Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Comparative Study of Database Security In Cloud Computing Using AES and DES Encryption Algorithms

Nora Abdullah Al-gohany [1*], Sultan Almotairi [2]

[1] *Computer Science Department, Faculty of Computing and Information Technology, King Abdul-Aziz University, Jeddah, Saudi Arabia.*

[2] *Department of Natural and Applied Sciences, Community College, Majmaah University, Al-Majmaah, 11952, Saudi Arabia.*

Received14 Jan. 2019; Accepted 15 Mar. 2019; Available Online 30 Apr. 2019

Abstract

Security is consider as one of the largest part important aspects in daily computing. The security is important in cloud computing especially for data save in cloud because it have sensitivity and import data as well many user can access to same data. Unfortunately the increase of the cloud user has been accompanied with a increase in malicious action in the cloud and data not be completely trustworthy. Because of that the cloud computing security become big issue in the cloud data. The danger of malicious in the cloud and the crash of cloud services have received a strong interest by researchers. Here, we present a comparative study between state-of-art approaches to overcome these issues. This paper test and compare between the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) in term of different input size that result the AES is faster than DES in the encryption time but in decryption the DES faster than AES from 20KB to 100 KB after that the DES rise sharply and AES rise slightly that make ASE faster than DES in the decryption time from 120 KB to 300KB.

I. Introduction

Cloud is the collection of servers, device and data storage that are located at dissimilar spaces and these sever and data storage are dependable for given that on demand service to its client with help out of internet. The service provide by cloud is not show in client computer. Client has to right to use these services with aid of internet association during subscribe them.

The major benefit of cloud computing is that it eliminate the require for client to be in similar place where hardware software and storage space is actually here. Cloud it achievable to save and right to use your data from everyplace and every time with no worrying about protection of hardware ,software and storage space. Cloud computing can divided into three service model [1], [2].

A. Infrastructure as a service (IaaS)

Displace in home servers, storage and network through provided that resources when the user need. Alternative of purchase a server, user nowadays can provide to user for a short period of time and remove it when period of time was ended. frequently paying through the hour just for what they really use.

B. Platform as a service (PaaS)

Insert a level to the infrastructure, given that a plat-

Keywords: *Cryptography, Data security, Decryption, Encryption, DES, AES.*

Production and hosting by NAUSS

* Corresponding Author: Nora Abdullah Al-gohany
Email: almotairi@mu.edu.sa

doi: 10.26735/16587790.2019.004

form leading to application be able to be written and deployed. These platforms try to help the programmers to concentrate on the commerce logic and release them from the fears of the physical infrastructure.

C. Software as a service (SaaS)

That main the application running on cloud infrastructures, usually provide to the user via a web browser.

Security is important issue and challenge when any user stores its important information in cloud. We can say cloud is secure when it verify three conditions: (a) Confidentiality (b) Integrity (c) Availability. Confidentiality refers to save data private and the unauthorized can't access to this data. Integrity refers that data saved in cloud only authorized user can be accessed, change and fabricated to data. Availability refers that computer method and resources are existing to authorized user at right time and not disallowed in this time.

Cryptography is a method of convert data from readable to unreadable during storage space and communication that it appears misuse to interloper. The unreadable appearance of data is identified as cipher text. The data is received with receiver it show in its original appearance which is identified as plain text. Exchange of plain text to cipher text is identified as encryption and exchange cipher text to plain text is identified as decryption. Encryption doing at sender side while decryption doing at receiver's side. The cryptography algorithms are:

a) Symmetric algorithms

In this algorithm, same key is use in both encryption and decryption that key identified as secret key encryption. Symmetric algorithms are easy require and smaller execution time as show in Fig. 1 (a). The example of symmetric algorithm the Advanced Encryption Standard (AES) algorithm and the Data Encryption Standard (DES) algorithm.

b) Asymmetric algorithms

This algorithm also identified public key encryption that different key is use in encryption and decryption. The two keys are identified private key and public key. The public key is send to the all user while the private key is set aside of the receiver. The public key is use by sender for encryption data and private key is use by receiver for decryption as show in Fig. 1 (b). The example of asymmetric algorithm the Rivest-Shamir-Adleman (RSA) algorithm and Diffie-Hellman (DH) algorithm.

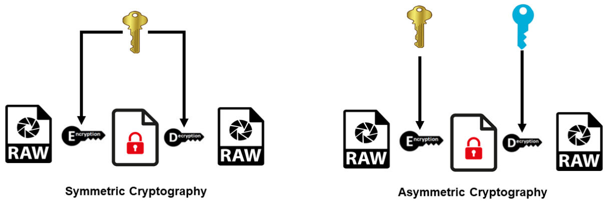

Fig. 1. (a) (Left) Symmetric, and (b) (Right) Asymmetric Cryptography.

The paper is organized as follows: in Section 2 Some of important existing algorithms is defined; related woke is discussed in Section 3; in Section 4 comparative study is described and finally in Section 5 testing and result DES and AES algorithms are described.

II. Some of Important Existing Algorithms

A. Data Encryption Standard (DES) algorithm

The DES algorithm is symmetric algorithms that take input with of 64-bit length plain text and 56-bit key that is eight bits of parity and give output that 64 bit block. In each around the plain text block has to move the bits. The eight parity bits are detached from the key through subjecting the key to its key in modify. As show in Fig. 2 the plain text and key will process by the following algorithm steps [1]:

1. The key is divide to two 28 halves.
2. Shift all partly of the key by one or two bits depending on the around.
3. recombined key and shorted it from 56 bits to 48 bits. This 48 bits key used to encrypt plain text in this round's block.
4. The result key from step (2) are used in after that round.
5. The block of data is divide into two 32-bit partly.
6. One partly is focus to an growth permutation to raise its size to 48 bits.
7. production of step (6) is enter in XOR with the 48- bit key result from step (3).
8. production of step (7) is feed into an S-box that exchange key bits and product the 48-bit block again to 32-bits.
9. production of step (8) is inter to a P-box with permute the bits.

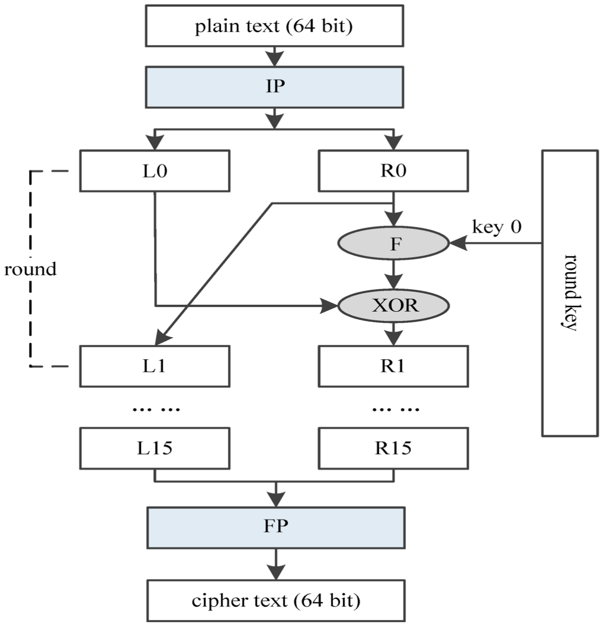

Fig. 2. Diagram of DES algorithm [16].

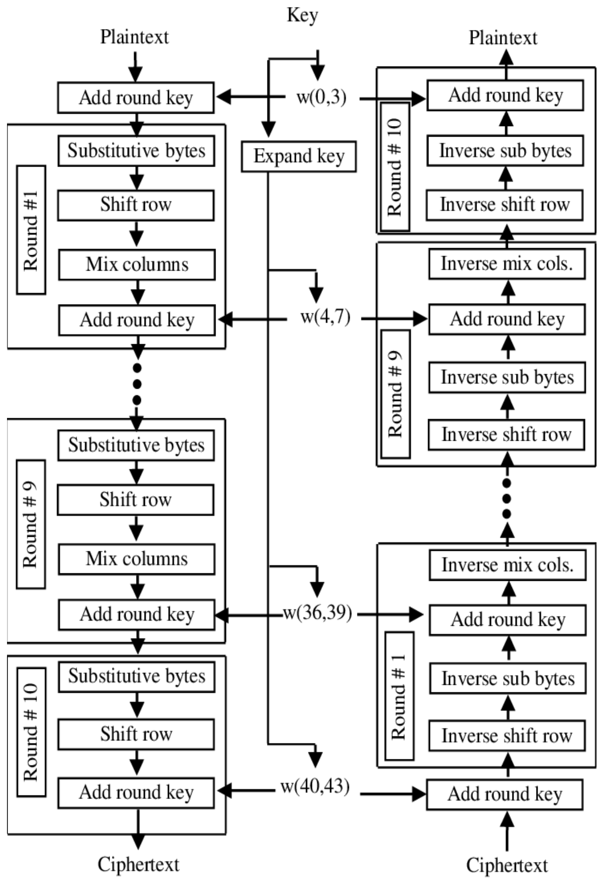

Fig. 3. Diagram of encryption and decryption AES algorithm [15].

10. The result of the P-box is enter in XOR with additional half of the data block.
11. The two data divide are swap and turn into the after that round's as input.

B. *Advanced Encryption Standard (AES) algorithm*

The AES algorithm is symmetric algorithms that take input with of 128 bit block plain text that product the set keys that use in round from the cipher key. As show in fig. 3 the plain text and key will process by the following algorithm steps [1]:

1. Initialize status array and put in the first round key to the being state array.
2. Do round from 1 to 9 by execute usual round which execute the following operations:
3. Sub Bytes: which the first transform that substitute a byte.
   a. Shift Rows: that transformation In the encryption.
   b. Mix Columns: it transforms every column of the location to a new column.
   c. Add Round Key, using K(round) :takings one column at a time. The procedure in Add Round Key is matrix summation.
4. Execute Final Round which execute the following operations:
   a. Sub Bytes.
   b. Shift Rows.
   c. Add Round Key using K(10).
   d. Cipher text is production of Final Round Step

III. Related Woke

A. *Encryption algorithm*

There are many study and survey of encryption algorithm that make good comparisons between them some of this are discuss her:

Mahajan, et al. [1], [2] explain and discuss AES, DES and RSA algorithms and compare performance of this algorithm in encrypt technique base in the study of its time of encryption and decryption by stimulated time. The strength point in this papers is explain the algorithm in more detail supported by figure and make good and comprehensive comparison between RSA, AES and DES algorithms that result the AES algorithm consumes smallest amount of encryption and RSA consume greatest encryption rate of time. Also that decryption of AES algorithm is the best algorithms.

Verma, et al. [3],[4] discuss the data security algorithm in cloud and make comparison between different algorithm. They explain many symmetric algorithms as DES, Tripe-DES, AES and BLOWFISH also asymmetric algorithm as RSA. Then comparative in term of key length, block size, rounds, power consumption, avalanche effect and many other terms. That results it AES and blowfish are very secure and good algorithms. The power and speed use in AES and blowfish algorithms are better when we compare to the others algorithms. When we use asymmetric encryption algorithm the RSA is protected and be able to use in application run in wireless network the reason of that its good speed and security.

Bisht, et al. [5] relative study of encryption algorithm in term of symmetric key (AES and DES) and asymmetric key (RSA and DH) algorithms. The strength point in this paper it analyze algorithms in term of key used, algorithm, key length, speed, tenability, power consumption, security, cost and implementation. That result AES and DES algorithms is appears to be excellent in terms of speed and power use while RSA and DH algorithms is appears to be excellent in terms of tenability. The symmetric key encryption the AES algorithm is appear to be better in cost, implementation and security terms. In RSA that is asymmetric key encryption algorithm is appear better in terms of speed and security.

Rihan, et al. [6] appraise the performance the some encryption algorithms that are AES and DES. The performance calculate of encryption algorithms in terms of processing time, CPU usage and encryption throughput. The strength point in this paper is experimental by simulation in Windows and Mac platform for a different text size. That results the AES in the execution time is better speed than DES in all platforms also DES achieve lost throughput than AES. In other hand, the AES consume more CPU than DES for each platforms.

B. Security in cloud computing

Security storage space in cloud computing has been the article of some research:

Arora, et al. [7] discuss a bout issue, method, challenge in cloud security and explain many security algorithms such as RSA, AES, DES and Blowfish. That use Net Beans IDE with Java to implementation of algorithms then doing good comparison that found AES algorithm uses smallest amount of time to executed cloud data and Blowfish algorithm is take smallest amount of memory requirement also DES algorithm consume smallest amount of encryption time. RSA consumes highest memory range and encryption time. The strength point in this paper in IDE tool that use in implementation for all algorithms that lead to desired production for the data in cloud is achieve. Also this paper good comparison among algorithms.

Bhardwaj, et al. [8] appraise symmetric and asymmetric algorithms with highlighting in symmetric algorithms it implementation in Java and make comparison by figure in term of computational cost for encryption between (DES, Triple DES and AES) that found AES take less cost and computational cost of decryption between (SHA 256 and MD5) that found MD5 take less cost and execute time but doesn't determent the algorithm of execute time.

Chezian, et al. [9] discover different data encryption technique as hybrid algorithm, DES algorithm and identity based encryption. They use mathematically approach. The strength point in this paper that be able to use as reference for built the full security solution. But doesn't implementation and show the different between algorithm.

Nigoti, et al. [10] study different security issue in cloud and many cryptographic algorithms that explain symmetric key algorithms include DES, Triple-DES ,AES and blowfish algorithms also explain asymmetric key algorithms include RSA and Diffie-Helman which produce encryption keys in symmetric algorithms. The result is DES and AES are more use from symmetric algorithms and DES is quite easy to apply then AES. This paper explain the algorithms in clear way but doesn't implementation and comparison algorithms.

Patwal, et al. [11] have presented some of literature survey cryptographic base in security algorithms used for cloud computing and discuss a few of the presented Algorithms in cloud security such as RSA,DES,AES and digital signature. This paper make good present and discuss of security algorithms used for cloud computing in especially the digital signature but doesn't implementation and compare between algorithms.

Sachdev, et al. [12] suggest easy data security model to ensure data confidentiality and security which data is encrypted using AES algorithm with 128 bit key length before it is transform to the cloud. The AES algorithm and make good explain how AES algorithm is work and why it use also comparing AES with other algorithms from previous study. It result use of ASE profit of fewer memory using up and fewer calculation time as compared to other algorithms. But in this paper doesn't exposure the previous study.

Khan, et al. [13] proposed system to achieve text files confidentiality using cryptographic algorithms to improve the security in cloud. In this system using DES and RSA algorithm to encryption text files and uploaded it in cloud storage space. In case of decryption and download text files inverse way first apply DES then RSA algorithm. The strength point in this paper is achieve multilevel of encryption and decryption algorithms that provide extra security for cloud storage space than using single level.

Mahalle, et al. [14] proposed hybrid encryption method that use both AES and RSA algorithms where in AES use 128 bit secret key and in RSA use 1024 bit key. The hybrid encryption system encrypts data by AES then RSA encryption. However, it decryption data by applied RAS then AES. This system provide high security and the key use cannot deduce because that use 1024 bit of RSA and 128 bit of AES keys. That execute the algorithms but doesn't comber it with other algorithms.

IV. A Comparative Study

In this section, we comparison between pervious related work as illustrated in Table I and II.

TABLE I

Comparison of our Solution Method with other Available Approaches

Paper	Cloud	Algorithm	Result	Advantage	Disadvantage
[1],[2]	X	AES, DES and RSA	AES algorithm consumes smallest amount of encryption and RSA consume greatest encryption rate of time. Also that decryption of AES algorithm is the best algorithmxs.	Explain the algorithm in more detail supported by figure and make good and comprehensive comparison between RSA, AES and DES algorithms also in [6] implementation Visual Studio Net packages	Doesn't exposure the previous study also the two papers is same result also the number same.
[3],[4]	X	AES, DES and Triple DES	In requisites of security and speed AES is improved higher than DES and Triple DES.	Good explain the algorithm and comparison	Doesn't implementation the algorithms get comparison depend in last study
[5]	X	AES, DES, RSA, DH	AES and DES algorithms is appears to be excellent in terms of speed and power use while RSA and DH algorithms is appears to be excellent in terms of tenability.	Analyze algorithms in term of key used, algorithm, key length, speed, tenability, power consumption, security, cost and implementation	Doesn't implementation the algorithms get comparison depend in last study

TABLE I

COMPARISON OF OUR SOLUTION METHOD WITH OTHER AVAILABLE APPROACHES (*Continued.*)

Paper	Cloud	Algorithm	Result	Advantage	Disadvantage
[6]	X	AES and DES	AES in the execution time is better speed than DES in all platforms also DES achieve lost throughput than AES. In other hand, the AES consume more CPU than DES for each platforms.	Calculate of encryption algorithms in terms of processing time, CPU usage and encryption throughput and experimental by simulation in Windows and Mac platform for a different text size	Doesn't exposure the previous study Also the algorithm run only in file data.
[7]	√	RSA, AES, DES and Blowfish	AES algorithm uses smallest amount of time to executed cloud data and Blowfish algorithm is take smallest amount of memory requirement also DES algorithm consume smallest amount of encryption time. RSA consumes highest memory range and encryption time.	IDE tool that use in implementation for all algorithms that lead to desired production for the data in cloud is achieve. Also this paper good comparison among algorithms.	Comparison in general terms not particularly specific
[8]	√	DES, Triple DES and AES SHA 256 and MD5	AES take less cost than DES and Triple DES also MD5 take less cost and execute time than SHA256	Implementation in Java and support the comparison by figure	Compare each group in different term also doesn't determent the algorithm of execute time
[9]	√	DES	The latest outlook of data security answer with encryption which is important	Be able to use as reference for built the full security solution	Doesn't implementation and show the different between algorithm
[10]	√	DES, Triple-DES ,AES , blowfish, RSA and Diffie-Helman	DES and AES are more use from symmetric algorithms and DES is quite easy to apply then AES.	Explain the algorithms in clear way	Doesn't implementation and comparison algorithms
[12]	√	AES	Use of ASE profit of fewer memory using up and fewer calculation time as compared to other algorithms	Make good explain how AES algorithm is work and why it use also comparing AES with other algorithms from previous study	Doesn't explains how key exchange and doesn't give more details of the experience also doesn't compare the AES algorithm with another algorithm

TABLE I
COMPARISON OF OUR SOLUTION METHOD WITH OTHER AVAILABLE APPROACHES (*Continued.*)

Paper	Cloud	Algorithm	Result	Advantage	Disadvantage
[11]	√	RSA,DES, AES	Show some of exist algorithm base in security algorithms for cloud	Good present and discuss of security algorithms used for cloud computing in especially the digital signature	Doesn't implementation and compare between algorithms
[13],[14]	√	[28] DES and RSA	Provide extra security for cloud storage space than using single level	Multilevel of encryption and decryption algorithms and take advantage of two algorithms	System occurs theoretically without actual application

TABLE II
COMPARISON BETWEEN SYMMETRIC ALGORITHMS DEPENDED IN PERVIOUS STUDY

Factors	AES	DES	Triple-DES
Build in	2000	1977	1998
Round number	10 or 12 or 14	16	48
Key Size	128, 192 and 256 bits	56 bits	168, 112 bits
Block Size	128 bits	64 bits	64 bits
Ciphering & deciphering key	Same	Same	Same
Security	Excellent	Not enough	Adequate
Execution time	More fast	Slow	Very slow

V. Testing and Result DES and AES Algorithms

In this section, we show and describe the testing results. In test using operating system windows 7 (64 bit) with Intel core i5 and RAM 4 gigabit. The code run in eclipse program with java language.

In the test we use the same key and different input file size (KB). That code read from file then encryption file and write in other file.

We result the AES is faster than DES in the encryption time but in decryption the DES faster than AES from 20KB to 100 KB after that the DES rise sharply and AES rise slightly that make ASE faster than DES in the decryption time from 120 KB to 300KB.

VI. Conclusion

Security issues is most challenges in cloud computing therefore the encryption algorithms have been applied in cloud data to make cloud data more secure. In this paper, we compare many recent study of DES and AES encryption algorithms. We compared and tested the two algorithm using different file size that result the AES is faster than DES in the encryption time but in decryption the DES faster than AES on small files. Whereas, the DES speed rise sharply and AES rise slightly that make ASE faster than DES in the decryption time on bigger files. Finally, the results proven that the AES is more efficient, fast, and elegant cryptographic algorithm.

TABLE 3
COMPARISON BETWEEN DES AND AES DEPEND ON ENCRYPTION / DECRYPTION TIME (SEC)

Size (KB)	DES encrypted	AES encrypted	DES decrypted	AES decrypted
20	0.038	0.027	0.005	0.011
50	0.042	0.037	0.012	0.017
60	0.053	0.034	0.016	0.019
80	0.058	0.044	0.019	0.024
100	0.062	0.049	0.024	0.026
120	0.075	0.059	0.035	0.026
150	0.08	0.06	0.036	0.028
200	0.096	0.066	0.043	0.032
250	0.103	0.073	0.057	0.036
300	0.129	0.075	0.076	0.048
300	0.129	0.075	0.076	0.048

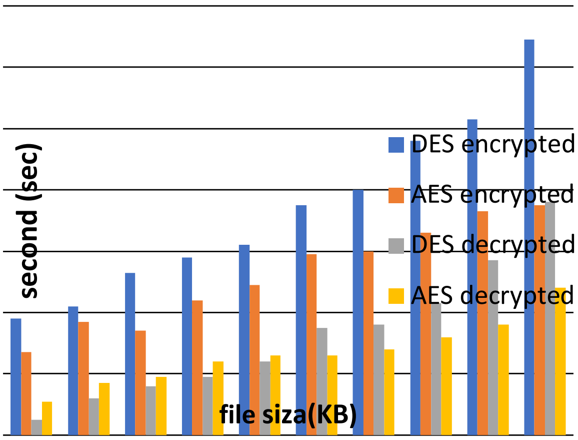

Fig. 4. Diagram of encryption and decryption

REFERENCES

[1] P. Mahajan and A. Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security,” *Glob. J. Comput. Sci. Technol.*, vol. 13, no. 15, pp. 15-22, 2013.

[2] B. Padmavathi and S. R. Kumari, “A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique,” *Int. J. Sci. Res.*, vol. 2, no. 4, pp. 170-174, Apr. 2013.

[3] A. Verma, P. Guha and S. Mishra, “Comparative Study of Different Cryptographic Algorithms,” *Int. J. Emerg. Trend Technol. Comput. Sci.*, vol. 5, no. 2, pp. 58-63, Apr. 2016.

[4] V. R. Pancholi and B. P. Patel, “Cryptography: Comparative Studies of Different Symmetric Algorithms,” *Int. J. Technol. Sci.*, vol. VI, no. I, pp. 4-7, 2015.

[5] A. Pansotra and S. P. Singh, “Cloud Security Algorithms,” *Int. J. Secur. Appl.*, vol. 9, no. 10, pp. 353-360, 2015, doi: 10.14257/IJSIA.2015.9.10.32.

[6] N. Bisht and S. Singh, “A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms,” *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 4, no. 3, Mar. 2015, doi: 10.15680/IJIRSET.2015.0403043.

[7] J. Srinivasan and D. Ranjith, “Impact of database security in Cloud Computing,” *in Proc. Int. Conf. Glob. Innov. Technol. Sci.*, 2013.

[8] R. Arora and A. Parashar, “Secure User Data in Cloud Computing Using Encryption Algorithms,” *Int. J. Eng. Res. Appl.*, vol. 3, no. 4, pp. 1922-1926, Jul.-Aug. 2013.

[9] R. Kaur and S. Kinger, “Analysis of Security Algorithms in Cloud Computing,” *Int. J. Appl. Innov. Eng. Manag.*, vol. 3, no. 3, pp. 171-176, Mar. 2014.

[10] G. Devi and M. P. Kumar, “Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm,” *Int. J. Comput. Trends Technol.*, vol. 3, no. 4, pp. 592-596, 2012.

[11] O. K. Jasim, S. Abbas, E. M. El-Horbaty and A. M. Salem, “Efficiency of Modern Encryption Algorithms in Cloud Computing,” *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 2, no. 6, pp. 270-274, Nov.-Dec. 2013.

[12] M. Patwal and T. Mittal, “A Survey of Cryptographic based Security Algorithms for Cloud Computing,” *HCTL Open Int. J. Technol. Innov. Res.*, vol. 8, pp. 1-17, March 2014.

[13] N. Jain, P. Jain and N. Kapil, “Enhanced data security model for cloud using ECC algorithm and third party auditor,” *Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET)*, vol. 5, no. 3, pp. 519-524, March 2016.

[14] S. S. Khan and R. R. Tuteja, “Security in Cloud Computing using Cryptographic Algorithms,” *Int. J. Innov. Res. Comput. Commun. Eng. (IJIRCCE)*, vol. 3, no. 1, pp. 148-154, January 2015.

[15] A. G. Wadday, S. M. Wadi, H. J. Mohammed and A. A. Abdullah, “Study of WiMAX Based Communication Channel Effects on the Ciphered Image Using MAES Algorithm,” *Int. J. Appl. Eng. Res.*, vol. 13, no. 8, pp. 6009-6018, 2018.

[16] X. Yang, Y. Hou, J. Ma and H. He, “CDSP: A Solution for Privacy and Security of Multimedia Information Processing in Industrial Big Data and Internet of Thing,” *Sens.*, vol. 19, no. 3, Jan. 2019, doi: 10.3390/s19030556.