Enhancing the security of private cloud using distributed multilevel architecture using hybrid cryptographic algorithms.

[1] Akansha Singh, [2] Brijesh Pandey
[1] M.TECH (CS), [2] Asst. Professor, Dept. of Computer Science and Engineering
Goel Institute of Technology and Management
Dr. APJ Abdul Kalam University Technical Lucknow, India

Abstract: One of the most promising and highly accepted technologies in current scenario of modern IT sector can be named as cloud computing .as the technology is highly accepted, the security threats related to cloud are also increasing proportionally. The aim of the conducted research is to encrypt and decrypt data efficiently and effectively. This research paper presents a multilevel hybrid model for encrypting transmitted cloud data. This model uses the following encryption algorithms UTF8, DES, Triple DES, AES, MD5, and Rjindael algorithms to generate new cloud architecture that encrypt and decrypt transmitted data. The algorithm will help researchers and users to secure their transmitted data and prevent it from being stolen and will also provide new paradigms for future enhancement of cloud security.

Index Terms **- UTF8, DES, Triple DES, AES, MD5, encryption, decryption, cloud computing.**

I. INTRODUCTION

While storing data onto the cloud, integrity and confidentiality play a very major and crucial role. This research work addresses the privacy issue of storage in decentralized cloud, understanding and application of symmetric cryptography for data security. In cloud computing systems, the data is stored on remote servers that can be easily accessed through the internet. In current era, cloud computing is a rapidly growing technology that involves wide range of services and applications that is required in almost every field.

Cloud storage services are used widely to store and automatically back up arbitrary data in ways that are considered cost saving, easy to use and accessible. They also facilitate data sharing between users and synchronization of multiple devices. But, a huge amount of crucial data that is processed and stored in the cloud systems. Losing these valuable data will be having huge negative impact on the data owners being individuals or organizations. And so, there is an increasing demand of protecting data stored on the virtual cloud systems.

II. PRESENT WORK

Cloud has many benefits but despite these benefits that a user can get from cloud there exist numerous limitations. When speaking about public or private cloud storage, data is no longer in the hands of the user, it is actually stored on remote servers, and it is mostly spread around the globe.

1. According to Lo'ai Tawalbeh1, Nour S. Darwazeh2, Raad S. Al-Qassas2 and Fahd AlDosari1, in "A Secure Cloud Computing Model based on Data Classification", cloud security can be increased by implementing a multilevel architecture for cloud security at different modules with different ciphers. By this the processing time and cost can be reduced or certainly managed in case of highly confidential or least confidential data items. [5]

2. In the research by Min Li in his paper, "Format-Preserving Encryption for Character Data", the security of data on a cloud can also be managed through UTF8 encrypting and decryption on a secured cloud setup. [3]

3. In the paper, "Using cryptography algorithm to secure cloud computing data and services", Eng. Hashem proposed a model of cloud security which used a hybrid algorithm of AES and RSA cryptographic cipher for data security.[4]

4. According to Gaurav R.patel in his paper, "hybrid encryption algorithm", he proposed a cryptographic model using RSA encryption algorithm and merging the encrypted cipher with bitwise XOR operation to increase the complexity of the encrypted message. He proposed to encrypt the plain text by two different keys after dividing the plain text into two equal halves. This model used more encryption time but did not provide any extra security to the plain text. [6]

5. Another paper "Enhancement of cloud security and removal of anti-patterns using multilevel encryption algorithms", by Utkarsh gupta and Mrs. Shivani saluja proposed a model in which the encryption is done at multiple levels where the login name and password is encrypted by blowfish algorithm and the files or string using AES algorithm. [7SS]

III. THE PROPOSED SECURE CLOUD COMPUTING MODEL BASED ON DATA CLASSIFICATION

Cloud provides various benefits and advantages to its customers. As cloud provides immediate access to all the data been stored on cloud from any distant location from any remote device using internet to its authenticated user. The increasing volume of personal and confidential data requires more focus on storing the data on cloud securely. Data can be combination of financial transactions, important documents, and multimedia contents. Implementing cloud computing services may reduce local storage reliance and dependability in addition to reducing operational and maintenance costs. However, users still have major security and

privacy concerns about their outsourced personal data because of possible unauthorized access within the service providers and also by unreliable medium of transaction.

The proposed enhanced security framework implemented on asp.net using C# is an efficient security framework that incorporates the various security preserving cryptographic techniques at multiple level of security.

This model focuses on two distinct and mostly faced problem by the cloud user i.e. data security and feasibility of computing process. While uploading any string or file the biggest issue is data security from both internal as well as external threats. But encryption of each and every data item by highly secure algorithms is also not technically and economical feasible. Therefore we propose a model where the data is not only encrypted by randomly generated and user defined keys but also it provides the ability to classify the data stored in the cloud into various classes divided on the basis of its level of confidentiality.

This model helps the organization to individually on client end to classify data into various categories on the basis of the data privacy and confidentiality. The most important data is encrypted using hybrid algorithms whereas the encryption algorithm security and efficiency reduces on reduced priority of data. Various algorithms are used in this model which is AES, DES, 3DES, MD5, BLOWFISH, RIJNDAEL algorithm and UTF8.

The proposed model has classified data uploaded on cloud into following classes:

- Basic level - least confidential
- Secure level – needs a little bit of security
- Confidential level – contains important data of any organization.
- Highly confidential level- contains very important data of any organization or individual that requires maximum security.

IV. FRAMEWORK DETAILS

a) Basic level - least confidential: The basic level is used for encrypting general text, string, and sentence. This type of data does not need a very high level of security and confidentiality. Here, this level provides a basic/fundamental level of security and is used by most of the products/services available online. This module suggests uploading the data over the cloud storage using blowfish encryption and decryption.

b) Moderate Secure level – needs a little bit of security: This level contains private data such as documents and files. Secure level is designed for data with medium confidentiality degree like personal files, photos and strings etc. In this level, the encryption is done at the client end i.e. it is based on client side encryption. At this level we use AES and DES both individually. The symmetric-key block encrypting algorithm with a fixed block size of 128-bits and a key length of 128bits in AES.

c) Confidential level – contains important data of any organization. This level contains protected data of any organization or individual that needs to be protected from the unauthorized access of internal or external users. This level is not only protected by external cloud service provider but also by internal agents of organization having access to the cloud but not to the files existing in this module. This level is protected by Rijndael algorithm for file encryption and decryption. Here the files are encrypted and then uploaded on cloud and these cannot be decrypted without download of files by the client.

d) Highly confidential level- contains very important data of any organization or individual that requires maximum security. This level contains 3DES and MD5 in hybrid structure where the string encrypted by MD5 is again encrypted by 3DES and for decryption the cipher is processed by 3DES and again by MD5.due to multiple algorithms the security of this level is maximum as compared to the other modules.

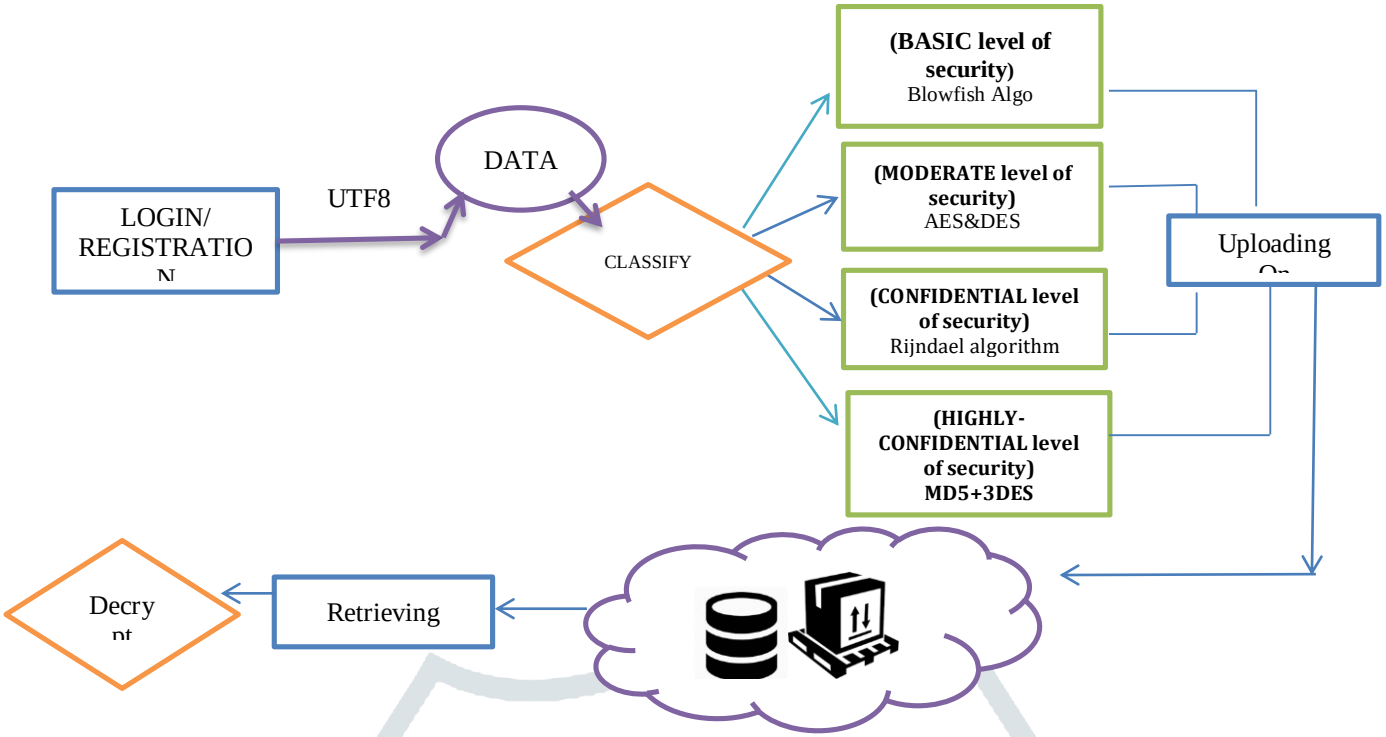

Fig 1: Proposed Model for data security

V. PERFORMANCE EVALUATION

We have built a simulator to evaluate the proposed framework. The simulator was developed using Microsoft .Net C# with the support of library System Security which is implemented within C# and using the default settings in Microsoft .NET Framework 3.5. We have done all necessary validations and verifications. All simulation experiments were conducted using the same platform: Intel(R) Core(TM) i3-5005U CPU, processor speed 2.00GHz, and RAM of 4 GB. The operating system is Microsoft Windows. We used the provided classes in Microsoft .Net environment to simulate UTF8 for login and registration and AES, DES, blowfish, 3DES , MD5 and Rijndael algo algorithm on multilevel architecture. Security library that provides the functionality of a cryptographic cipher are used for encryption and decryption of string and file stored at the cloud.

VI. DISADVANTAGES OF EXISTING SYSTEM

During the process of literature survey it is identified that till now there are many proposed models which are used as single or hybrid form of symmetric as well as asymmetric cryptographic algorithms. But each model focused on only providing security to each and every data uploaded onto the cloud. The level of security provided to each level is equal regardless the consideration of importance and privacy required to that particular data item. Each model provides a single modification of up gradation in the S-boxes or B-boxes or checks the efficiency of algorithms at a platform. Some of basic issues identified in the previous work are as follows:

- Implementing same cryptographic algorithm to each and every data being uploaded on the cloud without considering the importance or confidentiality of the data item.
- Implementing simple algorithm by modifying few steps or procedures lied in the traditional algorithm.
- Modification of cloud security by implementing traditional symmetric or asymmetric algorithm after processing the data by any classic substitution or transition cipher.
- Construction of simple models for evaluating the performance of each algorithm on different size of file or different bytes of string.

After the analysis of these issues in previous researches the proposed model is suggested in which several distinct algorithms are imposed on one single multilevel model constructed on asp.net framework.

VII. PERFORMANCE EVALUATION

We have built a simulator to evaluate the proposed framework. The simulator was developed using Microsoft .Net C# with the support of library System Security which is implemented within C# and using the default settings in Microsoft .NET Framework 3.5. We have done all necessary validations and verifications. All simulation experiments were conducted using the same platform: Intel(R) Core(TM) i3-5005U CPU, processor speed 2.00GHz, and RAM of 4 GB. The operating system is Microsoft Windows. We used the provided classes in Microsoft .Net environment to simulate UTF8 for login and registration and AES,

DES, blowfish, 3DES , MD5 and Rijndael algo algorithm on multilevel architecture. Security library that provides the functionality of a cryptographic cipher are used for encryption and decryption of string and file stored at the cloud.

VIII. DISADVANTAGES OF EXISTING SYSTEM

During the process of literature survey it is identified that till now there are many proposed models which are used as single or hybrid form of symmetric as well as asymmetric cryptographic algorithms. But each model focused on only providing security to each and every data uploaded onto the cloud. The level of security provided to each level is equal regardless the consideration of importance and privacy required to that particular data item. Each model provides a single modification of up gradation in the S-boxes or B-boxes or checks the efficiency of algorithms at a platform. Some of basic issues identified in the previous work are as follows:

- Implementing same cryptographic algorithm to each and every data being uploaded on the cloud without considering the importance or confidentiality of the data item.
- Implementing simple algorithm by modifying few steps or procedures lied in the traditional algorithm.
- Modification of cloud security by implementing traditional symmetric or asymmetric algorithm after processing the data by any classic substitution or transition cipher.
- Construction of simple models for evaluating the performance of each algorithm on different size of file or different bytes of string.

After the analysis of these issues in previous researches the proposed model is suggested in which several distinct algorithms are imposed on one single multilevel model constructed on asp.net framework.

IX. MODULES IN PROPOSED DATA SECURITY MODEL

The proposed model consists of following modules, where each is processed with regression and unit testing. Each module in the propose architecture has a significant role in the development of entire cloud simulator. The flow of data items between these separate modules is also validated usig passwords. The entire simulator consists of following modules:

- Login and registration
- About
- Basic level of security
- Moderate level of security
- Confidential level of security
- Highly confidential level of security

X. WORKING OF PROPOSED DATA SECURITY MODEL

The working of the proposed system can be understood with the help of some of its usage. Main usage that may help to understand the working of proposed data security model includes.

1. Key Management

Key management is one of the most crucial part of any data encryption. In the proposed model there exist both user defined key and randomly generated system key. These keys are used for encryption as well as decryption of data item whether string or file.

2. File Uploading

All the files or strings being uploaded on the cloud are encrypted and then uploaded onto the cloud system as these files need be securely placed upon the cloud architecture. The files / string reside on the cloud is encrypted/ encoded format. Even the cloud service provider cannot view these files before download i.e. decryption of files which is done at client end of the architecture.

3. File downloading.

The file download process contains the decryption algorithm fired on download click events. These files which are stored on the cloud in the form of encrypted data can only be viewed after decryption which is coded on client-side. This event can only be triggered by authorized data organizer or user of the cloud after the download command is fired.

XI. ADVANTAGES OF PROPOSED DATA SECURITY MODEL

The proposed architecture of cloud confirms the previous bugs and flaws are completely removed by the proposed architecture. The challenges and loop holes being observed during the literature survey of cloud security are tried to resolve to maximum extent.

i. The proposed architecture is designed by implementation of multiple cryptographic algorithms which makes the intrusion difficult and security somewhat higher than other previously proposed models.
ii. Data classification is the process implemented in proposed architecture of cloud that allows organizations and individuals to categorize/classify all different kinds of data, files and information assets according to its confidentiality degree, which will determine the extent of security the data needs.
iii. The proposed model consists of multilevel architecture, which enhances the efficiency of the overall cloud architecture.

iv. Levels implemented in cloud are different and independent of other levels proposed in the cloud.
v. The most confidential data is not encrypted by single algorithm rather hybrid architecture is proposed for security of highly confidential data.
vi. The files uploaded on the cloud are in encrypted manner and cannot be decrypted without downloading by the authorized user.

XII. ALGORITHMS FOR PROPOSED DATA SECURITY MODEL

The proposed hybrid and multilevel cryptography cloud architecture offer set of encryption algorithms:

1) Encryption of password by UTF-8.
2) Encryption algorithm using AES and DES algorithms.
3) Encryption algorithm using Blowfish algorithm.
4) Encryption algorithm using Rijndael algorithm.
5) Hybrid encryption algorithm MD5 and 3DES.

XIII. IMPLEMENTED MODULES OF PRIVATE CLOUD

The private cloud simulator implemented on .net framework 3.5. Version 2010 consists of a multilevel architecture in which each level is capable of encrypting and decrypting files using different symmetric key ciphers. The following image, fig 16 shows the basic view of the proposed cloud architecture:

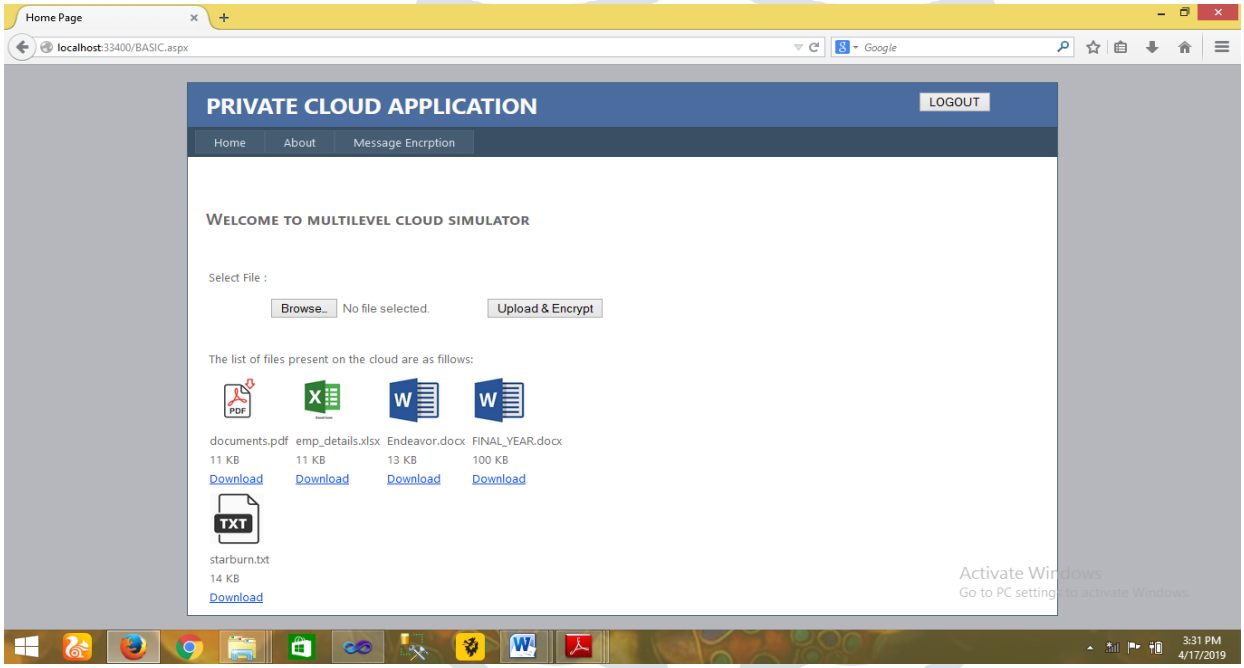

Fig 2: Basic view of proposed model on C# webpages.

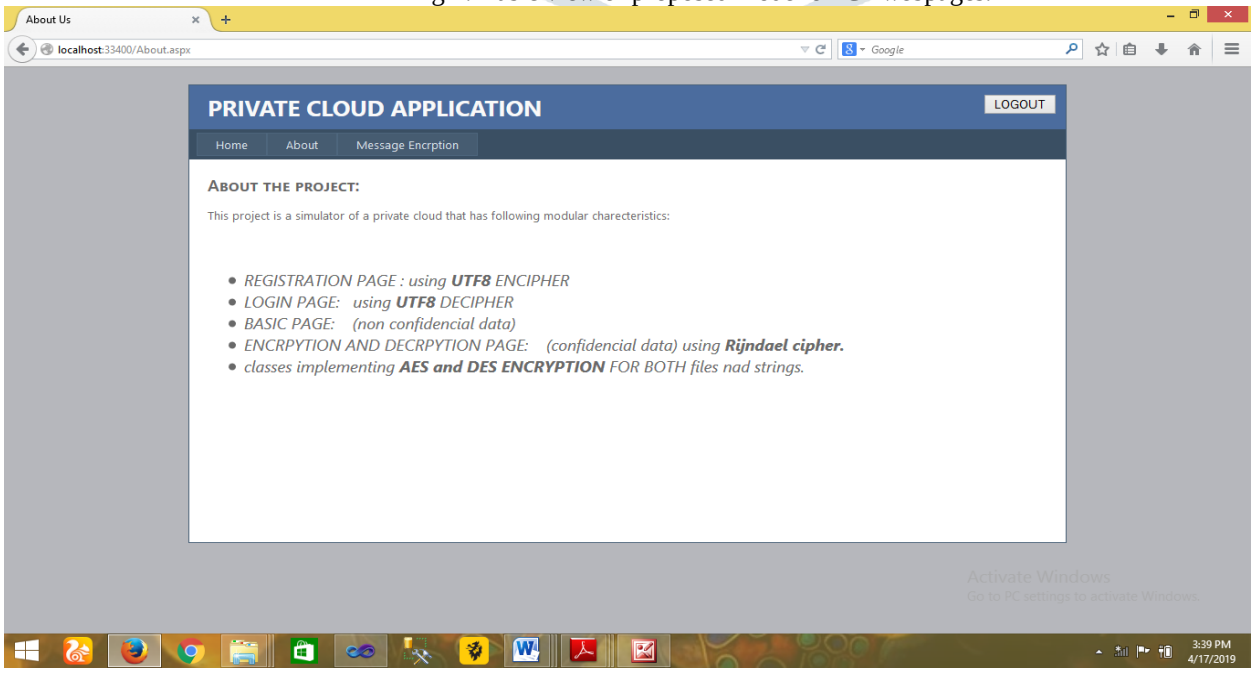

Fig 3: Elaboration of proposed model on C# webpages.

A. Experimental setup:

The experimental design was performed on a Core i3 machine with Windows 8.1 environment. The research was conducted in the suited environment according to the problem being investigated. Different file sizes were used ranging from 10 Kb to 20Mb for the performance analysis process. The language used to check the space and complexity was C# on asp.net platform. Time and space complexity depends on lots of things like hardware, operating system, processors, etc., but we have only taken execution time into consideration.

The aim of this work was to check the performance of different symmetric cryptographic algorithms on the basis of various parameters like encryption and decryption time, throughput, scalability, and security. All the implementations were done in the accurate manner to get the fair results. Exploratory research was used to evaluate these encryption algorithms and comparison was done on each of these algorithms.

B. Comparison between different algorithms:

The proposed model as shown in above figures is implemented on .net framework. All the algorithms (implemented individual or hybrid) are tested for their target approach of encrypting and decrypting the data and files on client side for finally uploading them on cloud platform. The performance matrix of each algorithm contains the encrypting, decryption and throughput of individual algorithm on the .net platform. Following tables contain the data collecting while testing and implementation of algorithms on cloud.

a) Encryption time taken by the algorithms:

Table 1: encryption time of all the algorithms in ms.

ALGORITHMS/ FILE SIZE	UTF-8 (ms)	AES (ms)	DES (ms)	BLOWFISH (ms)	RIJNDAEL (ms)	MD5+3DES (ms)
11 kb	0.0012	0.002	0.002	0.0008	0.001	0.027
16 kb	0.0012	0.029	0.023	0.0016	0.025	0.045
83 kb	0.0051	0.085	0.062	0.0042	0.072	0.68
108 kb	0.0062	0.574	0.468	0.0271	0.558	0.85
250 kb	0.0082	0.836	0.852	0.0294	0.852	1.13
500 kb	0.0099	1.021	1.005	1.056	1.001	2.55
5 mb	0.01	2.500	2.054	1.098	2.554	3.94
10 mb	0.11	3.780	3.020	2.058	3.720	3.93
15 mb	0.15	4.002	4.004	3.072	4.001	4.77
20 mb	0.5	5.472	5.432	4.221	5.452	4.79
Average	0.08018	1.8301	1.6922	1.15681	1.8236	2.2712

The following graph shows the encryption time of each algorithm with comparison:

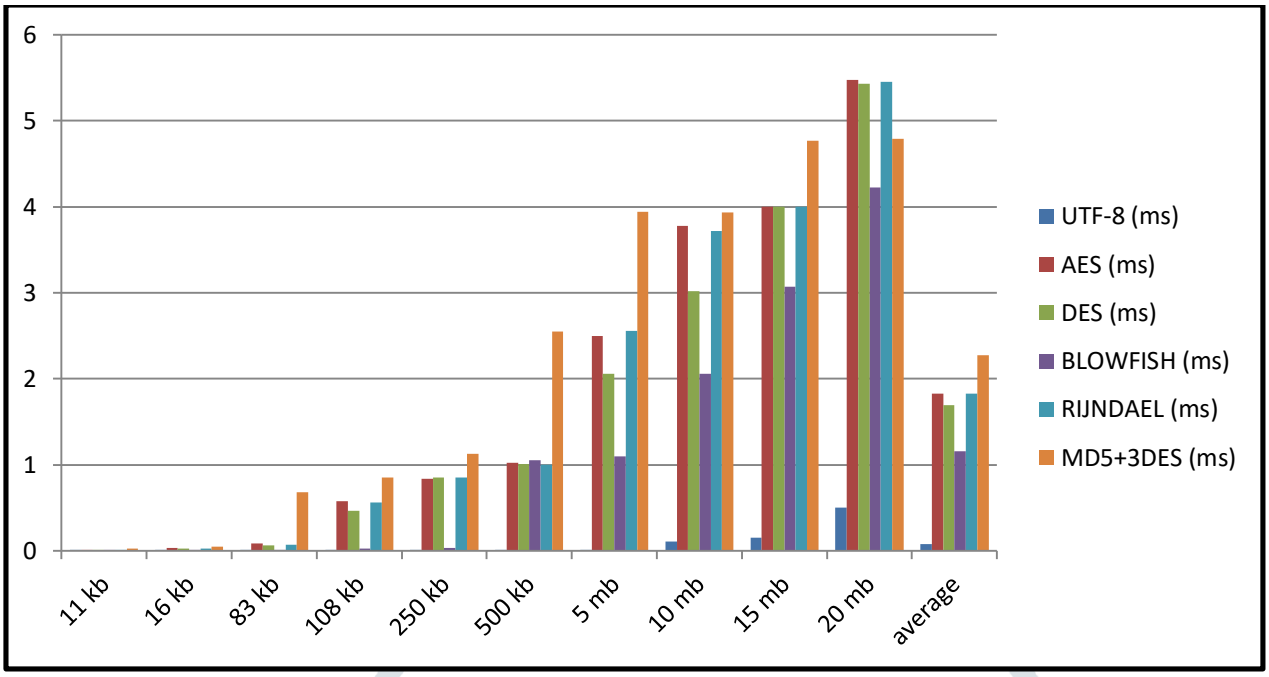

Fig 4: Graph comparing Encryption time of each algorithm.

b) Decryption time taken by the algorithms:

Table 2: Decryption time of all the algorithms in ms.

ALGORITHMS/ FILE SIZE	UTF-8	AES	DES	BLOWFISH	RIJNDAEL	MD5+3DES
11 kb	0.0017	0.0024	0.010	0.0017	0.0023	0.037
16 kb	0.0017	0.0026	0.016	0.010	0.0028	0.065
83 kb	0.0052	0.0116	0.032	0.151	0.0120	0.78
108 kb	0.0065	1.0216	0.046	0.162	1.0250	0.95
250 kb	0.0085	1.0310	1.005	1.017	1.0300	1.19
500 kb	0.0100	2.0334	1.062	1.262	2.0324	2.95
5 mb	0.0121	2.0441	2.065	1.782	2.0451	3.96
10 mb	0.1170	3.4721	3.078	2.084	3.4720	4.93
15 mb	0.1512	5.6510	3.871	2.92	5.6515	5.77
20 mb	0.5151	5.8212	4.889	3.97	5.8217	6.79
Average	0.0829	2.1091	1.6074	1.33597	2.10948	2.7422

The following graph shows the decryption time of each algorithm with comparison:

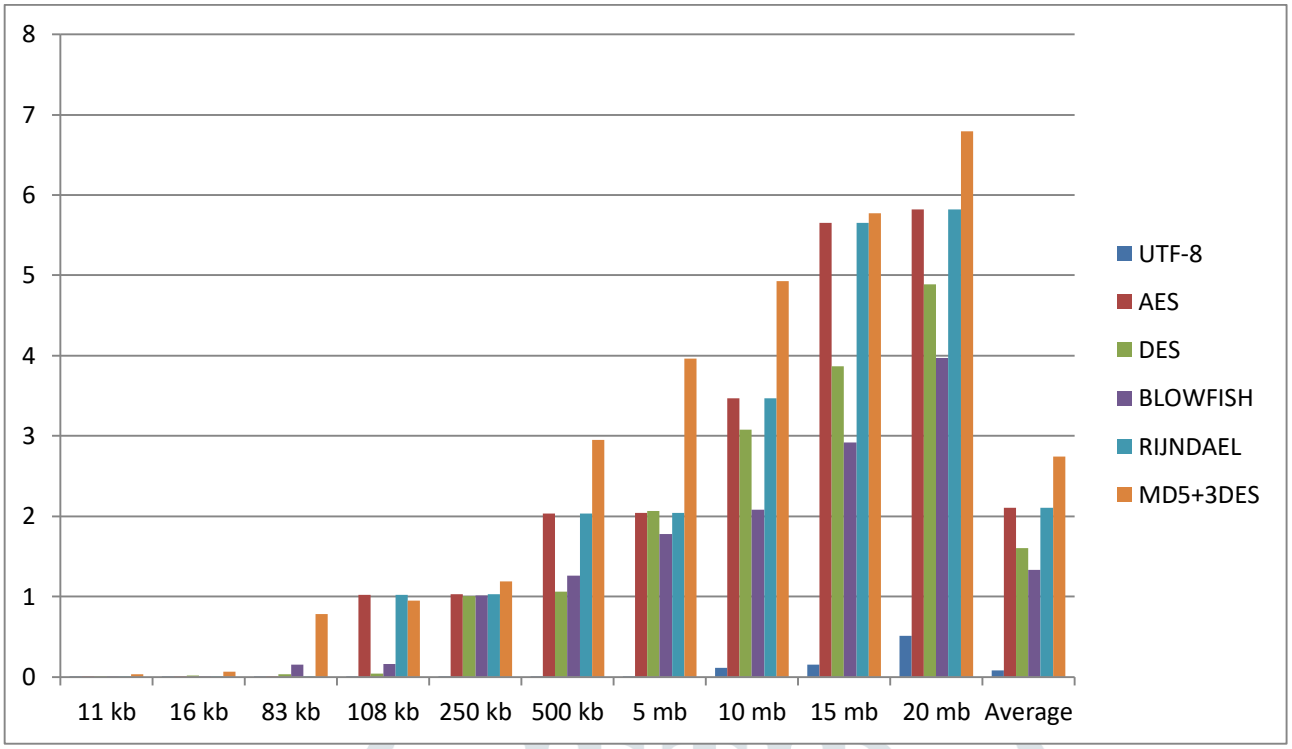

Fig 5: Graph comparing Decryption time of each algorithm.

c) Throughput of each algorithms:

Throughput refers to the amount of work that can be performed or the amount of output that be produced by a system or component in a given period of time. In context of ciphers, we may conclude throughput as the average of encryption and decryption of each algorithm compared to the file size it encrypts/decrypts.

Mathematically,

Throughput = total processing time/ file size. where,
Total time = encryption + decryption time.

Table 3: Throughput of all the algorithms.

ALGORITHMS/ FILE SIZE	UTF-8	AES	DES	BLOWFISH	RIJNDAEL	MD5+3DES
11 kb	0.00	0.0004	0.001091	0.000227	0.0003	0.005818
16 kb	0.00	0.001975	0.002438	0.000725	0.001738	0.006875
83 kb	0.00	0.001164	0.001133	0.00187	0.001012	0.01759
108 kb	0.00	0.014774	0.004759	0.001751	0.014657	0.016667
250 kb	0.00	0.007468	0.007428	0.004186	0.007528	0.00928
500 kb	0.00	0.006109	0.004134	0.004636	0.006067	0.011
5 mb	0.00	0.90882	0.8238	0.576	0.91982	1.58
10 mb	0.02	0.72521	0.6098	0.4142	0.7192	0.886
15 mb	0.02	0.643533	0.525	0.399467	0.6435	0.702667
20 mb	0.05	0.56466	0.51605	0.40955	0.563685	0.579
Average	0.01	0.29	0.25	0.18	0.29	0.38

The following graph shows the throughput of each algorithm with comparison:

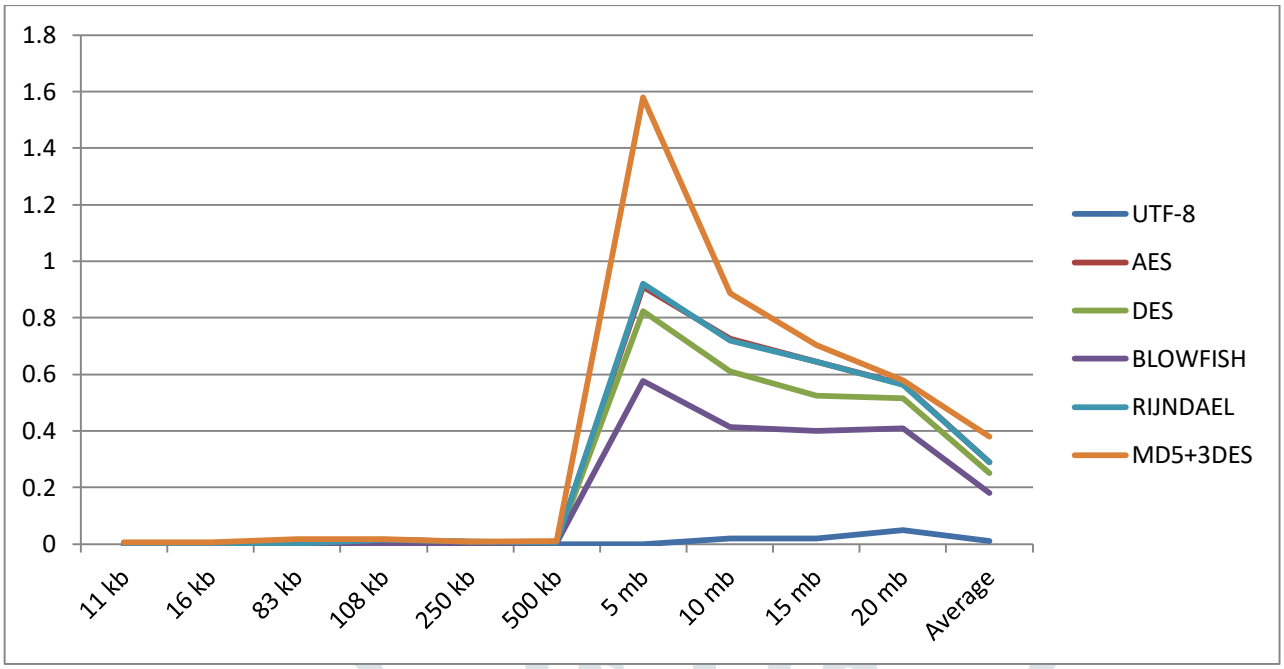

Fig 6: Graph comparing throughput of each algorithm.

d) Comparison and Security:

Table 4: Comparison of all the algorithms.

Factors	DES	3DES	BLOWFISH	AES	RSA	MD5	RIJNDAEL
CREATED BY	IBM in 1975	IBM in 1978	Bruce Schneier in 1993	Vincent Rijmen in 2001	Ron Rivest, Adi Shamir, and Len Adleman in 1978	Ron Rivest	Joan Deamen in 1997
KEY LENGTH	56 bit	128 bit	32-448 bit	128,192 or 256 bit	Depends on no f bits in modulus n	128 bits	128,192 or 256 bit
NO. OF ROUNDS	16	48	Variable (till all the P and S boxes are replaced)	10, 12 or 14	1	64	10, 12 or 14
BLOCK SIZE	64 bit	64 bit	64 bit	128 bit	variable	variable	128 bits
CIPHER TYPE	Symmetric cipher	Symmetr ic cipher	Symmetric cipher	Symmetri c cipher	Asymmetri c cipher	Hashing function	Symmetric cipher
SECURITY	64 bit	64 bit	64 bit	128 bit	Depends on no f bits in modulus n	128 bit MD	128 bit

C. Comparison between previous approach and our approach:

i. Distributed Multilevel Architecture Scheme: As declared by graph our Distributed multilevel architecture scheme is better than previous one because in our approach we use three type of architecture together which are for basic, confidential and highly confidential distribution of data which also beneficial for security purposes.

ii. Security Platform: For security platform we keep our data in different security zones. If any user wants to access the data he has to access the exact domain of data storage.

iii. Authentication: It is similar to all the other approaches of data security in cloud. Only authenticated users are allowed to access the data or enter the site. This is ensured by password authentication which is secured using UTF8 encoding.

iv. Role Based Access Control (RBAC):- In this only authenticated user can access the data. User cannot download the data which is uploaded by other user.

v. Multi algorithm Integration in single system:- In this our approach is stronger than previous ones. In this we use many algorithms but in previous approaches only limited algorithms are implemented.

XIV. RESULT

- The result show that the in the hybrid multilevel distributed cloud architecture encryption algorithm UTF8 has minimum encryption time and (MD5+Triple DES) takes the maximum time to encrypt the data comparing with other algorithms as shown in Table 4 and Fig.21.
- Also we may conclude that the decryption time of UTF8 is minimum and (MD5+Triple DES) is maximum by Table 5 and Fig 22.
- The experiment also justifies that the throughput of MD5+3DES is maximum as compared to all the other algorithms by Table 6 and Fig.23

REFERENCES

1. Akansha singh, “Cloud computing: A brief descriptive review along with its security issues and challenges”, IEEE International conference (IJAER) volume 14, number 2, Feb- 2019.

2. Akansha singh, “Descriptive analysis of cryptographic algorithms for securing cloud computing.”, JETIR February 2019, Volume 6, Issue 2 (ISSN-2349-5162)

3. Min Li, “Format-Preserving Encryption for Character Data”, JOURNAL OF NETWORKS, VOL. 7, NO. 8, AUGUST 2012

4. Eng. Hashem, “Using cryptography algorithm to secure cloud computing data and services”, AJER 2017 ISSN-2320-0936.

5. Lo’ai Tawalbeh1, Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari1 “A Secure Cloud Computing Model based on Data Classification”First International Workshop on Mobile Cloud Computing Systems, Management, and Security (MCSMS-2015).

6. GauravR.patel, “Hybrid encryption algorithm”, IJEDR volume 2 2014 ISSN:2321-9939.

7. Utkarsh gupta and Mrs. Shivanisaluja ,“Enhancement of cloud security and removal of antipatterns using multilevel encryption algorithms”, IJRAA 2018 ISSN:2349-7688.

8. G. Murali, “Comparison of cryptographic algorithm in cloud and local environment using quantum cryptography”, ICECDS-2017.

9. ShwetaKaushik, “Cloud data security with hybrid symmetric encryption”, International Conference on Computational Techniques in Information and Communication Technologies, 2016.

10. PrachiGarg,“Security Techniques for Cloud Computing Environment”, International Conference on Computing, Communication and Automation (ICCCA2017).

11. AkshayArora, “Cloud Security Ecosystem for Data Security and Privacy”, IEEE, 2017.

12. Julian Jang--Jaccard,“Cyber security threats in cloud computing”, Australian Journal of Telecommunications and the Digital Economy, 2013.