Comparison of Cryptographic Algorithms in Cloud and Local Environment using Quantum Cryptography

G. Murali
Computer Science and Engineering
JNTUACEP, Pulivendula
Andhra Pradesh, India
murlig521@gmail.com

R. Sivaram Prasad
Computer Science and Engineering
Acharya Nagarjuna University, Guntur
Andhra Pradesh, India
raminenisivaram@yahoo.co.in

***Abstract*—Cloud computing, has become a variable solution on top of virtualization for commoditization of computing resources. The existing security models are built with certain assumptions. The quantum key distribution provides the security by a new scheme called as Quantum Key Distribution Protocol for Cloud Computing which offers the benefits of quantum mechanisms to provide the secure cloud storage and data dynamics. This paper provides comparative analysis performance in local and cloud environment to identify the best environment using classical or quantum cryptography on various cryptographic algorithms.**

Keywords—Classical Cryptography; Quantum Cryptography (QC); cloud;Cryptographic Algorithms

I. Introduction

A. Quantum Cryptography

A Novel and Quantum Cryptography is produced from combining quantum mechanics with cryptography. Modern cryptography which is widely used in computer networks relies on computational complexity. In other words, breaking of the quantum computer with the quantum algorithm gives the final to the end of modern cryptography. Quantum is classified into two divisions based on security schemes known as single photon and entangled photon. An entangled state of quantum corresponds to the state between two particles where the measurement result is based on 1 particle which affects the another particles state that are physically separated from the particles which are measured [1]. Quantum Cryptography will use the characteristics of the quantum mechanics like superposition, entanglement. By the use of those properties, some of the information is secretly shared among users by the quantum channel. The information is a key or the message. Quantum cryptography is involved in the Quantum Key Distribution (QKD) protocols to share key and provide the Quantum Direct Communication (QDC) protocols which are used to send a message.

B. Quantum Key Distribution

Quantum Key Distribution (QKD) is one of the research where various protocols, scheme and the applications are used. QKD became more famous because it handles and tackles the main threats like impersonation and man-in-middle attack. In quantum cryptography authentication is the very hardest part because of its complexity level. Besides of this, key distribution problem is solved by quantum, it does not actually transfer any useful data. The cryptography strength is depending on the difficulty than that of an eavesdropper faces in breaking it. But Quantum Computing arrival, becomes easy to crack down any of the cryptosystem. Classical cryptography is no longer a secure communication method[2]. Securing data and data communication is a top priority because the consequences of unsecure data can have grave effects on both the economy and national security.

To provide security the Quantum cryptography always relies on the quantum mechanics laws where the traditional system to provide security in system depends on the computational difficulty of the encryption methods used.In this research by implementing Quantum Key Distribution (QKD) [3], to process in the authentication for the communication in a cloud infrastructure. The successful aim of the quantum key distribution protocols is to provide available parties, sender and receiver with randomly, correlatedly, and private classical data, to the key. There is a quantum channel to get into it, at their disposal, which is to be assumed that it is completely under the control of the adversary, Evesdropper. That means where the quantum state sender or receiver send by the channel, the outcome is completely arbitrary, the main problem is consistent with the quantum mechanics. In the additional of the quantum channel, the other parties will make utilize of public channel and the classical channel, assumed for authentication, by means, it cannot be alter or forge messages [4].

978-1-5386-1887-5/17/$31.00 ©2017 IEEE

C. Cloud

Quantum computing where Cloud is based, is the invocation of quantum simulators, emulators, or processors through the cloud. Quantum processing is accessed for the cloud servers. Cloud allows the accessed data is more easier than the users to process the data and store the data securely in own cloud or any third party server with various capabilities.

D. Cloud Security

The main threat in cloud computing is loss of data and leakage of information to the unauthorized person i.e., third party. Cloud computing is the merging of different computing entities, which are globally separated, but are connected electronically. Now a days geography of computation is facing towards the corporate servers, which brings a lot of issues in the security, like virtualization security, distributed computing, application security, identity management, access control and authentication [5]. The strong authentication of user is mostly useful for cloud computing to ensure that only user who have access can access to the server.

II. Proposed System

In this paper 3DES, DES, AES, and Blowfish algorithms comparison is conducted on the performance by using several various settings for processing different data filesizes i.e., from 100KB to 600KB to provide the algorithm's encryption/decryption time, throughput, and Avalanche effect of the one of the bit changes in the key and plain text in Cloud and Local environment, based on different performance metrics. Analysis is performed in local and cloud environment to identify the best environment using classical or quantum cryptography on various cryptographic algorithms by running different data file sizes using same metrics .

III. Methodology

A. Simulation and Settings

The simulation of the performance of DES, AES and Blowfish is done. For DES, AES and Blowfish available in java cryptography and java security, the implemention is performed. Based on the Cipher class which provides the main function of a cryptographic cipher which is used for encryption process and decryption process. Block ciphers are used to evaluate the results. Hence, the loaded data i.e., plaintext is divided into smaller block size.

B. System Parameters

The experiments are conducted using parameters like Performance and the Avalanche Effect. In the performance throughput of all the algorithms is calculated. In Avalanche Effect plain text change and key change are calculated. These experiments are performed so many times to measure the performance and avalanche effect.

C. Experiment Factors

Security features of each of the algorithm provides the strength against the cryptographic attacks. The factors determines the performance of the algorithm's and Avalanche effect based on encryption/decryption data blocks of various sizes.

IV. Results and Analysis

A. Quantum Results with cloud Environment

This section presents the results of various cryptographic algorithms integrated with BB84 protocol of Quantum Cryptography by considering the performance of metrics includes Encryption and Decryption time and Throughput when deployed in the cloud server.

(1) Performance

Table I. shows the computational time of various cryptographic algorithms with different file sizes varied from 100kb to 600kb integrated with BB84 protocol when deployed on cloud server. From fig. 1. it presents that TDES has better performance on Encryption and Decryption time when deployed on cloud compared to various cryptographic algorithms with very low computational time.

TABLE I. Encryption and Decryption with different file sizes

	100	**200**	**300**	**400**	**500**	**600**
DES	72	251	598	1927	2958	5997
TDES	71	253	584	1657	2405	4517
AES	70	281	615	1653	2815	4624
Blowfish	81	285	619	1702	2468	4839

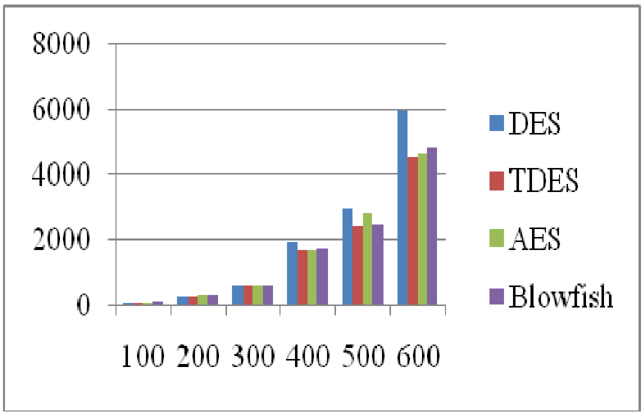
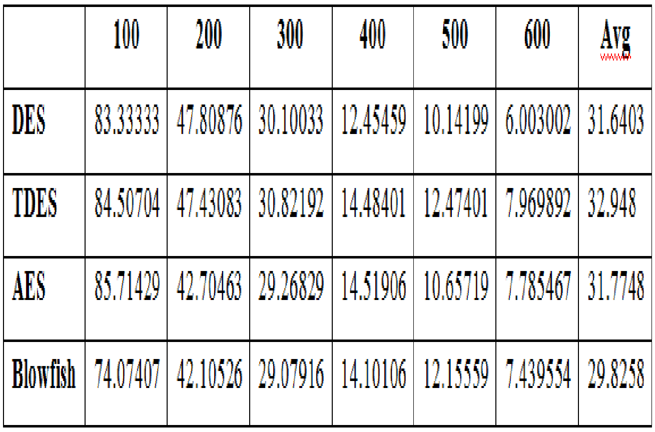


Fig. 1. Encryption & Decryption time with different file size

Table II. shows the computational throughput of various cryptographic algorithms with different file sizes varied from 100kb to 600kb integrated with BB84 protocol when deployed on cloud server. From fig. 2. it presents that TDES has better performance on throughput when deployed on cloud compared to various cryptographic algorithms with rate of 32.9 on average.

TABLE II. THROUGHPUT WITH DIFFERENT FILE SIZES



	100	200	300	400	500	600	Avg
DES	83.33333	47.80876	30.10033	12.45459	10.14199	6.003002	31.6403
TDES	84.50704	47.43083	30.82192	14.48401	12.47401	7.969892	32.948
AES	85.71429	42.70463	29.26829	14.51906	10.65719	7.785467	31.7748
Blowfish	74.07407	42.10526	29.07916	14.10106	12.15559	7.439554	29.8258

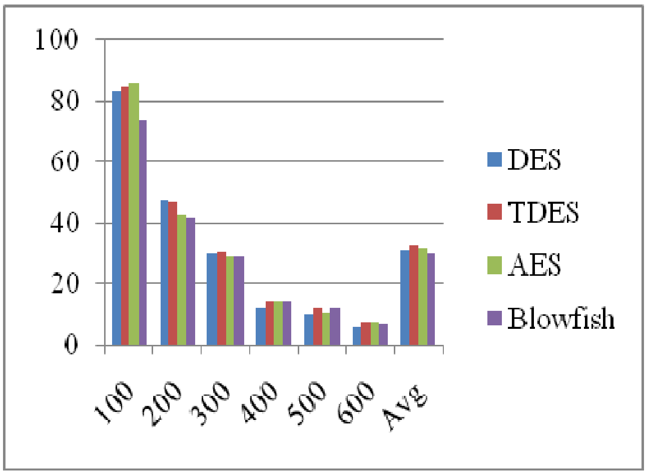


Fig. 2. Throughput with different file sizes

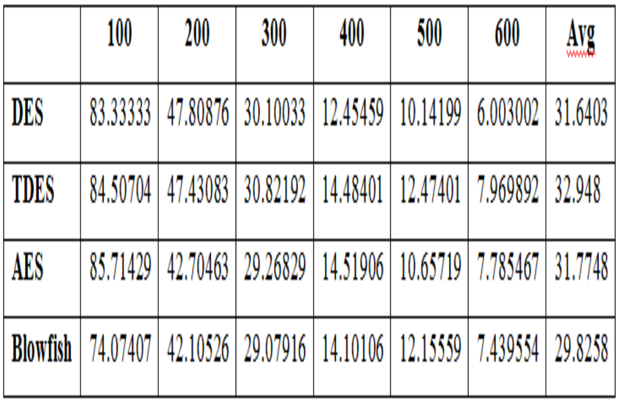
B. Quantum Results with Local Environment vs. Cloud Environment

This section represents the comparative analysis of various cryptographic algorithms integrated with BB84 protocol of Quantum Cryptography when deployed in both local and cloud environments.

(1) Performance

Table III. shows the computational analysis of Encryption and decryption time of various cryptographic algorithms integrated with BB84 protocol of Quantum Cryptography deployed on both local and cloud environment. From Fig. 3. the simulation results of cryptographic algorithms in cloud environment has better performance when compared with simulation results in the local environment.

TABLE III. ENCRYPTION & DECRYPTION WITH DIFFERENT FILE SIZES



	100	200	300	400	500	600	Avg
DES	83.33333	47.80876	30.10033	12.45459	10.14199	6.003002	31.6403
TDES	84.50704	47.43083	30.82192	14.48401	12.47401	7.969892	32.948
AES	85.71429	42.70463	29.26829	14.51906	10.65719	7.785467	31.7748
Blowfish	74.07407	42.10526	29.07916	14.10106	12.15559	7.439554	29.8258

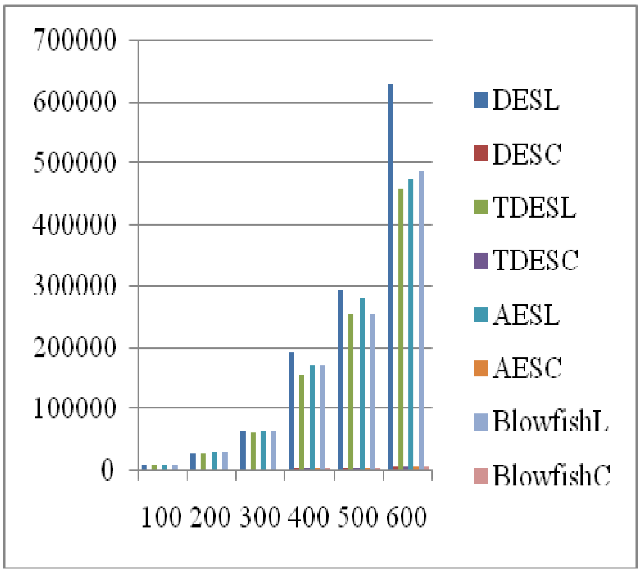


Fig. 3. Encryption & Decryption time with different file sizes

Table IV. shows the computational analysis of throughput of various cryptographic algorithms integrated with BB84 protocol of Quantum Cryptography deployed on both local and cloud environment. From Fig. 4. the simulation results of cryptographic algorithms in cloud environment has better performance with throughput rate when compared with simulation results in the local environment.

TABLE IV. THROUGHPUT WITH DIFFERENT FILE SIZES

	100	200	300	400	500	600	Avg
AESL	0.855431	0.414207	0.29073	0.141572	0.106907	0.075717	0.31409
TDESL	0.808952	0.445781	0.305141	0.152982	0.117968	0.078756	0.31826
DESL	0.820905	0.427548	0.296067	0.126668	0.102179	0.057399	0.30513
BlowfishL	0.733855	0.420816	0.289486	0.1411	0.117753	0.07383	0.29614
DESC	83.33333	47.80876	30.10033	12.45459	10.14199	6.003002	31.6403
TDESC	84.50704	47.43083	30.82192	14.48401	12.47401	7.969892	32.948
AESC	85.71429	42.70463	29.26829	14.51906	10.65719	7.785467	31.7748
BlowfishC	74.07407	42.10526	29.07916	14.10106	12.15559	7.439554	29.8258

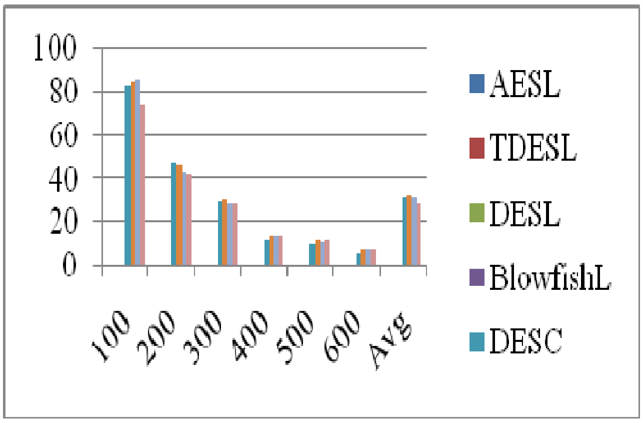


Fig. 4. Throughput with different file sizes

V. CONCLUSION

This paper illustrates the comparative analysis of various cryptographic techniques of Quantum Cryptography has performed to estimate the best environment among local and cloud environment. By this it is observation that cloud environment gives better performance and throughput compared to local environment.

REFERENCES

[1] Miss. Payal P. Kilor, Mr.Pravin.D.Soni,Wiedemann,"Quantum Cryptography: Realizing next generation", International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 2, February 2014.

[2] Aakash Goyal, Sapna Aggarwal and Aanchal Jain, "Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper", IEEE International Conference on Advanced Computing & Communication Technologies [ICACCT-2011] ISBN 81-87885-03-3.

[3] Ms. V. Padmavathi, Dr. B. Vishnu Vardhan, Dr. A. V. N. Krishna," Quantum Cryptography and Quantum Key Distribution Protocols: A Survey", 2016 IEEE 6th International Conference on Advanced Computing.

[4] Minal Lopes, Dr. Nisha Sarwade, "Simulation and Modeling approach for Performance Analysis of Practical Quantum Key Distribution" ,IEEE INDICON 2015.

[5] Zuriati Ahmad Zukarnain, and Roszelinda Khalid," Quantum Key Distribution Approach for Cloud Authentication: Enhance Tight Finite Key", International conference on Computer Science and Information Systems (ICSIS'2014) Oct 17-18 .