IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 11, November 2024| DOI: 10.15680/IJIRCCE.2024.1211100

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Enhanced Security Problems in Real-Time Scenario using Blowfish Algorithm

D.Prakasa Rao[1], P.Ram Kishor[1], B.Ramesh, M.Jayanthi Rao[1*]

Department of Computer Science and Engineering, Aditya Institute of Technology and Management, Tekkali, India

ABSTRACT: Cloud computing is a term that is deployed to illustrate multiple impressions of computing that include multiple computers linked through are all time large network of communication such as the internet. Cloud computing is a developing paradigm that has in recent times involved plenty of researchers because of its functionality to lower the expenses related to computing. Due to the growth of cloud computing procedures the quick increase in services of the cloud became outstanding. In this concern cloud facing lot of security problems. we proposed the scheme to enhance the Blowfish block security for cloud server. In proposed method total number of Blowfish rounds are altered by skipping few Blowfish rounds using round key. As a result, proposed scheme increases additional Blowfish cipher security against attackers apart from minimum to maximum size of Blowfish key. In addition to that the proposed method decreases encryption and decryption execution time and also provides security services Confidentiality, Integrity, and availability.

KEYWORDS: Cloud Computing, Cyber Security, Blow fish, Homographic Encryption

I. INTRODUCTION

Artificial Intelligence techniques imply that prove an ability to better way to understand current and future technology field requirements specially focused on Commerce and Governance systems based on economy AI plays a key role in part of monitoring the business environments with existing strategies, identifying the customers' requirements, and carrying out the vital techniques without or with negligible human intercessions and involvements. Subsequently, it overcomes any barrier between purchasers marking' requirements and the big impact of quality of Service (QoS).

Many corporations are transferring their facts garage to the cloud, however imposing effective security features is a ought to-have earlier than they decide to adopt cloud computing.

For facts security in cloud environments, we propose a cryptography symmetric key algorithm for encrypted and decrypted data, the usage of a multilevel cryptography-based safety model [1]. The proposed prototype increases data protection to the most volume feasible for both users and cloud service providers. The model gives the cloud user complete transparency in security.

Presently a day's Cloud processing has an incredible effect on IT undertaking. Alongside expanding advances, associations favor administrations of the cloud because of its gigantic points of interest. Even though administrations of cloud have various favorable circumstances they need security and protection at a few levels [2]. With expanding advances cloud administrations are gotten to by PDAs enabling clients to utilize highlights of the cloud ,for example ,sharing ,and putting away pictures, recordings, archives in various stages. Protection is dependably a critical part of data innovation.

Cloud services containing critical data which are accessed through the internet should ensure security prominently. The penetrating idea of cloud and convey a piece of information all through the countries may prompt more serious hazards in security [3].At the point when worried about Cloud Security, numerous focuses ought to be experienced, for example, protection, information security, and validation.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A portion of these targets of security is critical for cloud service Providers to incorporate[4]. Since Privacy is dealt with as an essential element of IT, information encryption and unscrambling will be the key means in guaranteeing information insurance.

Existing Security strategies "Veeraruna Kavitha. (2011), discussed issues facing with security" [5] that utilization calculations, for example, RSA, Diffie-Hellman, DES,AES,RC4,RC5,RC6,Blowfish,W7,and3 DES for information encryption have a few favorable circumstances and drawbacks at various levels which are symmetric and deviated in nature. Our interest is to present a Secure Cloud Environment that has focal points of symmetric and asymmetric encryption.

We utilize RSA Asymmetric calculation and AES Symmetrical calculation for information encryption and decoding [6]. We go for giving aCloud air that guarantees security at variouslevels, for example, secret phrase security, multifaceted confirmation, security in in formation transmission, and information encryption[7].The way client information is protected and processes are safely delegated to a remote cloud service provider become a key issue in Cloud computing.

Cloud service providers transmit information to clients remotely; therefore, the security of that information is at risk since it can easily be removed by hackers.

To protect the clients' information from hackers, this environment should implement appropriate security measures while operating a variety of harmful activities. Several strategies had been proven to mitigate protection problems, which includes key sharing, the usage of cryptographic algorithms.

Information, its stockpiling, transmission, and usage are analyzed within the context of protection problems and implementation of diverse mechanisms[8].This paper seeks to offer data safety towards special sorts of attackers with the aid of encrypting and decrypting purchaser information at cloud storage and at the purchaser-facet using symmetric key cryptography.

In Inclusion to services of cloud, deployment, security issues, and constraints in terms of cloud computing. These days, Improving the privacy & security of cloud data has become a vital concern and the Answer for this is to implement affirmative encryption modules while preserving and pushing the data into the cloud [9]. This entire study puts forward an innovative hybrid algorithm to improve cloud data security using encryption algorithms.

This study syndicates H graphic encryption besides blow-fish to improve cloud security [10]. Want to conclude that if at all the security problems are solved then the upcoming generations resolve to be the results aimed at cloud storage. which could benefit all types of data centers from small-medium to large.

II. LITERATURE REVIEW

The security of cloud computing has been the subject of significant research. Several authors have discussed various ways to achieve security, considering that this should be the primary concern for the users. Using Counter Propagation Neural (CPN) networks, A. Negi et al given a model showing how the encryption and decryption method, can be implemented.

A traditional security system is enhanced with this technology. An information security improvement involves three-tiered authentication. Additionally, the proposed solution incorporates the monitoring of the system in real-time and the operation of the forensic virtual machine. As a result of these techniques, an attacker or unauthorized handlerwould need to decrypt data at every level , which is a task that is far more challenging or difficult than decrypting it at a single level.
A model proposed by Security In Cloud Computing Using Blowfish Algorithm[1,2] as a means to improve data security. A novel cryptographic scheme is created by combining chaos and neural cryptography.The key generation is done using an alphanumeric encryption table.This algorithm is used by users to authenticate themselves, ensuring that data is protected from unauthorized user access.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

a homomorphic linear authentication algorithm is used as Third-Party Authentication (TPA).Meanwhile, their second scheme utilizes threshold cryptography.In the initial scheme, TPA does not learn anything about the important data during the auditing process, whereas the second scheme ensures that unauthorized users cannot misuse the stored data as a result of the audit.

recently proposed a Hybrid Encryption Scheme, it is helpful for the recognizable validation of client or user identity, and through a substantial check, they are for the most part utilized for a biometric interaction.

This proposed Blowfish algorithmic[1] approach design will establish anintensely safe climate and avoid unauthorized or unapproved access.

S.Singh et al. proposed a plan that utilizes Elliptic Curve Cryptography. Here, the information is encoded at the customer or user side and must be decrypted done through after transferring. Likewise, at the time of login, the client verifies themselves through various information boundaries.

K.Brindha et al. in suggest Visual Cryptography is a system focused on data stockpiling security issues. The data is saved at information servers in an encoded structural formation.

Only subsequently the validation based on authentication of the client would the specialist cooperate through functional data transformation to give keys to the common images. To get the mystery key to the data, the client should superimpose this scrambled picture by this key.

This Predicate Based Encryption focuses its implementation on both Platforms as a service and Software as a service This proposed technique also precludes unwanted exposure, unwanted leakage, and other unwanted breaches of confidentiality of cloud residentdata.

In 2011, V.S et.al wrote a paper titled Security Techniques for Protecting Data in Cloud. This paper aims tounderstand the security threats and identifythe appropriate security techniques used tomitigate them in Cloud computing .

The research identified a total number of 43 security challenges and 43 security techniques [19]. The most measured attribute is Confidentiality (31%)followed by Integrity (24%) and Availability(19%). In2011Ali Asghar Karahroudy wrote a paper titled Security Analysis and Framework of Cloud Computing with ParityBasedPartiallyDistributedFileSystem.

This paper proposed a technique called A Novel Technique of Data Security in Cloud Computing based on Blowfish with the MD5 method[7] This paper addressed the three aspects of security which are Confidentiality, Integrity, and Availability.

III. RELATED WORK

Communication or data transfer over a cloud network must be secure and confidential to maintain the value of the social network. Cryptography takes care of data security[3,4]. Cryptography manages the security of records that can be saved or transmitted thru the cloud. Secure and private communications or statistics transmission is a need of life cycle.

Figure.1: Cloud Platform as Services

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Cloud cryptography encrypts data from unauthorized access in the cloud shown in the fig-1, this makes it possible for users to acquire shared cloud data securely and easily.Using encryption in the cloud, data can be protected from unauthorized access and users can confidently access shared cloud data. Users can utilize cloud encryption to safely access data stored in the cloud[5,6]

Cloud providers secure the shared data they host with encryption techniques. Cryptography guarantees the integrity of the information without having to wait for cloud exchange.Using encryption techniques, cloud providers secure shared data without having to exchange information with each other.Encryption techniques can secure data sharing in the cloud while it is not waiting for data exchange. Cloud service providers are providing shared data and they are securing it with encryption techniques[7].
Cryptography techniques have been used to develop a large number of cloud computing security algorithms, which have proven crucial to the security of data in the cloud. Security algorithms for cloud computing had been advanced using cryptography strategies, that have grown to be very vital for data protection in the cloud environment[8]

Cryptography algorithm for cloud Security

The main part for the corporations within the cloud storage version is protection, as they usually shop their information inside the cloud and get admission to the information anywhere and whenever. With cloud computing, companies generally shop their statistics, which is out there anywhere at any time, however statistics security is their predominant problem for cloud computing.

Data transmission and verbal exchange over heterogeneous and related networks are secured with encryption models , the encryption algorithm used for cozy records communication is the key for comfy transmission and communication .

A secret's to begin with agreed upon with the aid of the interactive mutual customers, and conveying parties and saved in both parties and kept mystery. Presently, the important thing and the encryption set of rules stay used for scrambling the message beyond to sending it starting with one celebration then onto the following .

This text received, known as ciphertext, is acquired by way of the other birthday party who then decrypts it taking use of the same key and the decryption set of rules. At this time, the key is maintained as a mystery whilst the encryption and decoding algorithm stays the recognized key additives. As we currently understand, the secret is regarded to both the source and the destination on this cryptography machine, yet this key move is of brilliant importance and ends up being an undeniably hard challenge.

IV. PROPOSED METHODOLOGY

This section explains the design of enhancing cloud security using Blowfish algorithms. The proposed system in this study needs to secure the data in the cloud because this is the open source security is the major problem which is faced by each user. This study usages python software tools and cryptography techniques to enhance cloud security; the primary step is to provide the input text.

Cryptography consists of two phases, which are encryption and decryption; both encryption and decryption play a critical role in ensuring data security.

Plain text or secret messages are encrypted by using a secret key into ciphertext, a strange message, or a scrambled message. After encryption, the ciphertext is decrypted by using the same secret key used during encoding. To ensure security, a secret key needs to be kept secret since different combinations of the same plaintext result in different ciphertexts.In cryptography, there are numerous different schemes available for encryption, which are used to protect sensitive information.

It is a multilayer cryptography algorithm with homographic encryption in the first layer and blowfish encryption in the second layer. The first layer of homographic encryption is applied to the input text.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Thentheencryptionresultwillbeobtained.After that, the result of encryption is passed to this cold layer which is the blowfish encryption layer. The final output of the encryption layer is obtained.

Homographic Encryption:

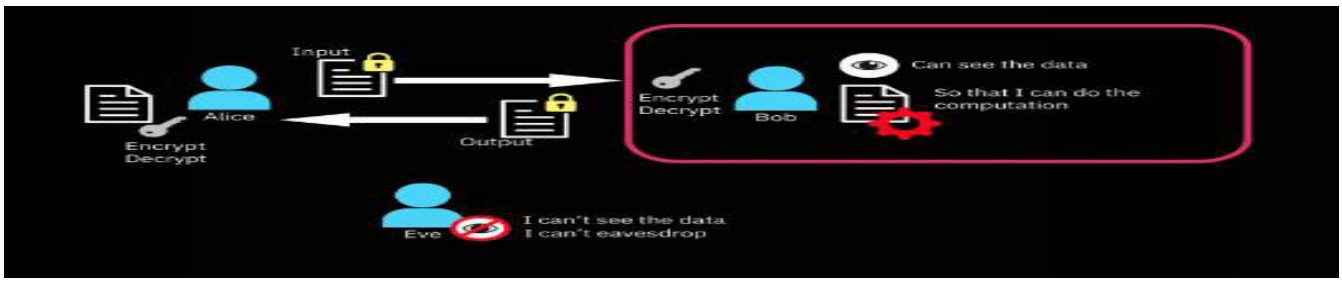


Figure 2:Homographic encryption systems

Homographic encryption system shown in the fig-2 are employed to carry out operations on encrypted information without knowing the private keys then the secret key holder will be only the client. When the output of any operation is decrypted it is relevant as if the calculation has been carried out already on raw data.

Encryption is homographic if: from Encrypt (x) and Encrypt (y) it is possible to evaluate Encrypt function (x, y)), where the function can be+,×and without using private keys. Among the distinguished homographic encryption according to the operations that permit the assessment of raw information the additive homographic encryption (only raw data additions) is the Paillerandcry ptosystems of Gold wasser–Micaliand the multiplicative encryption of the homography is the cryptosystem of ElGamaland RSA. Shown in the fig-3

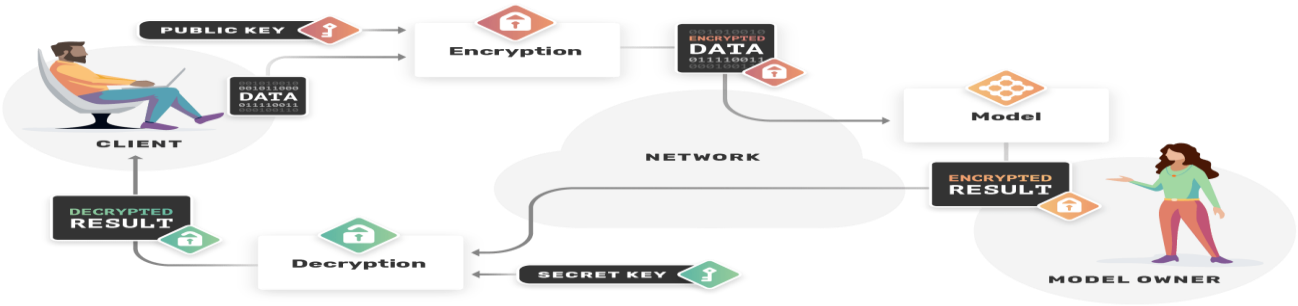


Figure 3:Cryptosystem

Ae is an algorithm of encryption with key a Ad is an algorithm decryption

Ad(Ae(m)×Ae(n))=m×n OR Encrypt(a(×)b)=Encrypt(a)(×)Encrypt(b)

Af(Af(m)×Af(n))=m+n OR Encrypt(a(+)b)=Encrypt(a)(+)Encrypt(b)

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Blowfish algorithm working on cloud server:

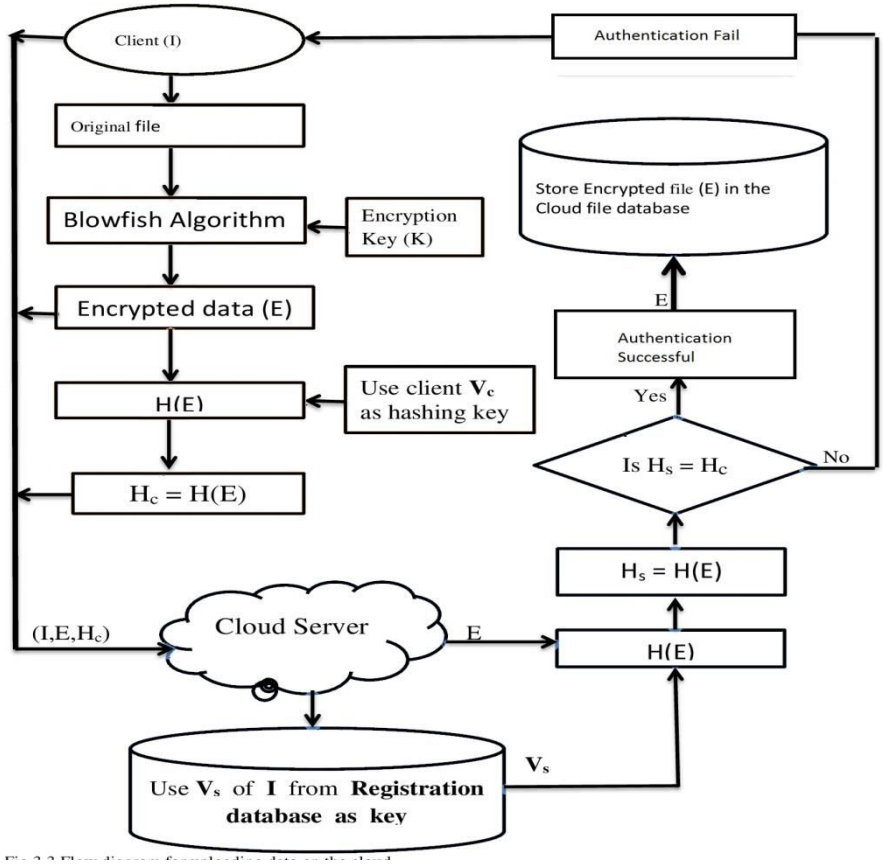


Figure.4: Blowfish Algorithm

The Blowfish algorithm Shown in th Fig-4 is used for developing security and privacy problems in the cloud. The blowfish algorithm is used to generate the key for security. Then the asymmetric key block is generated for the decryption and encryption of both techniques. Slightly new operators cannot use the file which is easily accessible in the network for anyone to contact the blow-fish key. Since one of the most secure cipher blocksis the blowfish key algorithm.

The software of cryptography benefitted the familiarity has the involvement of this research effort and kept the file in cloud surroundings securely. By its name, the customer can acquire the content, if they require the case. If their requirement the satisfied then process this system for obtaining the needed file. The name is decrypted by using the allotted attributes.

The encrypting key of random data in the name by acquiring from name's hidden policy with fulfilling the user's attributes. Through the random key, to extract the actual file after the process of decryption occupied in the satisfied of data. If illegal users cannot use the file then the file has been secured appropriately.

It denotes that the client is non-acceptable to access the authentic file because the client cannot decrypt the name of content effectively. Thus, the unauthorized user cannot download the content because the user does not have the right to decrypt the content(SaranyaandKavitha2017).

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A network encryption/decryption scheme is proposed in which DES and RSA are used to secure text data during its transmission. For instance, if the user would like to send text files, they must upload them into cloud storage and then apply DES encryption and RSA encryption techniques to the received file [28].

Key Preparation:

32 - bit Hexadecimal representation of initial values of sub- keys

p[0] : 243f6a88	p[9] : 38d01377
p[1] : 851308d3	p[10] : be5466cf
p[2] : 13198a2e	p[11] : 354e90c6c
p[3] : 03707344	p[12] : coac29b7
p[4] : a4093822	p[13] : c97c50dd
p[5] : 299f31d0	p[14] : 3f84d5b5
p[6] : 082efa98	p[15] : b5470917
p[7] : ec4e6c89	p[16] : 9216d5d9
p[8] : 452821e6	p[17] : 8979fblb

Steps involved in implementing the proposed system

Sender: Encryption:

1. Uploading the text file by the sender on cloud storage.
2. At the initial level of encryption, applying the DES and followed by RSA.
3. At the end, conversion of the plain text into the Cipher Text, maintained in the database.
4. Foreveryroundr(till18rounds)

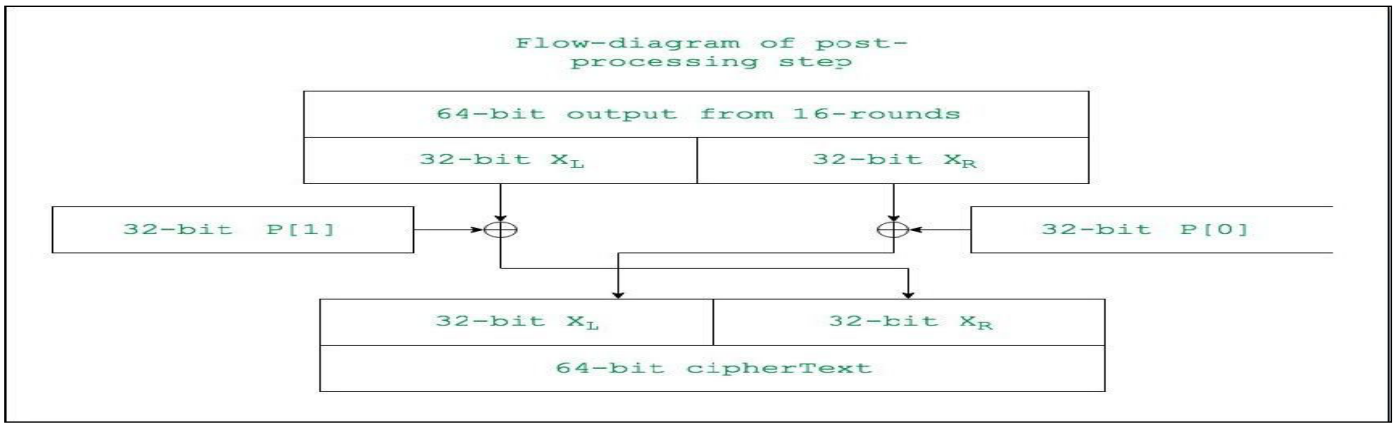
a) XOR left half(L of data with r^{th}p-array entry
b) Use the XORed data as input for f function of the blowfish algorithm
c) XOR the F-function output with the right half

(R)of the data
I. SwapLandRF-Function
a). Splitthe32- bitinputinto4eight/bit quarters, which are input to s boxes
b). S-boxes32bitoutput
c). Outputs are ordered modulo 232 and XORed to create an output of 32 bits and after the 16th spherical XOR L with K16 and R with K17 without the usage of the remaining swap.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Receiver: Decryption

The procedure of decryption is the same as encryption but P1,P2,…, and P18 are used in the opposite order. The package used to execute the code is Python language. Python is a dynamic, high-level, and interpreted programming language and is applicable to a huge quantity of applications. The python ideals are:

a) Simple is good than complex;
b) explicitisgoodthanimplicit;
c) counts of readability; and
d) the complex is good than the complicated.

Decryption:

a) At the receiver end, read the Cipher Text.
b) And then, apply the RSA algorithm for the decryption, and after that DES technique for decryption.

The equations of the blowfish algorithm are:
The block size for the algorithm chosen is 64 bits; five sub keys and arrays are used.

a) 18 entry p array
b) 256 entries boxes(S0,S1,S2,S3)

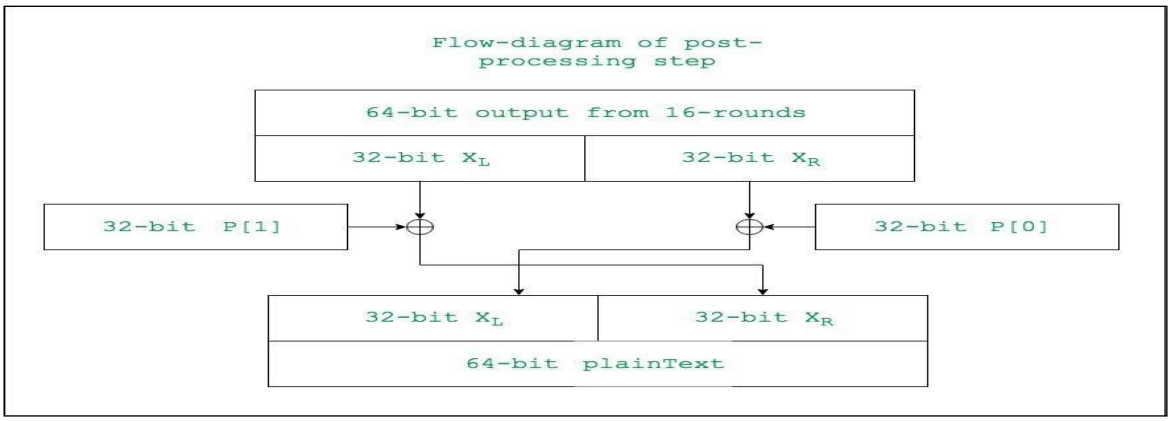
The major characteristics of Python are:

a) OOparadigm;
b) indentationwhitespaceusetorepresentblocks;
c) garbage gathered management of memory;
d) dynamic typing;
e) interpreted runtime;
f) huge third-party libraries repository; and
g) huge standard library.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Python is used in several firms and is used for the development of web, embedded applications, scientific computing, development of software, artificial intelligence, and security of information.

V.CONCLUSION

Data security in Cloud Computing is an important area that should be given much attention. Cyber security is the first line of defense to protect the data from unauthorized users in Cloud Computing . The proposed method Enhanced Security problems in Cloud Computing using Harmonic Encryption Technique, Blowfish Algorithm . Security is the issue when it comes to storing information in the cloud. This paper recommends a multilevel encryption algorithm that is used to secure all the sensitive data stored in the cloud. The proposed method gives 3 security services Confidentiality, Integrity, and availability. Based on the information presented in this study, through the analysis of various papers and the insight gotten from the implementation of the proposed Techniques.

REFERENCES

1.Vinod D. Rajput Kajal D. Jaisinghani "Security In Cloud Computing Using Blowfish Algorithm "International Journal of Mechanical Engineering,7(5).2022
2.Thimma Reddy B, Bala Chowdappa K, Raghunath Reddy S (2016) Cloud security using blowfsh and key management encryption algorithm. Int J Eng Appl Sci (IJEAS) 2(6):59–62
3. Abbas SA, Mohammed MQ (2017) Enhancing security of cloud computing by using RC6 encryption algorithm. Int J Appl Inf Syst 12(8):27–32
4. T. Ramaporkalai, —Security Algorithms in Cloud Computing Security Issues Of Cloud, 5(2), pp. 500– 503, 2017.
5.Ahmad I, Khandekar A (2014) Homomorphic encryption method applied to cloud computing. Int J Inf Comput Technol 4(15):1519–1530
6.Katende N, Wilson C, Kibe AM (2017) Enhancing trust in cloud computing using MD5 hashing algorithm and RSA encryption standard. Int J Sci Eng Res 8(3):550–564
7.H. Kaur, —A Novel Technique of Data Security in Cloud Computing based on Blowfish with the MD5 method, 3(6), pp. 828–837, 2017.
8. B. Joshi, Karuna P, Theofanos, Mary, And Stanton, —Framework for Cloud Usability NIST Special Publication 500-316 Framework for Cloud Usability,‖ pp. 1–18, 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details