Hybrid Cryptosystem using Modified Blowfish Algorithm and SHA Algorithm on Public Cloud

Aakash Gore
Department of Computer Science & Engineering.
Research Scholar, Swami Vivekanand College of Engineering Indore, M.P, India.

S. S. Meena
AssistantProfessor, Swami Vivekanand College of Engineering Indore, M.P, India.

Preetesh Purohit
Associate Professor, Swami Vivekanand College of Engineering Indore, M.P, India

ABSTRACT
Cloud computing has shaped the conceptual and infrastructural basis for tomorrow's computing. The world-computing infrastructure is quickly moving towards cloud-based design. Whereas it's important to require benefits of cloud based computing by suggests that of deploying it in varied sectors, the security aspects during a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved, that has resulted in a new business trend supported Cloud Technology. With the introduction of various cloud based services and Geographically distributed cloud service providers, Store sensitive data usually in remote servers with the chances of being exposed to unauthorized parties. If security isn't robust and consistent, benefits that cloud computing have to provide will have little believability. This paper presents an approach, which is based on modified blowfish algorithm and SHA algorithm for the security purpose on the cloud environment.

Keywords
Hybrid Cryptosystem, Cloud Security, SHA, Blowfish, File Splitting.

1. INTRODUCTION
Recent development within the discipline of could computing have immensely converted the way of computing as well as the proposal of computing resources. In a cloud based computing infrastructure, the resources are extra often than not in anyone else's premise or community and accessed remotely with the help of the cloud customers [1].

These offers the following three sensitive states or scenarios, which can be of detailed challenge throughout the operational context of, cloud computing are Transmission of exclusive sensitive knowledge to the cloud server,Transmission of knowledge from the cloud server to consumers' desktops andStorage of customers' individual knowledge in cloud servers, which might be some distance, flung server now not owned with the support of the consumers.

Blowfish encryption algorithm is symmetric algorithm with following parameters

- Basic: It uses addition, XOR, lookup table with 32-bit operands.
- Compact: it run in very less memory compare to other

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time.it will track the Feistel network.

2. LITERATURE REVIEW
In this paper [1], Author worked on RSA and Blowfish algorithm. RSA used for digital signature and Blowfish for cryptography. Blowfish is fasted and strong algorithm for encryption and decryption. They worked on Hybrid algorithm which work on symmetric and asymmetric cryptography on cloud computing. Author recommended increasing key size of algorithm to improve performance of overall system. They also recommended for input data as image or video.

As per given in paper [2], Researchers presented, adding new key (additional key) in X-OR operation in blowfish algorithm. With the help of additional key blowfish algorithm more robust and strong. They suggested increase key length of additional key; blowfish algorithm will give better result.

As per given paper [3], Author focus on cloud security using blowfish algorithm. They provide data security and data protecting using various channels. Author confirmed that proposed approach performs better in decreasing the safety threat on cloud.

In this paper [4], Author works Hybrid algorithm that is combination of two algorithms one is public key cryptography and another is secret key cryptography. They provide security on data at the time of uploading and downloading data from cloud server. Digital signature will use in future for data will reached at destination correctly.

In this paper [5], Author worked on RSA and MD. They used RSA partial homomorphic algorithm for encryption and description on data. MD5 calculate hash value on uploaded data, for authentication. In Future new combination of algorithm will improve performance of existing system.

3. PROBLEM FORMULATION
Due to openness and multi-tenant characteristics of the cloud, the ordinary security mechanisms are no longer suitable for functions and data in cloud. One of the most problems are as following:

- Due to dynamic scalability, service and location transparency features of cloud computing mannequin, all varieties of utility and data of the cloud platform have no fixed infrastructure and security boundaries. Within the occasion of security breach, it is problematic to isolate a particular resource that has a risk or has been compromised [2].
- Consistent with carrier supply items of Cloud computing, assets and cloud services could also be

owned by means of a couple of providers. As there's a clash of curiosity, it is complex to install a unified protection measure [3].

- Because of the openness of cloud and sharing virtualized assets via multitenant, consumer information is also accessed via different unauthorized users [8].

To resolve these security disorders many cryptography algorithms available. Cryptography can furnish offerings, akin to: integrity checking—reassuring the recipient of a message that the message has not been altered in view that it was once generated with the aid of a reputable source and authentication. Cozy the cloud way comfy the storage database hosted by means of the cloud supplier. Safety pursuits performed through encryption /decryption method. Encryption/Decryption method is mixture of three forms of algorithms.

4. EXISTING SYSTEM

In this days and age cryptography becomes a countless technique for information protection. There are two methods for information encryption, one in all them makes use of one key for encryption and decryption, and it is often called Symmetric Cryptography like DES and Blowfish. The other system uses two keys for encryption and decryption it's Asymmetric Cryptography like RSA Algorithm [4][5].

Blowfish is a 64-bit cipher and its key length extended from 32 bits to 448 bits, it has 16 rounds and generates the key dependent S-Boxes.

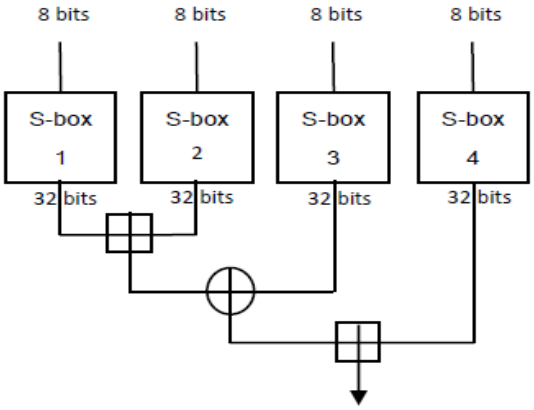

Figure 1 Substitution box of Blowfish

Above Figure-1 describe that fours S Boxes are used. These S box treats as submission box. Boxes derived from key, which is encrypted. Size of each S Box is 32 bit words.

In Figure-2 Function F splits its 32-bit input into four 8-bit.the block diagram of the Blowfish encryption algorithm like the Feistel network. There are 16 rounds (Feistel network); each round consists of a key dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. It replaces each byte by the contents of an S-box, and combines the results as follows

Letting signify addition modulo:

$$F(a, b, c, d) = ((S1[a]\ S2[b])\ S3[c])\ S4[d]) \ldots.(i)$$

The Key is converted from 448 bits to several sub-key arrays totaling 4168 bytes. The keys are generated before data encryption or decryption. The p-array consists of (P1, P2.P18) sub-keys each one is32-bit. And also four 32-bit S-Boxes each one consist of 256 entries (Sn, 0, Sn, 1,…Sn, 255).then 521 iterations are done togenerate all sub-keys.In this function, the only additional operations are four indexed array data lookup tables for each round.

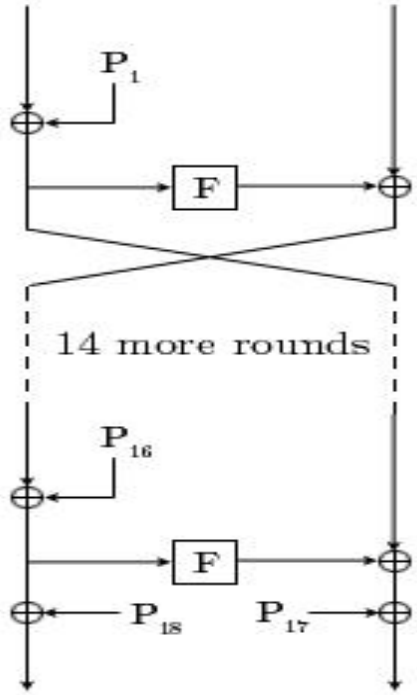

Figure 2 Fiestel Network of Blowfish algorithm

5. PROPOSED WORK

SHA and MD5 is used for message digest algorithm same as the older MD4.SHA and MD5 both use for calculate hash value.In proposed system we are using SHA algorithm with blowfish algorithm. Blowfish algorithm for encryption and decryption and SHA use for calculating hash value of file which is upload by user on cloud server.

The Secure Hash Algorithm takes a message of less than 264 bits in length and produces a 160-bit message digest which is designed so that it should be computationally expensive to find a text which matches a given hash. ie if you have a hash for document A, H(A), it is difficult to find a document B which has the same hash, and even more difficult to arrange that document B says what you want it to say.

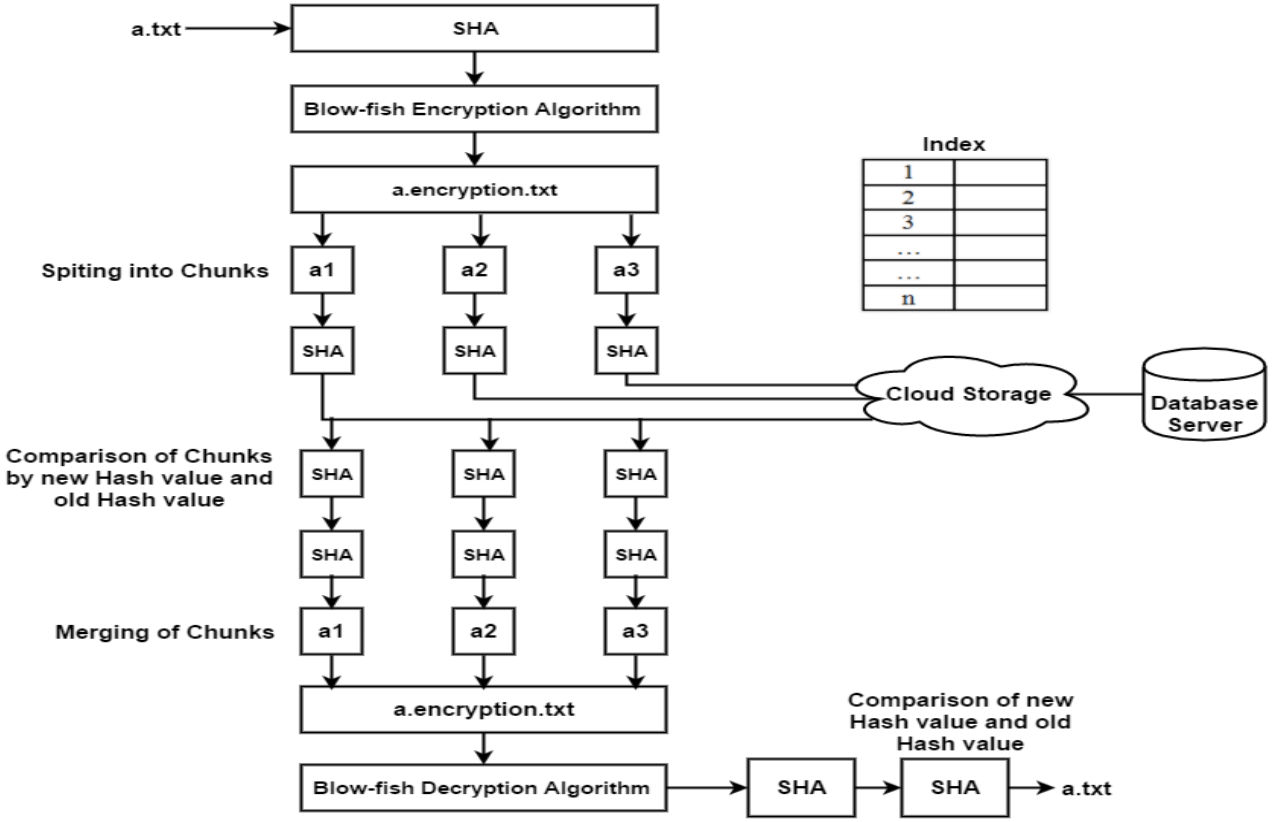

Figure 3 Proposed System using Blowfish and SHA

Proposed Algorithm BF_SHA (file , key)

{

1. x=get_file_data();
    a. //x be the input of 64 bit data
2. x will be divided into two halves x_1 and x_2.
3. $x_1=x_{1:32}$
4. $x_2= x_{33:64}$
5. Fori = 1 to 16 do
    a. $x_1 = x_1$ XOR P_i X-OR K_1
    b. $x_2 = F(x_1)$ XOR x_2X-OR K_2
    c. swap x_1 and x_2
6. After the sixteenth round, swap x_1 and x_2 again to undo the last swap.
    a. $x_2= x_2$ XOR P_{17}
    b. $x_1 = x_1$ XOR P_{18}.
7. Hash Value=Calculate SHA (x)
8. Recombine x1 and x2 to the cipher text:
9. Decryption in reverse order except p1,p2,…..p18.

}

The proposed work describes the combination of blowfish and Secured Hash Algorithm (SHA). Steps are as:

- Proposed System take input as a text file(a.txt). First calculate hash value using SHA algorithm.
- On text file apply encryption using Modified Blowfish Algorithm then splits the encrypted file into three equal size chunk (a1, a2 and a3)
- After chunks, calculate hash value of each chunks using SHA Algorithm and store chunks and its hash values on cloud server.
- Cloud Server creates and maintain index of chunks.
- When user downloads the file, first calculate new hash value of chunks and compare with its old hash value.
- If both new and old hash values are the same, then next step is to merge chunks else show message "file is corrupted".
- Next step gets encrypted file then decrypt the file by using blowfish algorithm.
- In last again calculate new hash value by using SHA algorithm and compare with old SHA value.
- If both are same file (a.txt) then download otherwise show message "file is corrupted".

6. RESULT

Proposed system implemented on open-shift public cloud. First, we create account on open shift and configure public cloud with following configurations

- JBoss Application Server
- MY SQL Server
- PHP MY Admin

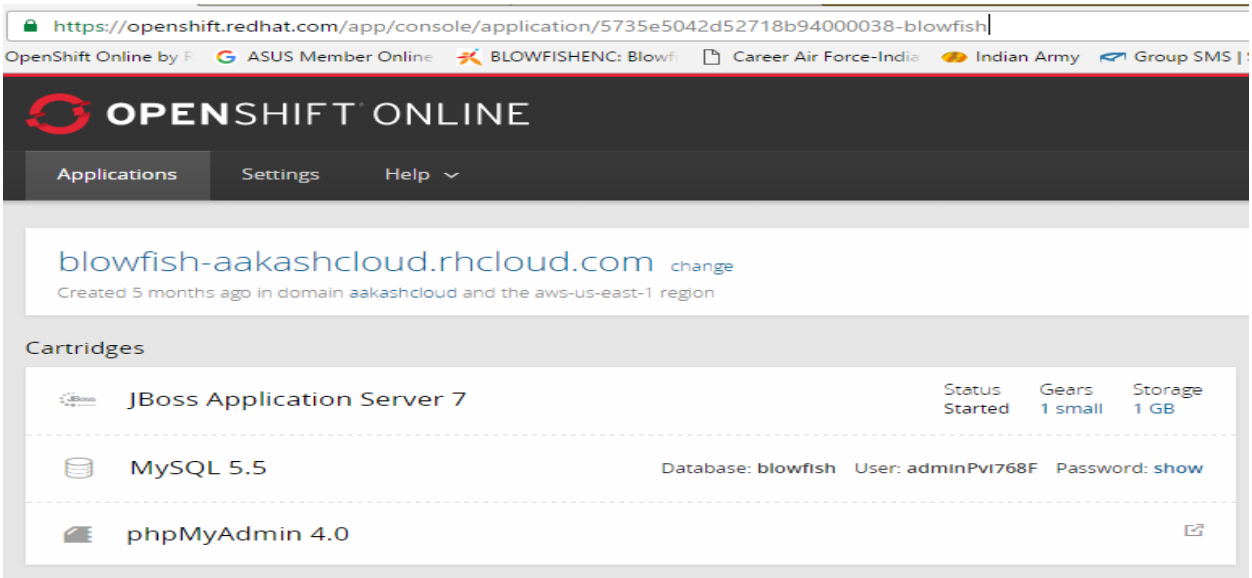

Fig. 4 Dash Board of open shift public cloud

Table 1 Encryption and Decryption time of Files

File Size	Encryption Time (ms)		Decryption Time (ms)	
	Blowfish	Modified Blowfish	Blowfish	Modified Blowfish
100 Bytes	757	694	35	32
10 KB	932	819	54	50
100 KB	1523	1380	80	72
1 MB	2890	2640	116	105

After a Configuration of public cloud, Configure Eclipse for open shift cloud.

In public cloud user can upload and download file. At the time of uploading calculate hash value of file using SHA and encrypt file using Modified Blowfish algorithm. Here we calculate encryption and uploading time of file.When user downloads file then decrypt file using Modified Blowfish algorithm and calculate hash value of file. At this time, we calculate decryption and downloading time of file.

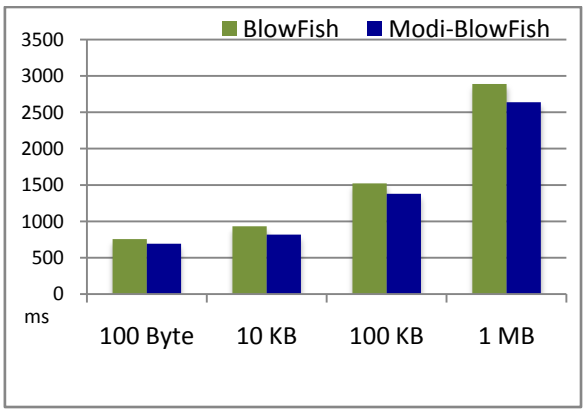

Fig. 5 Encryption Time of Different Size of Files

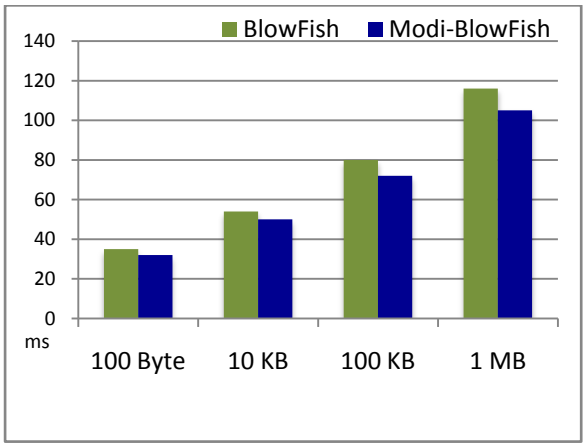

Fig. 6 Decryption Time of Different Size of Files

7. CONCLUSION

Security of data and trust drawback has invariably been a fundamental and difficult predicament in cloud computing. The proposed model improves the security issues related to cloud models and protection of file exchanging is solved. The above mentioned model is fruitful in data as a service, which can be extended in their service models of cloud. Problem of existing algorithm has been solved by combination of Blowfish and Secured Hash Algorithm (SHA).Implementation of proposed utility, which computes hash values of files at the knowledge owner facet, can eliminate the need of third occasion auditors. The consequent hash values from this utility are stored at secure regional hash repository. The information file can be retrieved again every time needed and checked for any arguments amongst events worried by using re-computing and matching the hash effect with the pre-computed hash value.

8. REFERENCES

[1] Viney Pal Bansal ,Sandeep Singh"A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs "RAECS UIET Panjab University Chandigarh 22nd December 2015 , 978-1-4673-8253-3/15/$31.00 ©2015 IEEE

[2] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha "A Study

of New Trends in Blowfish Algorithm" ,International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 2, pp.321-326

[3]B.Thimma Reddy, K.BalaChowdappa, S.Raghunath Reddy "Cloud Security using Blowfish and Key Management Encryption Algorithm "International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661, Volume-2, Issue-6, June 2015

[4] JasleenKaur, Dr. SushilGarg, "Security in Cloud Computing using Hybrid of Algorithms",International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015 ISSN 2091-2730.

[5] PriyankaOra , Dr.P.R.Pal "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography " IEEE International Conference on Computer, Communication and Control (IC4-2015).

[6] Dr. VivekKapoor, Rahul Yadav, "A Hybrid Cryptography Technique to Support Cyber Security Infrastructure", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 11, November 2015.

[7] B. Thimma Reddy, K. BalaChowdappa, S. Raghunath Reddy, "Cloud Security using Blowfish and Key Management Encryption Algorithm", International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661, Volume-2, Issue-6, June 2015.

[8] Hazem M. El bakry, Ali E. Taki_El_Deen, Ahmed Hussein El tangy, "Implementation of a Hybrid Encryption Scheme for SMS / Multimedia Messages on Android", International Journal of Computer Applications (0975 – 8887) Volume 85 – No 2, January 2014.

[9]AkhilBehl, "Emerging Security Challenges in Cloud Computing**",** in Proc. of World Congress on Information and communication Technologies ,pp. 217-222, Dec. 2011.

[10]Srinivasarao D et al., "Analyzing the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011.

[11] TingyuanNie and Teng Zhang "A study of DES and Blowfish encryption algorithm", in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.

[12] Jitendra Singh Yadav et al.," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" , International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 2,Aug. 2012.