with salting techniques to secure passwords stored in the database. Every record is encrypted, before storing the encrypted records in the database using a double encryption method, first of all the records is encrypted using a first algorithm and the output of the first encryption algorithm is used as an input to the second algorithm and the final output is stored in the database. For every records stored there is a unique passphrase which is also encrypted alongside with the record. The SHA512 is a secure hash algorithm that was used in the implementation of password storage policy together with randomly generated salting techniques

Mathematical Specification

In this work, the mathematical specification involves the mathematics behind the function of the new hybrid encryption model, hashing algorithm and the salting techniques, used in the implementation of the hybrid security system for database application. The mathematical specifications are given in Equation 1 to Equation 3

The hybrid encryption system used in this work is *n-tuple where n=5 with tuple attributes given as (P, C, K, E, D) and where each attribute is:*

P is a finite set of plaintexts,
C is a finite set of ciphertexts,
K is a finite set of keys,
E is a finite set of encryption algorithms,
D is a finite set of decryption algorithms.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

For each $k \in K$ there are encryption algorithms in E. The encryption algorithms are functions:

$$e_{kn}: P \rightarrow C_n \text{ for n =1} \quad (1)$$

Assuming that P=X, where X is a polynomial of higher degree

The first encryption algorithm using the integration of P(X) with respect to x.such that

$$e_{k1} = \int P dx = \int x dx \quad \forall \text{ n=1} \quad (2)$$

$$\int x\,dx = \frac{x^2}{2} + a_0 = \quad C_1$$

$\forall \; n = 2$ For the Second Encryption

Using equation 2

$$E_{k2} = \int C_1 = \int \left[\frac{x^2}{2} + a_0 \right] dx$$

$$= \quad \frac{x^3}{6} + a_0 + a_1 = C_2$$

Such that $e_{kn}: C_{n-1} \rightarrow C_n$. *for* $n > 1$

Also for each $k \in K$ there are decryption algorithms in D. The decryption algorithms are the derivatives of the functions.

Such that $d_{kn}: C_n \rightarrow C_{n-1}$ for n>1 (3)

Using Equation 3

$$D_{k2} = \frac{d}{dx} C_2$$

$$= \quad \frac{d}{dx}\left(\frac{3x^3}{6} + a_0 x + a_1 \right)$$

$$= \quad \frac{d}{dx}\left(\frac{x^2}{2} + a_0 = C_1 \right)$$

Such that $d_{kn}: C_n \rightarrow C_1$ for n=1

$$D_{k1} = \frac{d}{dx} C_1$$

$$D_{k1} = \quad \frac{d}{dx}\left(\frac{x^2}{2} + a_0 \right)$$

$$D_{k1} = \quad \frac{d}{dx}\left(\frac{2x}{2} + a_0 \right) = X$$

Such that $d_{k2}(e_{k2}(d_{k1}(e_{k1}(p)))) = p$ *for every plain text* $p \in P$.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

In other words, for every key k_1 and k_2 the function d_{k2} and d_{k1} is the inverse function of the function e_{k2} and e_{k1} respectively. In particular, this means that

$$p=d_{k2}(e_{k2}(d_{k1}(e_{k1}(p)))) = d_{k2}(e_{k2}(d_{k1}(e_{k1}(p')))) = p'.$$

The hybrid encryption algorithm is still the safest even though the encryption methods that is being employed might be known by a cryptanalyst or a hacker. Mathematically, this means that the cryptanalyst knows the functions e_1, e_2, d_1 *and* d_2.

This illustrates the basic premise of modern cryptography called the Kerckhoff's principle which says that the security of a cryptosystem depends on the secrecy of the keys and not the secrecy of the encryption algorithm itself.

If (P, C, K, E, D) is to be a successful cipher, it must have the following constraint properties:

1. For any key $k \in K$ and a plaintext $p \in P$, it must be easy to compute the ciphertext $e_k(p)$.
2. For any key $k \in K$ and a ciphertext $c \in C$, it must be easy to compute the plain text $d_k(c)$.
3. Given one or more ciphertext $c_1,c_2,c_3,\ldots,c_n \in C$ encrypted using the key $k \in K$, it must be very difficult to compute any of the corresponding plaintexts
   $d_k(c_1),d_k(c_2),\ldots d_k(c_n)$ without the knowledge of k.
4. Given one or more pairs of plain text and their corresponding cipher text
   $(p_1,c_1),(p_2,c_2),\ldots p_n,c_n)$, it must be difficult to decrypt any ciphertext c that is not in the given list without knowing k. This is known as security against a chosen plaintext attack.

Hashing and Salting Algorithm Model Description

The main point of one-way hash function is that any encrypted text cannot be decrypted. From this point, we need to choose the noninvertible matrix from the hill cipher to use it inside the practical one-way hash algorithm. First we take non-invertible matrix, multiply it by plaintext as column vector with modular value n to generate the hash value H. The sender of the message calculates the hash value or message digest by using the model. After that the message and the hash value are sent to the receiver who makes the same calculations by using the model to generate a message hash value. Finally, the receiver compares between the messages digest from the sender and the hash value that he calculated.

H (V) = V. R mod N.
H (V) = hash value generated.
V =randomly generated number as salt and plaintext message as column vector
R = non-invertible matrix.
N = modular value.
We use the R as a non-invertible matrix that cannot be reversed, which is used to generate hash value using this formula:
H(V) = V . R mod N. R cannot be reversed,
If we Calculate the determinant of this matrix d where d = |R|, then does not relatively prime to N , so R−1does not exist and we cannot calculate the value of (H(V))-1.

Algorithm

In this work, several algorithms were used in the process of implementing a hybrid security system for database applications.These algorithms are High Level Description Hybrid Encryption Algorithm and AES Algorithm

High Level Description Hybrid Encryption Algorithm

State = X, Generate Random Keys k

1. AddRoundKey (State, Key k) [Initial Round, Add Round Key: each byte of the state is combined with a block of the round key using bitwise XOR]
2. For r = 1 to (Nr - 1)
   a. Sub Bytes (State, S box) [Sub Bytes: a non-linear substitution step where each byte is replaced with another according to a lookup table]
   b. Shift Rows (State) [a transposition step where the last three rows of the state are shifted cyclically a certain number of steps]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

c. MixColumns(State) [MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.]
d. AddRoundKey(State, Keyr) [Add Round Key]

End

AES Algorithm

Final Round (no MixColumns)

1. SubBytes(State, S box)
2. ShiftRows(State)
3. AddRoundKey(State, Key,Nr) Y = State
   Then Y is split into two 28 halves
4. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
5. The halves are recombined and subject to a compression permutation to reduce the key from. 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
6. The rotated key halves from step 2 are used in next round.
7. The data block is split into two 32-bit halves.
8. One half is subject to an expansion permutation to increase its size to 48 bits.
   Output of step 7 is exclusive-OR'ed with the 48- it compressed key from step 5.
9. Output of step 8 is fed into an S-box, which substitutes key bits and reduces the 48 bit block back down to 32-bits.
10. Output of step 9 is subject to a P-box to permute the bits.
11. The output from the P-box is exclusive-ORed with other half of the data block. k. The two data halves are swapped and become the next round's input.

IV. RESULTS AND DISCUSSION

Experimental results for the different algorithms AES, RSA and the new hybrid technique are shown graphically and in tabular form on the basis of different parameters. The result obtained from the experimental process are gotten from the calculation of the time consumed in both operations "encryption, decryption" and comparing it with the different algorithm. The evaluation of the strength and performance of the proposed hybrid algorithm was calculated in this processes. This comparison was conducted on two text files of size 153 kb and 868 kb for the three algorithms.

Table 1 Comparisons of RSA, AES and New Chucksz Hybrid Encryption (CHES) of encryption time, decryption time and size of encrypted file.

S. No.	Data Size (kb)	Algorithm	Execution Time (Sec)	Performance	Response Time (sec)
1	153	AES	1.50	High	1.00
		RSA	7.30	Lower	2.30
		Hybrid	8.20	Higher	0.89
2	868	AES	2.30	High	1.80
		RSA	8.30	Lower	4.00
		Hybrid	9.00	Higher	1.00

Table 1 is the results of experiments where the two different individual algorithms are tested with data of different sizes alongside the new hybrid algorithm to determine the execution time, performance and the response time.

From Table 1, the time taken by new hybrid encryption algorithm for both encryption and decryption process is a bit higher compared to the time taken by AES and RSA algorithm.Multiple comparisons were done on the previous algorithms using different parameters. The first comparison is given between the execution time and response time of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

text file with size 153 Kb and in the second, same comparison but with the 868Kb file size. The last one calculates/analyses the performance of the system. Figure2 shows the comparison time for encryption of both algorithms, here we found RSA algorithm consuming a long time to complete the encryption operation for all files compared with the AES and the proposed algorithm, and the file with size 868Kb take the longest time
This makes the new hybrid encryption algorithm much more secure since it will take a longer time to decrypt such files and also require the use of two secret keys which cannot easily be guessed by an unauthorized user.

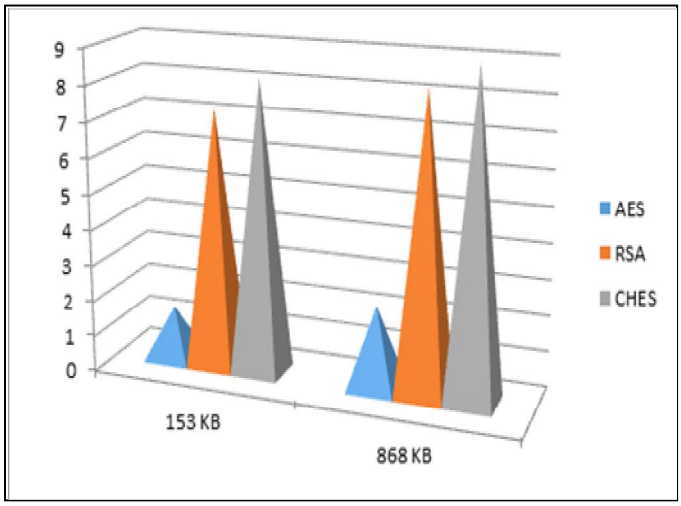

Figure 2: Comparison of Encryption Time among AES, RSA and CHES

Figures 2 is a graphical representation of the different algorithms with respect to the encryption time and the results obtained from the experiment carried out with data of different sizes.

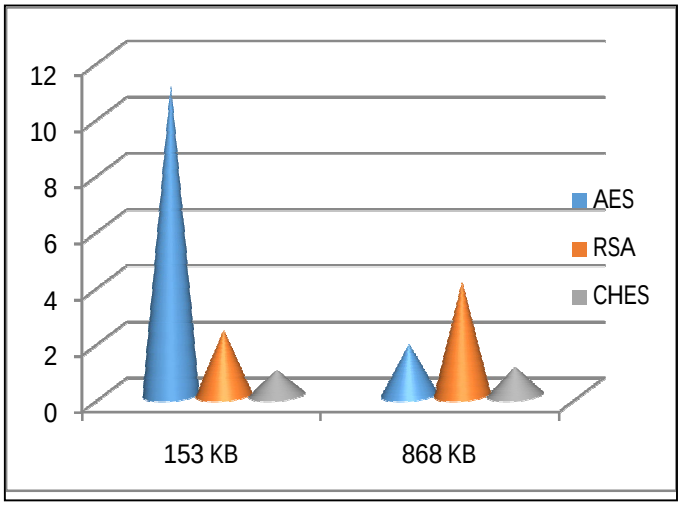

Figure 3: Comparison of Response Time among RSA, AES and CHES

Figure 3 is a graphical representation of the different algorithms compared to the response time with data size of 153kb and 868kb.Figure 2 and Figure 3 show time taken for encryption and the size of the encrypted file on various size of file by three algorithms, it can be deduced that the new hybrid encryption algorithm takes much longer time compared

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

to time taken by AES and RSA. Since the hybrid algorithm takes longer time for both encryption and decryption, it makes it more secure, since the higher the encryption process the longer it will take for a hacker to break the encryption algorithm, since computing power is on the increase, speed will not be a problem in the nearest future and as such, in certain classified database, we cannot trade security with speed.

V. CONCLUSIONS AND RECOMMENDATIONS

Summary

In this work an analysis of some existing cryptographic algorithms wasdonehighlighting some of the advantages and drawbacks. As a result, we resorted to combining some of these algorithms to develop a more efficient hybrid system. This new hybrid system was implemented for encryption of data that are stored in the database as the last line of defence such that the information will not be easily accessible or interpreted by an unauthorized user. Consequently, it will take an unauthorized user who gains access to the database server and the database itself a very long time to decode the entire content stored since each of the records were encrypted using a randomly generated key. This approach offers a solution for various weaknesses that must be faced in a security cryptographic system including: Key encryption management, computing time and ensure all the security goals are met. SHA512 hash function was used because it is more secure and the size is usually very large compared to other hash functions. We consider that the computing time is an important aspect which has to be optimized as much as possible by design a new hybrid encryption model that uses Rijndael AES symmetric encryption and RSA features. We chose this technique because, according to NIST, it has better security and efficiency characteristics than DES. Rijndael -AES was used because of the following reasons of its resistance against all known attacks, speed and code compactness on a wide range of platforms and design simplicity.

Conclusion

This paper introduces the concept of a hybrid encryption as a promising approach to enhance data security. Our proposed approach is the combination of RSA and AES encryption models as well as SHA512.The main advantage of this system is that the hybrid encryption algorithm utilized the features of already existing algorithms which are very secure and difficult to break, since it requires two different keys and algorithm. The strength of the security is improved by means of combining symmetric and asymmetric methods of encryption where retrieval of key is very difficult. Using hybrid encryption technology gives full play to the respective advantages of two kinds of encryption algorithm and provides more reliable and efficient security for organization database.

Further Research

For further research, encryption of a network packets that are being transmitted over an insecure channel can also delved into. More so, data that are been transmitted over the web at the client side using the web browser could be area of focus.

REFERENCES

[1] A. Alanazi, O. Hamdan. B.B.Zaidan and A.A.Zaidan, “New Comparative Study between DES, 3DES and AES within Nine Factors”, Journal of Computing. vol. 2, issue 3. pp.152-157, 2010.
[2] C. Charomie, “Implementation of hybrid encryption method using Caesar â€tmcharomie”, 2010
[3] I.A.L.I.Shoukat, A. Al-dhelaan, M. Al-rodhaan, A.B.U.Bakar, and S. Ibrahim, “Practical Evaluation of Hybrid Cryptosystems”, pp.133-141, 2013
[4] N.B.Arshad,S.N. Shah, A.Mohamed and A. Mamat,“The Design and Implementation of Database Encryption”, vol. 1, issue 3, 2007.
[5] M.P. Jhanwar and R.Barua,“A Hybrid Public Key Encryption in Standard Model and A New Intractibility Assumption”, Stat-Math Unit Indian Statistical Institute Kolkata, India, 2009.
[6] C. Wi, “Implementation of hybrid encryption method using Caesar cipher algorithm”, Unpublished master thesis, University Malaysia Pahang (UMP), Pahang, Malaysia, 2010.
[7] P. Kuppuswamy, and C. Chandrasekar, (2011), ‘Enrichment of security through cryptographic public key algorithm based on block cipher’, Indian Journal of Computer Science and Engineering, Vol. 2, No. 3, pp. 347-355.J, 2011.
[8] Thakur and N. Kumar, “DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering, vol. 1, issue 2, 2011.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

[9] R.P.Jignesh,S. Rajesh and K. Vikas, "Hybrid Security Algorithms for Data Transmission using AES-DES", International Journal of Applied Information Systems (IJAIS),vol. 2, no.2, 2012

[10] C.M. Pratap, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" Journal of Global Research in Computer Science, vol. 3, no. 8, 2012

[11] G. Mateescu andM. Vladescu, "A Hybrid Approach of System Security for Small and Medium Enterprises", Proceedings of the 2013 Federated Conference on Computer Science and Information Systems, pp. 656-662

[12] P.Kuppuswamy andS.Q.Y Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm". MIS Review, vol. 19, no. 2, pp.1–13. http://doi.org/10.6131/MISR.2014.1902.01

[13] N. Singh and P.D. Kaur, "A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks". International Journal of Database Theory and Application, vol. 8, no. 3, pp. 145–153, 2015

[14] M.O Onyesolu and N.O.Ogwara, "On Information Security using a Hybrid Cryptographic Model", International Research Journal of Computer Science (IRJCS), ISSN: 2393-9842, Issue 11, Volume 4, November 2016

[15] S. Rani and H. Kaur, "Implementation and Comparison of Hybrid Encryption Model for Secure Network using AES and Elgamal", International Journal of Advanced Research in Computer Science, vol.8, no.3, 2017