QALAAI ZANIST SCIENTIFIC JOURNAL
*A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil, Kurdistan, Iraq*
Vol. ( 3 ), Issue ( 1 ) Winter 2018
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

# ENHANCING THE DATA SECURITY IN CLOUD COMPUTING BY USING NEW ENCRYPTION METHOD

**Farah Qasim Ahmed**
Information Technology, Lebanese French University, KRG – Iraq frhalyousuf@lfu.edu.krd

**Amin Salih Mohammed**
Information Technology, Lebanese French University, KRG – Iraq
kakshar@gmail.com
College of Engineering, Software Department, Salahddin University-Erbil
amin.mohammed@su.edu.krd

**ARTICLE INFO**

***Article History:***
Received: 11/1/2018
Accepted: 7/2/2018
Published: Winter 2018

**Doi:**
**10.25212/lfu.qzj.3.1.40**

***Keywords:***

*Cloud computing, encryption algorithm, AES, 3×AES, DES, T-DES*

## ABSTRACT

With the huge growth of the critical data that saved in the cloud, the security of the cloud should be safer. The growing of the cloud users attended with the rising of the harmful attacks and natural processes. Many weaknesses and security advisories are discovered. The idea of using the cloud is not considered as a new term but was traded widely these days with the improvement of business and general investments, which completely depends on internet services in executing the work with accuracy and professionally. This paper proposed a new encryption technique that protects the data before it is saved to cloud services and retrieved, hence the confidentiality of the data can be secured. Also, this paper compares proposed method (3xAES) with AES and T-DES algorithms by calculating the key generation, encryption and decryption time for each algorithm. 3×AES technique is more efficient and secured, more than AES because it encrypts the text 3 times and each time it needs a different key for encrypt and decrypt. Comparing between 3×AES with AES and T-DES and the result was that 3×AES has a higher security than AES and 3DES, due to the triple encryption for the 3×AES algorithm. By increasing the key length, the higher security will occur, so the algorithm 3×AES with the key length 256, will put in advance over AES and 3-DES for securing the data that save on the cloud computing.

## I. INTRODUCTION

The The term of cloud computing indicates to the resources that are available upon requested through the network. It is can be defined as a number of services that provided to the client, these services used to save the data through the network. The client can access these data anytime and anywhere he wants by using internet and one of the services that provided by CSPs (Cloud Service Providers). Cloud computing basically consists of applications running distantly which is accessible to all its clients. This technology proposes access to a huge amount of advanced supercomputers and their resultant processing power, connected at many locations around the world, therefore offering speed in the tens of millions of calculations per second. Cloud offers sensible cost savings and speed to customers. (Zhou, 2013). The purpose of using encryption is to make sure that no one can access the data (it can be a text, file, application, or so on) or view them except the person who has the decryption key that can decrypt these data. So, the person who doesn’t have the decryption key, will not be able to read these encrypted data (Sahai & Waters, 2005, pp. 457-473).

With encryption, the information that is spared in the cloud will be more secured. In the event that every one of the suppliers use encryption, they ought to know what sorts of encryption they need to utilize. The key length ought to be figured and measured likewise. The encryption algorithms are not equivalent. There is a great deal of encryption calculations that have issues of spillage security.

The main objectives of this paper are remote data confidentiality protection and secure the data in transmission.

## II. Analysis of Literature

Cloud computing is used vastly by many users for their own aim (as a private cloud), or small enterprises to run their data (as a private or a public cloud) and so on. Because the users of the cloud will be able to transfer the data to the cloud, as shown in Figure1, a hacker who has access to the internet can hijack or/and modify the user's data. So, we need to ensure that the data confidentiality will be secured (Pearson, 2009).

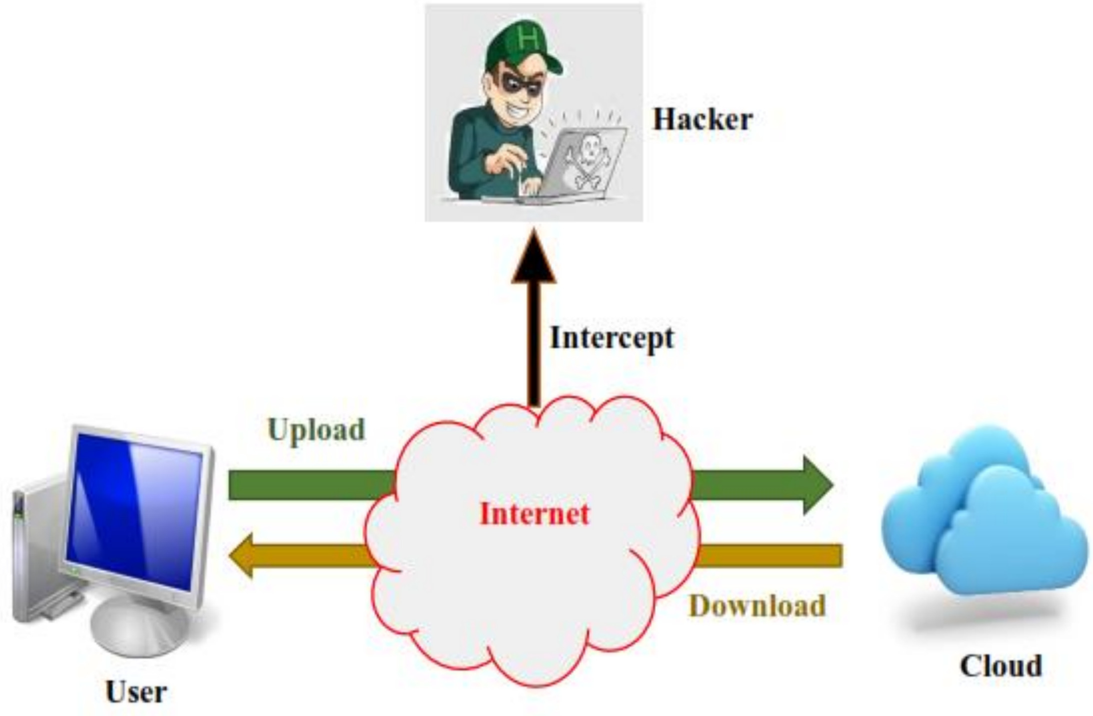

Figure 1: interception of data between the user and cloud

Jin Li, et al, in 2014 said that more often than not basic information must be scrambled due to the security of the information, which makes dynamic database utilize an extremely resisting work. The creator proposed (L-EncDB) for tending to these difficulties, another light system for encryption of the database, which spares the structure of the database. They fabricated another FPE framework, which can be utilized to make the encoding of all information that has of character strings put away in the database (Li, et al, 2014). Also, Qin-long H., et al, 2013, proposed a protection and secure DRM framework utilizing a structure as a part of encryption in cloud computing called homomorphic encryption. They offered an effective DRM structure in cloud computing, which permits suppliers to get assistance from outer sources scrambled substance to bring together substance server and permits the client to bring substance with the permit issued by permit server. The outcomes of their study demonstrate that the exhibited framework has a lower computational confusion and has abnormal state effectiveness and protection (Huang et al, 2013).

There are lot of companies or organizations who don’t trust the way that they store their critical data and applications on the systems that they don’t control, so in this paper we proposed an algorithm that evaluate the performance of the encryption techniques that protect the data confidentiality on cloud computing environment. So, the popular AES and T-DES encryption algorithms are used in this thesis to encrypt the text that uploaded to the cloud, also 3×AES will be used to compare the encrypted text and duration time that each algorithm will take while doing the encryption and decryption processes.

## III. Encryption and its characteristics:

Encryption is an encoding process for the data or the message that can be written by the person who has a secret key and access for encryption and cannot be understood unless it decrypted with the secret key in place. The encryption structure is called the core data or the message as a plaintext, then it will be encrypted with one of the algorithms that called (encryption algorithm) creating a text called (ciphertext), this ciphertext will not have the same meaning with the plaintext except when decrypted (Bhanot & Hans, 2015).

There are two main techniques for encryption, these are public (asymmetric) encryption, private (symmetric) encryption (Elminaam et al, 2008). This paper will use Symmetric (private) encryption technique.

There are many issues and threats in cloud computing which consist of privacy, segregation, storage, reliability, data security, capacity and more. But the most important of these issues is security. Generally, there are many users or clients that used a cloud computing like regular users, academia, and large companies. Each one of these clients has different purposes for using cloud computing. One of the security methods that used in cloud computing is encryption. The process for encryption in cloud computing is that the uploaded data will be encrypted before it is saved in cloud computing. Using AES algorithm in cloud computing is more efficient, it is used in most of the applications and approved from many application providers who need to secure their data and it is replacing the DES as approved standard in most used application because of its simple designing, low cost in memory, and it's a high speed. There are some disadvantages in AES, the structure of algebraic is too simple, and the methods that encrypt each block are the same.

## IV. The Implemented Solution:

With encryption, the information that is spared in the cloud will be more secured. Symmetric Encryption system has been implemented. This implemented arrangement found the computational efficiency of this sort of encryption which can deal with the encryption for the huge size of information, likewise the more extended key length, the more encryption calculation will be. Likewise, the long length will give an assurance more than other key lengths in light of the fact that these long keys are all the more computationally compelling. This theory is utilizing this sort of encryption since sharing the key sick not happen (Waqar et al, 2011). 3×AES algorithm was proposed to encrypt the uploaded data to the cloud computing, it has the same structure and implementations for AES but it with triple encryption to secure the data that save in cloud computing. This algorithm uses the key three times, it encrypts with the secret key and the same key will be used for the second encryption and will be used third time with third encryption. This process will expand the encrypted text (ciphertext) and makes it more secured.

## V. Performance Measurement:

In this paper, seven (7) algorithms have been used. For an AES algorithm using the key sizes are (AES-125, AES-192, and AES-256). For 3×AES used key sizes are 3×AES -128, 3×AES -192 and 3×AES -256). For T-DES, the key size T-DES-168 is used. SQLite with a version 0.8.3.1 and Eclipse Java EE IDE for Web Developers, Version: Mars.2 Release (4.5.2) are used for building this model, and tested on Intel(R) Core(TM) i3-2348M CPU with 4.00 GB RAM. This model is built to encrypt a text and upload it to the cloud, (cloud that used here is OneDrive), and decrypt this text when retrieve. First of all, the security key will be generated, and then a text file is created in OneDrive before uploading the text, after that the encrypted text will be uploaded to this text file that has been created in OneDrive. When the file is retrieved, the model will decrypt the text that is saved in this text file with the same security key that is used in the encryption process, and then retrieved.

## VI. Key Generation Time

The key generation time for each algorithm will be calculated in this model. Table 1 below shows the key-generation time for each used algorithm, (calculated time for each table is measured by millisecond, and text size is measured by byte).

Table 1: Encryption time for each algorithm

| | AES-128 | AES-192 | AES-256 | 3×AES-128 | 3×AES-192 | 3×AES-256 | T-DES-168 |
|---|---|---|---|---|---|---|---|
| **50** | 0.553765 | 0.426592 | 0.422576 | 0.617761 | 0.493527 | 0.483262 | 2.957005 |
| **150** | 0.411528 | 0.416774 | 0.415882 | 0.665769 | 0.511136 | 0.491414 | 2.840268 |
| **250** | 0.647473 | 0.425253 | 0.417221 | 0.523424 | 0.491741 | 0.495758 | 3.0093902 |
| **350** | 0.614636 | 0.451581 | 0.583218 | 0.484611 | 0.471661 | 0.513791 | 3.005157 |
| **450** | 0.426592 | 0.422575 | 0.433731 | 0.657291 | 0.477461 | 0.463181 | 2.766457 |
| **550** | 0.451241 | 0.624716 | 0.489956 | 0.489164 | 0.481477 | 0.513791 | 2.873561 |
| **650** | 0.431618 | 0.615183 | 0.418561 | 0.487725 | 0.487725 | 0.483263 | 2.880646 |
| **750** | 0.418561 | 0.613744 | 0.416775 | 0.493526 | 0.745643 | 0.511483 | 3.004929 |
| **850** | 0.471661 | 0.434177 | 0.417667 | 0.513615 | 0.713515 | 0.514499 | 2.901057 |
| **950** | 0.432392 | 0.439532 | 0.445779 | 0.847383 | 0.547519 | 0.497197 | 2.940249 |
| **Key Gen. Avg.** | **0.4846456** | **0.4850026** | **0.4461365** | **0.5770147** | **0.5420305** | **0.4945527** | **2.917872** |

The Figure 1 below shows the relationship for the key generation time for each algorithm.

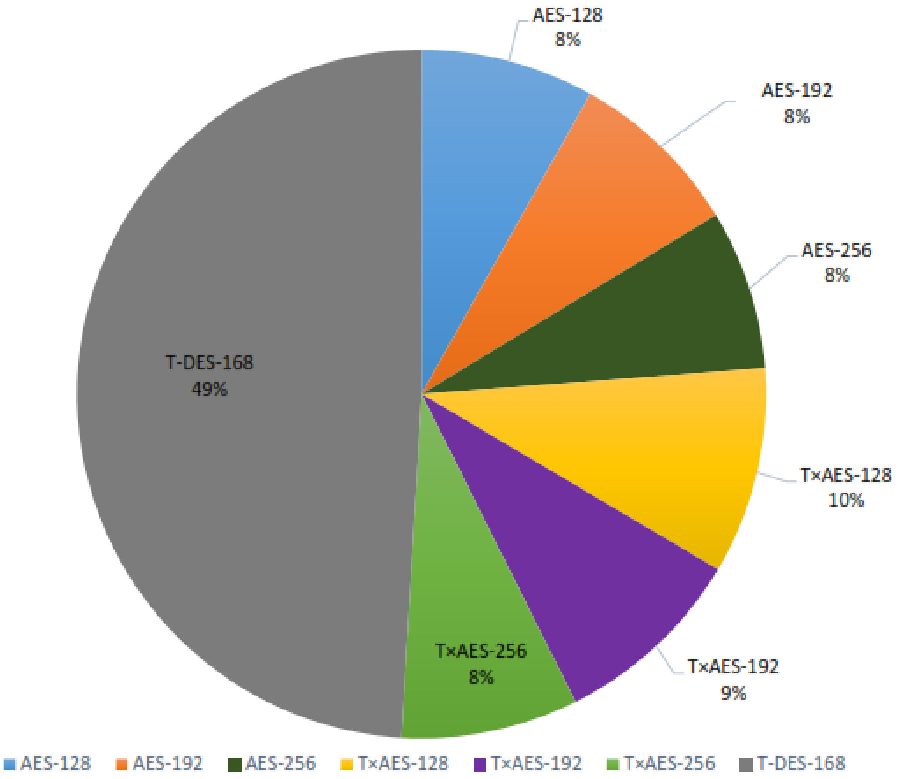

Figure 1: Key Generation Time

Table 2 and the chart graph above show that the time is different among the algorithms. The key generation time for T-DES with the key size (168-bits) has a higher time compared to 3×AES and AES with all key sizes. By comparing the average time for AES and 3×AES, we find that 3×AES has a higher key generation time with each corresponding key size for both algorithms.

## I. Encryption Time:

Table 2: Encryption time for each algorithm

| | AES-128 | AES-192 | AES-256 | 3×AES-128 | 3×AES-192 | 3×AES-256 | T-DES-168 |
|---|---|---|---|---|---|---|---|
| **50** | 29.697337 | 32.418433 | 30.182386 | 25.124397 | 26.846835 | 30.032008 | 20.617481 |
| **150** | 26.359555 | 24.150729 | 29.558114 | 27.050315 | 26.683962 | 30.446553 | 14.873644 |
| **250** | 22.98072 | 24.452824 | 26.095834 | 26.531798 | 33.703569 | 31.370691 | 16.495234 |
| **350** | 23.044976 | 25.530464 | 24.098074 | 33.897231 | 27.905733 | 30.547401 | 16.208309 |
| **450** | 25.85264 | 28.953476 | 26.656742 | 37.978428 | 30.536692 | 28.471550 | 13.799129 |
| **550** | 24.544748 | 24.978481 | 27.212742 | 25.739745 | 35.591557 | 26.345276 | 16.880774 |
| **650** | 25.509045 | 24.913778 | 26.607211 | 25.163666 | 25.107887 | 28.372041 | 18.337259 |
| **750** | 35.617439 | 27.677711 | 28.610773 | 35.687497 | 24.832118 | 30.170339 | 15.189127 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **850** | 24.546532 | 26.071292 | 27.467092 | 29.646914 | 30.535353 | 28.813806 | 17.179300 |
| **950** | 22.870948 | 24.801774 | 26.804444 | 27.998102 | 30.242627 | 28.550532 | 17.818743 |
| **Average time** | **22.41416** | **26.39489** | **27.32934** | **29.48181** | **29.19863** | **29.31202** | **16.7399** |

Figure 2 below represents the relationship between the encryption times for all used algorithms.

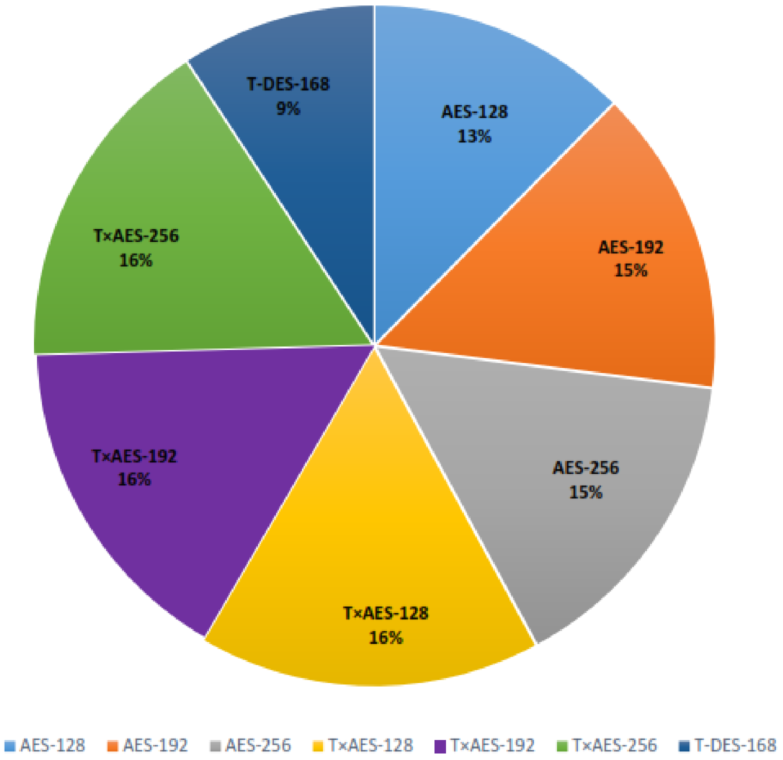

Figure 2: Encryption Time

As shown in Table 2 and the chart graph above, the encryption time for each algorithm is calculated to know the duration each algorithm takes to encrypt a text. The encryption time for 3×AES is higher than AES and T-DES, also comparing the average between AES and 3×AES, we find that AES will take less encryption time.

## II. Decryption Time:

Table 3: Decryption time for each algorithm

| | AES-128 | AES-192 | AES-256 | 3×AES-128 | 3×AES-192 | 3×AES-256 | T-DES-168 |
|---|---|---|---|---|---|---|---|
| **50** | 1.199014 | 1.141004 | 1.131186 | 1.932165 | 1.780894 | 1.836227 | 1.426588 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **150** | 1.248545 | 1.283351 | 1.376165 | 2.405613 | 2.329754 | 2.919221 | 1.907621 |
| **250** | 1.477460 | 1.490400 | 1.438190 | 2.963843 | 4.263258 | 2.963398 | 2.881735 |
| **350** | 1.464519 | 1.481029 | 1.824177 | 3.378389 | 3.369465 | 3.388206 | 1.730023 |
| **450** | 1.589909 | 1.626500 | 1.682276 | 4.519839 | 3.733586 | 4.033005 | 1.954029 |
| **550** | 1.676923 | 1.800528 | 1.788032 | 4.514485 | 4.802301 | 4.903149 | 2.196776 |
| **650** | 1.973664 | 1.819270 | 2.262818 | 5.442191 | 5.451116 | 5.026754 | 2.319935 |
| **750** | 1.902715 | 1.897805 | 2.680933 | 5.955354 | 5.427913 | 6.551959 | 1.963846 |
| **850** | 2.036137 | 2.054432 | 2.816586 | 5.169993 | 5.244959 | 5.236927 | 1.884864 |
| **950** | 2.062910 | 2.202579 | 2.200793 | 5.978111 | 5.767938 | 5.588108 | 2.358311 |
| **Average time** | **1.66318** | **1.75617** | **1.92012** | **4.22599** | **4.21712** | **4.24469** | **2.06237** |

Figure 3 below represents the relationship between the decryption times for all used algorithms.

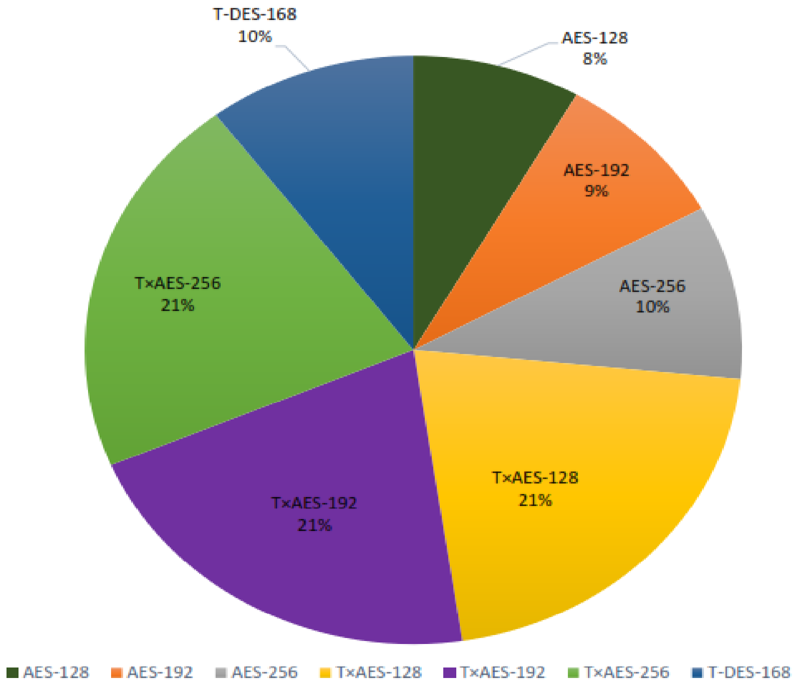

Figure 3: Decryption Time

Table 3 and the chart graph above show the decryption time for each algorithm that calculated to know the duration each algorithm takes to decrypt a text. The decryption time for 3×AES is higher than AES and T-DES, also comparing the average between AES and 3×AES, we find that 3×AES will take more time for decryption process.

The encryption, decryption, and key generation time depend on the instantaneous CPU status, because the speed for the CPU is not the same all the time, the "Idle status" means that the CPU is at a slow speed, for example, "when we are doing almost nothing", also it will take a faster speed when it is overloaded.

## III. Text Length:

Table 4: Text Length before and after Encryption for Each Algorithm

| | AES-128 | AES-192 | AES-256 | 3×AES-128 | 3×AES-192 | 3×AES-256 | T-DES-168 |
|---|---|---|---|---|---|---|---|
| **50** | 90 | 90 | 90 | 196 | 196 | 196 | 76 |
| **150** | 220 | 220 | 220 | 438 | 438 | 438 | 208 |
| **250** | 352 | 352 | 352 | 700 | 700 | 700 | 352 |
| **350** | 484 | 484 | 484 | 944 | 944 | 944 | 484 |
| **450** | 636 | 636 | 636 | 1206 | 1206 | 1206 | 624 |
| **550** | 766 | 766 | 766 | 1444 | 1444 | 1444 | 754 |
| **650** | 898 | 898 | 898 | 1732 | 1732 | 1732 | 898 |
| **750** | 1030 | 1030 | 1030 | 1970 | 1970 | 1970 | 1030 |
| **850** | 1182 | 1182 | 1182 | 2232 | 2232 | 2232 | 1174 |
| **950** | 1312 | 1312 | 1312 | 2496 | 2496 | 2496 | 1304 |

The 3×AES encryption algorithm was not used for encrypting to secure data in cloud computing before, and by using it, it noticed that it takes time more than AES for generating the key, encryption, and decryption. 3×AES can secure the text that uploaded to the cloud more than AES, because of the triple encryption that it has, that means it encrypts the text three times. Even though it has a large text length after encryption more than AES, but it is compatible with newer PCs specifications that evolved these days, that have a high computational power and a large capacity that can handle the length for the text after encryption.

## IV. Conclusions:

Cloud computing is the primary structure that can share the information in a framework, business procedures, and programming. Also, it's the fundamental structure that can share the information in a foundation, business procedures, and programming. (Amidst 2015). 3×AES encryption algorithm used in this paper with the key sizes (128, 192, and 256-bits) for text encryption that saved on the cloud. This algorithm has a comparison between AES with key lengths (182, 192 and 256-bits) and T-DES with a key length 168bits. The performance measurement for these three algorithms shows that the increasing of the key length for the algorithm the higher security for this algorithm. The key generation time for each algorithm has been measured, the result also shows that T-DES with the key size (168-bits) has a higher time comparing with 3×AES and AES, and 3×AES has a higher key generation time comparing with AES with all corresponding key size for AES and T-DES algorithm. Encryption time for each algorithm has been measured and found that the encryption time for 3×AES is higher than AES and T-DES, also comparing the average between AES and 3×AES, we found that AES will take less encryption time. Also, the decryption time for 3×AES is higher than AES and T-DES, also comparing the average between AES and 3×AES, we found that 3×AES will take more time for decryption process.

## References:

- Agoyi, M., & Seral, D. (2010, September). SMS security: an asymmetric encryption approach. In Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on (pp. 448-452). IEEE.
- Beimborn, D., Miletzki, T., & Wenzel, S. (2011). Platform as a service (PaaS). Business & Information Systems Engineering, 3(6), 381-384.
- Bhanot, R., & Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. International Journal of Security and Its Applications, 9(4), 289306.
- Daemen, J., & Rijmen, V. (2013). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.
- Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: issues and challenges. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on (pp. 27-33). Ieee.
- Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2008). Performance evaluation of symmetric encryption algorithms. IJCSNS International Journal of Computer Science and Network Security, 8(12), 280-286.
- G. Ramesh & Dr. R. Umarani (2012). Performance Analysis of Most Common Symmetrical Encryption Algorithms. International Journal of Power Control Signal and Computation (IJPCSC) Vol3. No1. Jan-Mar 2012 ISSN: 0976-268X.
- Jiménez Martínez, D. (2013). Privacy and confidentiality issues in cloud computing architectures.
- Jiménez Martínez, D. (2013). Privacy and confidentiality issues in cloud computing architectures.
- KARTIT, Z., & EL MARRAKI, M. (2015). Applying Encryption Algorithm to Enhance Data Security in Cloud Storage. Engineering Letters, 23(4).
- Kovachev, D., Renzel, D., Klamma, R., & Cao, Y. (2010, May). Mobile community cloud computing: emerges and evolves. In Mobile Data Management (MDM), 2010 Eleventh International Conference on (pp. 393-395). IEEE.
- Li, J., Liu, Z., Chen, X., Xhafa, F., Tan, X., & Wong, D. S. (2015). L-EncDB: a lightweight framework for privacy-preserving data queries in cloud computing. Knowledge-Based Systems, 79, 18-26.
- Manvi, S. S., & Shyam, G. K. (2014). Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey. Journal of Network and Computer Applications, 41, 424-440.
- Meyer, C. H., & Matyas, S. M. (1982). Cryptography: a new dimension in computer data security: a guide for the design and implementation of secure systems. John Wiley & Sons Inc.

- Pearson, S. (2009, May). Taking account of privacy when designing cloud computing services. In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing (pp. 44-52). IEEE Computer Society.
- Saravanakumar, C., & Arun, C. (2014, November). Survey on interoperability, security, trust, privacy standardization of cloud computing. In Contemporary Computing and Informatics (IC3I), 2014 International Conference on (pp. 977-982). IEEE.
- Wang, Z. (2011, October). Security and privacy issues within the Cloud Computing. In Computational and Information Sciences (ICCIS), 2011 International Conference on (pp. 175-178). IEEE.
- Waqar, A., Raza, A., & Abbas, H. (2011, November). User privacy issues in Eucalyptus: a private cloud computing environment. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on (pp. 927932). IEEE.
- Wohl, A. (2010). Software as a Service (SaaS). The Next Wave of Technologies: Opportunities from Chaos, 97-113.
- Zhang, H., Jiang, G., Yoshihira, K., Chen, H., & Saxena, A. (2009, July). Intelligent workload factoring for a hybrid cloud computing model. In Services-I, 2009 World Conference on (pp. 701-708). IEEE.
- Zhou, M. (2013). Data security and integrity in cloud computing.

## الخلاصة

مع التقدم السريع للبيانات الحرجة التي يتم خز نها على الحوسبة السحابية، أمن السحابة يجب ان يكون اقوى . التطور الحاصل لمستخدمي الحوسبة السحابية المرافق لتطور الهجمات الفايروسية ادى الى اكتشاف نقاط ضعف في امن الحوسبة. الفكرة من استخدام الحوسبة السحابية ليس جديدا بحد ذاته، فقد تم استخدامه بتوسع في الحقبة الاخيرة مع التطور الحاصل في التجارة والاستثمارات التي يعتمد كليا على خدمات الانترنت لتنفيذ الاعمال الدقيقة التي تحتاج الى خزن في اماكن يتم استخدامها لاحقا.

في هذا البحث تم اقتراح تقنية تشفير جديدة التي تحمي البيانات قبل خزنها على الحوسبة السحابية ويتم استعادة البيانات بعد فك التشفير، لذا فان سرية البيانات سيتم حمايتها . التقنية التي تم اقتراحها في هذا البحث هي (3xAES) وتم مقارنتها مع خوارزمية AES والـ T-DES بحساب وقت توليد المفتاح، وقت التشفير، ووقت فك التشفير لكل خوارزمية. من هذا البحث نستنتج ان خوارزمية 3xAES هي اعلى امن وكفاءة من T-DES يرجع ذلك لسبب التشفير الثلاثي للخوارزيمة. حيث تم محاولة اختراق وسرقة النص المشفر المخزون لكن كانت هناك صعوبة بمعرفة الرقم السري او المفتاح الذي تم تشفير النص به.