Using Hybrid Approach Based Cryptography Algorithm to Enhance the Data Security in Cloud Computing

Pushpendra Tiwari[1], Dr. Md. Vaseem Naiyer[2]

[1]Research Scholar,[2]Professor,
Dept. of Computer Science, Madhyanchal
Professional University, Bhopal

Abstract:The present era is completely the era of technology. In this era, usefulness of data is a very important aspect. All the data available in electronic form is being shared with the help of electronic devices. The creation of electronic data is also being done at a very fast and large scale, the security of which has emerged as an important aspect. The irregularity of the generated electronic data has become so much that checking it and maintaining it properly has become a challenging task. Due to this, its authenticity and security is an important aspect. It is also true that engineering is incomplete without data and electronic work is also proving to be incomplete. Understanding the need and importance of these electronic data, we also have to maintain their authenticity and quality by authenticating them. Cryptography technology also provides the facility to maintain the process of transfer of these electronic data consistently and to transmit the data without any irregularity. The process of cryptographic technology is a very important and essential aspect which cannot be ignored. Through cryptographic technology, the work of transfer and transmission of electronic data is completed in a normal manner without losing the data.

Keywords: Cryptography, Cloud computing, algorithms, Data Security etc.

I. Introduction:

Cloud computing is the use of remote servers hosted by third parties to store, process, and manage data. That is, cloud mainly refers to saving user's data in an offsite storage system that is maintained and managed by the cloud provider. This means that instead of storing the data information on the user's computer's hard disk or other storage device, the client stores it safely in a cloud database where the Internet provides the connection between the user's computer and the cloud server database. Cloud services are especially attractive to small organizations and startups. Cloud computing is the most popular topic of discussion in the information technology and research world today. The information technology world is expecting a big miracle. Small organizations and startups benefit from cloud services as they invest less in on-premises data center resources. Can start their operations faster. Cloud storage is the best option because it is a new utility computing model in which resources are pooled to provide the desired information as a service to many users by sharing existing resources. In this, we provide a secure hosting platform to the client to implement the services. Cloud computing is actually a combination of various traditional computing technologies such as distributed computing technology, grid computing technology, load balancing technology, virtualization technology, etc. It unifies all these functionalities and evolves into a new model that everyone can rely on for everything. The technology used for security in cloud computing is called cryptography technology. Cryptography technology is mainly of two types, symmetric cryptography technology and asymmetric cryptography technology. In symmetric cryptography technology, the sender of the message and the receiver of the message have the same key called the public key, is used to encrypt and decrypt data, whereas in asymmetric cryptography technically both have different keys. Public key for encryption and private key for decryption. Essential in cryptography is the process of hiding information so that only authorized users can receive and access it. The two operations in this process are encryption and decryption. Encryption is the process of converting plain text data into an incomprehensible cipher text by an encryption algorithm and then in the decryption process it is reversed to the original data by the decryption algorithm. As a result, data security and privacy can be ensured by using proper encryption and decryption mechanisms.

Cloud computing is a sophisticated technology that helps in managing data and applications as per the user's needs. Cloud computing is reliable and stable, so most businesses do not need to invest in or manage their own computer infrastructure. It provides resources such as applications, services, and software services to customers. Cloud computing is a capital saving technology for any type or size of business and organization, just like electricity bill water they have to pay for cloud computing resources as per their consumption. Cloud computing is famous for providing on-demand

network access to a pool of productive computer resources, namely the Internet, servers, and storage applications. It can be easily provided and discharged, with minimal management or service provider involvement. Most of the students, application developers, executives, and businessmen use cloud because it is simple and convenient. Although the cloud has many advantages, it also has some drawbacks, one of which is data security concerns. With cloud services becoming easily accessible and available to everyone, the possibility of sensitive information falling into the wrong hands is increasing. . Organizations cannot take risks with their sensitive information. Therefore, there is a need to solve the security issue of cloud computing. Cloud is beneficial because of its features like on-demand administration, resource pooling, broad net access, rapid flexibility and most importantly. Risk management, auditing and logging, data access controls, identity management, integrity controls, infrastructure, and dependency threats are all security concerns for cloud computing.

II. Classification of cryptography technique

Above we presented an idea of all the forms related to cryptography. Which will prove useful to understand and analyze various aspects related to cryptography? We will now present a discussion and discussion on various aspects of the following types of cryptography

a. symmetric-key cryptography

Symmetric key cryptography refers to an encryption technique through which any type of data can be encrypted and decrypted with the same key. Here it is simple and easy to exchange this cryptography key between the sender and the recipient. The best-known symmetric key cryptography system is the Data Encryption System (DES). It is a technique under which messages are encrypted and decrypted using the same key. In this type of encryption, both sides of the keys used are kept secret, thereby protecting them from attack by hackers.

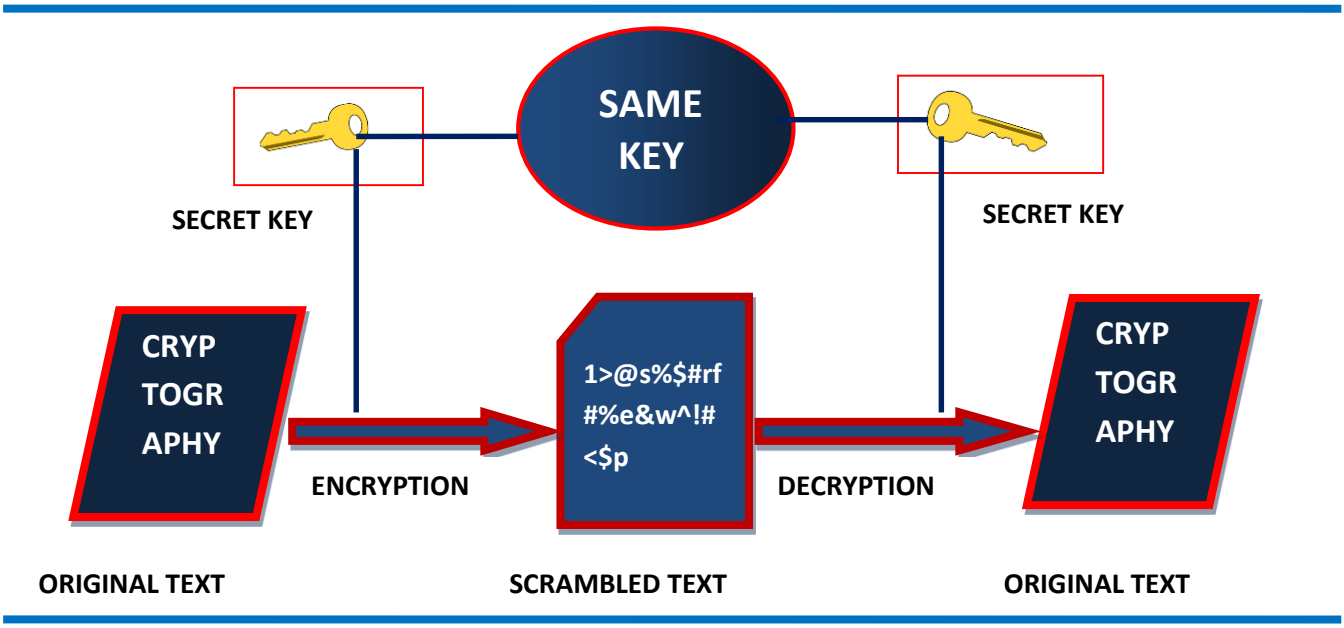

Figure 1 symmetric-key cryptography

The use of symmetric key cryptography requires this encryption of content made available on servers over the Internet, including securely accessing banking applications, UPI payments, and online browsing. Some of these applications are as follows:

Figure 2 The use of symmetric key cryptography

Payment Applications: Many online banking and UPI payment applications begin the process of verifying personally identifiable information before proceeding with your transaction to the applications at the time of access and payment. Through this, useful information is predicted to get rid of fraudulent activities and prevent cyber crime.
Securing personal data: When a website or server stores your personal information and your usage information, whether it is an organization or an individual, it is further protected by using this encryption. It is used to protect important information to prevent external attacks or espionage.
Secure Socket Layer (SSL) / Transport Layer Security (TLS) handshake: This helps prevent third parties, including your Internet Service Providers (ISPs), from intercepting sensitive data during website visits. Any organization uses these keys to ensure maximum security and exchanges encryption keys as needed. Symmetric encryption verifies the authenticity of the website's server, and provides the key to generate a session, rather than using an insecure HTTP website format.

b. Asymmetric-key cryptography

Asymmetric key cryptography is a technique that allows any type of digital content to be accessed by using two different keys called a private key and a public key. This type of encryption technique uses two different keys instead of one. There is no need to keep such keys secret because this key is used only once in a message, the same key can be reused multiple times, but it accepts only a particular condition. . Using this technology is comparatively a bit difficult, as any type of digital content can be unlocked using only two different keys. Here one key is used to perform the encryption operation and the other key is used for the decryption technique. Public keys are most commonly used for asymmetric keys. It also becomes very difficult to exchange these keys.

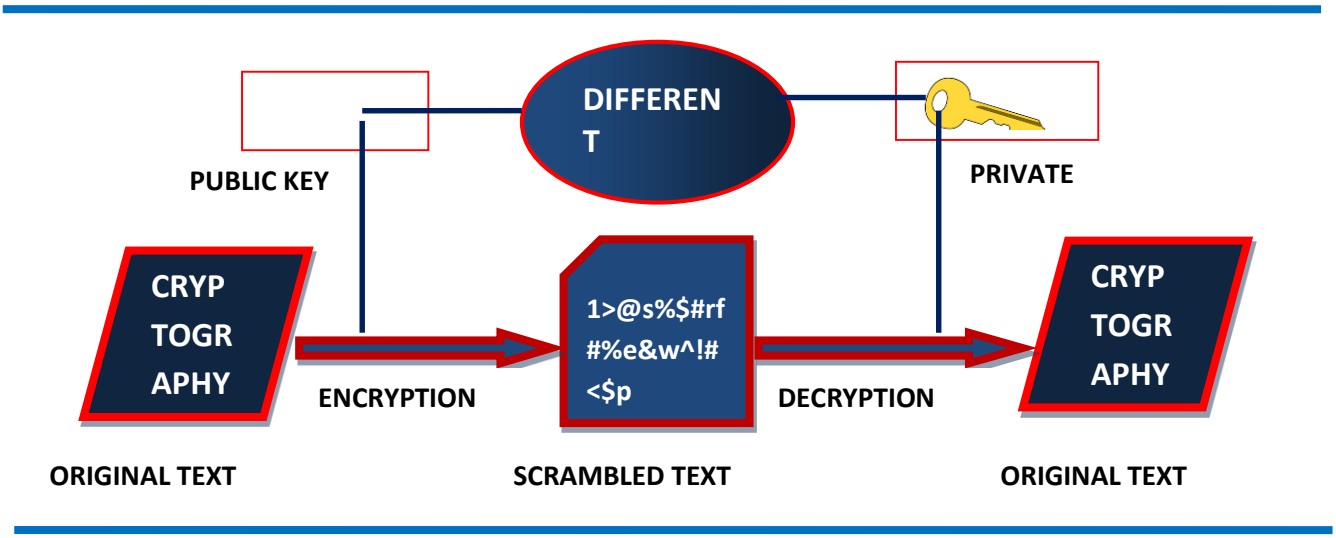

Figure 3 Asymmetric-key cryptography

Need for the use of Asymmetric Key Cryptography Complete Introduction to Asymmetric Key Cryptography In this process of verification is adopted for authentication. Some of the applications for this task are as follows:
Digital Signatures: With the help of asymmetric key cryptography techniques it is possible to verify the authenticity of the origin and signature of all types of digital content documents.
TLS/SSL Handshake: Asymmetric key cryptography is used to verify the authenticity of a website's server and exchange the required encryption keys and generate a session using those keys to ensure maximum security. It plays an important role in providing security instead of insecure HTTP website format.
Crypto currency: Block chain algorithms are used through asymmetric key cryptography for the purpose of making crypto currency transactions untraceable and maintaining the integrity of its decentralized architecture.
Key sharing: This cryptography technique can also be used to exchange hidden keys for symmetric encryption, as keeping such keys individual is very important for this system.
Access Control: Using access control, cryptography ensures that only groups with proper credentials have access to a resource. Only people with the appropriate decryption key can access the resource for this type of encryption.

Protection from Hackers: Cryptography is a very important technology for online communication. It provides a secure technology for transmitting any personal information such as passwords, bank account numbers and other sensitive and private data through the Internet.
Protection against attacks: Cryptography technology works to protect against a variety of attacks, including replay and man-in-the-middle cyber attacks. This technology enables a variety of strategies to detect and prevent different types of attacks.
Compliance with legal requirements: Cryptography is also able to help companies meet various legal requirements to provide data security and privacy.

III. Research Methodology

Any research work is incomplete without research methodology. It is an essential task to use one or the other research method to complete the research work. The research methodology used in the present research work is as follows:

- Analytical Research Methodology
- Applied Research Methodology

Analytical research method has been used to analyze the traditional cryptographic techniques, with the help of which a comparative study has also been presented. Applied research methods have been used to enable the implemented cryptographic algorithms to be implemented. In between both the methods, quantitative and qualitative research methods have also been used. Qualitative research method has been used to perform and apply the quantitative and presented algorithms to conduct research work based on the quantity of different algorithms in the analysis of traditional algorithms. With whose help only success has been achieved in reaching a certain result.

IV. DES algorithm:

DES is a symmetric algorithm. Under this, a key is used to complete the process of encryption and decryption. DES is a block cipher algorithm, through which data is encrypted in 64 bit block plaintext. A 64-bit block is input from one end of the algorithm, and comes out of a 64-bit block at the other end. The key length is 56 bits. The key is usually used as a 64-bit block, but every eighth bit is used for a parity check. This parity bit operates on the smallest and most significant bit of the key bytes. Here i can be any 56-bit number and it can be changed at any time. Some rare numbers are considered weak keys, but this can be easily avoided. In this, all the security lies inside the key itself.
To understand it simply, this algorithm is a combination of two basic techniques of encryption, obfuscation and propagation. The basic building block of DES is a single combination of keys, known as a round. This involves applying the same combination of techniques to the plaintext block 16 times for a total of 16 rounds. This algorithm works on numbers 1 up to 64 bits using standard arithmetic and logical operations.
This can be understood in detail through the following diagram:

L= Ri-1
R1 = Li-1
F(R-I Kt)

V. RSA Algorithm

Encryption is a process by which the original message (plaintext) is converted into an unreadable format (cipher text). Through this the original information is hidden. Decryption The encrypted information is converted into plaintext. This type of overall process is called cryptography process. The process of cryptography also uses two keys, one private key and the other public key. The person obtaining the public key can send and receive encrypted messages over any

communication medium. However, the recipient can only decrypt the received message with the private key. On the basis of key value, the cryptographic process is divided into two parts which are symmetric and asymmetric respectively.

RSA is public-key cryptography method (Sangwon et al. 2020). It uses two keys for the encryption and decryption process. The algorithm steps are: It uses private key, public key. It uses two prime numbers p, q:

Step 1: n = p*q 5.1

Pi (n) = (p-1) (q-1); Here pi (n) is calculated 5.2

"e" is a public key , "d "is a private key is calculate by the following expression
Step 2: d*e mod (pi) =1 5.3
The encryption is shown by the following expression
Step 3: M"= M e mod n; M" cipher text, M plain text, Public key (e, n) 5.4
Step 4: The Decryption expression is as follows
M= M "d mod n; M" cipher text, M plain text, Private Key (d, n)

The RSA algorithm is an algorithm that provides greater strength to the symmetric key encryption technique and provides confidentiality during communication.

VI. Hybrid approach based cryptosystem Algorithm (HBCA)

This chapter deals with crypto systems developed on hybrid basis. It also provides detailed introduction on the process of key generation, encryption, decryption of RSA algorithm, DES algorithm. An explanation of the experimental results demonstrating the performance of the proposed model is also provided here. Finally, performance analysis, requirements, total execution time, energy consumption and comparative study and analysis against security attacks are presented. Relies on HBCA to complete the modern treatment process under remote e-health care. Persons with malicious intent do not have access rights, so physical sensory data is used. Cryptographic techniques are used to maintain the confidentiality of the data being transmitted. At present, the use of new quantum computers easily breaks the factorization of prime numbers of the traditional RSA algorithm. The proposed method uses four prime numbers to complete the process of encryption and decryption, in which the secret quantum key is used. This HBCA algorithm is at best difficult or impossible to break**:**

Step 1 Select p and q, r, s, all four of the prime numbers, p, q, r, s being different 5.5
Step 2: Calculate n = p ∗ q ∗ r ∗ s 5.6
Step 3: Calculate Pi(n) = (p-1) ∗ (q -1)∗(r-1) ∗(s-1) 5.7
Step 4: Choose random variable "e" value and "e" is public key value
Step 5: "e" is a public key, "d "is a private key is calculate by the following expression d*e mod Pi(n)=1 5.8
Step 6: QK is a secret quantum key generated with the help of enhanced BB84 quantum cryptography protocol
Step 7: Encryption Process C=(Me mod (n))QKmod n 5.9
Step 8: Decryption Process M=(Cd mod (n))QK mod n 5.10

The internal process flow of the proposed technique is shown in Figure 5.2. In its first step, it has been clarified that four prime numbers are selected to provide high confidentiality in body sensed data transmission. The n value is then calculated using equation 5.6.
Pi (n) is then calculated using equation 5.7. Here "e" is a public key value and "d" is a public key value. The value of the private key is determined through Equation 5.8, while the value of the public key is usually selected manually. The secret quantum key is generated based on QK EBB84QCP. The process of encryption and decryption is completed using equations 5.9 and 5.10.

VII. (1). Text Encryption

Full Encryption Algorithm is used for encrypting the multimedia files to get the simple data. Traditional algorithms are not suitable for encrypting very large files and highly redundant data. Under the presented research work, such a model has been designed that it is able to perform the required task closely on the basis of selective encryption scheme in file encryption and decryption time, file size and throughput. In this study, a randomly generated text file has been prepared to complete the task of encryption and decryption. Processes files of file sizes up to 5, 10, 15, 20, 25, and 30 KB respectively, received as input. This word count is 758, 1516, 2274, 3032, 3790, and 4548 and character count is approximately 5097, 10194, 15291, 20388, 25485, and 30582 KB. The parameters considered for encryption and decryption of commonly received files are as follows:
Input: Text File (.txt)

Output: Encrypted file
Implementation Model: Block-Based Encryption Model
Comparison: AES, DES, RSA, and Blowfish
Evaluation: File size and Encryption time.

Table 1.Text Encryption

Size Indexing		
5KB	**10KB**	**15KB**
0000-0234	00000-00585	00000-00936
0234-0468	00585-01170	00936-01872
0468-0702	01170-01755	01872-02808
0702-0936	01755-02340	02808-03744
0936-1170	02340-02925	03744-04680
1170-1404	02925-03510	04680-05616
1404-1638	03510-04095	05616-06552
1638-1872	04095-04680	06552 -07488
1872-2106	04680-05265	07488-08424
2106-2340	05265-05850	08424-09360
2340-2574	05850-06435	09360-10296
2574-2808	06435-07020	10296-11232
2808-3042	07020-07605	11232-12168
3042-3276	07605-08190	12168-13104
3276-3510	08190-08775	13104-14040
3510-4985	08775-10045	14040-15169
20KB	25KB	25KB

Figure 4 Present the original text file of size 5kb, encrypted using the proposed model and next image is encrypted file which shows that all are taken in stream cipher for the encryption.

(a) Plaintext (b) Ciphertext

On the basis of text file size (KB) Table no. A comparative study has been presented at 3.2. The proposed model compares the results based on encryption with those obtained through traditional algorithms. The performance obtained by the presented model has been evaluated mainly on the basis of two properties, firstly, on the basis of the size of the encrypted file and secondly, on the basis of the time taken to encrypt the multimedia file.

Table 2 Text Encryption

Plain text size in	Cipher text size in (KB)			
KB	Blowfish	AES	DES	RSA
5	6.76	6.86	6.86	5.21
10	13.52	13.70	13.70	10.27
IS	20.27	20.55	20.55	15.43
20	27.03	27.39	27.39	20.89
25	33.78	34.25	34.25	25.79
30	40.5	41.09	41.06	30.51

The encryption algorithm exhibits an extension of the size of the cipher text. Here different algorithms have been worked out for encrypting a plaintext of size 5 kb and generate cipher texts of size 6.76 kb by Blowfish, 6.86 kb by AES and DES and 5.21 kb by RSA. As a result, it is found that the RSA algorithm produces smaller cipher text size files than other traditional algorithms and requires less memory for secure storage. Figure 3.6 below shows the average percentage increase in cipher text size.

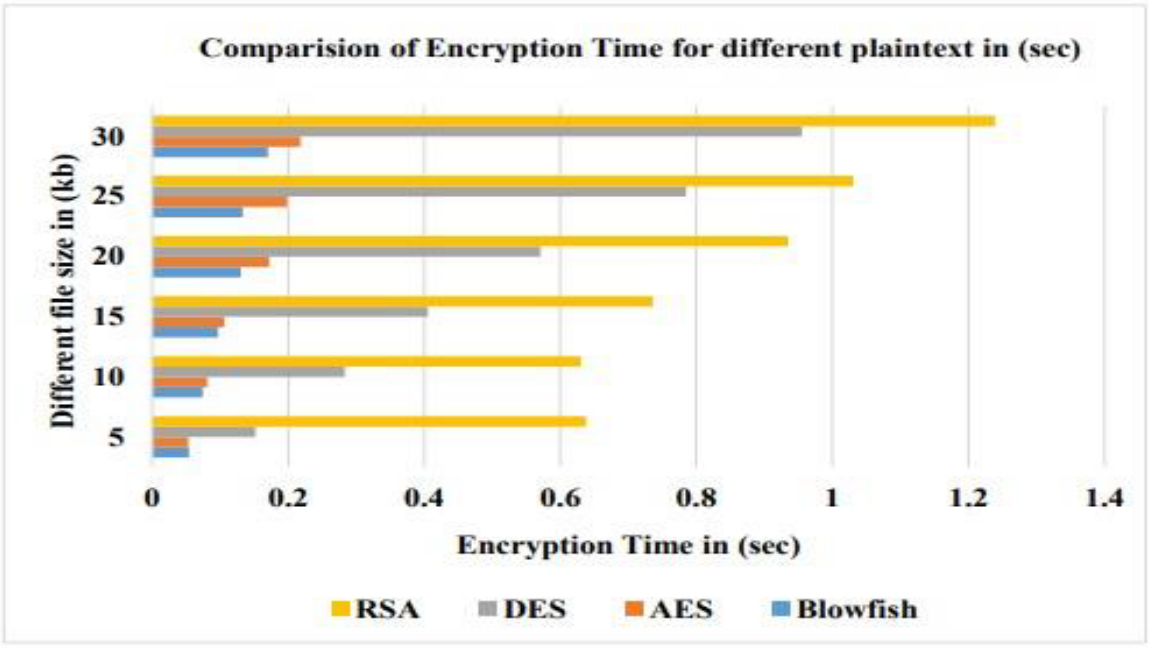

Figure 5 Comparison of Encryption Time (sec) for deferent algorithm

VII . (2). Image Encryption

Under the proposed model, the work of testing has also been done by saving the image under different types of multimedia applications. The present study is based on the format encryption of image .jpg. Here the benchmark of the image has been downloaded from the website named http://www.imageprocessingplace.com/root_files_V3/image_databases.htm and the work of encryption has been completed on these images. The task of storing the pixel value of the image has also been completed. A comparison of the pixel values of the original and encrypted images is presented to demonstrate the process of image encryption. Here four grayscale images of size 256 × 256 namely cameraman, house, lina and mandrill are used. The following parameters have been used to complete the encryption and decryption of image files:
Input: Image file (.jpg)
Output: Encrypted file
Implementation Model: Block-Based Encryption Model
Algorithm: AES, Blowfish, XOR, and RSA
Key Size: 256 bit
Evaluation: File size and Encryption time.

Table 3 Image Encryption

Cameraman	House
00000-16380	00000-32760
16380-32760	32760-65520
32760-49140	65520 -98280
49140-65520	98280-131040
65520-81900	131040-163800
81900-98280	163800-196560
98280-II4660	196560-229320
I14660-131040	229320-262080
131040-147420	262080-294840
147420-163800	294840-327600
163800-180180	327600-360360
180180-196560	360360-393120
196560-212940	393120-425880
212940-229320	425880-458640
229320-245700	458640-49I400
245700-262750	491400-525106
Lena	Mandrill
00000-16380	00000-16380
16380-32760	16380-32760
32760-49140	32760-49140
49140-65520	49140-65520
65520-81900	65520-81900
81900-98280	81900-98280
98280-114660	98280-114660
114660-131040	114660-131040
131040-147420	131040-147420
147420-163800	147420-163800
163800-180180	163800-180180
I80180-196560	180180-196560
196560-2I2940	I96560-2I2940
2I2940-229320	212940-229320
229320-245700	229320-245700
245700-262598	245700 -262750

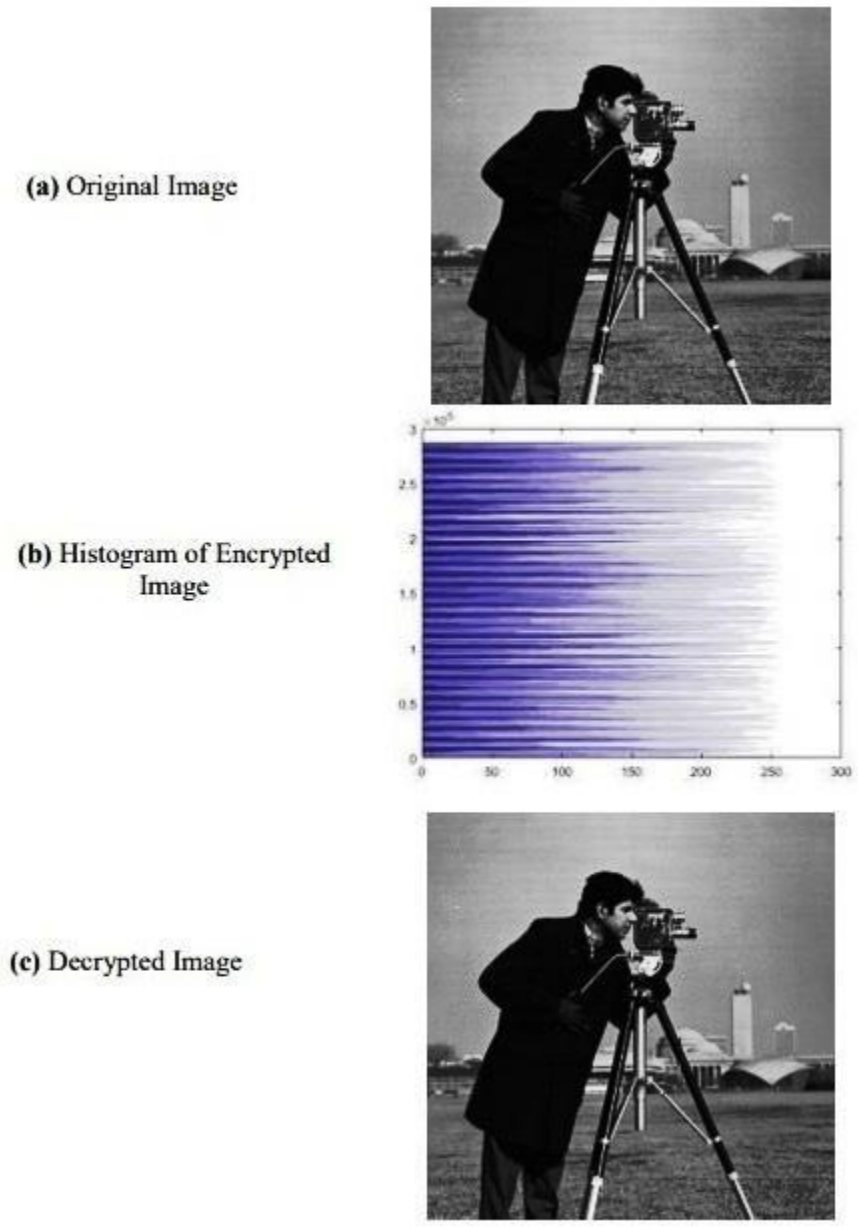

Figure 6 Encryption and decryption of camera man image

File Name Resolution (256 x 256)		Size in (kb)		Cipher text Size in (kb)	
Blowfish	AES		XOR	RSA	
Cameraman	112	242	254	125	230
House	45	119	120	120	98
Lena	116	259	267	129	242
Mandrill	76	167	179	128	145

Table 4 Image Encryption

The size comparison of original and encrypted grayscale image is given in Table no. Displayed under 3.5. As a result of this comparative study, it is found that for different core sizes such as 112, 45, 116, and 76 kb, the Blowfish algorithm produces cipher texts of 242, 119, 259, and 167 kb, the AES algorithm yields cipher texts of 254, 120, 267, and 1. generates a file size of 79 KB, the XaOR algorithm produces cipher tests of 125, 120, 129, and 128 KB, and other traditional techniques related to lower size, the RSA technique produces cipher test as of 230, 98, 242, and 145 KB.

HBCA Working with Text Data

Table 4.1 - Encryption of Text Data Plain Text	P	N	A	K
Key	369&			
Add Key into Text	369&PNAK			
Ascii code	51545738801106575			
Binary code	00110011 00110110 00111001 00100110 01010000 01101110 01000001 01001011			
1st complement	11001100 11001001 11000110 11011001 10101111 10010001 10111110 10110100			
Decimal value	204201198217175145190180			
Segregate BY 4	30211261+3$1/2-0			
Cipher text	30211261+3$1/2-0			

Table 5 - Encryption of Text Data

Cipher text	30211261+3$1/2-0
Key	369&
Add Key into Text	369&30211261+3$1/2-0
Ascii code	3216+$/-
Multiplication by 4	204200196216172144188180
Binary code	11001100110010011100011011011001101011111001000110111111010110100
1st complement	00110011001101100011100100100110010100000110111001000000101001011
Decimal value	801106575
Plain Text	PNAK

Table 6 Decryption of Text Data

HBCA Working with Image Data

Image File	Image Size	Binary Form	Original Message	Password	Cipher Text (PKA)
Baboon.png	43.7KB	00110001001100 10 00110011001101 00 00110101001101 10 01010100011011 11 00100000011000 11 01101000011000 01 01101110011001 11 01100101001000 00 01110100011010 00 01101001011100 11 00100000011011 00	To change this license header choose License Headers in Project Properties	123456	3231302 32221*3 $073’0 %3’2$1 &0&273 ”3%3% 2#073$3 %2’0&2 $1#0&2 73%3& 2’2&3&

Table 7- Encryption of Image Data

VIII. ER Diagram of model

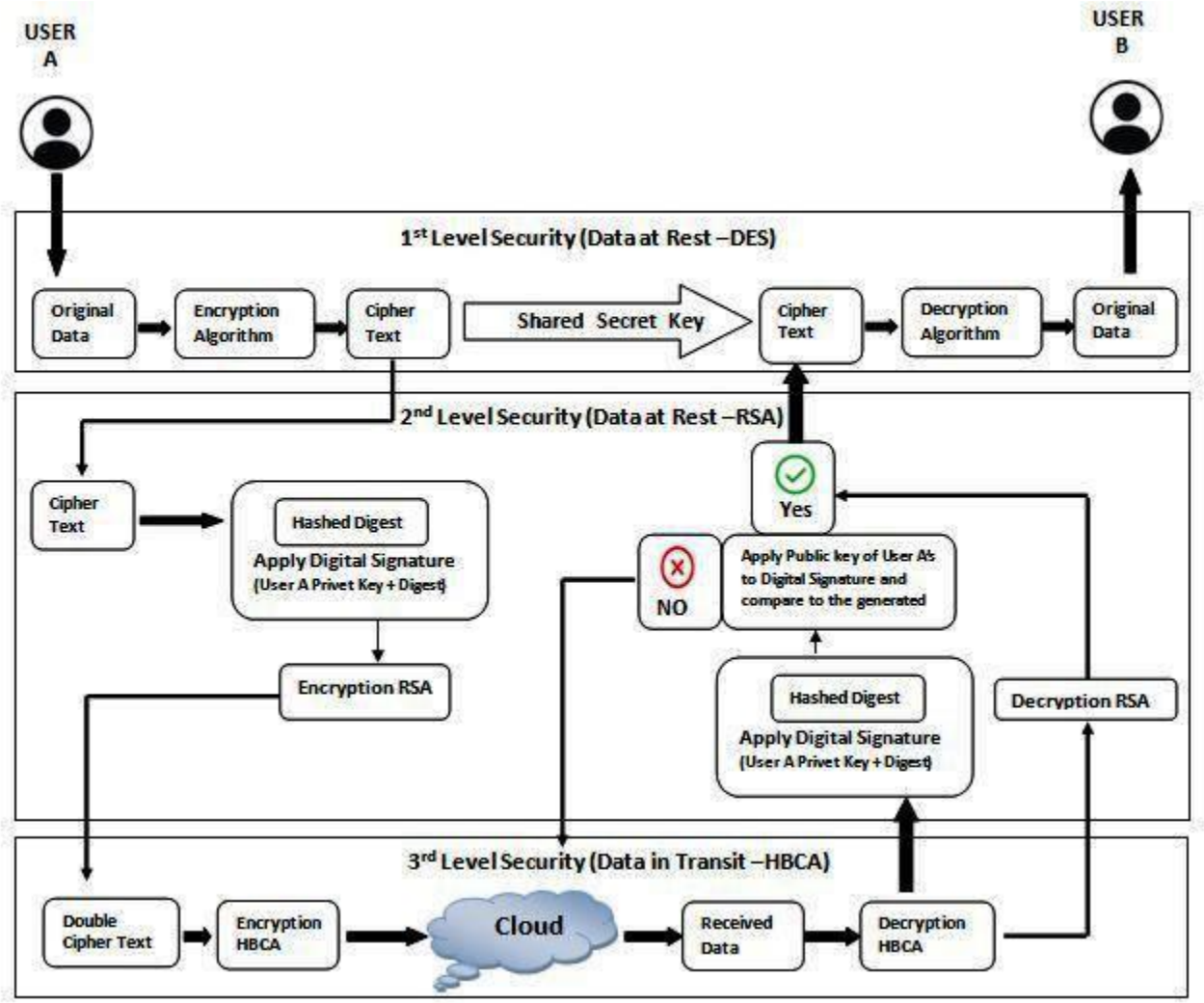

Figure 7 ER Diagram of RSA, DES and HBCA

IX. EXPERIMENTAL RESULTS

The experimental results of the hybrid algorithm are shown here. This proposed system assumes the value of key size as 64, 96, 150, 208, 298 for key generation, encryption and decryption process. The performance of the proposed model has been evaluated through important factors such as key generation time, encryption time and decryption time, memory requirement, total execution time and energy consumption. The system is evaluated to be robust against brute force attacks, timing attacks and mathematical attacks. Key Generation HBCA (Hybrid Approach based cryptographic algorithm) is a major algorithm, under which a strong key is created which increases the security of the entire system. The proposed model uses four primes to complete the key generation process, and in addition, a secret quantum key is included in the encryption and decryption process. Four prime numbers and their mathematical calculations take more time which is safer in HBCA.

Cryptographic Algorithms	Key Size (Bits)	Key generation time (ms)	Encryption time (ms)	Decryption time (ms)	Total Execution time (ms)
	65	167	480	922	1549
	98	194	820	1478	2455
RSA	155	273	1110	1876	3212

	215	391	1356	2198	3978
	299	486	2756	2788	3989
DES	65	176	490	912	1539
	98	188	840	1434	2465
	155	288	1120	1856	3213
	215	399	1378	2199	3945
	299	488	2766	2798	3899
Proposed system HBCA	65	218	867	1698	2756
	98	267	1278	2397	3978
	155	423	1456	2978	4823
	215	552	1566	3598	5678
	299	698	3619	5919	10229

Table 8 EXPERIMENTAL RESULTS

Comparative study and analysis between the three RSA, DES and HBCA has clarified that the proposed method takes more time to execute as compared to RSA whereas in HBCA the process of key generation, encryption and decryption is more complex. There is calculation. This can increase the total execution time of HBCA. Yet there are only two prime numbers in RSA, DSA. Therefore, this can be executed in less time as compared to the proposed method.

X. COMPARATIVE ANALYSIS AGAINST SECURITY ATTACKS

Cryptography is the science of designing an unreadable format of the plain text, which can be used by different types of attackers to break the cipher text in different ways and the plain text can be recovered from the encrypted text. In general, the main attacks in RSA cryptosystem are as follows:

- Brute force attacks
- Timed attacks
- Mathematical attacks

Attacks	**RSA**	**DES**	**Proposed system HBCA**
Brute force Attacks	Yes	Partial	No
Timing Attacks	Yes	Yes	No
Mathematical Attacks	Yes	Yes	No

Table 9 Comparison of security attacks

The above Table 5.7 shows the comparison of security attacks in RSA, DES and HBCA. Also included are robust methods to protect against brute force attacks, timing attacks, and mathematical attacks. The proposed system is suitable for sensitive information communication system.

XI. Conclusion

The presented research work is completely focused on creating an algorithm to streamline the secure transfer process of digital content generated in the field of cloud computing. At present, various types of electronic data are being produced, which have become very important in human life. Security of transfer and transmission of generated electronic data has become an important and challenging task. Through this research work, a review of various literature related to watermarking has also been presented, which makes it clear what and how much is the result of the work done in this field. How is this research work different from other research works? The relevance of the presented research work has been presented only after reviewing the related literature and the direction and condition of the research has been decided. An analysis of various traditional techniques is presented, providing a clear picture of the

right direction to take to overcome the shortcomings of cryptographic algorithms currently being implemented. Analysis of different methods as a solution to any type of problem is an important and useful task, which helps in reaching the right result. An in-depth analysis of both availability frequency based and location based methods has been presented, which has helped in highlighting the weaknesses observed in the availability methods. The analysis of both the above methods RSA and DSA has been completed through tables, graphs and diagrams.

XII. Reference:

Two-Level Security in Cloud using Cryptographic
Techniques, RBA, Network Intrusion and Detection
System
1 Sharvari Pawar, 2 Suresh Rathod , 3 Mandar Mahadeokar
1,2,3 Computer Department, Pune University
Pune, Maharashtra, India

Two Layer Symmetric Cryptography Algorithm for Protecting Data from Attacks
Muhammad Nadeem1, Ali Arshad2, Saman Riaz2, Syeda Wajiha Zahra1, Shahab S. Band3 and Amir Mosavi4,5,6,*

Data security in Cloud by Dual Layer Encryption
Mr. Himanshu Taiwade1, Miss. Pragati Meshram2, Miss. Janhavi Dixit3, Mr. Devendra Raut4, Mr. Zeeshan Sabir5
1Professor, Dept. Computer Science and Engineering, Priyadarshini Institute of Engineering and Technology, Nagpur, India
2-5Dept.Computer Science and Engineering, Priyadarshini Institute of Engineering and Technology, Nagpur,India

Cloud Computing Security by Using Hybrid Cryptography Algorithm
Prof. Satish Kumar Soni1, Saurabh Mishra2 1professor & Head of Computer Science Department, JNCT Rewa M.P. 486001 India 2scholar, Computer Science Department, JNCT Rewa M.P. 486001 India

DATA SECURITY IN CLOUD COMPUTING
Shailesh Shyamlal Gupta*1
*1Department OF M.Sc Information Technology Part 1, South Indian Welfare Society,
Mumbai, Maharashtra, India.