BLOWFISH ENCRYPTION ALGORITHM FACILITATE TO SECURE USER DATA OF HYBRID CLOUD IN CLOUD COMPUTING ENVIRONMENT : A STUDY

Narale, S.A.[1] & Butey, P.K.[2]

Department of Computer Science, Dharampeth M.P.Deo Memorial Science College,Nagpur,
Department of Computer Science Kamla Nehru Mahavidyalaya,Nagpur,
Snehal.narale2012@gmail.com,buteypradeepk@yahoo.co.in

ABSTRACT

Cloud computing is a technology which offers different services (like network, server) to the users as you pay on basis. Cloud is free pool of resources [1,2]. Cloud computing has several advantages but apart from this it has to face challenges also. One of the major challenge of cloud computing is security. Security of data plays vital role in cloud computing environment. Data security assures various parameters like integrity of data, confidentiality of data and authentication of data [3]. Now a day's awareness and concern regards to cloud computing and information technology has growing. Most of the data system and processes used data security algorithms to protect cloud data[4]. Hybrid cloud is nothing but integration of two public or private clouds or public, private cloud independently. Resource sharing is one of the advantages of cloud computing while sharing data or transferring data from one cloud to another cloud due to overloading user always wants to security about his data. Symmetric and asymmetric algorithms are used for the security of the data. In this paper researcher presents brief overview on blowfish algorithm a type of symmetric algorithm which emphasis on security of user's data. Blowfish algorithm helps to reduce power consumption in cloud computing. There are various cryptography techniques like DES, Blowfish,RC5, AES, RSA, 3DES , Diffie-Hellman[6,7]. These techniques are used in protecting the data in those applications which are running in a network environment. One more thing should be discussed in this paper is how users data should be secure with minimum cost

Keywords: *Cloud Computing, Blowfish Algorithm, Cloud Security, Hybrid cloud*

INTRODUCTION

Cloud computing is a technology which offers various services to the users as per the requirement. It is not technology but it is a way of delivering computing resources based on the existing technologies like virtualization. Cloud computing is closely linked with IaaS, SaaS and PaaS as service model. It also recommended public, private, hybrid and community cloud ad deliver cloud . One of the benefit of the cloud computing is , it reduces cost of the hardware that have been used by the user at other end. Cloud is nothing but free pool of resources like hardware, software, network and server. As there is no need to install hardware and software at the users end because it is stored somewhere else at another location. Cloud computing assist to access the data from the data center ubiquitously from any location with location independently. Instead of buying the infrastructure or software to run the process and save the bulk of data they just buy as per user requirement on pay basis.

Cloud networks uses various services through minimum utilization of resources to get maximum output. Cloud technology provides a way which requires and utilizes its resources in the best way.[1]

Cloud computing has various advantages over traditional computing which include agility, cost reduction, location and device independency, scalability. Cloud computing has to face the challenge of data security and integrity of the data. Different models and algorithms are proposed to study security issues of the data. The scheme used in the model falls into two categories private and public auditability of the cloud. Private cloud is more efficient than public cloud in terms of security of users' data when data could be share from one cloud to another.

Hybrid cloud is one type of the type of delivery model of cloud computing. The term hybrid cloud is nothing but integration of private and public cloud or community cloud. Resource sharing and resource utilization is one of characteristics of cloud computing in which resources are shared as per users requirement. The process of sharing resources from one cloud to another cloud (from private to public, public to community likewise). When data is transferred or migrate from one cloud to another cloud due to over loading, at the time of migration of data user has concern out its data security and confidentiality of the data. To overcome this problem diverse security algorithms are used in cloud computing environment.

Various cryptography techniques like DES, Blowfish, RC5, AES, RSA, 3DES , Diffie-Hellman[2] are used to provide security to the data. These techniques are fall into two categories according to the symmetric and asymmetric algorithm. These techniques are used in protecting the data in those applications which are running in a network environment. In this research paper, researcher focuses on blowfish encryption algorithm which is used for the protection of the data. Blowfish is type of symmetric algorithm in which only one key is used for encryption and decryption [1,2].

LITERATURE SURVEY

Rachna Arora, Anshu Parashar [1] mentions that today's era demand of cloud is increasing so the security of the cloud and user is on top concern. Hence, proposed algorithms are helpful for today's requirement. Encryption algorithms play an important role in data security on cloud and by comparison of different parameters used in algorithms, it has been found that AES algorithm uses least time to execute cloud data. Blowfish algorithm has least memory requirement. DES algorithm consumes least encrypt-ion time. RSA consumes longest memory size and encryption time.

Shakeeba S. Khan1 , Prof.R.R. Tuteja2[2] focused on Cloud computing which is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc.

Jean Raphael Ngnie Sighom *, Pin Zhang and Lin You [3] , mentions that the Cloud computing is a multi-tenant environment, where resources are shared. Threats can happen from anywhere; inside or outside the shared environment. Deciding whether to migrate sensitive data or keeping it on premise is one of the most important decisions faced by personal users, as well as small and medium-sized enterprises.

Eng. Hashem H. Ramadan, Moussa Adamou Djamilou [4] focused on the security of the data over the cloud storage .cryptographic techniques are used to encrypt and decrypt data. In this research paper researcher proposed security algorithms, which are compatible with each other AES and RSA algorithms. The proposed system that we are designing to use multilevel cryptography, first we are encrypting the data using the AES algorithms and then we are encrypting the output from the first level using RSA algorithms then uploading it over the cloud storage.

Faheem Gul, 2Aaqib Amin, 3 Suhail Ashraf [5] mentions about the cloud security. AES encryption is the fastest method that has the flexibility and scalability and it is easily implemented. On the other hand, the required memory for AES algorithm is less than the Blowfish algorithm. AES algorithm has a very high security level because the 128, 192 or 256-bit key are used in this algorithm. It shows resistance against a variety of attacks such as square attack, key attack, key recovery attack and differential attack. Therefore, AES algorithm is a highly secure encryption method. Data can also protect against future attacks such as smash attacks. AES encryption algorithm has minimal storage space and high performance without any weaknesses and limitations while other symmetric algorithms have some weaknesses and differences in performance and storage space.

Papri Ghosh, Vishal Thakor, Dr. Pravin Bhathawala[6] proposed different encryption algorithms to make cloud data secure, vulnerable and gave concern to security issues, challenges. The comparisons between AES, DES, Blowfish and RSA algorithms are shown. Comparison is done to find the best security algorithm, which has to be used in cloud computing for making cloud data secure which cannot be hacked by attackers. Encryption algorithms play an important role in data security on cloud. Through the comparison, it has been found that 1) AES algorithm uses least time to execute cloud data. 2) Blowfish algorithm has least memory requirement. 3) DES algorithm consumes least encryption time and 4) RSA consumes longest memory size and encryption time.

Akashdeep Bhardwaja*, GVB Subrahmanyamb , Vinay Avasthic , Hanumat Sastryd[7] mentions that Cloud computing is emerging trends in technology industry, public and private enterprise and corporate organizations are either using the Cloud services or in process of moving there but face security, privacy and data theft issues. This makes Cloud security a must to break the acceptance hindrance of the cloud environment. Use of security algorithms and ensuring these are implemented for cloud and needs to be properly utilized in order to ensure end user security. The authors analyzed Symmetric algorithms for different encryption and encoding techniques, found AES to be a good candidate for key encryption and MD5 being faster when encoding.

Omar Mohammed Abdul rahman Abdulkareem1, N. Shanker2 [8] discuss about encryption algorithm and scheme by which data can be protect .Encryption is done by the Blowfish algorithm by this technique the data is encrypted/decrypted fast. In this research paper researcher focus on the system which is used for "Protection the Data of public cloud by encryption of data by applying symmetric key algorithm".

Kishore Kumar1, Dr. M. Gobi2[9] focus on the role of Blowfish & Two fish algorithms that are helpful in addressing the cloud security issues, in which our research would be focusing.

B.Thimma Reddy, K.Bala Chowdappa, S.Raghunath Reddy[10], discuss various cryptographic algorithm like AES,DES,Blowfish and many more can be adopted in cloud computing environment for optimization of data security. Researcher also mention about how to provide security to the data while transmission of data.

Satish Khadke, Sayyed Mustafa and Syed Akhtar[11] discuss the hybrid cloud model and its implementation for providing security to the data . it also make a glance on the autherization of deduplication.

1Eter Basar*, 2Ankur Pan Saikia, 3Dr. L. P. Saiki[12] mention various security issues and challenges of cloud computing.,

Pooja devi,Amit Verma[13] , discuss the workflow of processing of blowfish algorithm in cloud computing environment to provide better security to the data using MD5 method. In this paper researcher also focus on the encryption and decryption of data.

Miss Pulatsya Kanasagara1, Prof. Tushar J Raval2, Prof. Karishma A chaudhary3[14] discuss various data encryption algorithm which are using in cloud computing environment for better enhancement of security

EXISTING ALGORITHM FOR CLOUD SECURITY

There are various security algorithm used in cloud computing environment to secure data stored on cloud. Some of them are discussed as below.

1. Data Encryption Standard (DES) Algorithm

At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm [3].

2. RSA Algorithm

RSA is an algorithm which is used for encryption and decryption of data. It is utilized for public-key cryptography which involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key [3,14].

3. AES

AES is a symmetric key encryption algorithm which used 128 bit block and key length of 128-bits. In cloud computing environment user send request to cloud service provider for utilization of resources and cloud service provider offered services as per the requirement of the user. In this process user decides to use cloud services and then migrate data on cloud. It will first encrypt using AES algorithm and then send it to provider. AES has replaced the DES as the 56 bit keys of DES were no longer considered safe[3,14].

4. DIFFIE HELLMAN

DIFFIE HELLMAN algorithm designed to generate a shared secret key for exchanging information confidentially. DH is one of the earliest, practical examples of public key exchange implemented within the field of cryptography and provides the basis for a variety of authenticated protocols[3,14]

5. BLOWFISH

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier. This is being used in a huge number of cipher suites and encryption products. One of the strong symmetric key cryptographic algorithms is BLOWFISH. It encrypts 64 bit blocks with a variable length key of 128-448 bits. The objectives of designing blowfish algorithm are as follows:

- ➢ Blowfish encryption rate is fast on 32-bit microprocessors.
- ➢ It requires less than 5 kb memory for execution.
- ➢ For the making of design and implementation simple blowfish algorithm uses only Simple primitive operations such as addition, XOR and table look up.
- ➢ It is secure and flexible. Blowfish suits applications where the key remains constant for a long time (e.g. Communications link encryption), but not where the key changes frequently (e.g. Packet Switching)

Since the data is encrypted and decrypted by secret key, using blowfish algorithm encryption method the data over the cloud and secret key encryption/decryption is extremely quick as compare to public key encryption [5].

Implementation of blowfish algorithm in software provides good rate.AES algorithm gives more attention on the standard of encryption. The DES or IDEA can use blowfish as drop-in replacement wherein it takes 32-448 bits of a variable length key for both domestic and exportable uses. This process uses large key-dependent S-boxes and a 16-round Feistel cipher, which resembles CAST-128 in structure where fixed S-boxes are used [6].

SECURITY ISSUES OF HYBRID CLOUD IN CLOUD COMPUTING ENVIRONMENT

Security is one of the most significant aspects in everyday day computing. Cloud computing uses various new technologies and services in our day to day life applications. Cloud provides various services to the customers that will beneficial for them. Apart from the advantages of cloud computing, it has to face many challenges related to the security like data security, trust, expectations and performance issues. In hybrid cloud, due to the problem of overloading, the load may be distributed or transferred amongst other cloud to balanced load[7]. Data may be transferred from one cloud to another it may be either from public to private cloud likewise. Security of data at end user level is one of the crucial aspects in the cloud computing environment. In Cloud computing hybrid cloud has to face various security issues some of them are as follows given in Fig1:

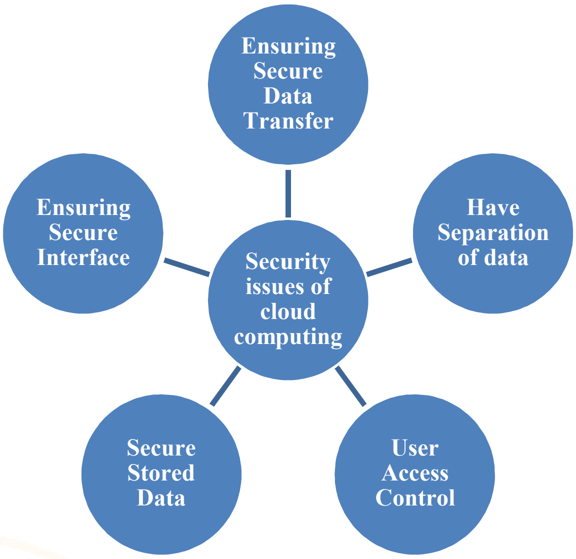
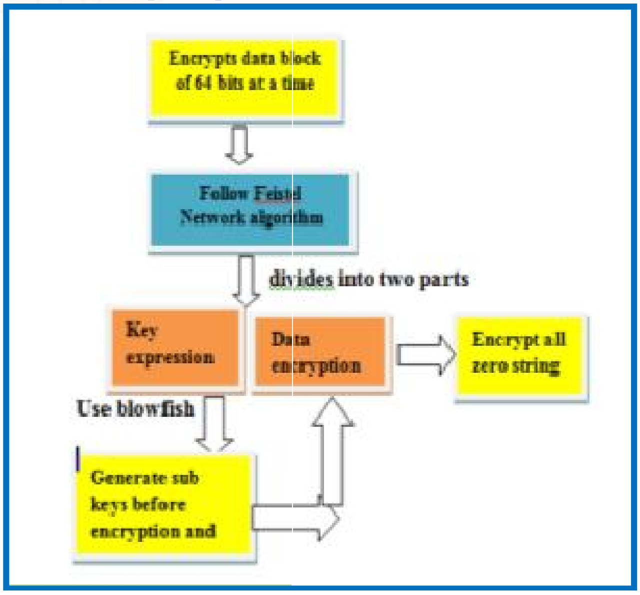

Ensuring Secure Data Transfer
Ensuring Secure Interface
Security issues of cloud computing
Have Separation of data
Secure Stored Data
User Access Control

Fig 1: Security Issues of Cloud Computing

Asymmetric and symmetric encryption helps to secure data in cloud computing environment**.** In asymmetric algorithm one key is used for encryption called the Public key and a different but inter related key for Decryption called the Private keys when performing transformation of plain text into cipher text[7,8]. The main asymmetric algorithms are ECC, Diffie-Hellman and RSA. Another type of algorithm is Symmetric algorithm in which a single secret key is shared to encrypt as well as decrypt data. AES, 3DES, RC6 and Blowfish these are symmetric algorithms use for encryption of data.

1. WORKING PRINCIPLE OF BLOWFISH

Fig 2.shows the working flow of blowfish algorithm and Fig 3 illustrates BLOWFISH encryption scheme used in hybrid cloud environment[8, 13].


Encrypts data block of 64 bits at a time
Follow Feistel Network algorithm
divides into two parts
Key expression
Data encryption
Encrypt all zero string
Use blowfish
Generate sub keys before encryption and

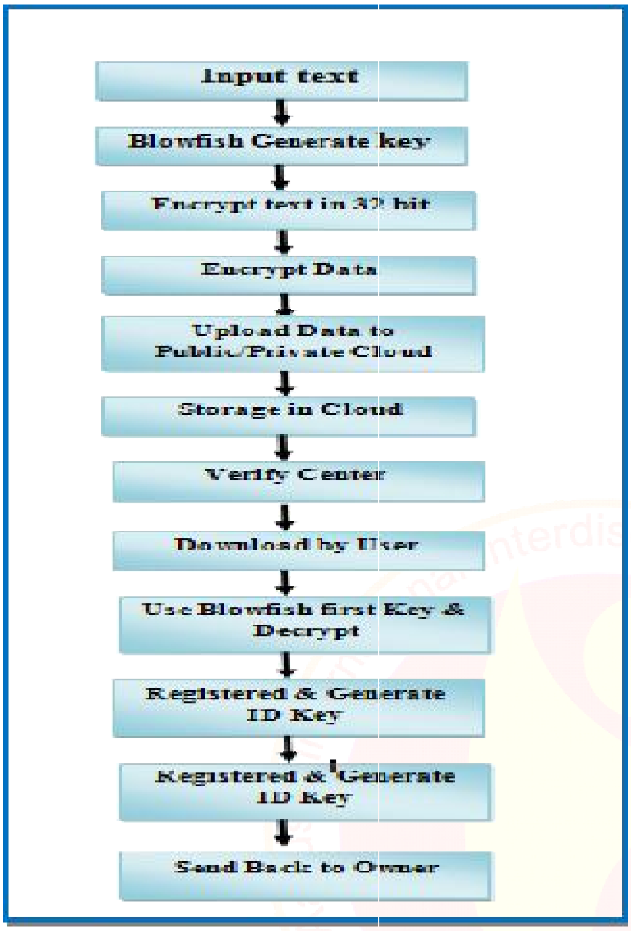


Fig 2: Working Principal of Blowfish

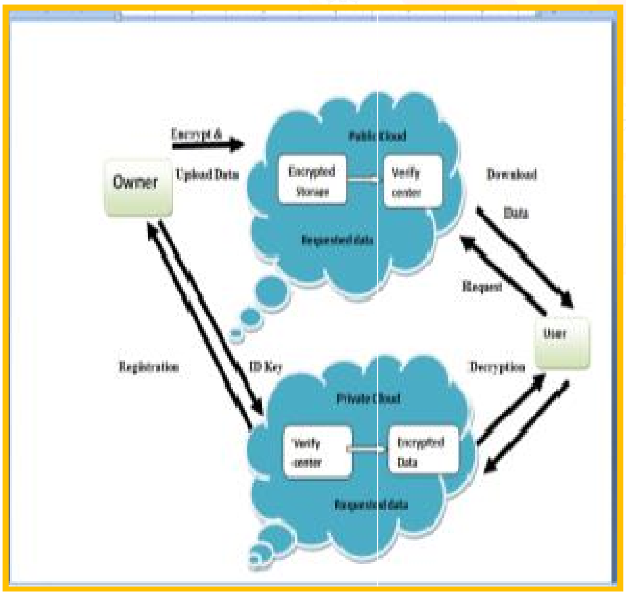


Fig 3 : BLOWFISH Encryption Scheme in Hybrid Cloud

1. Objective of the Work

- Provide security in hybrid cloud computing environment.
- Secure management of virtualized resource using resource provisioning.
- Availability, recovery and auditing.
- Identification and privacy in computing.
- Dynamic data operation security[12].

2. Data Encryption Algorithm:

```
Divide x into two 32-bit halves: xL, xR
For i = 1to 16:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR[14]
```

3. Advantages of Blowfish in Cloud Computing Environment

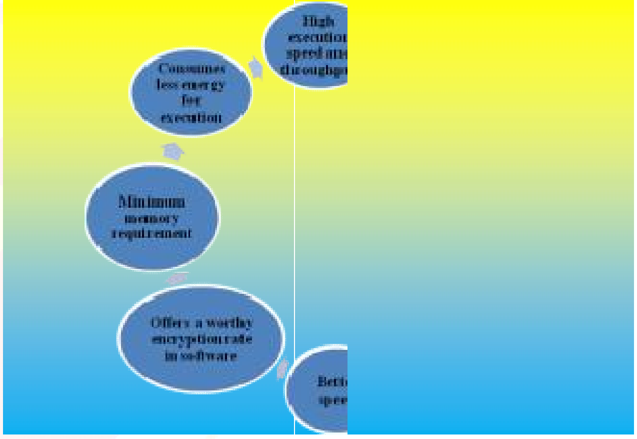

High execution speed and throughput
Consumes less energy for execution
Minimum memory requirement
Offers a worthy encryption rate in software
Better speed

Fig 4 : Advantages of Blowfish

RESULT AND DISCUSSION

Implementation of symmetric Encryption BLOW Fish algorithm in hybrid cloud will help to provide better network security in cloud computing environment as well as it will facilitate user to secure data from cloud. Data migration is one of the issue of cloud computing. In hybrid cloud when data is transmitting from public cloud to private cloud due to overloading at that time the security of data is crucial aspect of cloud . After balancing load blowfish encryption algorithm generate key to encrypt and decrypt data for protection . The following are few benefits of encryption in the cloud environment [9]. The encryption helps to

a. Substantiate the privacy of the institutional data, where the encrypted data used in transmission as well as storage location.

b. It will help to offer Confidence about the data backups regarding safety of the data in cloud environment.

c. It will facilitate to enlarge potential of profits to customers with sensitive or regulated data by maintaining the key by cloud data owner.
d. Help to accomplished secure multi tenancy in cloud computing environment.

CONCLUSION

Cloud computing technology is an emerging technology. The major problem that has to face is security about user's data. In this research paper researcher discussed various security algorithms which will help to secure users data stored on cloud. There are various symmetric and asymmetric encryption algorithms like AES, DES, RSA, Blowfish and Diffie Hellman algorithm. Blowfish algorithm is a symmetric encryption algorithm which generates two keys that will help the user to provide protection to the data that is stored in the cloud. Blowfish encryption method is fast method to encrypt and decrypt the data by secret key[10]. This method use encryption algorithm which is quick as compare to other encryption method like public key method. Blowfish algorithm gives high performance with less through put in cloud computing environment. It will facilitate to secure data in hybrid cloud of cloud computing environment. In hybrid cloud architecture data is secure and for better management of virtualized resources Blowfish algorithm assist to protect data from cloud. By implementation of blowfish in cloud the speed of transformation of data will improve. Data is encrypted and decrypted using only one public key which can be generated using blowfish algorithm to identify data from cloud[11]. In future, more work has to done on implementation of security algorithm at higher level of cloud storage in cloud computing environment for better advancement in security of big size data. **SN 2392]**

REFERENCES

1. Rachna Arora, Anshu Parashar(2013), Secure User Data in Cloud Computing Using Encryption Algorithms , International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 4, PP.1922-1926
2. Shakeeba S. Khan1 , Prof.R.R. Tuteja2(2015), Security in Cloud Computing Using Cryptographic Algorithms , International Journal Of Innovative Research In Computer And Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1,PP 148-154
3. Jean Raphael Ngnie Sighom *, Pin Zhang And Lin You(2017) ,Security Enhancement For Data Migration in the Cloud, Future Internet, PP 1-13.
4. Eng. Hashem H. Ramadan, Moussa Adamou Djamilou (2017), Using Cryptography Algorithms to Secure Cloud Computing Data and Services ,American Journal Of Engineering Research (AJER) American Journal Of Engineering Research (Ajer) E-ISSN: 2320-0847 P-ISSN : 2320-0936 Volume-6, Issue-10, PP-334-337.
5. Faheem Gul, 2aaqib Amin, 3 Suhail Ashraf[2017], Enhancement Of Cloud Computing Security With Secure Data Storage Using AES ,International Journal Of Computer Science and Mobile Computing a Monthly Journal of Computer Science and Information Technology ISSN 2320–088x Impact Factor: 6.017 IJCSMC, Vol. 6, Issue. 7, PP.27 – 32.
6. Papri Ghosh, Vishal Thakor, Dr. Pravin Bhathawala[2017], Data Security and Privacy in Cloud Computing Using Different Encryption Algorithms, International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 7, Issue 5, ISSN: 2277 128x
7. Akashdeep Bhardwaja*, Gvb Subrahmanyam b , Vinay Avasthic , Hanumat Sastryd[2016] , Security Algorithms For Cloud Computing, Science direct International Conference On Computational Modeling and Security Procedia Computer Science 85 (2016) PP 535 – 542.
8. Omar Mohammed Abdul Rahman Abdulkareem1, N. Shanker2[2015], Implementation of Data Encryption by Using Blowfish Encryption Algorithm to Protect Data in Public Cloud, International Journal Of Innovative Technologies, ISSN 2321-8665 Vol.03,Issue.02, PP:0229-0232.
9. Kishore Kumar1, Dr. M. Gobi2[2017], Comparative Study On Blowfish & Two Fish Algorithms For Cloud Security , International Journal Of Current Trends in Engineering & Research (Ijcter) E-ISSN 2455–1392 , Scientific Journal Impact Factor : 4.23, Volume 3 Issue 9, PP. 1 – 11.
10. B.Thimma Reddy, K.Bala Chowdappa, S.Raghunath Reddy[2015], Cloud Security

Using Blowfish And Key Management Encryption Algorithm, International Journal Of Engineering And Applied Sciences (Ijeas) Issn: 2394-3661, Volume-2, Issue-6, , PP 59-62.

11. Satish Khadke, Sayyed Mustafa and Syed Akhtar[2017], Design and Implementation of a Hybrid Cloud Approach for Secure Authorized Deduplication, International Journal Of Computer Applications (0975 – 8887) Volume 163 – No 6, PP 5-8.
12. 1eter Basar*, 2ankur Pan Saikia, 3dr. L. P. Saikia[2017], A Survey On Security Issues Of Cloud Computing, International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 7, Issue 5, ISSN: 2277 128x,PP 171-188.
13. Pooja Devi,Amit Verma[2017], Data Security In Cloud Computing Based On Blowfish With Md5 Method, Devi Pooja, Verma Amit; International Journal Of Advance Research, Ideas And Innovations In Technology, Issn: 2454-132x , Impact Factor: 4.295 , Volume3, Issue4,PP 149-154.
14. Miss Pulatsya Kanasagara1, Prof. Tushar J Raval2, Prof. Karishma A Chaudhary3[2017], A Review On Data Encryption Algorithm In Cloud Computing, Vol-3 Issue-5 , IJARIIE-ISSN(O)-2395-4396 6668 ,2017,PP 259-267.