iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** I **Month of publication:** January 2022

DOI: https://doi.org/10.22214/ijraset.2022.40028

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

Working Analysis of Multistage Cloud Security Algorithms

Pradumn Kumar[1], Subhash Singh Parihar[2]
[1]*Assistant Professor*, [2]*Associate Professor, Department of Computer Science & Enginnering, PSIT, Kanpur, India*

Abstract: ***The security of Cloud computing has been a quickly developing administration which has numerous highlighted services over internet which reduces the cost and operating expenses. The greatest favorable position of cloud administrations is that one can work online in the cloud, whenever the term online comes it automatically concerns about data security. Cloud security gives better approaches for conveying security arrangements till now. In cloud storage we require security for the data so we will encrypt our data into cipher text before uploading and whenever we want access just decrypt cipher text with security policies. In this paper we are analyzing the symmetric encryption algorithm with asymmetric algorithm like DES, RSA and AES, IDEA, Blowfish etc to provide security to cloud data from attackers. By this encryption technique economically allows cloud access.***

Keywords: AES, 3DES, RSA, DES, BLOWFISH, IDEA, CRYPTOGRAPHY

I. INTRODUCTION

In today's life digitalization is very important because every works like emails, data storage, social media, banking, shopping etc are done over internet. So internet is main role performer of any information. Cloud computing is a model which provide information, data , files and applications on the server and whenever customer requested to access their data , it cached on customer's devices from any location. By this cost should be reduced for computation, storage, and infrastructure cost. Cloud computing is a term which can be reusable again and again. Here customer has to pay only for required services or data. Server and data are publically provided in cloud computing [1]. Assume two companions who share basic mystery data need to part up. Presently the issue that emerges is that they need to speak with one another from far of a separation. This separation welcomes meddler to stop, catch or meddle the correspondence between two companions with the end goal to access mystery data [9]. According to the situation both companions will choose secret box to store their mystery data and they will keep away from this and the process of unlocking the secret box known by them only. When first companion sealed box to the second, he/she opens it utilizing the safe mix key. This is the means by which cryptography works. Cryptography is a strategy for putting away and obscure basic and mystery data in an enigmatic frame with the goal that just individuals expected to peruse it can have its entrance. The encryption is led by changing over plain content into figure content by means of utilizing proper security calculations and later on decoding is directed which is returning the figure content into plain content. The proposed designing of cloud storage is layered and supportive and the discussed key developments incorporate sending, accumulating virtualization, data affiliation, movement, security, etc [4].

In this paper we are using third party cloud storage for storing data instead of primary cloud storage. Because here we are accepting strong encryption process via multistage encryption. By this data can be access from database by only genuine client by their own security terms and conditions. These terms and conditions (policies) are applied to the front-end database. But for the back-end storage we use third party cloud storage so here only genuine client is accessible [2].

All the Database server and storing devices are stored in database cloud services. Database as a Service(DBaaS) is cloud storage services which provide infrastructure for applicants in transparent mode [11]. There is always doubt in application owner for security purpose then there are various administrators are available to manage security.

Cryptography gives the highlights made reference to as under.

1) *Data Principle*: Data principle implies that data is significant just on the off chance that it is right. It is worried about keeping up and guaranteeing the accuracy of data.
2) *Verification*: Verification refers to deciding if somebody is in actuality what they are proclaiming to be.
3) *Non-Abrogation*: It refers to the affirmation that a gathering or an individual can't preclude the validness from securing their mark and communicate something specific that they started.
4) *Secretiveness*: It identifies with robbery, unapproved access and loss of protection.

©IJRASET: All Rights are Reserved

It is a result of this cryptography that cloud is more secure when contrasted with conventional security frameworks. The contrast between cloud security and conventional security framework is made reference to in given Table 1[6].
Cryptography is a strategy connected for encryption and decryption. For encryption and decryption there are so many accessible strategies in cryptography. These strategies can be for the most part arranged into two notable gatherings, i.e. Traditional and open key Cryptography [8].

Table 1: Comparison between conventional securityframework and Cloud Security framework

Conventional Security framework	Cloud Security framework
In house server center	Third party server center
High forthright expenses	Low forthright framework costs
Moderate scaling	Rapidly scalable
Lower effectiveness	Higher effectiveness
Longer time to showcase	Decrease9d time to showcase
Higher expenses	Use based expenses

Regular cryptography is likewise referred as symmetrical encryption or only one key encryption. Same key is utilized for both encrypting and decrypting. Open key cryptography is referred as deviated encryption or open key encryption. Separate keys are utilized for encrypting and decrypting the data. Fig.2 speaks to the improved show for conversional encryption system. The first comprehensible message, refers as plaintext, is changed over into clearly irregular questionable message, referred as Cipher text. The encryption procedure comprises of a calculation and a key. The key is an esteem free on the particular of the plain content. The calculation will deliver a diverse yield contingent upon the particular key being utilized around then. Changing the key changes the yield of the calculation.

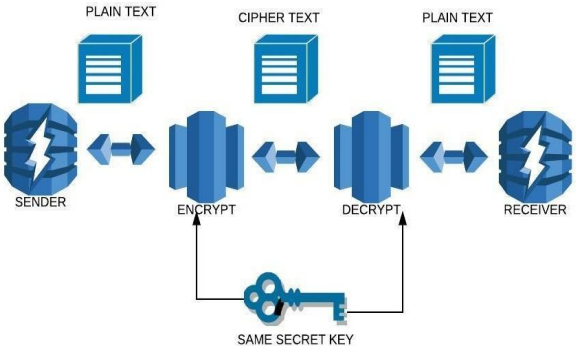


Fig1. Encryption process

Once the Cipher text is created, it might be transmitted to distributed storage. Upon gathering, the Cipher text can be changed back to the first plaintext by utilizing a decoding calculation with a similar key that was utilized in encryption[7].

II. DISTRIBUTION OF CLOUD

Distributed cloud is a public cloud computing service that helps you to run public cloud infrastructure in more than one specific locations - no longer simplest in your cloud provider's infrastructure however on premises, in different cloud vendors' data centers, or in 1/3-party records centers or collocation facilities - and manipulate the whole thing from a single control plane[12].

A. Private Cloud

This cloud computing is fundamentally the same as in nature to public cloud and incorporates "adaptability" and "dependability"[5]. However, the primary difference in private cloud is that, it is planned just for single association. Private cloud is likewise referred to as an inner cloud or corporate cloud. Private cloud affords computing services to a private inner network (in the business enterprise) and decided on customers rather than the majority. Private cloud affords a high stage of security and privateness to statistics thru firewalls and inner hosting. It also ensures that operational and touchy information are not handy to third-celebration providers. HP records facilities; Microsoft, Elastra-non-public cloud, and Ubuntu are the instance of a private cloud.

B. Public Cloud

The general public cloud offers a not unusual platform that may be accessed via most of the people through an internet connection[15]. A public cloud, running running on a payment version used and controlled through some intermediaries e.g. Cloud provider company. In a public cloud, the identical repository is shared with the aid of a couple of users. Public clouds are owned, owned, and operated by businesses, government businesses, institute universities or a mixture thereof. Amazon Elastic Compute Cloud (EC2), Microsoft Azure, IBM Blue Cloud, solar Cloud, and Google Cloud are examples of public clouds. Out in the open cloud, the cloud merchant at the seller's places has the processing model. The buyer has no detectable quality and control over where the processing show is facilitated.

C. Hybrid Cloud

In this public cloud and private cloud works together to perform the activity. The principle intention to mix these clouds (Public and private) is to create unified, automatic, and well-controlled computing surroundings. In the Hybrid cloud, non-important sports are achieved by way of the public cloud and essential sports are performed by using the non-public cloud. Specifically, a hybrid cloud is used in finance, healthcare, and Universities. The satisfactory hybrid cloud company corporations are Amazon, Microsoft, Google, Cisco, and NetApp.

D. Community Cloud

A cloud that's mutually utilized by various organizations and is usually framed-up for closely held and operated by the organizations or by the cloud company supplier[15]. Community cloud computing refers to a shared cloud computing carrier surroundings this is targeted to a restricted set of businesses or personnel (together with banks or heads of trading companies). The organizing precept for the community will range, however the individuals of the network normally share comparable security, privateness, overall performance and compliance necessities. community contributors may additionally wish to invoke a mechanism this is regularly run with the aid of themselves to study the ones seeking entry into the community.

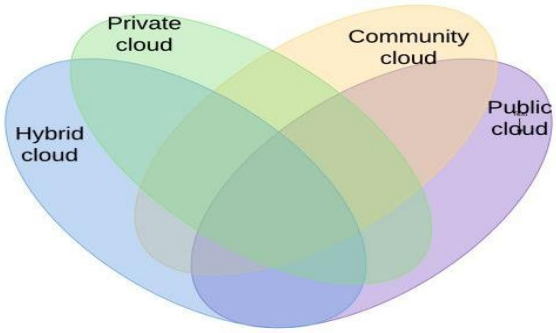


Fig2. Distribution of cloud

III. SECURITY CONCERNS IN CLOUD STORAGE

A. Facts Rupture

Cloud too faces the identical threats as traditional networks used to stand. however because of the big amount of records stored inside the cloud, the security worries become an attractive challenge and desires to deal very severely. The impact of the damage relies upon the sensitivity of the facts. Breaches associated with fitness data, exchange and highbrow assets frequently prove to be more devastating. Whenever records breach takes location, groups ought to incur heavy fines or even face court cases. Oblique affects like lack of goodwill may have long-term effects.

B. Negotiated Authorization and damaged Verification

A records rupture happens due to poor strength passwords, worst certification and not sufficient robust keys. Companies often apportion distinctive permissions to their personnel for acting obligations appointed to them. But those companies frequently neglect to alternate these passwords whilst employees go away the employer. Verification structures like One time password, phone calls verification, and smart chip cards make it difficult to sign in with lifted passwords for intruders. Many programmers typically commit a blunder of writing credentials and crypto logic keys at intervals the provision code itself. Keys must be protected and it's extremely useful to alter these protection keys sporadically. In addition, centripetal identification right into one repository has its personal dangers[13].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Hacked Interfacesand Apis

APIs are supplied by using each cloud service today. the security of cloud offerings depends upon the security of API. weak APIs and interfaces divulge organizations to protection troubles like integrity, availability, confidentiality, and responsibility. APIs are most inclined because those are reachable from the open net.

D. Account Hijacking

Attackers can snoop on activities, alter data and manipulate transactions via cloud offerings. Many assaults can be released by the usage of cloud application. groups must deny the sharing of account credentials between users and services.

E. Malicious Insiders

The insiders confer with the modern-day or former employees of an company. Any corrupt worker in the cloud surroundings can smash the complete infrastructure and control facts. corporations should manage the whole encryption procedure. powerful monitoring and auditing administrator activities want to be carried out basically. appropriate training is a critical component for control to avoid errors[13].

F. Permanent facts Loss

As the cloud computing has been in existence due to the fact that a few years now, it has matured to a totally sturdy and sturdy era. these days the reviews of permanent records loss due to issuer errors could be very uncommon. however nevertheless malicious hackers are in a continuous try and completely delete records on the cloud to harm businesses and moreover, cloud statistics centers are as at risk of herbal calamities as any other facility.

To ensure the safety of crucial records, cloud providers constantly recommends distribution of facts and packages amongst a couple of zones. Off-line garage and every day information backup are very critical in cloud environments. every time the load of preventing facts loss isn't of cloud provider company [14]. suppose a client encrypts his/her information before importing it to the cloud, then it's miles the sole obligation of the patron to protect his/her encryption key. If a secret is misplaced, so is the facts. Cloud provider providers also need to attend to compliance regulations like how long companies have to maintain audit records and other applicable documents.

IV. DATA ENCRYPTION

Data encryption is a process in which original data must be converted into cipher text. Cipher text is not understandable for anyone.

A. Data Encryption Standard

Data Encryption Standard (DES) is symmetric encryption algorithm. There are 16 round identical operations. The size of each block is 64-bit, with length 64-bit key[15]. To place it in easy terms, DES takes 64-bit simple text and turns it right into a 64-bit cipher text. And on account that we're talking about asymmetric algorithms, the same key is used when it's time to decrypt the textual content.

The set of rules process breaks down into the following steps:

1) The method starts off evolved with the 64-bit plain text block getting exceeded over to an preliminary permutation (IP) feature.
2) The preliminary permutation (IP) is then carried out on the plain textual content.
3) Then, the preliminary permutation (IP) creates halves of the permuted block, referred to as Left plain text (LPT) and right plain textual content (RPT).
4) Every LPT and RPT is going via sixteen rounds of the encryption process. Eventually, the LPT and RPT are rejoined, and a final Permutation (FP) is completed at the newly blended block.
5) The end result of this manner produces the desired 64-bit cipher text.

There should be following rounds performed for this and that are given below[8]:-

a) Expansion
b) XOR operation with round key
c) Substitution and permutation

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

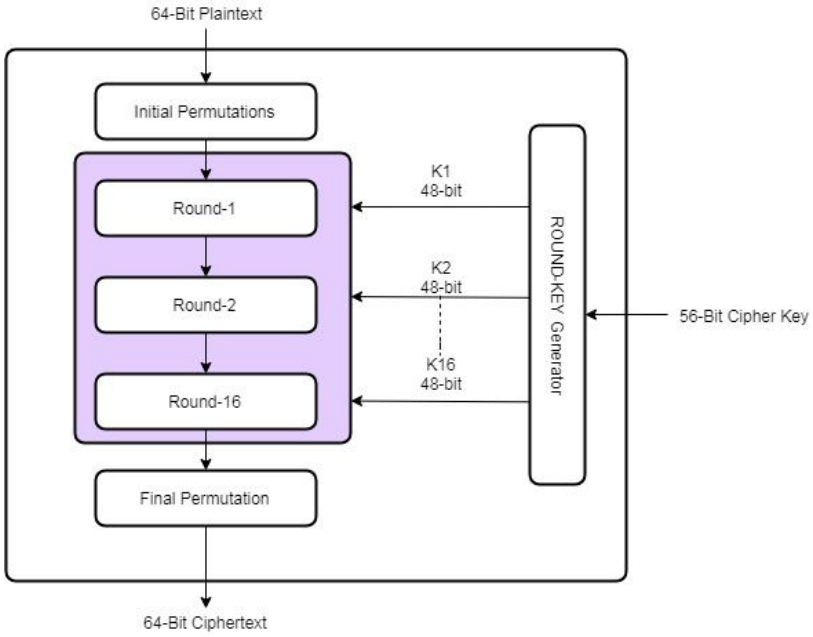


Fig3. DES Algorithm

B. Triple DES

DES cipher's key size of 56 bits was suitable when this algorithm was created but due to increase in computational power creates brute-force attacks feasible. So variation DES comes in form of Triple DES (Encrypt-decrypt-encrypt). Triple DES uses three applications of DES and in which two independent DES keys to produce an effective key length of 168 bits. Triple DES is every other mode of DES operation. It takes three 64-bit keys, for an standard key length of 192 bits. In Stealth, you surely kind within the complete 192-bit (24 character) key in place of coming into every of the three keys in my view. The Triple DES DLL then breaks the user-furnished key into three sub keys, padding the keys if necessary so they're every 64 bits long. The method for encryption is precisely similar to regular DES, however it's far repeated three instances, hence the name Triple DES. The facts is encrypted with the primary key, decrypted with the second one key, and subsequently encrypted again with third key.

Triple DES runs 3 instances slower than DES, but is a great deal greater secure if used well. The method for decrypting something is the same as the manner for encryption, besides it is accomplished in opposite. Like DES, facts is encrypted and decrypted in sixty four-bit chunks. despite the fact that the enter key for DES is 64 bits long, the actual key utilized by DES is most effective 56 bits in duration. The least big (right-maximum) bit in each byte is a parity bit, and has to be set in order that there are continually a bizarre wide variety of 1s in every byte. These parity bits are omitted, so best the seven maximum good sized bits of every byte are used, resulting in a key length of fifty six bits. Because of this the effective key electricity for Triple DES is really 168 bits due to the fact every of the three keys carries 8 parity bits that aren't used during the encryption manner. The implementation should be done by Block cipher with symmetric secret key with block length of 64 bits and with key length of 56, 112, 168 bits.

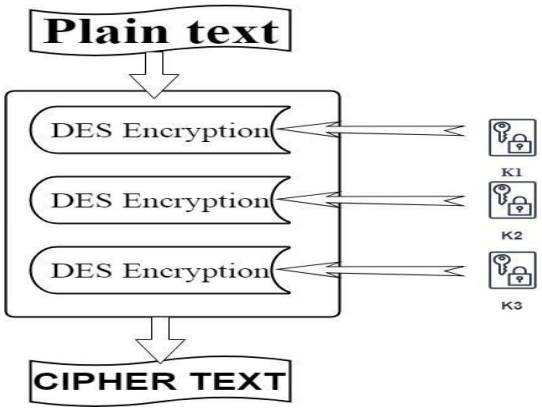


Fig4. TRIPLE-DES Algorithm

©IJRASET: All Rights are Reserved

The whole encryption and decryption is as follows-

1) Plain text blocks should be encrypt by using single DES key K1.
2) Now output of step 1 should be decrypt by using single DES key K2.
3) Finally output of step 2 should be encrypt by using single DES key K3.
4) The output of step 3 will be the cipher text.
5) Similarly decryption should be done in reverse order from key K3 to K1.

C. Advanced Encryption Standard

Advanced Encryption Standard is symmetric encryption algorithm. In AES the number of rounds are not fixed for operations.AES encrypts and decrypts data of 128 bits of the data block. AES generally uses three different key size of 128, 192, 256 bits which depends on the rounds like 10, 12, 14 [12].Now a day's cryptography, AES is extensively espoused and supported in each computer code and hardware. Till date, no sensible scientific discipline attacks against AES have been discovered. Also, AES has erected-in inflexibility of crucial length, that permits a degree of'unborn-proofing'against progress within the capability to perform total crucial quests[16]. However, when for DES, the AES security is assured only if it's properly enforced and smart key management is utilized.

AES follows substitution and permutation network structure. In each processing rounds there are four steps:-

1) Byte Substitution(In this S-box is used to perform substitution of blocks)
2) Shift Rows
3) Mix Column
4) Add round Key(X-ORed operation with data)
5) Byte Substitution, Shift Row, Mix Column and Key Addition

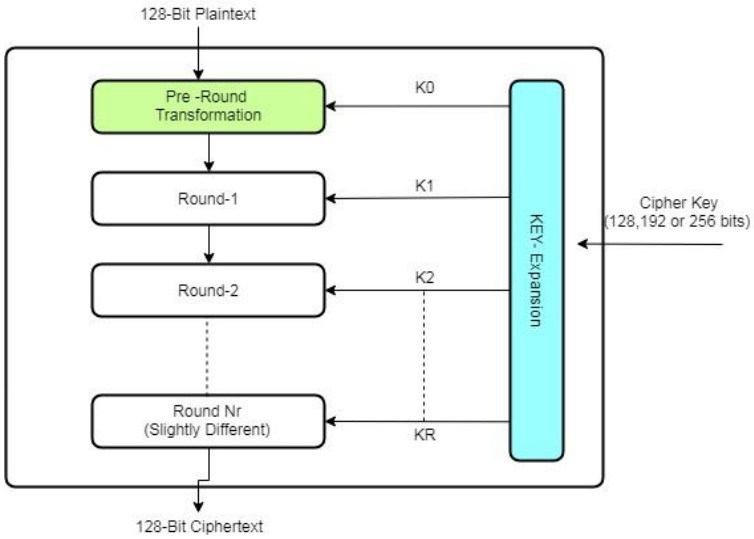


Fig5. AES Algorithm

D. Blowfish

Blowfish Algorithm is developed by Bruce Schneier. Blowfish algorithm is a symmetric key block cipher algorithm. In Blowfish there is 64 bit of block size and variable key length of 32 bits to 448 bits. Blowfish follows Feistel structure of 16 rounds. Each round of Blowfish is XORed operation with key expansion technique. Blowfish is public domain that is open of free for everyone. Blowfish algorithm is done by two parts one is sub-key generation and other is data encryption[17]. Sub key will be generated by operational steps and that are given below:-

1) Put the keys in array with 32 bit each.
2) K1,K2,…….Kn (1<=n<=14)
3) P-array will initialize and each of 32 bit P1,P2……P18
4) Initialize 4 S-Boxes and 25632 bit entry on each boxes
5) S1=s0, s1,……s255 S2=s0,s1… s255
6) S3=s0,s1… s255

7) S4=s0,s1, s255
8) P-array , S-boxes (Hexadecimal form of pi)
9) Now
- P1= P1 XOR K1
- P2= P2 XOR K2
- P3= P3 XOR K3.
- P14= P14 XOR K14
- P15= P15 XOR K1
- P16= P16 XOR K2
- P17=P17 XOR K3
- P18=P18 XOR K4

10) Take 64 bit plain text and every will be start from zero bits

When all the p and S-boxes are replaced then sub key will be generates and working and functioning of Blowfish is given below in the P and S boxes diagram –

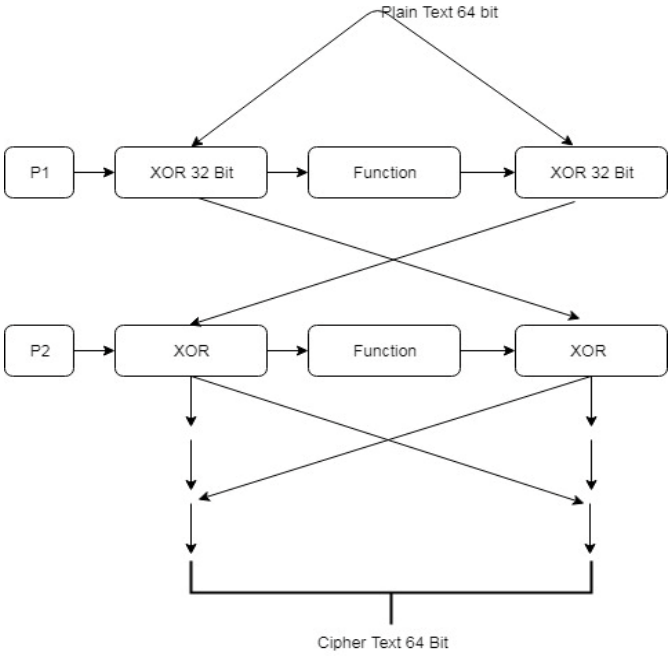


Fig6. P-Box

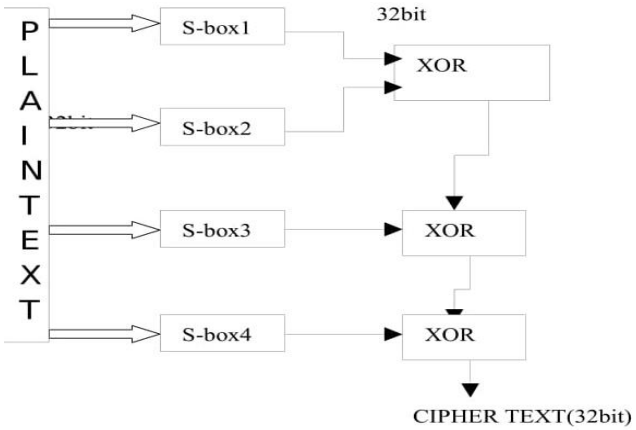


Fig7. S-Box

E. River Shamir Adelman

River Shamir Adelman (RSA) algorithm is proposed on 1977.RSA is asymmetric key encryption algorithm.RSA algorithm generally use public key for data encryption. But in RSA data decryption is done by personal private key which is only known to the user.RSA uses 1024 bits key for encrypting and decrypting data. RSA algorithm select two distinct number randomly and multiply them. As a result you will get new number that will be key term. Public and private key will be generate on the basisof key term[12].

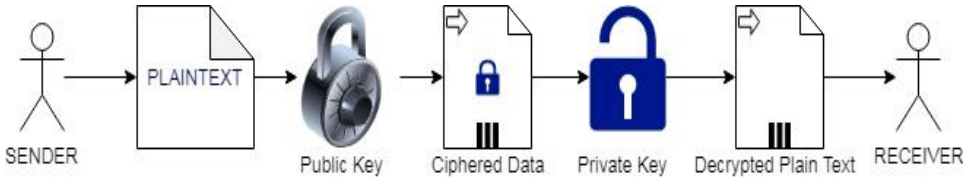


Fig8.RSA Algorithm

F. International Data Encryption Algorithm

International Data Encryption Algorithm (IDEA) is proposed by Xuejial Lai and James Massey in 1990. IDEA is symmetric block cipher algorithm. It was generally meant for the replacement of DES algorithm. Here the size of plain text is 64 bits and size of key is 128 bits and it is divided in 52 sub keys. The generated output data will be cipher text of 64 bits. There are 8 rounds identical operation and in each round 6 keys are used. For transformation 4 final keys will be used for both encryption and decryption.

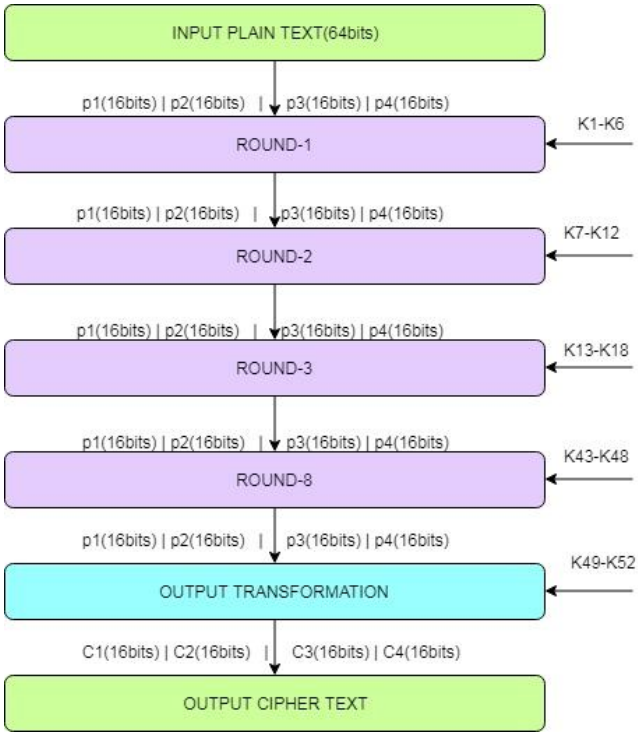


Fig9. IDEA Algorithm

IDEA uses different algebraic operations on 16 bit blocks:-

1) XOR
2) Addition(modulo 2^16)
3) Multiplication(modulo 2^16+1) Key generation process in IDEA
4) First of all we will see how these 52 keys are generated.
5) The 128 bit key is divided into 8 sub parts that is 16 bits each.
6) Then the 128 bit key is cyclically shifted to the left by 25 position, so by doing this we will have one new 128 bit key.
7) Now similarly as above it is divided into 8 sub blocks and will be used in next round.
8) The same process will be performed 9 times and 56 keys will b generated from which the first 52 keys will be used.
9) So likewise from k1 to k52keys are generated .

Idea encryption algorithm follows 14 steps for full rounds, the original cipher block is divided into 4 parts of 16bits sub-blocks. All 64 bit block will combined all sub blocks .Ineach round 6 sub keys are required. Sequence of operations ineach round required:-

a) Multiplication of P1 and sub key K1
b) Then Add P2 and sub key K2 & Add P3 and sub key K3
c) Again Multiplication of P4 and sub key K4
d) Then Apply Bitwise XOR to step1 and step3 & step2 and step4
e) Multiplication of step5 and sub key K5
f) Add step6 and step7
g) Multiplication of step 8 and sub key K6
h) Add step 7 and step 9
i) Apply Bitwise XOR to (step 1 and step 9), (step 3 and Step 9), (step 2 and step 10) & (step4 and step 10).

Same operations will be performed in 8^{th} round

- Multiplication of P1 and sub key K1
- Multiplication of P2 and sub key K2
- Multiplication of P3 and sub key K3
- Multiplication of P4 and sub key K4

The combination of all these blocks will be output and decryption will be done in reverse order of encryption process. This way our data will fully secured in both encryption and decryption process.

V. MULTI STAGE ENCRYPTION

In Multistage Encryption, the client is separated into numerous domains. In every domain, we apply diverse encryption algorithm. Multi-stage encryption algorithm guarantees the security of the information. In this paper, we have investigated the blend of different encryption calculations for performing Multistage Encryption.

A. Private Domain

Private key encryption is the first kind of encryption. Tracing all the way back to the appearance of cryptography, private key cryptosystems were the first and keep on being the most well-known. When utilizing private key cryptography, the two players much each have, or if nothing else trade the private key. "Key" can be a piece deluding - the actual key is truly the code that is utilized to scramble and unscramble the information being encoded.

With an old code, similar to the Caesar Cipher, the private key was essentially a number that compared to the number each in order character should have been moved. In current advanced encryption conspires, the keys are presently restrictively troublesome calculations that no cutting edge PC might at any point proficiently break. Each user has to keep the secret keys and access their data via encryption method in private domain. User has to maintain their privacy regarding domain and secret keys. User grants their benefits by requesting data. So inthis we should use RSA algorithm for encryption of data.

B. Public Domain

Public key cryptography is really a genuinely ongoing creation, tracing all the way back to 1973, it utilizes a public/private key pair. The keys are deviated, the public key is really gotten from the private key. It very well may be utilized to encode while the private key can be utilized to unscramble. The public key is additionally equipped for confirming marks left by the private key. In public domain there will be multiple authorities and each authority maintaining their attributes. User will also play role in public domain and here customers get their secret keys from key authorities. They don't require communicating with data owner. To access data they have to have to follow certain policies [3][10] .

C. Implementation

We have discussed multiple encryption algorithms aboutthe securities and these algorithms have their own performance analysis So in this paper we will use combination of two different algorithm in private as well as public domain. Firstly encryption will be done then decryption will be done on reverse order.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

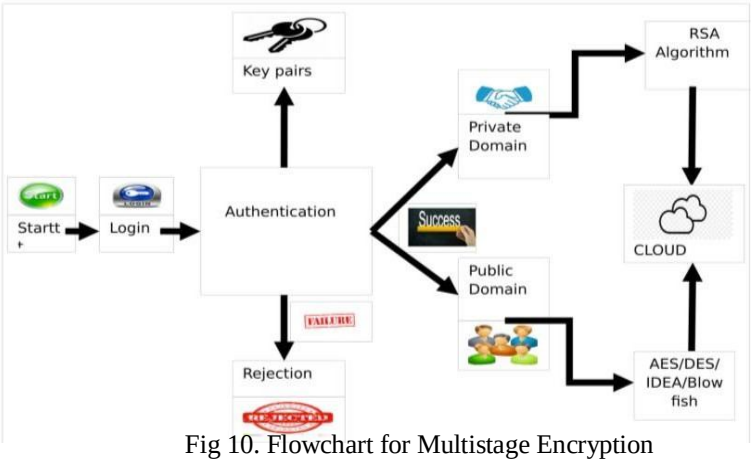


Fig 10. Flowchart for Multistage Encryption

According to the our design all symmetric algorithm are using for encryption and decryption in second place and calculated the performance and security level and time.

There are few steps to understand the working process ofmodel and that are given below:-

1) Start the system and check Data User's credentials in any picture form.
2) Acquiring the credentials of User's, check whether it is valid or not
3) After validation both public and private keys for RSA are used in primary stage for encrypting then public key will exchanged with client along User's ID. Then private key will be send via highly secured email.
4) After sign in , the client can upload their data with the help of public key
5) Now RSA will encrypt the data into cipher text
6) Cipher text file will be further encrypted with the help of DES, AES, IDEA, BLOWFISH encryption algorithm. After encryption this file will be send to cloud for storage with the help of third party cloud server.

VI. PERFORMANCE ANALYSIS

A. Combination of RSA and DES

In private domain encryption should be done by the RSA algorithm while in public domain DES algorithm is used for encryption. The number of clients in public domain is various so the proposed method bunches the accessible clients. Here hierarchical clustering algorithm is used for grouping the customers according to their specific roles.

B. Combination of RSA and AES

In private domain encryption should be done by the RSA algorithm while in public domain AES algorithm is used for encryption. The number of clients in public domain is various so the proposed method bunches the accessible clients. Here hierarchical clustering algorithm is used for grouping the customers according to their specific roles.

C. Combination of RSA and IDEA

In private domain encryption should be done by the RSA algorithm while in public domain IDEA algorithm is used for encryption. The number of clients in public domain is various so the proposed method bunches the accessible clients.

D. Combination of RSA and TRIPLE DES

In private domain encryption should be done by the RSA algorithm while in public domain TRIPLE DES algorithm is used for encryption. The number of clients in public domain is various so the proposed method bunches the accessible clients.

E. Combination of RSA and BLOWFISH

In private domain encryption should be done by the RSA algorithm while in public domain BLOWFISH algorithm is used for encryption. The number of clients in public domain is various so the proposed method bunches the accessible clients.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

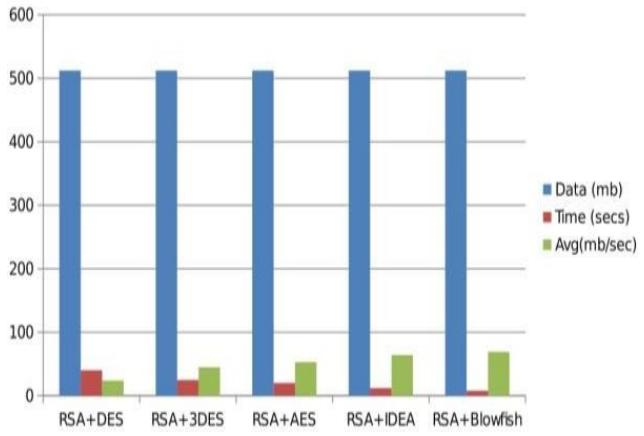
VII. COMPARISON ANALYSIS

Here we are performing our test over 512 MB data with the combination of public domain and private domain. So in public domain different types of algorithms are used while in private domain RSA algorithm is fixed for all public domain's algorithms. After performing the test we get some results and we saw that RSA+Blowfish have best results on comparison with others in every aspect like time, speed performance and encryption speed.

The results are given in below table with all combinations:-

Algorithm	Data	Time (sec)	Avg. Mb/sec	Performa-nce	Security level	Encryption Speed
RSA +DES	512	40	22-26	Low	Adequate	Very slow
RSA + 3DES	512	25	40-50	Medium	Adequate	Medium
RSA + AES	512	20	52-54	Good	Good	Medium
RSA + IDEA	512	12	63-65	High	Secure	Fast
RSA + Blowfish	512	8	68-70	Very High	Highly secure	Very fast

Result Analysis Bar Graph-



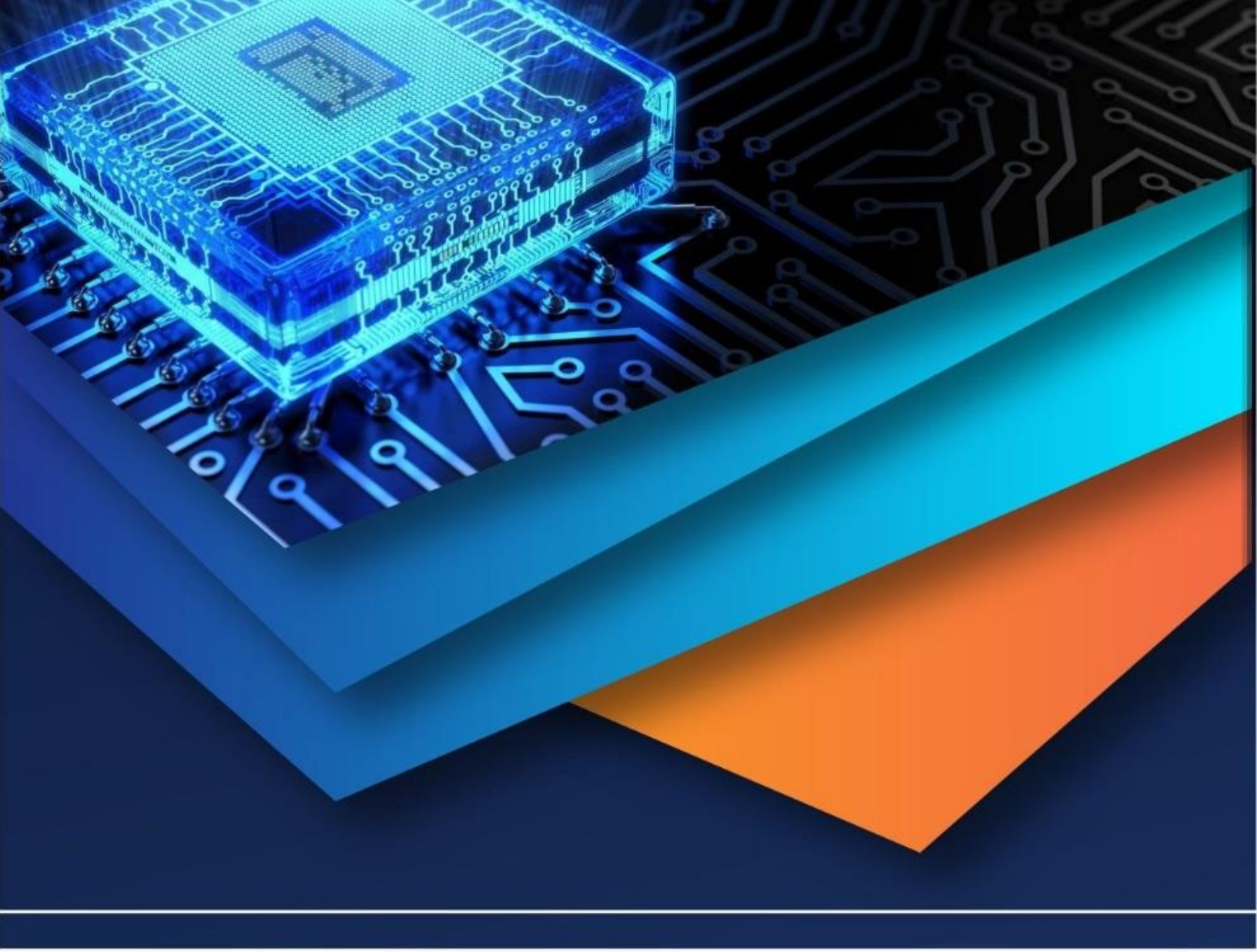
VIII. CONCLUSION & FUTURE SCOPE

Still cloud computing is an advancing and new worldview where registering is considered as an on-request administration. Once the association takes the choice to change to the cloud it lets completely go over the data. The cloud security relies upon confided in cryptography and registering. In this manner, in this concentrate on just the approved client can get to the data. Regardless of whether certain unapproved client gets the data purposefully or inadvertently or on the other hand on the off chance that the client hold onto the data, the client can unscramble it and access it because of strategies of encryption. Because of the half breed calculation proposed in this concentrate on it would be much secure to get hacked. In this paper many algorithms are examined for multi-stage encryption. And according to the comparison analysis RSA+ BLOWFISH gives better results in every moment than others. In future some new algorithms can be used for multi-stage encryption techniques to protect the data in cloud storage. In future many more hybrid combinations are possible to secure cloud data with some updated key size and algorithms.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] Krishna Keerthi Chennam, Lakshmi Muddana, Rajani Kanth Aluvalu, "Performance Analysis of various Encryption Algorithms for usage in Multistage Encryption for Securing Data in Cloud", International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017
[2] Oracle," Oracle transparent data encryption," http://www.oracle.com/technetwork/database/options/advanced-se curity/index-099011.html, September 2013
[3] Wang, Qian, Cong Wang, Kui Ren, Wenjing Lou and Jin Li, "Enabling public audibility and data dynamics for storage security in cloud computing", IEEE transactions on parallel and distributed systems,Vol.22, No.5, pp.847-859, 2011.
[4] Rashmi Mate and Mohd. Saif Wajid, "A Review of big data deduplication and dynamic ownership management in cloud storage" International journal of Advanced Research In Computer Science.Vol 9,pp 0976-5697, 2018
[5] Steven Mathew, Sarita Gulia, Varinder Singh,Vivek dev "A Review Paper on Cloud Computing and its Security Concerns" International Conference on Research in Intelligent and Computing in Engineering.Vol 10 pp. 245–250,2017
[6] Rajleen Kaur, Amanpreet Kaur, "A Review Paper on Evolution of Cloud Computing, its Approaches and Comparison with Grid Computing" International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6060-6063
[7] D,Palanivel Rajan, Dr. S. John Alexis, "Comparative study on data Encryption Algorithms in cloud platform", international journal Of Research and Technoloy.vol 6, 2017
[8] Nishant rai, Manoj Kumar, "Comparative Study of Security Algorithms in Cloud Computing", International Journal of Innovative Research in Engineering & Management (IJIREM)ISSN: 2350-0557, Volume-2, Issue-2, March-2015
[9] Murali, R. Sivaram Prasad, "Comparison of Cryptographic Algorithms in Cloud and Local Environment using Quantum Cryptography", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017)
[10] Singh, Anirudha Pratap, and Syam Kumar Pasupuleti, "Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing", Elsevier on Procedia Computer Science, Vol.93,pp.751-759, 2016.
[11] H. Hacigum¨ us¸, B. Iyer, and S. Mehrotra, "Providing database as a service," in Proc. of the 18th IEEE International Conference on Data Engineering, February 2002
[12] M.Sudha1 , M.Monica2, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography" Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012 Copyright © World Science Publisher, United States.
[13] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, " Data Security in Cloud Computing with Elliptic Curve Cryptography" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012
[14] Neha Tirthani, Ganesan R, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", Academia research.
[15] Gurpreet Kaur1 , Manish Mahajan, "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms", . Journal of Engineering Research and Application ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.782-786
[16] Bih-Hwang Lee; Ervin Kusuma Dewi; Muhammad Farid Wajdi, "Data security in cloud computing using AES under HEROKU cloud', 2018 27th Wireless and Optical Communication Conference (WOCC) ISSN: 2379-1276.
[17] K. R. Sajay,Suvanam Sasidhar Babu,Yellepeddi Vijayalakshm, "Enhancing the security of cloud data using hybrid encryption algorithm", Journal of Ambient Intelligence and Humanized Computing20july 2019, https://doi.org/10.1007/s12652-019-0143-1



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)