Proposed Encryption Technique for Cloud Applications

Nazar Kamal Khorsheed, Omeed Kamal Khorsheed, Majdi Zakaria Rashad,Taher Tawfeek Hamza

Abstract— Recently, the amount of confidential information that stored within the Cloud has been largely increased. Thus, the issue of security became more important than before. The data and services of cloud have been rabidly spread to support the expandable and secure data centers. However, these centers can be easily hacked at any time and from anywhere. With the increase of cloud users, the number of malicious activates on the cloud has been also increased. Thus, the need to ensure the safety of information that being exchanged between the users and the cloud became more significant. Many security and authentication techniques have been proposed to secure the exchanged data. These techniques aim to keep the authentication, privacy and reliability levels of data. In this paper, a simple model for data protection has been proposed. A new algorithm has been proposed to secure the stored data within the cloud. RC5 and AES algorithms have been used within this algorithm to increase the level of security and complexity, thus the attackers cannot reach to the stored data. In addition, this proposed algorithm has been applied on a shopping website that designed within this work. The performance of this algorithm has been measured and compared with the performance of RC5 and AES algorithms. The level of security, the running speed, the level of complexity and the resistance against the known attacks have been used to measure the performance of these three algorithms. The results indicated that the performance of this proposed algorithm was the best among the other algorithms.

Index Terms— cloud computing, encryption, security, confidential information, privacy, authentication, reliability, running speed, aes, rc5..

1 Introduction

Cloud computing technology has been determined by the "National Institute of Standards and Technology (NIST)" as "a model for enabling a compatible and on-demand network access into a shared pool of configurable computing resources". These computing resources may be; multi-networks, storage devices, servers, applications, and other services [1]. In addition, cloud computing has been considered as a new version of computing, where effective and easily virtualized resources are supplied as free tools over the web. Recently, this technology became used in many fields due to its importance. Large number of professional experts expected that the cloud computing will reform the structure of "Information Technology (IT)" approaches and the IT system environment [2].

In general, cloud computing are used for enabling large number of users and subscribers to access into the data and applications that stored on the cloud. Thus, the use of cloud computing should enhance the computing system, IT system and the quality level of the provided services. In addition, the services provided by cloud computing technology should effectively meet the standards and requirements of users [3].

Clouds can be categorized according to the owner into four main types, which are [4];

- **Public Cloud**; which is the most common type of cloud computing, where services are easily available to the general public. Within this type, the clients, individuals or firms can access to these services over the web at any time and from anywhere. This type is implemented by the large firms to store large amount of data. There are many service providers for this type such as; Google, Microsoft and Amazon.
- **Private Cloud**: this type is known as internal cloud, which is implemented within the infrastructure of private business or organization. This private infrastructure is integrated with the cloud set-up structure. In addition, private clouds used in the big companies and government institutions, where they like to store their data in a well-organized environment and in a secured place.
- **Hybrid Cloud**: this type represented by the integration of private and public clouds with each other. This type also allows firms to store the more critical data or the applications within the same firewall structure. Furthermore, hybrid type used to handle the less critical data that stored on the public cloud.
- **Community Cloud**: By this type, the firms with similar goals and vision are allowed to share their underlying framework and thereby increasing their outcomes. In addition, community clouds allowing cost sharing property which can be formed by creating a virtual data center that derived from the virtual machines.

During the recent years, the use of cloud computing has been largely increased, thus the data stored within the cloud should be secured. At the beginning, data were encrypted at the cloud side only, so the users became fear from the loss of data or hackers activates. This reduced the number of users who wanted to store their critical data on the servers of the cloud [5] [6] [7]. To overcome this issue, the data became encrypted at the client side before sending them into the cloud side. This method prevents the exchanged data from loss, damaging and hackers' activities.

In this paper, a new encryption algorithm has been proposed to secure the data stored within the cloud. RC5 and AEs encryption algorithms have been applied within this algorithm. Furthermore, this proposed algorithm has been applied on a shopping website that designed within this work. JAVA and SQL programing languages have been used to write the code of the proposed algorithm. This suggested model aims to protect the users' data from the activities of the attackers.

This paper has been organized as follow; in section II, many related works have been viewed and discussed. Where, the proposed algorithm has been discussed in section III. In section IV, the data flow diagram and the platform of the suggested system have been shown and discussed. After that, the results obtained from the achieved experiments have been viewed and discussed in section V. In section VI, a discussion has been performed to measure and evaluate the performance of the proposed algorithm, where, a summary about the entire work has been provided in section VII.

2. Related Works

The first appear of data encryption concept was in 1972 by IBM. Then, this concept had been adopted by the government of U.S. as a standard encryption technique. The author in [8] proposed a symmetric encryption algorithm of key-block cipher. This algorithm was based on the heterogeneous structure. The length of key that utilized within this algorithm was 56-bit, while the length of text block was 64-bit. In addition, data can be encrypted by this algorithm through performing 16 iterations for processing.

Going to the year of 1987, Rivest designed 'Cipher4', which is a stream cipher from RSA Data Security. This designed method was the most common and fast symmetric key algorithm in that period. The length of keys within this method was extended between 1to 256 bits [9] [10]. Also, in 1991, Xuejia Lai and James Massey designed the "International Data Encryption Algorithm (IDEA)", which can be considered as an enhancement for the proposed standard encryption. This symmetric algorithm was based on the substitution-permutation structure. In addition, the length of key within this algorithm was 128-bit, while the length of text block was 64-bits. The number of iterations that can be performed within this algorithm was 8.5 iterations [11].

Furthermore, the Blowfish algorithm has been proposed by Bruce Schneier in 1993. This algorithm had simple and fast block encryption, which made it a suitable to be used within the "Secure Socket Layer (SSL)" protocol and other similar protocols. This algorithm had the heterogeneous structure, where the length of key was extended between 32 to 488 bits [12]. The authors in [13] presented 'Cipher5' algorithm, which is a symmetric block-cipher algorithm that designed by Rivest in 1994. This algorithm had been planned to be suitable for both hardware and software. The length of key within this algorithm extended between 0 and 2048 bits, while the number of iterations extended between 1- 255.

Carlisle Adams and Stafford Tavares designed 'CAST-128' in 1996, which is a block cipher algorithm that used in many applications. The utilized structure within this algorithm was heterogeneous structure, where the number of iterations that performed by this algorithm was extended between 12 and 16. In addition, 'CAST-128' algorithm utilized 64-bit block and length of key extended between 40-bit and 128-bit [14]. On the other hand, '3DES' algorithm had been suggested and designed in 1998. This algorithm utilized three different keys for encryption process. The total size of these keys was 168 bits, where all these three keys were symmetrical. The high security provided by this algorithm attracted the government of U. S. to use it [15].

In 1998, Ron Rivest created 'Cipher6' algorithm, which had been derived from its predecessor 'Cipher5'. The structure of this algorithm was the heterogeneous structure. In addition, four registers were used within this algorithm, thus it became able to perform many operations at the same time. The size of block that used within this algorithm was 128-bits; while the length of key may be 128-bit, 192-bit or 256-bit. The number of iterations that should be performed for data encryption was 20 rounds [16] [17].

The authors in [18] presented the block cipher 'MARS', which was designed by IBM in 1998. The heterogeneous structure had been used to design this block cipher. A key with length that extended between 128 and 256 bits had been used within this block cipher. However, the size of this block was128 bit. At the same year, Vincent Rijmen and Daemen designed "Advanced Encryption Standard (AES)" encryption algorithm. The heterogeneous structure had been used to design this algorithm, where the number of iterations that should be performed to encrypt the data was 10, 12 or 14 rounds. Also, this algorithm utilized keys with length extended between 128 and 256 bit, while the size of block in this algorithm was 128 bit [8].

3. THE PROPOSED ALGORITHM

- **RC5 Encryption Algorithm**

Cryptography is dividing into two main encryption techniques, which are; asymmetric key encryption technique and

symmetric key encryption technique. Within these techniques, the secret keys are used to perform encryption and decryption processes. On the other hand, there are many symmetric key algorithms that used to secure the data like; RC6, RC5, RC4 and RC2 [19]. In this paper, RC5 algorithm has been used to perform the encryption process. RC5 is a fast block cipher, which is designed to be suitable for both software and hardware implementation. Also, it is a parameterized algorithm, where the block size, length of secret key and number of rounds are variable. This makes the level of security and the characteristics of performance more flexible. The figure below illustrates the classification of cryptography

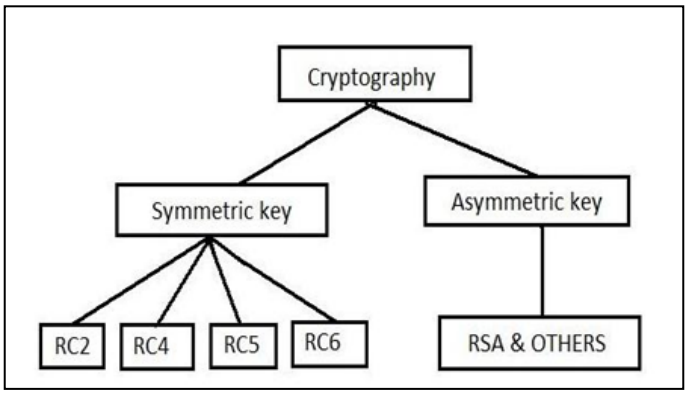

Figure 1: categorization of cryptography, [19].

- **AES Encryption Algorithm**

AES is the official encryption method adopted by "National Center for Standards and Technology (NIST)". This algorithm has been largely used around the world, where it is considered as a safe method for the encryption. The appropriate length of key that used within this algorithm is the reason for its stability. Furthermore, AES is a symmetric block cipher, thus the same key is used for both encryption and decryption. The size of block that accepted by this algorithm is 128 bits, where three keys with 128, 192 and 256 bit length are used within this algorithm. The standard name for this algorithm is modified into AES-128, AES-192 or AES- 256 based on the length of key. At present, the most common key size likely to be used is the 128 bit key. On the other hand, the number of AES parameters depends on the length of key, where the number of rounds can be also determined based on this length [20].

- **Combination between CR5 and AES**

The proposed method in this paper presents a symmetric combination between two symmetric encryption algorithms; RC5 and AES algorithms. This method has been proposed to save the data stored on the cloud by providing the privacy and integrity to the users' identities. AES has been combined with RC5 to eliminate the restrictions in encryption process. RC5 with 128-bit block has been used in this method [5]. This proposed algorithm consists of three main stages which are;

- Key expansion stage
- Data Encryption stage
- Data Decryption stage

All these stages have been discussed in the following subsections. The figure below illustrates the block diagram of the entire suggested algorithm

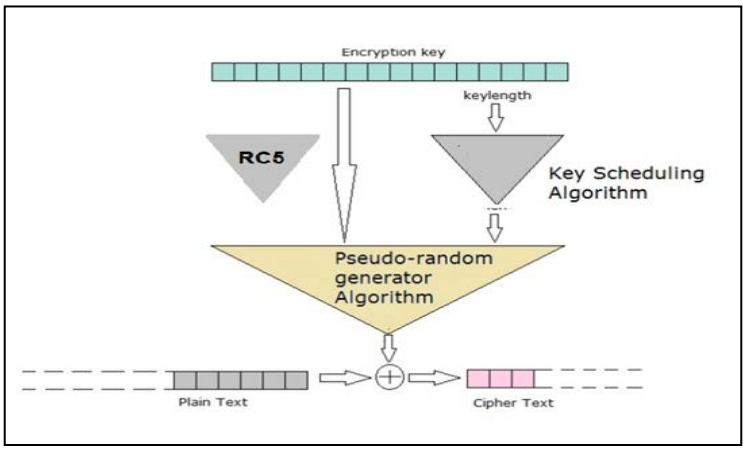

Figure 2: block diagram of the proposed algorithm.

3.1 Key Expansion Stage

Within this stage, the plaintext and user key are used to determine the parameters of key expansion. Furthermore, the expanded key table array (S), which contains the random binary words are generated within this step. The binary words within this table are then used within the encryption and decryption stages. The following parameters of RC5 and AES algorithms will be determined in this stage;

- Number of words in key
- Number of bytes in word
- Number of registers
- Number of rounds
- Length of round key array
- Bit shift value

For this proposed algorithm, the values of RC5 coefficients have been determined as below; w = 32, r = 20 and b = (16, 24, and 32). Four 32-bit registers have been used within the implementation, where a block with size 128-bit has been used. In addition, the number of iteration has been assigned to 20 rounds. On the other hand, the value of bit shift for AES has been assigned to 5 bits, where the length of round key array has been set to 44 keys [21] [22].

3.2 Encryption Phase

Within this step, keys are generated from the information of user, where RC5 and AES algorithms have been applied to encrypt these generated keys. A key with b-bytes length is provided by the user; where additional zero bytes may be appended to this key. Then, the obtained plaintext will be stored as a series of c words with w-bit length. The lower order byte is stored as L[0], while the higher order byte is stored as L[c-1]. After that, the round key array will be constructed in this form

S [0 ….. 2r + 3], where r represents the number of rounds. Finally, the stored key array will be encrypted by RC5 and AES algorithms to generate the encrypted keys [22] [23]. The figure below illustrates the block diagram of key generation process using RC5 and AES algorithms

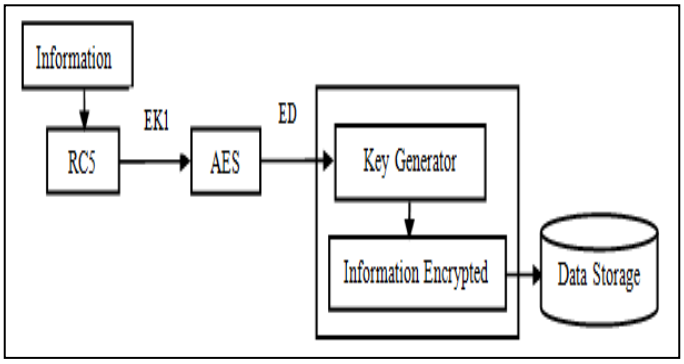

Figure 3: block diagram of key generation process using RC5 and AES

Furthermore, the code of key generation process is shown below, where both RC5 and AES are applied. In this method, c has been set to 4, which represents the number of registers. These registers have been represented by A, B, C and D symbols. The first byte of plaintext has been placed in the least significant byte of register A, while the last byte of plain text has been placed in the most significant byte of register D. Thus, the arrangement of registers became as this; (A, B, C, D) = (B, C, D, A)

Plaintext stored in four w-bit input registers
A, B, C, D
20 rounds
32-bit round keys $S[0, \dots, 43]$;
Output:
Ciphertext stored in A, B, C, D;
Procedure:
$B = B + S[0]$ // Pre-whitening
$D = D + S[1]$
for $i = 1$ ***to*** 20 ***do***
{
$t = (B \times (2B + 1)) < 5;$
$u = (D \times (2D + 1)) < 5;$
$A = ((A \oplus t) < u) + S[2i];$
$C = ((C \oplus u) < t) + S[2i + 1];$
$(A, B, C, D) = (B, C, D, A);$
}
$A = A + S[42]$ // Post-whitening
$C = C + S[43];$
End sub

Figure 4: the code of encryption phase using CR5 and AES.

3.3 Decryption Phase

Within this phase, the original information can be retrieved from the encrypted data. This process involved the same steps that in encryption process but in the backward. The figure below illustrates the block diagram of the decryption process.

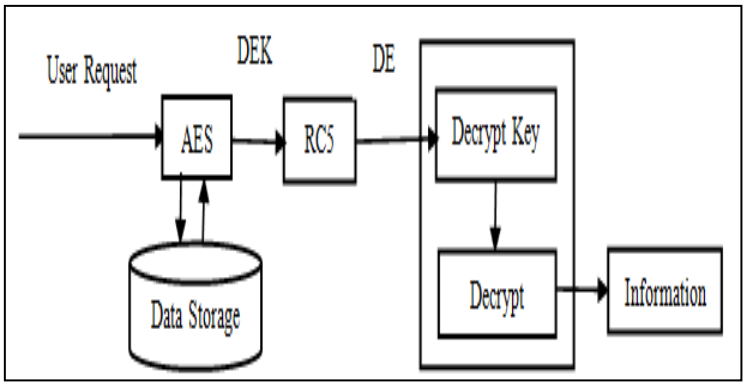

Figure 5: block diagram of decryption process.

Furthermore, the code of decryption process is shown in the figure below, where both RC5 and AES have been applied. In decryption process, the input of decryption algorithm is represented by the initial output of the encryption process, where this output is stored in the four registers as a ciphertext. Also, the first byte of ciphertext has placed in the least significant byte of register A, while the last byte of ciphertext has been placed in the most significant byte of register D.

Input:
Ciphertext stored in four w-bit input registers A, B,C,D;
Number r of rounds
w-bit round keys S[0,…,2r + 3];
Output:
Plaintext stored in A,B,C,D;
Procedure:
C = C - S[2r + 3];
A = A - S[2r + 2];
for i = r **down to** 1 **do**
{
(A,B,C,D) = (D,A,B,C);
u = (D x (2D + 1)) < $\log_2$ w;
t = (B x (2B + 1)) < $\log_2$ w;
C = ((C - S[2i + 1])> t) $\oplus$ u;
A = ((A - S[2i]) > u) $\oplus$ t;
}
D = D - S[1];
B = B - S[0];
End Sub.

Figure 6: decryption algorithm code.

4. THE PROPOSED SYSTEM

An online shopping website has been designed to allow the users from doing their shopping online. The RC5 and AES algorithms have been used to secure the data of the users. Thus, the password of any user will be encrypted by these algorithms and this will secure the data stored within the cloud from the attacker activities. The algorithm of this system has been written by Java and ASP programming languages, where this algorithm represents the encryption and decryption processes. The entire algorithm has been shown in Appendix A.

4.1 Data Flow Diagram of the proposed System

Data flow diagrams are one of the three essential perspectives of "Structured Systems Analysis and Design Method (SSADM)". The sponsor of a project and the end users will need to be briefed and consulted throughout all stages of a system's evolution. With a data flow diagram, users are able to visualize how the system will operate, what the system will accomplish, and how the system will be implemented. For this system, the diagram of data flow is shown in the figure below.

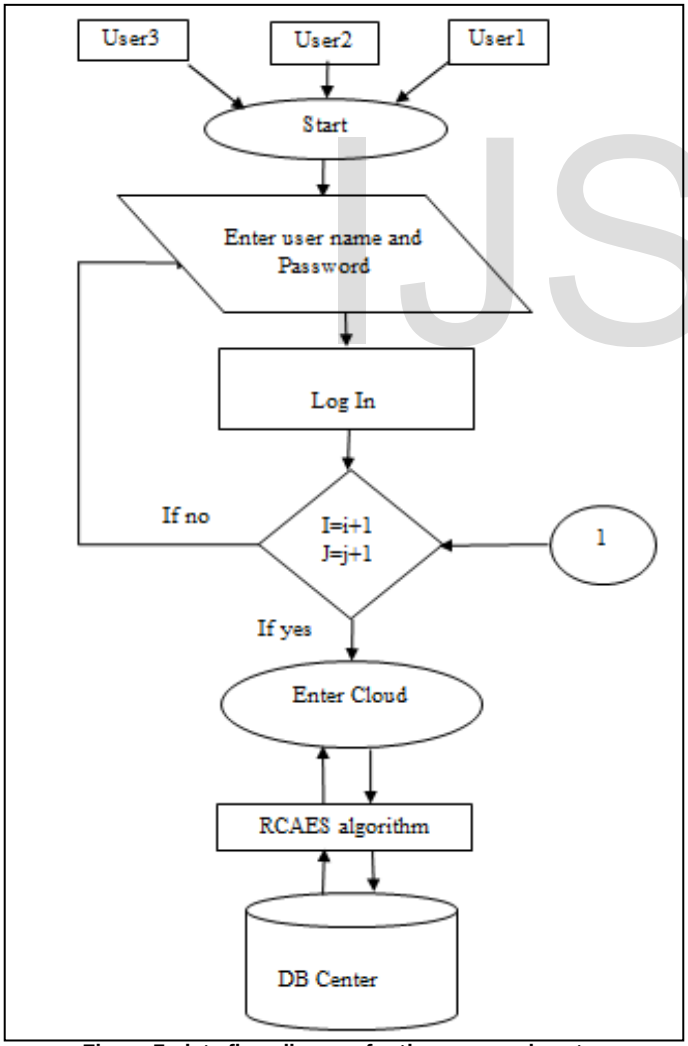

Figure 7: data flow diagram for the proposed system.

4.2 System Platform

The bitnami "Xampp Control Panel as a Platform (XAMPP)" has been used within this system. This platform provides the users with the latest versions of their favorite applications and development stacks. Also, XAMPP supports Windows, Mac OS X, Linux, VMware and VirtualBox. Furthermore, it supports many popular cloud platforms such as; "Amazon Web Services (AWS)", Microsoft Azure and Google Cloud Platform. This platform has been used within this system to create the shopping database. The database of shopping has been saved in XAMPP folder.

After creating the XAMPP folder, the website has been run by choosing the internet explorer browser and writing in the search panel "Localhost/xampp/shopping". The interface of the designed website has been appeared as below;

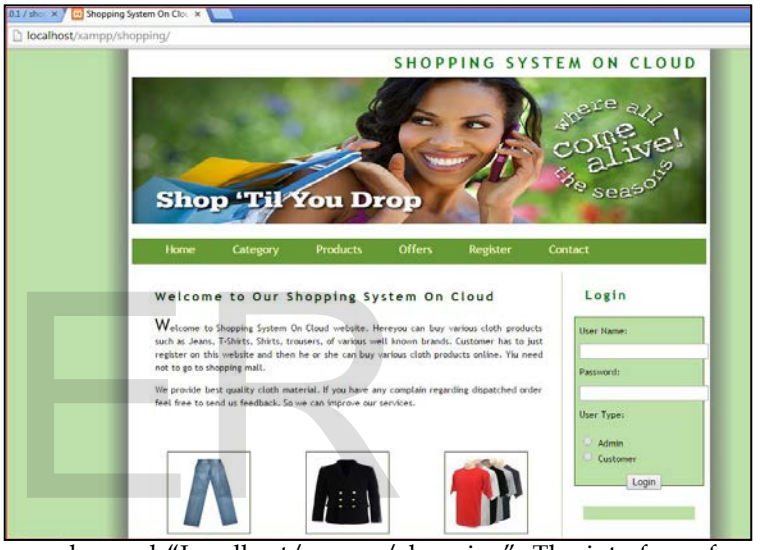

Figure 8: the interface of the designed website.

5 THE OBTAINED RESULTS

In this section, the performance of the proposed algorithm has been measured and compared with the performance of RC5 and AES algorithms. The time that required for encrypting and decrypting the password has been measured with respect to the size of this password. The number of bits within the passwords has been increased to measure the relationship between the size of the password and the time required for encryption and decryption. The performance of RC5, AES and the proposed algorithm is shown in the figure below;

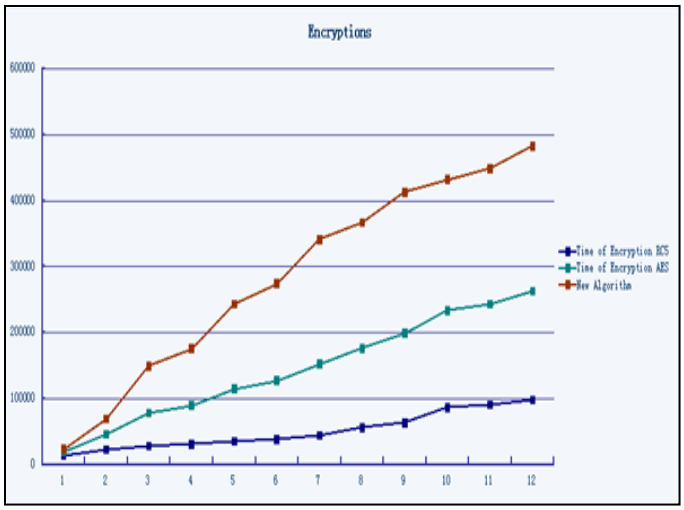

Figure 9 : time required to encrypt data in RC5, AES and the proposed algorithm

As shown from the figure above, the new proposed block cipher algorithm spends few seconds more than the other algorithms; this means that it does not take long time. Thus, the new proposed algorithm is very robust and located within the acceptance range.

Furthermore, the time required to decrypt different passwords with different sizes is shown in the figure below, where this time has been measured for RC5, AES and the new proposed algorithm.

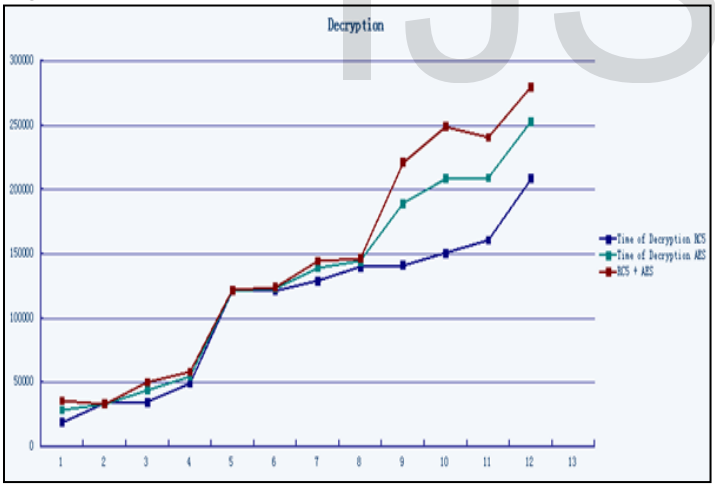

Figure 10: time required to decrypt data in RC5, AES and the proposed algorithm.

As shown form the figure above, the proposed algorithm has behavior is likely to the other two algorithms. In addition, the time required for decryption in this algorithm is approximately equal to that required by RC5 and AES algorithms. This means that this new algorithm located within the acceptance range among many algorithms.

Furthermore, the time required to perform the encryption and decryption processes has been measured for passwords with 8, 15 and 19 bit size. This time has been measured for RC5, AES and the proposed algorithm. The results of these measurements are shown in the table below.

Table 1: time required for encryption and decryption in RC5, AES and the proposed algorithm.

Password Size	Operation	Running time in AES (sec.)	Running time in RC5 (sec.)	Running time in the Proposal Algorithm (sec.)
8 char	Encryption	3	5	4
	Decryption	4	5	4
15 char	Encryption	6	7	5
	Decryption	7	6	5
19 char	Encryption	10	15	9
	Decryption	11	15	9

6 DISCUSSION

This system has been proposed to increase the security level for the data stored in the cloud. Thus, the RC5 and AES algorithms have been applied within this system for this purpose. The performance of this proposed system has been compared with the performance of RC5 and AES algorithms. Based on the obtained results, the performance of the new algorithm overcomes the performance of the other two algorithms. This can be confirmed through the speed of this algorithm, the resistance against the known attacks, the level of security and the complexity level. The results indicated that the complexity of encryption or decryption operations depends on the length of key or the block size. Furthermore, the results proved that the proposed algorithm achieved suitable speed, high security level and high resistance against the known attacks as compared with the other two algorithms.

7 CONCLUSION AND FUTURE WORKS

A new algorithm has been proposed to enhance the level of security for the data stored within the cloud. This algorithm has been applied on a shopping website, which has been designed within this work. RC5 and AES algorithms have been integrated and used within this algorithm to encrypt and decrypt the data of users. The suggested algorithm and the proposed system have been explained and discussed within this

paper. The performance of this new algorithm has been measured and compared with the performance of RC5 and AES algorithms. The level of security, the speed of running algorithm, the complexity and the resistance against the known attacks have been used to measure the performance of these three algorithms. The results indicated that the performance of this proposed algorithm was the best among the other algorithms. Furthermore, this algorithm provides the following features;

- The proposed algorithm enhances the confusion and diffusion criteria that face the stases the complexity degree against the attacker task by consuming more time to achieve the analytical process.
- The proposed algorithm is different from the other algorithms by using different; initial permutation, final permutations, round permutations and round content.
- The proposed algorithm increases the randomness of the used secret key by expanding the original key through the stream generator. This provides higher randomness as a new long secret key with higher randomness property.

Finally, this algorithm can be enhanced by adding another encryption technique to increase the security level and to prevent the hacker's activities. Also, other features can be added to the proposed algorithm to protect the entries between cloud, consumer and cloud provider.

REFERENCES

[1] R. L. Krutz and R. D. Vines, "Cloud Security, A Comprehensive Guide to Secure Cloud Computing, *Wiley Publishing, Inc*., 2010.

[2] B. Furht, "Hand book of Cloud Computing, Cloud Computing Fundamentals", *Department of Computer & Electrical Engineering and Computer Science, Florida Atlantic University, Boca Raton, FL, USA*, 2010.

[3] F. Gens, "New IDC IT Cloud Services Survey: Top Benefits and Challenges", *IDC eXchange*, Available at: http://blogs.idc.com / ie/ p = 730, February, 2010.

[4] L. Delaney, "A Global Trade Source", *Ltd. Company*, ldelaney@globetrade.com , 2010.

[5] J. S. Ward and A. Barker, "Observing the clouds: a survey and taxonomy of cloud monitoring", *Journal of Cloud Computing: Advances, Systems and Applications*, pp. 1-30, 2014.

[6] Sh. S. Khan and R. R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", *International Journal of Innovative Research in Computer and Communication Engineering*, pp. 148-154, vol. 3, no, 1, 2015.

[7] M. S. Bajwa and Himani, "A Concern towards Data Security in Cloud Computing", *International Journal of Computer Applications*, vol. 114, no. 11, pp. 17-19, March, 2015.

[8] A. K. Mandal, C. Parakash and M. A. Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on*, pp. 1-5, March, 2012.

[9] E. Dawson, H. Gustafson, M. Henricksen and B. Millan, "Evaluation of RC4 Stream Cipher", Information Security Research Centre Queensland University of Technology, July, 2002.

[10] N. Singhal and J. P. S Rania, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, pp. 177-181, August, 2011.

[11] M. I. Alam and M. R. Khan, "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 10, pp. 713-720, 2013.

[12] M. A. Mushtaque, H. Dhiman, Sh. Hussain and Sh. Maheshwari, "Evaluation of DES, TDES, AES, Blowfish and Twofish Encryption Algorithm Based on Space Complexity", International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 4, April, 2014.

[13] Z. Zhao and S. Shiliang, "Image Encryption Algorithm Based on Logistic Chaotic System and S Boxes Scrambling", *Image and Signal Processing (CISP), 2011 4th International Congress on* , vol. 1, pp. 177-181, October, 2011.

[14] T. Nie, Y. Li and Ch. Song, "Performance Evaluation for CAST and RC5 Encryption Algorithms", *Computing, Control and Industrial Engineering (CCIE), 2010 International Conference on*, vol. 1, pp. 106-109, June, 2010.

[15] M. Halas, I. Bestak, M. Orgon and A. Kovac, "Performance Measurement of Encryption Algorithms and Their Effect on Real Running in PLC Networks", *Telecommunications and Signal Processing (TSP), 2012 35th International Conference on*, pp. 161-164, July, 2012.

[16] K. Aggarwal, J. K. Saini and H. K. Verma, "Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers", *International Journal of Computer Applications*, vol. 68, no. 25, pp. 10-16, April, 2013.

[17] A. T. Hashim, J. A. Mahdi and S. H. Abdullah, "A Proposed 512 bits RC6 Encryption Algorithm", vol. 10, no. 1, pp. 11-25, 2010.

[18] H. Singh, A. S. Danewalia, D. Chopra and N. Kumar, "Randomly Generated Algorithms and Dynamic Connec tions", *International Journal of Scientific Research in Network Security & Communication*, vol. 2, no. 1, pp. 1-4, 2014.

[19] A. Menezes, P. V. Orschot, and S. Vanstone, "Public-Key

Encryption",1996.

[20] H. Nover, "Algebraic cryptanalysis of AES ,An Overview", *International Journal of Engineering and Technology (IJET)* , 2013.

[21] P. Pandey, P. Dhasal and R. Pandit, "Implementation of RSA RC5 Algorithm in Cloud", *(IJCSIT) International Journal of Computer Science and Information Technologies*, vol. 6, no. 1, pp. 224-227, 2015.

[22] M. U. Shnkarwar and A. V. Pawar, "Security and Privacy in Cloud Computing:A survey", *Springer International Publishing Switzerland 2015*, pp. 1-11, 2015.

[23] N. K. Sowmya, H. B. Bhuvaneswari and A. C. Nuthan, "Implementation of advanced encryption Standard-192 bit using multiple keys", *IEEE Transaction*, vol. 5, pp-34-39, 2012.