ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Robust Cryptographic Technique for Improving Data Security in Cloud Computing

Shouket Ahmad Kouchay

Research Scholar, Department of Computer Science, India

ABSTRACT: Cloud computing has revolutionized the IT world. Cloud computing is not only beneficial for everyday users but also for large enterprises, as it is capable of sharing large data in different forms and to safeguard that valuable data in secure storage, security management procedures must be implemented. Cloud computing is dynamically flexible as well as sizable and cost-efficient involving important virtual tools. There is not adequate security in usual asymmetric encryption, as single secret key in this algorithm could be hacked by some attackers. So there arises an improved data protection requirement. Different and effective ways to secure cloud computing has been introduced but the data remains at constant threat by security exploits. Secure storage in cloud computing is a fundamental move for the IT world. This research proposes an effective Cryptographic technique for securing the data in Cloud Computing that provides better security and accountability to data in the cloud. The primary analysis of the proposed technique demonstrates better performance results. This research also highlights many security issues in different encryption algorithms.

KEYWORDS: RSA, blowfish algorithm, Cloud computing, encryption, decryption, data security

I. INTRODUCTION

The term cloud computing came from "on-demand computing" where data is shared over the internet. As cloud computing is based on open network environment security issues arise now and then, mostly concerned with privacy and trust [1]. Thus, it makes important for us to do this research and apply new techniques to prevent security problems.

The more cloud locations are prone to risk when data is distributed in the cloud. The organizations will always be exposed to huge risks while connected to the internet as their critical data could get exposed to the outside world due to a security issue in cloud computing. At present, virtual world criminals can effortlessly access cloud data storage. When coming towards individual cloud data storage, vital data files and records are linked to third party software which opens doors to vulnerability and data breach, it is becoming one of the most common and primary issues in cloud security. What makes cloud storage vulnerable is that it stores individuals or organizations data which can be accessed by different sources linked to the cloud network. It is obligatory to supply a secure connection over several network resources. [2]

Large service providers are represented by organizations (such as Amazon, IBM) using cloud networks are delivering software-based service. Cloud-based software is brought into the cloud network, and it appears as it has been provided by a cloud user. When cloud users use the system, they are redirected to the malware instead of their real software. [2].

Flooding attacks cause both direct and indirect denial of service (DoS). Usually, when a cloud finds a lot of requests for a particular server, it accounts for additional computing power to that service to handle all the requests. This is the general idea of cloud computing. However, in the real situation, this would provide an advantage to the “hacker”. After that, the hacker only needs to focus on his flooding attack on a single server so that he can gain access to cloud account services. This is service is known as direct ' Denial of Service’ because the hacker focuses on a particular service to get it down. [4].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

There are different security risks in cloud computing like Poor Cloud security, Denial of service, Lock-in effect, Downtime. The other security risks like Resource exhaustion, Confidentiality and the Integrity of the data in the cloud result in the financial, economic and reputational losses and can make an organization inoperable. So there is an important need to study cloud computing security issues and find methods to minimize these risks and their impact.

So to mitigate the security threats in cloud storage, we must first understand trust issues linked to cloud computing storage. Generally, cloud computing users don't have full control over the available assets in the cloud and data exposure risk is always there. Our research is dedicated to address the common as well as rare issues that arise constantly in cloud computing and also to present effective technique (the combination of RSA and improved Blowfish algorithm) to mitigate or prevent such problems in the future.

II. RELATED WORK

Cloud computing is not only beneficial for everyday users but also for large enterprises, as it is capable of sharing large data in different forms. This makes sharing very riskier and makes trusting the client almost impossible. The issue of trusting cloud computing doesn't lie in the technology itself. Cloud computing is very beneficial for both users and the service provider, as it provides services that cost less and are easy to put into use. Unluckily, cloud computing was adopted before the arrival of effective technology to handle annoying challenges of trust [5].

The idea behind cloud computing is to provide innovative data sharing services over the network changing the way we used to share data resources before. There are a lot of security and data protection vulnerabilities in authentication techniques such as eavesdropping, replay, exhaustive and dictionary attacks, etc. The cloud services have been adopted by business companies and institutions to empower their customers [6]. But despite using this cloud technology, the information exchange in cloud services has become vulnerable in terms of security issues.

The authors describe the process of AES and RSA in their encryption and decryption. They think the hybrid algorithm improved the speed of RSA encryption and decryption and also solves the key management problem in the AES algorithm [7].

Fang presented an overview of the AES algorithm, and then the significance of the security in the cloud storage system, they proposed an approach for the security mechanism of users' files when uploading and downloading using AES algorithm. [8]. The Schneier [9]proposed Blowfish, a new secret-key block cipher. Also, this paper discussed the requirements for a standard encryption algorithm. While it may not be possible to satisfy all requirements with a single algorithm, it may be possible to satisfy them with a family of algorithms based on the same cryptographic principles.

In Cloud Storage, any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources, the encryption algorithm [8] plays a vital role. It is a fundamental tool for protecting the data.

The comparative study by Faung shows different encryption algorithms kind; Asymmetric and symmetric, block cipher and stream cipher. These EA are AES, IDEA, DES, RC4, and RSA. At the conclusion, he found from the experimental results, that RSA has the least performance efficiency as compared to DES, AES, IDEA and RC4 algorithm. Also, conclude that the performance of RC4 algorithm is best as compared to all other algorithms discussed in this paper. [10]

Existing methods like DES and RSA algorithms experimented by authors [11] for cloud storage security is with only single level encryption and decryption. This type of encryption can be breached with ease. Several techniques have been proposed by various researchers like DSA and RSA and AES and RSA. But DES is extremely susceptible to attacks, Weak keys is also a big issue and is exposed to brute force attack. Some AES versions are slower and complex to implement on small blocks [12].

The space between implementation and innovation is wide enough to stop cloud computing users, complete trust. So to remove this gap, we must first understand trust issues linked to cloud computing. Generally, cloud computing users don't have full control over the available assets in the cloud and data exposure risk is always there. Many enterprises want the minimal cost and effective benefits of cloud computing, without losing control and security. The security that

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

is generally applied at the network border tends to disappear in cloud built computing, where networks without robust firewalls are connected by many types of cloud consumers with private and public data hubs [13].
Various researches have been conducted to address the common as well as rare security issues that arise constantly in cloud computing and also to present effective techniques to prevent such problems in the future. [12] [14].

Some of the data sharing transaction enterprises don't even scan the user accessing their network, such as salesforce.com [10]. The first thing we tend to consider is a clear understanding of cloud infrastructure for the organization before moving towards the next stage which is to dig deeper into this network-based technology. The devices that are linked to cloud network must be secure with innovative technology whether they are general pcs or smartphones [11].

Organizations must enforce NAC (Network Access Control) polices for better control and usage. But to ensure that robust security techniques are aligned properly, the use of VPN (Virtual Private Network) must be considered before connecting the device to the cloud [12]. When servers are not invigilated properly, the organization is at high risk of exposure to threats and network attacks. This research will help to mitigate the threats and vulnerabilities that any cloud user has faced or might face in the future.

III. RESEARCH METHODOLOGY FOR PROPOSED TECHNIQUE

The proposed technique uses a combination of RSA and improved Blowfish algorithm to produce encryption whenever the user uploads data in the cloud storage. The improved Blowfish algorithm reduces the computational cost by applying shifting and transformation techniques on certain rounds by decreasing the number of rounds in the algorithm.

The pattern is reversed of the same algorithms in a decrypted form when the user downloads a file from a cloud network, making it as secure as possible. The technique is intended to secure and preserve data. The Architecture of the proposed technique is shown in figure 1.

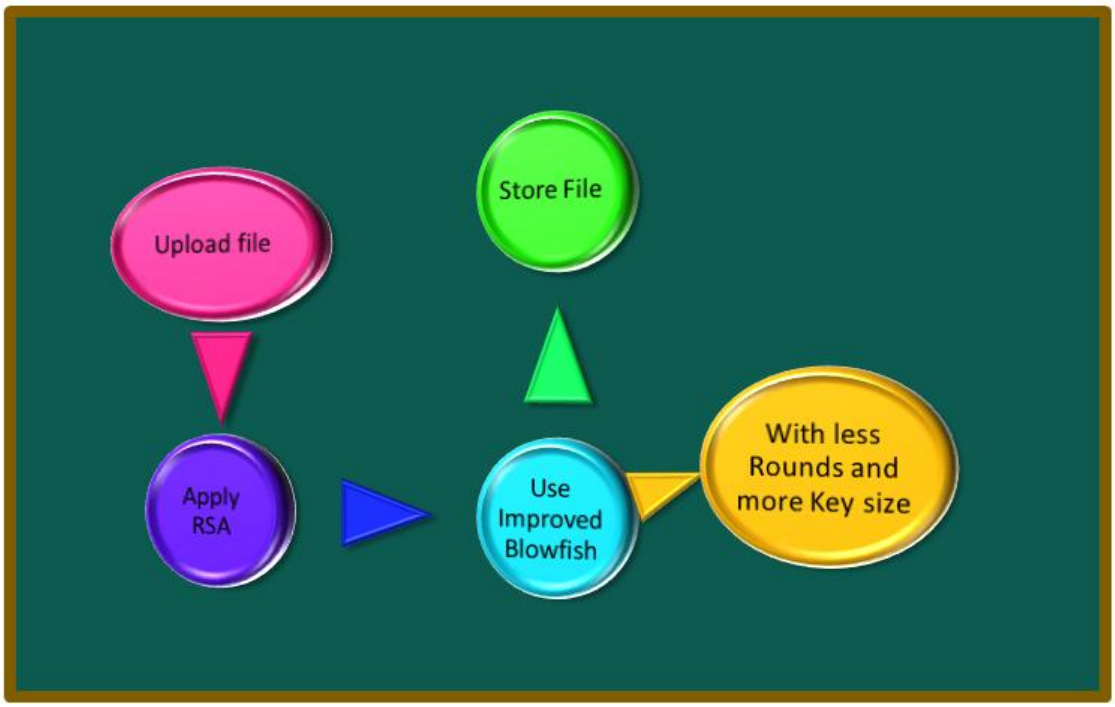

Figure 1. The architecture of the proposed technique

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

We are projecting a blend of two diverse algorithms to abolish any data breach in the cloud storage. The combination of RSA and improved Blowfish algorithm is very effective because RSA algorithm is mainly used in modern computers whereas improved Blowfish (Cipher) produces a very effective encryption rate in software and is complex, secure enough to handle all levels of tasks by applying transformation and shifting method.Certain rounds in this algorithm can be taken less and more block size to increase its performance.

There are many reasons we are going to use an algorithm to do that, the main two reasons are:

1. *Algorithms use less drive space.*
2. *Algorithms can help in storing data while making it undetectable.*

For instance, if someone tries to breach into an individual's cloud storage and examine it, they will be able to retrieve data even after its being deleted. As data leave traces in the drive even after being deleted. But, using these (RSA & Improved Blowfish algorithms) to encrypt the data, anything that is stored will not appear in its actual form and it'll be almost impossible to retrieve for the Cyber Criminals.

Why use RSA?

RSA algorithm is one of the most commonly used asymmetric algorithms. It works based on the private key as well as the public key. It involves multiplication of two large prime numbers and once the key is created, it discards the numbers.

RSA uses two keys (Private and Public). Private Key will be used for decryption and public key for encryption. Public key involves three steps:

1. Key Generation
2. Encryption
3. Decryption [1]

Why use Blowfish?

Blowfish algorithm a symmetric key algorithm is based on Feistel Network; it runs simple encrypted tasks sixteen times. The size of the block is 64 bits, but the stretching key length is possible up to 448 bits. It will be very effective in Cloud Storage because hefty microprocessors can function efficiently by using encrypted data. [15]. The 64 bits of plain text is divided into two parts of size 32 bits. The key size of blowfish is large than DES and cannot be can be decrypted easily like other algorithmsi.e. DES. The application of a single blowfish round with two Sboxes connected with XOR added to the plaintext increased the speed performance of the algorithm [16]. The Blowfish algorithm is efficient in power consumption has been confirmed by author [17]

The Improved Blowfish algorithm works in a very effective and secure way due to following reasons:

1. It divides every block into half.
2. Both the right and left halves are further divided.
3. The newly created right half of the block is the last result when the left half is XOR'd.[7]
4. The data encryption contains permutation, key, operations and XORs 32-bit words with sixteen repeated functions [3].
5. Decreasing the no. of rounds and increasing key size in the Blowfishalgorithm makes it more efficient.

The security problems are the primary concern in cloud computing, especially privacy and loss of data, but effective techniques are going to provide easily applicable methods to prevent or minimize the security issues.

Although our experimental results have shown that blowfish algorithm takes less time for encryption and decryption process than RSA and AES, but the combination of RSA and Improved blowfish algorithm have shown overall better performance.

The flow of data being uploaded through the combination of RSA and improved Blowfish algorithm encryption techniques in the Cloud is shown in figure 2.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

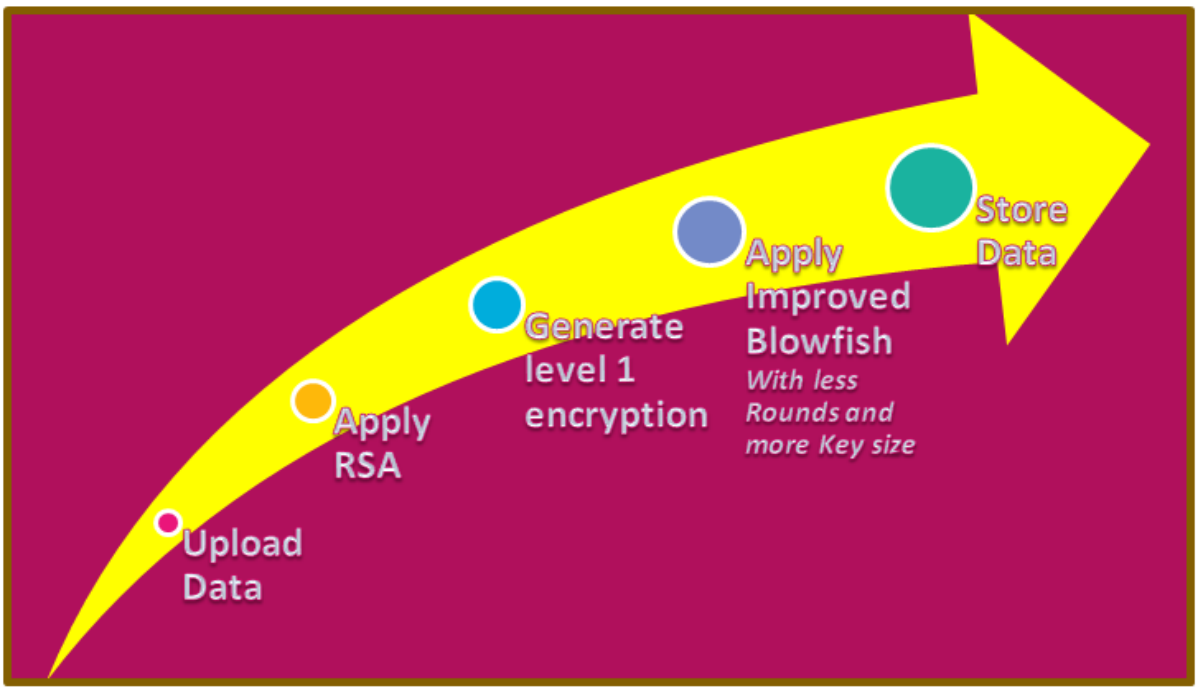

Figure 2.*Flow of a data being uploaded through RSA and Improved Blowfish algorithms in the Cloud Storage*

IV. CONCLUSION

Although cloud computing has many benefits, it is also an attraction to security risks. Just as nothing can be perfect, so as Cloud computing can still significantly improve and can be utilized more efficiently. We have proposed a secured encryption and decryption technique for improving Cloud Data Security. Various encryption algorithms and security concerns have been thoroughly reviewed. The experimental results of the proposed technique demonstrate overall better performance results. The combination of RSA and improved Blowfish algorithm is very effective technique to mitigate the security risks and their impact.

REFERENCES

[1]. Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International journal of Computer Science and Information Technology Vol2 (3), 242-249 2012.
[2]. Kevin Curran, Sean Carlin and Mervyn Adams, “Security issues in cloud computing”, Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.
[3]. Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.L. (2006) On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing. 109-116.
[4]. Wu, B., Chen, J., Wu, J. and Cardei, M. (2007) A survey of attacks and countermeasures in mobile ad hoc networks. Signals and Communication Technology, Part II, 103-135.
[5]. “Demystifying Cloud Computing” by Qusay F. Hassan, Faculty of Computers and Information, Mansoura University, Egypt
[6]Shouket Ahmad, "Innovative CAPTCHA-Based Authentication Technique for Cloud Data Protection". International Journal of Emerging Technology and Advanced Engineering, V6(9). (2016)
[7] ChengliangLiang,Ning Ye Reza Malekian4, RuchuanWang,"The Hybrid Encryption Algorithm of Lightweight Data in Cloud Storage", 2nd International Symposium -2016
[8] Fang, Z., Sun, Y., Sun, Y., & Yang, J. (2013, July). The Reseach of AES algorithm and application in cloud storage system. In 2nd InternationalConference on Science and Social Research (ICSSR 2013). Atlantis Press.
[9] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

[10]Alam, M. I. (2013). A Comparative Analysis of Different EncryptionTechniques of Cryptography. International Journal of Advanced andInnovative Research (2278-7844), 160.
[11]. LimorElbaz&Hagai Bar-El, "Strength Assessment of Encryption Algorithms", October 2000, website: http://www.discretix.com/PDF/Strength%20Assessment%20of%20Encryption%20Algorithms.pdf
[12] Cloud Security Alliance,"Security Guidance for Critical Areas of Focus in Cloud Computing" V3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.-2011
[13]. Effective Ways of Secure, Private and Trusted Cloud Computing by Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta and ManojDiwakar ; CSE & IT, Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh, 173215,India
[14] Shouket Ahmad Kouchay "Data Protection in Cloud Computing-vulnerabilities, challenges and Solution". International Journal of Computer Trends and Technology (IJCTT) V34(4):179-185, April 2016. ISSN:2231-280
[15]. B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.
[16]. Velte, T., Velte, J., Elsenpeter, R. (2009). Cloud Computing: A Practical Approach. McGraw-Hill Osborne Media
[17] Kondawar, S. &Gawali, D. (2016). Security algorithms for wireless medical data. Online International Conference on Green Engineering and Technologies (IC-GET). IEEE.