Selected Encryption Techniques for Cloud Security: A Review

Olomi Isaiah Aladesote, Olanrewaju Victor Johnson, Mutiu Ganiyu

Abstract— The only way to have secure information in the cloud is to use cryptographic techniques to counter the activities of professional hackers. This paper presents a comparative survey of selected encryption techniques used to secure cloud computing data resources. The results of existing works on the selected techniques were collated and used for the basis of the analysis. Based on the following metrics: memory usage, encryption and decryption time, throughput, security, turnability, entropy, avalanche and power consumption, Advanced Encryption Standard (AES) and Blowfish were found to a competitive advantage over other cryptographic methods for securing a cloud computing infrastructure.

Index Terms— Advanced Encryption Standard, Blowfish, Cloud, Cryptography, Hackers, Throughput, Security.

1 Introduction

COUPLED with technological advances, there is a pressing need to secure this information and data against intrusion(s) [1], [2], communication in this information is exposed to different safety concerns [3]. Security of the computer can be considered to safeguard the whole computer system against damage and to guide illegal access to information and data. The best way to secure information is to employ cryptographic technology in all types of communication since information is ensured when confidence, completeness and availability are guaranteed, also known as the CIA trinity as shown in Fig. 1 [4], [5]. The data must be transformed into a form that is illegal to access or users cannot read or known its original content.

In spite of the great success stories, versatility, flexibility and acceptance of the cloud, security threats and private protection remain a major issue, [6] pointed out. To a large extent, the potential danger to cloud infrastructure is to include attacks like Denial of Service (DoS), Distributed DoS, Cloud malware injection attacks, Man-in-the-Middle, spoofing, information disclosure, crash attack. Convergent perspectives demonstrate the suggestive nature of a wide variety of cloud service providers and government organizations to protect and strengthen not merely cloud users' secrecy but also the business continuity of the cloud. Subject to various challenges to compromise the cloud about privacy and unauthorized access, the most prominent targets are data privacy and security. The danger is more evasive today with varying cyber-attacks, such as those triggered by Ransomware. Considerable progress has been made with access control (i.e., a security barrier that restricts the operation and access of cloud infrastructures to enforce data privacy).

- *O.I. Aladesote, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM).*
  E-mail: gs57427@student.upm.edu.my, lomaladesote@yahoo.com
- *O.V Johnson, School of Computer Sciences Universiti of Sains Malaysia, 11800, Penang, Malaysia.*
  E-mail: olajohnson@student.usm.my, olajohnson@fedpolel.edu.ng
- *M. Ganiyu, Department of Computer Science, Federal Polytechnic, Ile-Oluji, Nigeria.*
  E-mail: mutganiyu@fedpolel.edu.ng

The predominant techniques are Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Identity-Based Access Control (IBAC), Rule-Based Access Control System (RuBAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC). But the aspect of data encryption is still challenging and daunting. Therefore, this paper takes a dissecting look at the existing literature on the selected encryption methods side-by-side with their experimental work to provide an assessment of their usability for securing cloud resources.

The paper is arranged as follows: the introduction is discussed in section 1, section 2 provides a brief overview of both cloud computing and cryptography. The selected methods are discussed in section 3, section 4 is for related works, the approach used, analysis of reviewed encryption methods and discussion are presented in section 5, while conclusion is presented in section 6.

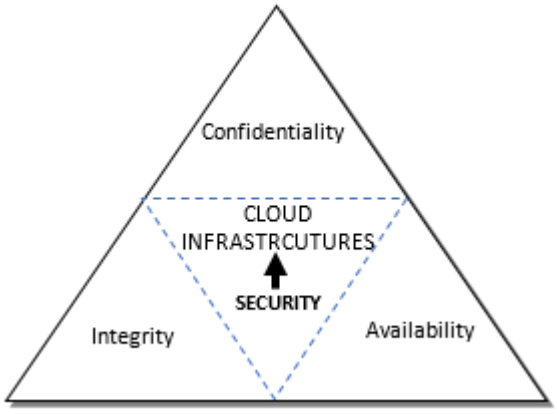

Fig. 1 The CIA triad Security Model

IJSER

2 The Cloud Era

Cloud computing is the term used to describe the provision of Information Technology (IT) services, which can be accessed anywhere at any time on the Internet in such a way that user pays for what they used. Such services include software, hardware, networking, and storage. One of the major weaknesses of cloud computing is the security of storing data on servers. To solve this problem, a cryptography algorithm must be used to protect data to ensure proper control and security of sensitive data. The following are security threats that arise in cloud computing: security of data stored, separation of private and corporate data, security of interface and user access control [7].

It is classified as next-generation computing that is: internet-based, highly scalable, non-transparent and distributed computing systems in which computational resources are offered "as a service". Such services include software, hardware, networking, and storage. Notable cloud architectural models are: 1) Public cloud: resources are dynamically allotted, self-service basis over the Internet. Billing is applicable based on consumption of pay-as-use basis; 2) Private cloud: resources are dedicated to a single or a set of allied organizations as an intranet functionality. The billing may usually be on a subscription basis as little commitments are required; and 3) Hybrid cloud: provides the flexibility and approach from both private and public cloud [8], [9], [10]. Based on the available three cloud models, the following cloud services could be provided independently or in a cooperative approach, namely: 1) Platform as a Service (PaaS): provision of Operating OS, firmware, Middle and development stacks; 2) Infrastructure as a Service (IaaS): provisions of processing cores, networks and storage; and 3) Software as a Service: provisions of application, licensing, web servers and software development and provisioning tools.

3 Cryptography Algorithms

Cryptography can be defined as a process of making data and information unreadable to unauthorized individuals, and the essence of a cryptographic algorithm is to encrypt and decrypt messages to prevent unauthorized access to them [11]. The functions of cryptography include privacy or confidentiality, authentication, integrity, non-repudiation and key exchange [12]. Cryptography algorithms can be grouped into symmetric and asymmetric [5]. This can be grouped into two parts: symmetric (secret key) and asymmetric (public key) [13]. Symmetric (secret key) uses a single key for both encryption and decryption while asymmetric (public key) uses one key for encryption and another decryption. The only approach to securing data is to use the cryptography technique [14]. The following evaluation metrics: scalability (memory usage, encryption rate & compilation efficiency), security (measurement of the length of the key in bits), flexibility (minor modifications), etc. can be used to measure the performance of any cryptography algorithm [11].

The following are cryptography methods examined in the paper:

3.1 Advanced Encryption Standard (AES)

AES was developed to strengthen the weaknesses of the Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES). It has the following features:

1. AES allows for three different key lengths: 128, 192, or 256 bits.
2. To encrypt 128 –bit keys consists of 10 rounds of processing, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.
3. All other rounds are alike except for the last round in each case.
4. Each round of processing includes one single-byte-based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.
5. AES also has the notion of a word. A word consists of four bytes, that is, 32 bits. Therefore, each column of the state array is a word, as is each row.
6. The decryption algorithm of AES differs from the encryption algorithm.
7. It can be used in many applications

3.2 Data Encryption Standard (DES)

DES was developed in the 1970s by International Business Machines (IBM) and adopted by the National Bureau of Standards (NBS). It has the following features:

1. DES is a Feistel block-cipher employing a 56-bit key that operates on 64-bit blocks.
2. It has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations.
3. DES was based on an earlier cipher from Feistel called Lucifer which, some sources report, had a 112-bit key.
4. DES was defined in American National Standard X3.92 and three Federal Information Processing Standards (FIPS), all withdrawn in 2005: FIPS 46-3: DES (Archived file), FIPS 74: Guidelines for Implementing and Using the NBS Data Encryption Standard.

3.3 Rivest-Shamir Adleman (RSA)

This was developed by three researchers: Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. RSA is a popular cryptography technique used for key exchange or digital signatures or encryption of blocks of data. It has the following features, among others:

1. It can generate both Public and private keys.
2. The data is encrypted with either public or private key and it must be decrypted with equivalent public or private key.
3. It creates digital signatures and verifies digital signatures.
4. It encodes encrypted output to Base64, Hex, Quoted-Printable, or URL-encoding
5. Its key sizes are from 512 bits to 4096 bits.
6. It supports hash methods

3.4 Triple Data Encryption Standard (3DES)

This was developed by IBM in 1970. It is a symmetric block

cipher with the following features:

1. it performs 3 iterations of DES encryption on each block.
2. As it is an enhanced version of DES so is based on the concept of Feistel Structure. The 3DES uses a 64-bit of plain text with 48 rounds and a Key Length of 168-bits permuted into 16 sub-keys each of 48- bit length.
3. It also contains 8 S-boxes and the same algorithm is used in reverse for decryption.

3.5 Blowfish

Designed in 1993. It is known to be the most efficient encryption algorithm among all existing methods. The following are some of the most notable characteristics of blowfish:

1. The variable key length ranges from 32 bits to 448 bits, with a block size of 64 bits.
2. It has two basic procedural steps. The first step is to expand the key and the second is to encrypt the data.
3. The P-array is of 18 subkeys of 32-bit each. Others are four 32-bit S-boxes, each with 256 entries and employing XOR encryption operations.
4. It has a wide range of applications makes use of it with no need for frequently changing keys.

4 Related Works

[4] propose Super-Encryption Cryptography with IDEA and WAKE Algorithm to apply super-encryption, whereby the original message would be encrypted with International Data Encryption Algorithm (IDEA) and then also re-encrypted with Word Auto Key Encryption (WAKE). The result shows that the combination of these methods makes it difficult for attackers to decrypt messages. [1] carry out a Comprehensive Evaluation of Cryptographic Methods by analyzing five (5) cryptography methods using the following metrics: memory space, encryption time, decryption time, memory used, avalanche effect, entropy and number of bits required for encoding optimally. The work is motivated by the fact that many researchers had carried out theoretical comparisons but were not supported with implementations. The implementation of these methods is done in java using Eclipse IDE. The researchers conclude that each of the cryptography techniques has its strengths and weaknesses and that knowledge about each technique will help in selecting the best for any task.

[5] carry out a study of Encryption Methods (RSA, DES, 3DES and AES) for Information Security. A review of existing related works is done and the result of the experiment shows that the AES algorithm is most efficient in terms of speed, time, throughput and avalanche effect. [13] works on the exploration of efficient symmetric AES algorithm to present the basic encipherment and decipherment process of Advanced Encryption Standard (AES) symmetric algorithm, the result shows that the AES algorithm provides high security for data. [7] presents a general review and comparison of the symmetric type of Cryptographic methods that could be used to encrypt applications and services in cloud computing, to ensure end-user security. File size, encryption computation time and encoding computational time are used to select the right methods. The researchers found out that found AES is the best for key encryption and MD5 is faster when encoding. [15] carry out a comparative study between symmetric and asymmetric encryption methods using a different set of metrics. The results prove that AES and Blowfish are the most secure and efficient symmetric encryption algorithms, while RSA asymmetric encryption algorithm is good in terms of speed and security. This makes it useful for application in a wireless network.

5 Methodology and Performance Evaluation

Four common conventional encryption techniques were selected for the review viz-a-viz: RSA, DES, 3DES, and Blowfish. Metrics such as memory used, encryption/decryption time, entropy, avalanche effect, speed of execution, throughput power consumption and others were considered for the assessment. The performance evaluation was presented in a tabular form and used as a scorecard for the selected methods.

The performance evaluation of the selected methods was based on the implementation results of four authors: [1], [2], [5], [11]. These researchers based the evaluation performance of these methods on certain metrics: encryption & decryption time, security, resource consumption, etc. International Data Encryption Algorithm (IDEA) and Word Auto Key Encryption (WAKE) would have been used for the evaluation but the researchers do not use any metrics to measure the performance of their work. Tables 1, 2, 3 and 4 show the results of the adopted works for the assessment.

6 Discussion and Conclusion

A scorecard comparative approach in a tabular form was employed on Tables 1, 2, 3 and 4 to provide for the analysis of the selected encryption methods. Follows are the deductive inference point in Tables 1-4 as:

1. AES uses a very small time to perform both encryption (conversion of plaintext to ciphertext) and decryption (conversion of ciphertext to plaintext) when the data size is large when compared with other methods.
2. AES requires a small memory space for its implementation.
3. Both AES and Blowfish are excellent when an input is changed slightly, the output changes significantly (Avalanche effect)
4. Information in AES cannot be easily guessed by an attacker (Entropy). Only the Blowfish algorithm is better in this regard.
5. Both AES and Blowfish compete favourably have high throughput.
6. RSA is proven to be highly secured but consumed much power on low-energy devices.

The above findings from the scorecard suggests therefore that both AES and Blowfish are can compete favourably in providing better security for the cloud. We subsequently opine

therefore the need to have a hybridization of the two techniques to harness their areas of strength for better cloud security. Though we were not able to consider IDEA and WAKE in our scorecard analysis since both reviewed and selected experimental works failed to present formidable experiment results on them. Future research should provide further details into this and more so modern encryption methods are emerging.

TABLE 1
EXPERIMENTAL RESULT 1, [1]

Metrics/Methods		**RSA**	**DES**	**3DES**	**AES**	**Blowfish**
Memory Used		Highest	High	Very High	Low	Very Low
Encryption time	Small file size (25KB)	Highest	High	High	Highest	Very Low
	Large file size (3MB)	Highest	High	Very High	Very Low	Low
Decryption time	Small file size (25KB)	Low	Highest	Very High	High	Very Low
	Large file size (3MB)	Highest	Very High	High	Very Low	Low
Entropy		High	Low	Low	Very High	Highest
Avalanche effect		Very Low	Very High	High	Highest	Low
Number of bits required to encode optimally		High	Very Low	Low	Highest	Very High

IJSER

TABLE 2
EXPERIMENTAL RESULT 2, [5]

Metrics/Methods	RSA	DES	3DES	AES
Speed	This is the slowest of all	It is slow	It is very slow	It has a very high speed
Security	It has the least security features	It is loose in security	It is secured	It has an Excellent in security

TABLE 3
EXPERIMENTAL RESULT 3, [15]

Metrics/Methods	RSA	DES	3DES	AES	Blowfish
Resources consumption	Very high	Require more CPU cycle and memory	Require effective resource consumption	Consumes resources when data and block size big	Requires preprocessing
Security	Very high	Inadequate	Vulnerable	High	High
Throughput	Very high	Medium	Medium	Very High	High
Cryptanalysis resistance	Brute force attack difficult to achieve	Vulnerable to linear and differential cryptanalysis	Vulnerable to differential brute force, attackers can analyze plaintext	Strong against truncated differential linear interpolation and square attack	Vulnerable to differential brute force attacker
Tunability	Yes	No	No	No	No
Avalanche Effect	Slower Encryption / Decryption	Less than AES	Medium	Faster Encryption / Decryption, less time than DES	Faster except when changing keys
Power consumption	Very high	Low	Low as compared to DES, AES, RSA & Blowfish	Low	High

IJSER

TABLE 4
EXPERIMENTAL RESULT 4, [2]

Metrics/Methods	RSA	DES	3DES	AES	Blowfish
Power consumption	High	Higher that AES	Higher that AES	Higher that Blowfish	Very Low
Security	Timing attack	Brute Force	Brute Force chosen- plaintext, known plaintext	chosen- plaintext, known plaintext	Dictionary attack
Throughput	Low	Lower than DES	Lower than AES	Lower than Blowfish	Very Hogh
Encryption Ratio	High	High	Moderate	High	High
Tunability	Yes	No	No	No	Yes
Speed	Fast	Fast	Fast	Fast	Fast

REFERENCES

[1] P. Patil, P. Narayankar, D.G Narayan, and S.M. Meena, "A Comprehensive Evaluation of Cryptographic Methods: DES, 3DES, AES, RSA and Blowfish", *Procedia Computer Science*, 78, 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[2] M.A. Panhwar, S. Ali Khuhro, G. Panhwar, and K.A. Memon, "SACA: A Study of Symmetric and Asymmetric Cryptographic Methods," *IJCSNS International Journal of Computer Science and Network Security*, 19(1), 48, 2019, http://paper.ijcsns.org/07_book/201901/20190107.pdf

[3] R. Rahim, S. Lubis, N. Nurmalini, and H. Dafitri, "Data Security on RFID Information Using Word Auto Key Encryption Algorithm," *Journal of Physics: Conference Series*, 1381(1), 2019, https://doi.org/10.1088/1742-6596/1381/1/012042.

[4] D. Abdullah, R. Rahim, , A.P. Utama Siahaan, A.F. Ulva, Z. Fitri, M. Malahayati, and H. Harun, "Super-Encryption Cryptography with IDEA and WAKE Algorithm," Journal of Physics: Conference Series, 1019(1), 2–7, 2018, https://doi.org/10.1088/1742-6596/1019/1/012039

[5] G. Singh and S. Supriya, "A Study of Encryption Methods (RSA, DES, 3DES and AES) for Information Security," International Journal of Computer Applications, 67(19), 33–38, 2013, https://doi.org/10.5120/11507-7224

[6] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," *IEEE Access*, Vol. 7, pp. 74361-74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

[7] A. Bhardwaj, G.V.B. Subrahmanyam, V. Avasthi, and H. Sastry, "Security Methods for Cloud Computing," Procedia Computer Science, 85(Cms), 535–542, 2016, https://doi.org/10.1016/j.procs.2016.05.215.

[8] M. Almorsy, J. Grundy, and I. Müller, "An Analysis of the Cloud Computing Security Problem," *ArXiv*, 2010, abs/1609.01107.

[9] S. Nalini and J. Andrews, "Recent security challenges in cloud computing," *Computers & Electrical Engineering*, Volume 71, Pages 28-42, ISSN 0045-7906, 2018, https://doi.org/10.1016/j.compeleceng.2018.06.006.

[10] G. Ramachandra, M. Iftikhar, and F. Khan, "A Comprehensive Survey on Security in Cloud Computing," *Procedia Computer Science*, 110. 465-472, 2017, 10.1016/j.procs.2017.06.124.

[11] R. M. Pandav and V.K. Verma, "Data Security Using Various Cryptography Techniques: a Recent Survey," International Journal for Research in Engineering Application & Management, 1(09), 1–4, 2015, https://www.ijream.org/papers/INJRV01I09001.pdf

[12] S. Thitme, and V.K. Verma, "A Recent Study of Various Encryption and Decryption Techniques". 1(3), 92–94, 2016.

[13] S. Mewada, "Classification of Efficient Symmetric Key Cryptography Methods," International Journal of Computer Science and Information Security, 14(2), 105–110, 2016, https://doi.org/10.13140/RG.2.2.30465.66402.

[14] H. Nurdiyanto, R. Rahim, and N. Wulan, "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement," Journal of Physics: Conference Series, 930(1), 2017, https://doi.org/10.1088/1742-6596/930/1/012005

[15] M. Vanitha and R. Mangayarkarasi, "Comparative study of different cryptographic methods," International Journal of Pharmacy and Technology, 8(4), 26433–26438, 2016.

IJSER