Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-019-01403-1

ORIGINAL RESEARCH

Enhancing the security of cloud data using hybrid encryption algorithm

K. R. Sajay[1] · Suvanam Sasidhar Babu[2] · Yellepeddi Vijayalakshmi[3]

Received: 25 March 2019 / Accepted: 12 July 2019

Abstract
Cloud computing is a term which is employed to explain different concepts of computing that includes several PCs linked through a real time network of communication such as internet. Cloud computing is a developing paradigm which has in the recent times attracted lot of researchers because of its capability to decrease the costs related with computing. Due to the rapid growth of cloud computing techniques the rapid raise of services of cloud became outstanding. In today's world data security is a challenging problem. The essential issue related with cloud computing is the security of cloud and the proper cloud implementation over the network. In cloud the models of security namely confidentiality, authentication, accessibility, data recovery and data integrity. It includes services of cloud, model of deployment, security problems and barriers in cloud computing. Nowadays, enhancing security of data in cloud has become a major concern and the solution for this is to apply appropriate encryption techniques while storing the data in the cloud. This study proposes a hybrid algorithm to enhance security of cloud data using encryption algorithm. The main purpose of using encryption algorithms is to secure or store huge amount of information in cloud. This study combines homographic encryption and blowfish encryption to enhance cloud security. It can be concluded that if the security issues are resolved then the future will be the solutions for cloud storage for small as well as large firms.

Keywords Security · Cloud computing · Encryption algorithm · Homographic encryption algorithm · Blowfish encryption algorithm

1 Introduction

1.1 Overview of cloud computing

Cloud computing is a new growth in the networking and computer science field. It has provided the ways of opportunity to satisfy the small and medium scale enterprises aspirations that do not need to waste money in purchasing resources of hardware. It offers an equal chance for all to shine. Cloud computing is based on virtualization principle that there is an individual huge machine and several clients are sharing this machine with a view that they have their own dedicated resources (Handa and Singh 2015). The three main barrier in cloud computing is availability, integrity and access. The main barrier in cloud is accessibility when there is an unauthorized access to information the capability of changing on the data of client emerges. Similarly availability is another barrier where the data must be available every time for clients without having issues that influence the storage and lead to the data of cloud loses. Integrity is another barrier in cloud to correct the data and the security field to control or secure data on cloud and have main lay on service provider (Tannu and Karambir 2017). According to Rahman et al. (2018) the storage of cloud data is an essential cloud computing service known as infrastructure as a service (IaaS). Every day it is acquiring familiarity

✉ K. R. Sajay
sajaykr@gmail.com; sajay.k.r@vidyacademy.ac.in

Suvanam Sasidhar Babu
sasidharmails@sngce.ac.in

Yellepeddi Vijayalakshmi
vijayasasi11@gmail.com

[1] Research & Development Centre, Bharathiar University, Coimbatore, India

[2] Department of Computer Science and Engineering, Sree Narayana Gurukulam College of Engineering, Kolenchey, Ernakulam, India

[3] Department of Computer Science and Engineering, Karpagam University, Coimbatore, India

Published online: 20 July 2019

because of several advantages but the developing privacy and security problems have become a primo subject to service providers as well as users.

1.2 Issues and security of cloud

Shinde and Taur (2015) have stated that nowadays the major issue in adoption of cloud is its privacy and security. The prospects of intrusion within the environment of cloud are several and with greater gains. Privacy and security problems to providers of cloud service who are hosting the services. The provider must assure that their infrastructure is protective and client's application and data are secured by implementing security mechanisms and policies. Shereek et al. (2014) has mentioned that security plays a major part to the down acceptance of cloud computing among users. It is critical to estimate the cloud providers security method quality because several providers are not ready to expose their infrastructure to public, manage and create a secure space of cloud is a challenging task. The security of cloud data relies on using proper security procedures and strategies. According to Sangeetha et al. (2018) storage and security are interdependent and developed security needs an effective technique of storage. As fragmentation takes a major part in effective storage, storage capacity and retrieval cost determines the fragmentation type. Fragmentation is a method where a document is divided into many uniform or fixed size blocks known as partitions where the documents confidentiality level was not regarded. The security problems in cloud data can lead to loss of economy and also a bad reputation if the platform is oriented huge public and are the cause behind the huge adoption of this new solution. The data stored in cloud for customers indicates essential data. This is why the data infringement by an unauthorized 3rd party is unacceptable. Users must be careful while storing their information in cloud storage and all the data must be encrypted before it is transmitted to cloud storage (Arockiam and Monikandan 2014).

1.3 Various algorithms of encryption

According to Nasarul Islam and Mohamed Riyas (2017) the algorithms of encryption have an essential role in the cloud security field. Several algorithms are available for security of cloud and most useful algorithms of cloud security are AES, DES, RSA and MD5. The Data Encryption Standard is a block cipher with symmetric key by the National Institute of Standards and Technology (NIST) and it utilizes secret key for both decryption and encryption. It performs on 64 bit data blocks with 56 bits key. The size of round key is 48 bits and the complete plaintext is classified into 64 bit size blocks. The Data Encryption standard algorithm comprises of 2 permutations and 16 fiestel rounds.

Pallikonda and Yeshwanth Reddy (2017) have mentioned that Advanced Encryption Standard also referred as Rijindael is utilized for protecting data and it is a symmetric block cipher that has been examined and is used vastly nowadays for cloud security. The user determines to utilize services of cloud and will shift their data on cloud. Then user passes their service needs with cloud service provider and selects best services provided by provider. Bhardwaj et al. (2016) has stated that RSA algorithm is best applicable for travelling data from cloud and web-based environment. In performing with cloud computing the data of end user is encrypted and then stored on cloud. When the data is needed the end user requires placing a request to provider of cloud service for data access. For this the provider of cloud service authenticates the user first to be the authentic owner and provides the information to requester using RSA algorithm. Katende et al. (2017) has mentioned that Message Digest algorithm (also referred as MD5) was evolved by Ron Rivest. It generates 128 bits message digests and it is a bit fast. In MD5 algorithm the input text is processed in 512-bit blocks and the result of the algorithm is a group of four 32-bit blocks which comprises the 128 bits message digest. It involves various steps which involves append length, padding, classify the input into 512-bit blocks, process blocks and initialize chaining variables.

1.4 Homographic and blow fish algorithm

There are several algorithms used to enhance the cloud security but this chapter integrates homographic and blow fish algorithm to enhance the security of cloud in an efficient way. Ahmad and Khandekar (2014) used homomorphic encryption which is a new security concept which enables offering outcomes of evaluations on encrypted information without knowing raw information on which the evaluation was undertaken with respect to confidentiality of data. According to Kaur and Kinger (2014) blow-fish algorithm was one of the most similar public algorithms offered by Bruce Scheiner. Blow-fish is a key of variable length with 64 bits cipher block and no attack is known to be successful against this. Blow-fish algorithm is better than other algorithms in power consumption and throughput. Ramaporkalai (2017) stated International Data Encryption Algorithm (IDEA) is a best algorithm of symmetric key and it accepts 64 bits plain text and 128 bits key size. IDEA comprises of 9 rounds and entire rounds are relevant except the one. Gowthami Saranya and Kousalya (2017) have stated that cloud computing is the recent trend in information technology but security is the largest barrier in this field. Every day new prevention method of security is discovered but it is not a permanent solution. Encryption is the best method of security with different encryption techniques applied in cloud computing environment. Thus, it can be

inferred that cloud computing provides much storage space to user and security to that data to make the cloud much strong in future.

2 Literature review

Bangar and Shinde (2014) explained the features of cloud computing and to secure cloud by applying various techniques of encryption. This study also explained about hybrid systems and implemented the cryptographic algorithms like symmetric algorithms like Data encryption standard, advanced encryption standard and asymmetric algorithms like Dieffie Hellman, digital signature and RSA. This study also utilized different attacks so that intruder is not capable to attack the cloud information. This study also compared different algorithms of encryption which was scalable or not.

Lenka and Nayak (2014) proposed a research on enhancing data security in cloud computing using RSA encryption and MD5 algorithm. Cloud computing is a technique through which people can share services, data and resources among people through internet. Since the data is shared through internet security is regarded as a major problem. Many security problems emerges like integrity, authentication and confidentiality in cloud computing. In this research, new model of security have been proposed. The architecture offers a process through which a secure communication is acquired as well as hiding the data from unauthorized users. In this model an integration of digital signature and RSA encryption technique is implemented which can easily with entire kinds of cloud computing characteristics like internet as a service, platform as a service and software as a service. This integration process offers 3 way security that is authentication, verification and security of data. In this research an RSA encryption algorithm is proposed for data confidentiality and MD5 algorithm is used for authentication.

According to the study of Dharini et al. (2014) cloud computing is a developing technique and shared data, software, resources and hosting to consumer on the basis of pay as you use. The major problems in cloud computing is the security of data protection and it decreases the development of cloud computing. The needs of security during the sensitive data transmission and critical application to shared environment of cloud. Over public network for secure communication data can be secured by encryption method. This study proposed techniques of encryption for secure transmission of data, SSL over RSA with magic square offers add on security to cryptosystems. To offer the integrity and confidentiality of data in transmission to and from cloud providers in this study methods of cryptography RSA algorithm are explained and it integrates magic square algorithm with RSA algorithm when implementing security of data in cloud computing.

In the study of Mushtaque et al. (2014) due to rapid development of telecom technology and limitation for transmission of information there is a requirement to use an effective cryptographic algorithm which takes small amount of space after encryption for cipher text. Some metrics of performance such as speed, throughput and time makes the algorithm good. This study found and analyzed an effective encryption algorithm which takes less space among these algorithms of encryption such as TDES, DES, BlowFish, AES and TwoFish. It was found that TDES is good than all other algorithms. DES takes small space than TDES but DES is not a secure encryption technique because after 2^{56} imagination brute force attack can crack this algorithm. TDES is a powerful algorithm but it takes double more space than DES.

Stephen (2014) discussed to protect data using techniques of encryption so that attackers do not theft the information. The security of data is a major concern when used sends the files into cloud and this study explained the techniques of encryption that plays an essential part to secure information and to correct or secure data integrity. The techniques of encryption used to encrypt the user information in cloud and algorithms used are symmetric encryption proposed was to store huge amount of information in cloud storage.

Sidhu and Mahajan (2014) proposed a study on enhancing security in cloud computing structure by hybrid encryption. This study refers a scheme where the plain text is first transformed to whitened text comprising text in the format of hexadecimal using MD5 which is again transformed to encrypted type using Advanced Encryption standard algorithm. Thus it employs two algorithms of encryption one for already encrypted text and one for plain text. The scheme is easy in its method and can be implemented easily but from the viewpoint of security its feasibility is questionable as substantial encryption algorithm use is carried out but no care has been undertaken to protect the keys for data encryption.

It has been stated in Gunasekaran and Lavanya (2015) study that cloud computing is a new paradigm of computation that provides a creative model of business for a firm to adopt information technology without upfront investments. It offers huge computing and data storage to consumers over internet. Cloud computing acquired huge responsiveness from the sector but still there are several problems that are hindering the development of cloud. The data security in cloud is one of the major problems which are much complicated in cloud computing implementation. These problems of security are avoided by different algorithms of encryption. This study presents a review on different algorithms of encryption to develop the security of data in cloud computing.

In the study of Kartit et al. (2015) it has been stated that security of data in cloud storage is a main barrier restricting

its spread and there are different views on the cloud computing security with advantages and disadvantages. This study proposes a secure; privacy preserving and simple inter cloud data sharing architecture based on an encryption algorithm which targets to secure the data stored in cloud from unauthorized access. This study aims to offer a solution that assures the data storage securely in cloud.

Khorsheed et al. (2015) has mentioned that the need to assure the safety of data being exchanged between cloud and users became much essential. Several authentication and security techniques have been proposed to secure the exchanged information. These techniques aim to maintain the privacy, reliability and authentication of data. This study proposed an encryption algorithm to secure data stored within the cloud and these algorithms have been applied are AES and RC5 encryption algorithms. This makes the performance and security level mush flexible and offers the integrity and privacy to identities of users.

Masthanamma and Lakshmi Preya (2015) proposed an efficient data security in cloud computing using the RSA Encryption process algorithm. Nowadays cloud computing is a developing techniques which provides open resources on internet. It is providing huge number of data to users and distributed information over network. But the major problem is it does not have security in distributing information. It becomes the major barrier in the environment of cloud computing. So to develop the security an algorithm named RSA is proposed. It is a new method and it met the needs of public key systems and by employing this algorithm it will develop the data security and consumes reduced cost and time.

According to the study of Thimma Reddy et al. (2016) a user can access the services of cloud as a utility service and initiate to employ them instantly. The fact that services are accessible anywhere and at anytime lead to many hazards. The main goal of the research is to offer security in cloud and secure the data transmission through different trusted channels by using encryption. The BFT algorithms offers liveliness and safety over multi cloud model. Decryption and encryption with blow-fish uses an ample number of sub keys and their method offers a better growth in reducing the cloud computing threats.

According to the research of Neha (2016) in nowadays scenario information security (IS) plays an essential role. Cloud computing is a technique that offers access to computing and information resources from anywhere where a network is available. There is a requirement to protect the stored data on cloud. The main aim behind the encryption algorithm design must be security against uncertified attacks. However, for all applications of cloud computing cost and performance of implementation are main concerns. Encryption algorithm would not be of much use if it is protective but gradual in performance. The performance and security of encryption algorithms must be equal. In this research encryption algorithms namely two-fish, Advanced Encryption Standard and Blowfish has been discussed to examine every algorithm's performance level.

Yugandhara et al. (2016) discussed the cloud storage or data storage concept. The storage of cloud uses the service Infrastructure as a Service (IaaS) and it mentions the security. The best approach to solve the problems of cloud was the techniques of encryption and this study discussed the algorithms like has based message authentication codes (HMAC) and Advanced Encryption Standard (AES). The main purpose of this study was to secure huge amount of information in systems of cloud and store encrypted information into the server of storage which will helps the user to send the information to cloud without fear of information being lost.

Abbas and Mohammed (2017) proposed a study on enhancing security of cloud computing by using RC6 Encryption algorithm. Security issues has been regarded as the most essential part in upsetting the approval or acceptance of cloud computing. In this study RC6 algorithm has been proposed to develop the security level for the stored data by user within the cloud. This algorithm has been used on proposed system to acquire the properties of trusted surroundings. The proposed algorithm shows resistance against attacks that have been used to estimate the algorithm performance.

Salem et al. (2017) discussed the privacy preserving public auditing mechanism and employed the independent entity third party auditor (TPA). The main purpose of the research was to change the information or to develop the integrity and audit the information. This research used the techniques of encryption namely Secure Hash Algorithms (SHA) and Advanced Encryption Standard (AES) scheme and employed the concept of reduplication or to provide rights of access to server. The main aim of the research was to detect the duplicate information and reduce the bandwidth.

Table 1 shows the reviews of enhancing data security in cloud using encryption algorithms.

3 Proposed system

This section explains the design of enhancing cloud security using encryption algorithms. The proposed system in this study needs to secure the data in cloud because security is the major problem which is faced by each user. This study uses two algorithms namely homographic encryption and Blowfish encryption algorithms. This study uses python software tool and cryptography technique to enhance the cloud security. The flow diagram of the proposed system is given in Fig. 1.

From the above flow chart, the first step is to provide the input text. It is a multilayer cryptography algorithm

Table 1 Reviews of enhancing data security in cloud using encryption algorithms

S. no.	Authors	Year	Encryption algorithm used	Findings of the study
1	Bangar and Shinde	2014	DES, AES, Diffie Hellman, digital signature, RSA	Enhance the security of cloud
2	Dharini et al.	2014	RSA with magic square algorithm	Boosts the add on security to the system and increase computational speed of cloud environment
3	Lenka and Nayak	2014	RSA and MD5 algorithm	Handles authentication and security effectively in cloud computing surroundings
4	Mushtaque et al.	2014	TDES, AES, DES, two-fish and blow-fish	TDES is better than all other algorithms
5	Stephen	2014	Symmetric encryption algorithm	User assures that the information is stored only on secured storage and it cannot be used by intruders or administrators
6	Sidhu and Mahajan	2014	Hybrid encryption (MD5 and AES)	Prevents inside attacks in architecture of cloud service
7	Gunasekaran and Lavanya	2015	RSA and AES algorithms	Enhance the data security in cloud computing
8	Kratit et al.	2015	AES and RSA Algorithm	Secure the information and increase resistance to malicious attacks
9	Khorsheed et al.	2015	AES and RC5 algorithm	Increase the complexity and security so that attackers cannot reach the stored data in cloud
10	Masthanamma and Lakshmi Preya	2015	RSA algorithm	Increase the data security and consumes reduced cost and time
11	Thimma Reddy et al.	2016	Byzantine fault tolerance algorithm	Reduce the safety threat on cloud
12	Neha and Kaur	2016	AES, blow-fish, two-fish algorithms	Determine the cloud performance in terms of consumption of power and memory and throughput
13	Yugandhara et al.	2016	Advanced Encryption Standard (AES) and hash based message authentication code (HMAC)	Helps user to pass the information to cloud without fear of information being lost
14	Abbas and Mohammed	2017	RC6 algorithm	Protects Users data against threats and attacks
15	Salem et al.	2017	Advanced Encryption Standard (AES) and message digest5 (MD5)	Enhances public audibility, correctness of storage, develops availability of data and preserves confidentiality of data

with homographic encryption in the first layer and blow-fish encryption in the second layer. The first layer of homographic encryption is applied to the input text. Then the encryption result will be obtained. After that the result of encryption is passed to the second layer which is the blow-fish encryption layer. The final output of encryption layer is obtained.

3.1 Algorithm used

This study uses two algorithms namely homographic encryption algorithm and blow fish encryption algorithm. Each algorithm is explained below briefly:

3.2 Homographic encryption

Homographic encryption systems are employed to carry out operations on encrypted information without knowing the private keys (i.e. no decryption) 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. An encryption is homographic if: from Encrypt (x) and Encrypt (y) it is possible to evaluate Encrypt funct (x, y)) where funct can be $+, \times$ and without using private keys. Among the distinguished homographic encryption according to the operations that permits to assess on raw information the additive homographic encryption (only raw data additions) is the Pailler and cryptosystems of Goldwasser–Micali and the multiplicative encryption of homography is the cryptosystem of El Gamal and RSA.

A_e is an algorithm of encryption with key a

A_d is algorithm of decryption

$$A_d\left(A_e(m) \times A_e(n)\right) = m \times n \; OR \; Encrypt(a(\times)b)$$
$$= Encrypt(a)(\times)Encrypt(b)$$
$$A_f\left(A_f(m) \times A_f(n)\right) = m + n \; OR \; Encrypt(a(+)b)$$
$$= Encrypt(a)(+)Encrypt(b)$$

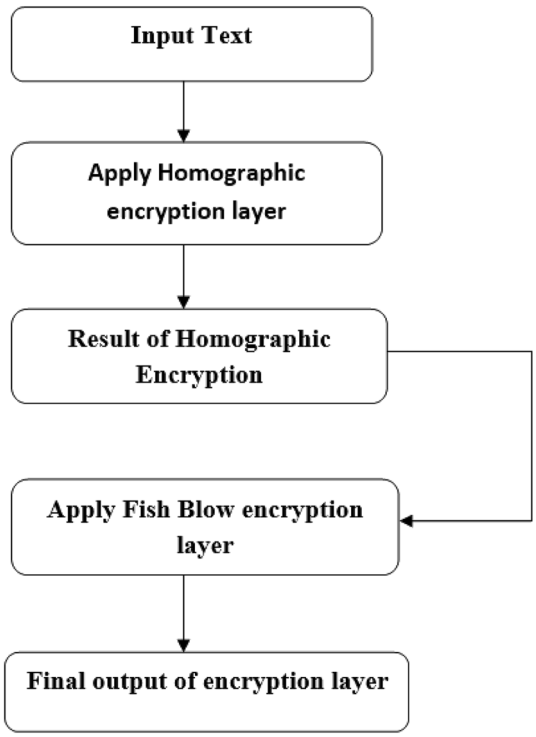


Fig. 1 Flow diagram of the proposed system

The first property is known as additive homomorphic encryption and the second property is referred as multiplicative homomorphic encryption. An algorithm is completely homomorphic if both the first and second properties are fulfilled simultaneously (Tebaa and Hajji 2014). The equations of homographic encryption are:

1. **Generation of key**
   In generation of key the odd integer is selected from some interval p, d $[\eta - 1/2, \eta/2]$
2. **Encryption (p, a)**
   To encrypt a bit a ϵ <0,1>
   $C = ab + 2f + g$, f, g selected randomly such that $|2g| < |a/2|$
3. **Decryption (p, c)**
   (c mod p) mod 2 Decrypt bit
4. An integer 'η' is given the above process is followed to encrypt every bit of 'η' and concatenated to obtain the cipher text for first layer.

3.3 Blow fish algorithm

The blow fish algorithm is used for developing the security and privacy problems in the cloud. The blow fish algorithm is used to generate the key for security. Then a symmetric key block is generated for decryption and encryption of both the technique. Any new users cannot use the file which is freely available in the network for anyone to access the blow fish key. Since one of the most secure cipher blocks is the blow fish key algorithm. In the software of cryptography benefitted the familiarity has the contribution of this research work and stored the file in cloud surroundings securely. By its name the customer can acquire the content if they require the file. If they need the content then process this way for acquiring 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. Using the random key, to extract the actual file from the process of decryption taken in the content of data. If unauthorized users cannot use the file then the file has been secured in an appropriate way. It denotes that the customer is not permitted to access the actual file due to the customer cannot decrypt the name of content effectively. Thus, the unauthorized user cannot download the content because the user does not have the rights to decrypt the content (Saranya and Kavitha 2017). The equations of blow fish algorithm are: The block size for the algorithm chosen is 64 bits, five sub keys and arrays are used.

1. 18 entry p.array
2. 256 entry sboxes (S0, S1, S2, S3)

Encryption

1. For every round r (till 18 rounds)

(a) XOR left half (L of data with rth p-array entry
(b) Use the XOR_{ed} data as input for f function of blow fish algorithm
(c) XOR the F-function output with right half (R) of the data
(d) Swap L and R

F-Function

1. Split the 32 bit input into 4 eight/bit quarters, which are input to s boxes
2. S-boxes 32 bit output
3. Outputs are ordered modulo 2^{32} and XORed to generate an output of 32 bits and after 16th round XOR L with K16 and R with K17 without using last swap.

3.4 Decryption

The process of decryption is same as encryption but P1, P2,…,P18 are used in the reverse order. The package used to execute the code is Python language. Python is a dynamic, high level and interpreted programming language and is applicable for vast number of applications. The python ideals are denoted in the Python Zen of which many statements

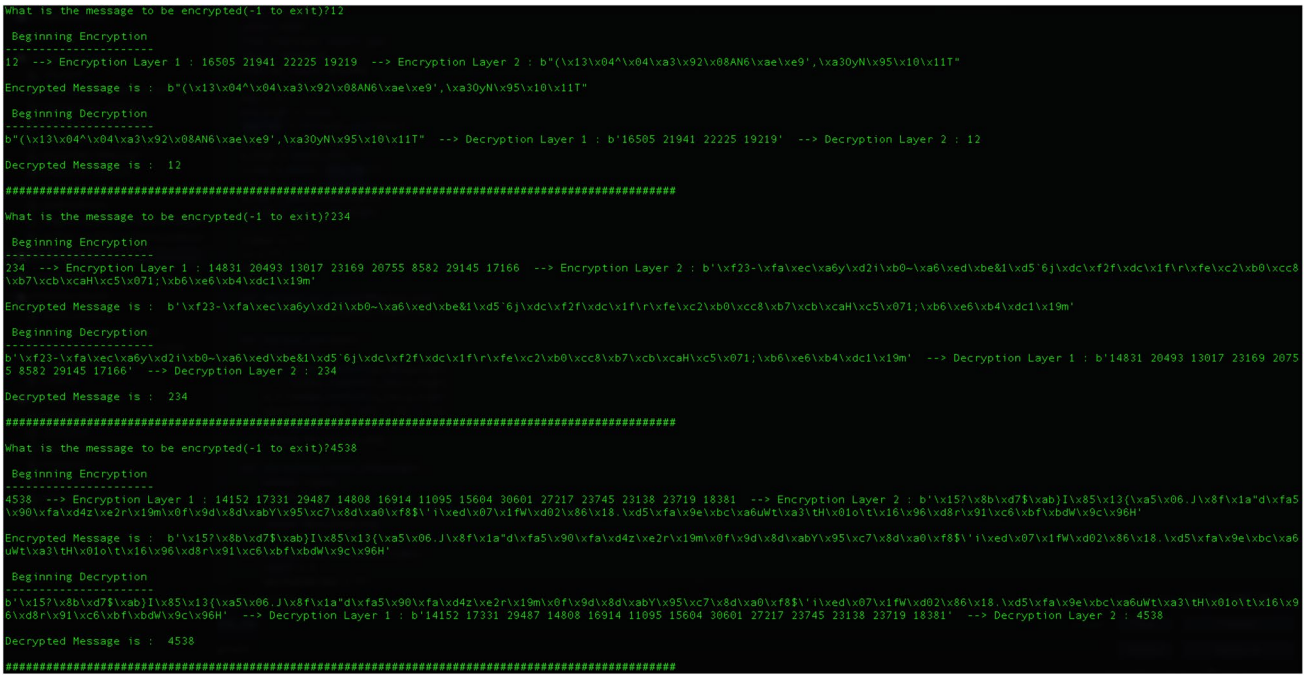
are: (1) simple is good than complex; (2) explicit is good than implicit; (3) counts of readability; and (4) complex is good than complicated. The major characteristics of Python are: (1) OO paradigm; (2) indentation whitespace use to represent blocks; (3) garbage gathered management of memory; (4) dynamic typing; (5) interpreted run time; (6) huge third party libraries repository; and (7) huge standard library. Python is used in several firms and is use for development of web, embedded applications, scientific computing, and development of software, artificial intelligence and security of information.

4 Discussion and results

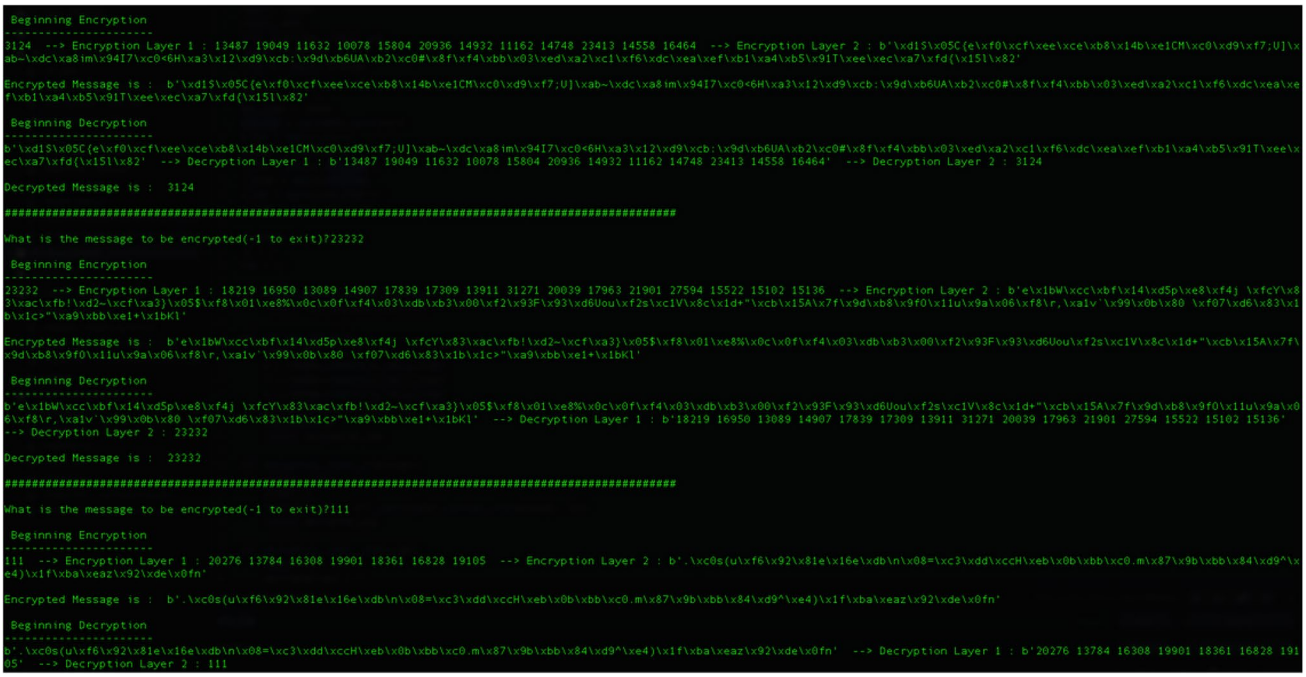
The main aim of this study is to enhance the cloud security using homographic encryption and blow fish encryption algorithms. The homographic encryption basically works on bits so this study uses input integer N, then convert it into binary and each of its bits are encrypted using homographic encryption and after that all these strings are concatenated and passed to second layer of blowfish algorithm. Similarly for decryption the same process steps are used as encryption but first it takes the encrypted text as the input then applies it in the blowfish decryption layer then the decrypted message is passed to homographic layer for decryption and after that bit is obtained then resemble the bits and convert that to original integer. In this way the multi-layer approach works. This is much secure as the multiple layer of encryption and it is also reversible.

Similarly, in Blow fish encryption algorithm the process of key generation creates a secure key for both the process of decoding and encoding is used. Blowfish is a symmetric block cipher that can use for protecting the data securely and similar key are used for both the function of decryption and encryption. The benefits of using blow fish encryption algorithm are: (1) 64 bit size of block; (2) huge data blocks are manipulated; (3) effective algorithm; (4) scalable key from 32 bits to 256 least bits; and (5) carry out easy operations. The blow fish algorithm is also referred as variable length cipher of key block. This is applicable for many applications because the key does not alter and is quicker than most algorithms of encryption. The text files have been selected for decryption and encryption of cloud information. This methodology can be implemented using python software tool and cryptography technique to enhance the cloud security. This chapter shows the comparison of the results on the basis of encryption and decryption time and hybrid of homographic and blow fish algorithm to decrypt and encrypt the file. The output results of the study are:

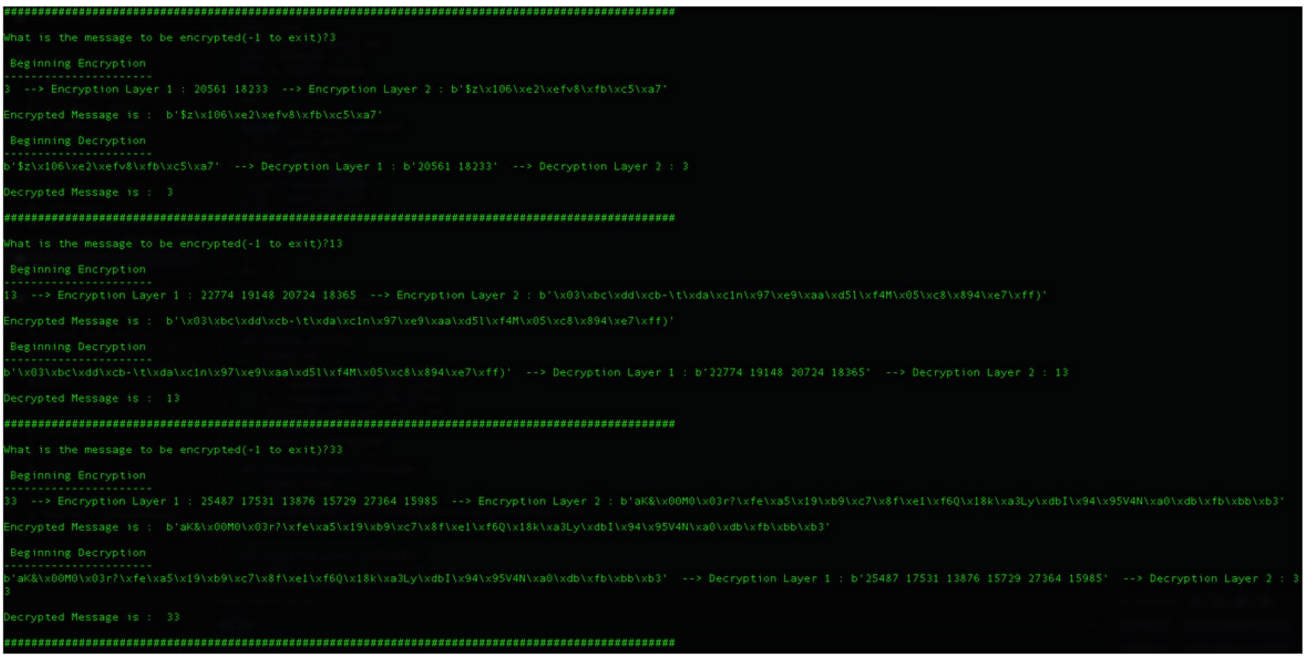
Step 1 The encryption is carried out in the input text



Step 2 The decryption is carried out in the input text



Step 3 The final output of encryption layer



5 Conclusion and future scope

Still cloud computing is an evolving and new paradigm where computing is considered as an on-demand service. Once the firm takes the decision to transform to the cloud it loses control over the information. The cloud security depends on trusted cryptography and computing. Thus, in this study only the authorized user can access the information. Even if certain unauthorized user acquires the information intentionally or accidentally or if the user seizes

the information, then the user can decrypt it and access it due to techniques of encryption. Due to the hybrid algorithm proposed in this study it would be much secure to get hacked. This hybrid algorithm also offers a security technique and better storage using encryption algorithms over the architecture of cloud. The need to use the techniques of encryption is to secure more amount of information so that the hacker did not attack the data. The homographic encryption methods performance is flexible by design and perform computations securely. Similarly, the performance of blowfish algorithm is proportional inversely to the size of key and if the size of key will increase then the performance will decrease and vice versa. Blowfish algorithm is used for developing the security and privacy issues in the cloud. It generates the key for security and a symmetric key block is used for both decryption and encryption. The homographic encryption offers a new dimension to storage in cloud and also offers data confidentiality as in no stage information is exposed in plain text. In future this study is helpful to develop the cloud security in cloud computing. As the need of security enhances, the reliable system of authentication are needed which can help to reduce the unauthorized access and also helps for securing the data. Although the storage of cloud has several benefits still there many issues regarding security that must be resolved. In future the same process can be enhanced with the use of various other algorithms and efficacy of performance is predicted. Thus, it can be concluded that if the security issues are resolved then the future will be the solutions for cloud storage for small as well as large firms.

References

Abbas SA, Mohammed MQ (2017) Enhancing security of cloud computing by using RC6 encryption algorithm. Int J Appl Inf Syst 12(8):27–32

Ahmad I, Khandekar A (2014) Homomorphic encryption method applied to cloud computing. Int J Inf Comput Technol 4(15):1519–1530

Arockiam L, Monikandan S (2014) Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. Int J Adv Res Comput Commun Eng 2(8):3064–3069

Bangar A, Shinde S (2014) Study and comparison of cryptographic methods for cloud security. Int J Comput Sci Eng Inf Technol Res 4(2):205–213

Bhardwaj A, Subrahmanyam GVB, Avasthi V, Sastry H (2016) Security algorithms for cloud computing. Procedia Comput Sci 85:535–542

Dharini A, Saranya Devi RM, Chandrasekar I (2014) Data security for cloud computing using RSA with magic square algorithm. Int J Innov Sci Res 11(2):439–444

Gowthami Saranya R, Kousalya A (2017) A comparative analysis of security algorithms using cryptographic techniques in cloud computing. Int J Comput Sci Inf Technol 8(2):306–310

Gunasekaran S, Lavanya MP (2015) A review on enhancing data security in cloud computing using RSA and AES algorithms. Int J Adv Eng Res 9(4):1–7

Handa K, Singh U (2015) Data security in cloud computing using encryption and steganography. Int J Comput Sci Mob Comput 4(5):786–791

Kartit Z, Azougaghe A, Idrissi HK, El Marraki M, Hedabou M, Belkasmi M, Kartit A (2015) Applying encryption algorithm for data security in cloud storage. In: Sabir E, Medromi H, Sadik M (eds) Advances in ubiquitous networking. Springer, Singapore, pp 141–154

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

Kaur R, Kinger S (2014) Analysis of security algorithms in cloud computing. Int J Appl Innov Eng Manag 3(3):171–176

Khorsheed NK, Khorsheed OK, Rashad MZ, Hamza TT (2015) Proposed encryption technique for cloud applications. Int J Sci Eng Res 6(9):693–698

Lenka SR, Nayak B (2014) Enhancing data security in cloud computing using RSA encryption and MD5 algorithm. Int J Comput Sci Trends Technol 2(3):60–64

Masthanamma V, Lakshmi Preya G (2015) An efficient data security in cloud computing using the RSA encryption process algorithm. Int J Innov Res Sci Eng Technol 4(3):1441–1445

Mushtaque MDA, Dhiman H, Hussain S, Maheshwari S (2014) Evaluation of DES, TDES, AES, bowfish and twofish encryption algorithm: based on space complexity. Int J Eng Res Technol (IJERT) 3(4):1922–1933

Nasarul Islam KV, Mohamed Riyas KV (2017) Analysis of various encryption algorithms in cloud computing. Int J Comput Sci Mob Comput 6(7):90–97

Neha MK (2016) Enhanced security using hybrid encryption algorithm. Int J Innov Res Comput Commun Eng 4(7):13001–13007

Pallikonda S, Yeshwanth Reddy S (2017) Securing cloud data using encryption algorithms. Int J Adv Res Sci Eng 6(11):1188–1193

Rahman MO, Hossen MK, Morsad G, Roy AC, Chowdhury SA (2018) An approach for enhancing security of cloud data using cryptography and steganography with E-LSB encoding technique. Int J Comput Sci Netw Secur 18(9):85–92

Ramaporkalai T (2017) Security algorithms in cloud computing. Int J Comput Sci Trends Technol 5(2):500–502

Salem MZ, Sabbeh SF, EL-Shishtawy T (2017) An efficient privacy preserving public auditing mechanism for secure cloud storage. Int J Appl Eng Res 12(6):1093–1101

Sangeetha SKB, Vanithadevi V, Rathika SKB (2018) Enhancing cloud security through efficient fragment based encryption. Int J Pure Appl Math 118(18):2425–2436

Saranya V, Kavitha K (2017) A modified blowfish algorithm for improving the cloud security. Elsiyum J 4(3):1–6

Shereek BM, Muda Z, Yasin S (2014) Improve cloud computing security using RSA algorithm with Fermat's little theorem. IOSR J Eng 4(2):1–8

Shinde MR, Taur RD (2015) Encryption algorithm for data security and privacy in cloud storage. Am J Comput Sci Eng Surv 3(1):34–39

Sidhu A, Mahajan R (2014) Enhancing security in cloud computing structure by hybrid encryption. Int J Recent Sci Res 5(1):128–132

Stephen O (2014) The study of the application of data encryption techniques in cloud storage to ensure stored data integrity and availability. Int J Sci Res Publ 4(10):1–7

Tannu, Karambir (2017) Enhancing data security in cloud using encryption techniques. Indian J Comput Sci Eng 8(3):280–283

Tebaa M, Hajji SE (2014) Secure cloud computing through homomorphic encryption. arXiv preprint arXiv:1409.0829

Thimma Reddy B, Bala Chowdappa K, Raghunath Reddy S (2016) Cloud security using blowfish and key management encryption algorithm. Int J Eng Appl Sci (IJEAS) 2(6):59–62

Yugandhara K, Ashwini J, Pooja P, Suchita P, Pawar JS (2016) Secure data storage and forwarding in cloud using AES and HMAC. Int Res J Eng Technol 03(02):75–79