Analysis and Encryption Technique using Multi-Dimensional Protection in Cloud Computing

Ankur Saxena [1], Raj Kumar Paul [2],
[1,2]Department of Computer Science & Engineering,
RKDF University, Bhopal, India

Abstract: In this day and age where each measurement of human life is seeing new advancements relatively consistently, the conventional processing is likewise enhancing exponentially. A standout amongst the most progressive change is the origination of Cloud computing. Cloud computing bolsters appropriated benefit situated engineering, multi-client and multi-space regulatory framework. Along these lines, it is more inclined to security dangers and vulnerabilities. It not only offers a high degree of mobility, flexibility to its user, it provides a hassle free environment.

In this paper, it is talk about a portion of the systems that were implemented to data security and propose availability data in cloud. giving multi-dimensional security to cloud framework, up to a specific degree this arrangement additionally obliges the need to framework availability. We have used AES and Blowfish as encryption techniques and CHAP (Challenge Handshake protocol) as an authentication technique to achieve some of the security goals.

Keywords: Cloud Computing, Encryption Techniques, Authentication, Security, CHAP, AES.

I Introduction

Cloud Computing is a combination of IT administrations given by many specialist co-ops. The term cloud was begun from the web and is likewise a stage that gives individuals the open door for sharing assets, administrations and data internationally [1].

As per the Cloud definition given by Cloud Security Alliance Group [6], Cloud figuring advocates the utilization of accumulation of administrations, applications, information and foundation which involves a reusable pool of PCs, processors, data and capacity media. These reusable parts can be quickly provisioned, executed and decommissioned, scaled-up or down to give an on-request utility model of designation and utilization of assets [2].

Gartner defines cloud computingas a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies. Strong confidentiality means cloud providers will not be able to access the data. For example confidential and classified business information, government secret information, etc. Applications that execute in the cloud can poise several factors including load balancing, bandwidth, size of data and security [3, 4]. One of the key obstacles to cloud approval is data security and privacy, because the user and the service provider are not contained in the same trusted domain.

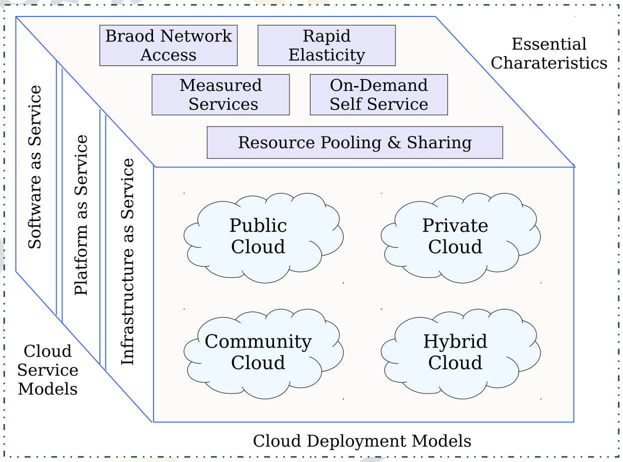


Figure 1: Cloud Computing

Security issues are increasingly significant in lower layer Infrastructure as a Service (IaaS) to higher Platform as a Service (PaaS). These cloud layers are deployed (public, private, community, and hybrid) in high end MCC (Mobile Cloud Computing). Users vacillate to shift into the cloud because of certain ambiguities in its architecture that makes cloud computing insecure [5].

II Characteristics of Cloud Computing

Following inherent characteristics of cloud computing makes it a highly promising computing platform to use [6].

On-Demand Self-Service

Users of cloud computing have the flexibility to easily manage the resources like processors, storage media and network resources as per their need, and more surprisingly it does not require any manual intervention of any administrator or service provider.

Broad Network Access

Cloud capabilities are distributed over the internet which makes it broadly available and increases its usability to any remote or local area. These services are accessed via standard mechanisms and users have the flexibility to use any thin or thick client applications (from their Desktops, laptops, PDAs, mobiles etc.) to leverage cloud service.

Resource Pooling

CSP's resources are pooled to serve multiple end users using a multi-tenancy model with the ease of allocating and deallocating the resource based on the consumers need. Due to the distributed nature of cloud services, these resource provisioning is transparent to the end users.

Measured Service

Cloud enabled systems have the capability to track and optimize the use of pooled resources according to consumers' usage, and the users are charged on fair usage policy.

Rapid Elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time [7, 8].

III Problem Identification

We have reviewed into a portion of solutions proposed by various authors/researchers to strengthen the security of a cloud system implementation; every one of them were focused to give better confirmation and information encryption methods [9].

Anyway sending a straightforward validation and encryption process will not be adequate to evacuate all sort of vulnerabilities identified with cloud framework security (client ID, information classification) and system availability. If some of these vital aspects is not provisioned with sufficient means, it may lead to two issues.

- Security
- Availability

Another essential perspective separated from verification and information security is framework accessibility, so regardless of whether the cloud framework gives both; a solid validation and solid information security includes yet at the same time needs in giving high accessible of the cloud framework (because of successive blackouts/downtimes) at that point additionally the cloud system will not be robust [10, 11].

Thus remembering every one of these viewpoints, in our proposed work we have recommended a joined answer for increment the cloud system **security** and **availability** In the following area we will give the points of interest of proposed work [12].

IV Proposed Work

As stated in problem statement the major challenges to a cloud system implementation are Data Security and confidentiality. Therefore as part of the proposed work, we have targeted these major concerns using following approaches:

1. Data residing in the cloud storage
2. Data transmission via network
3. User identification and Authentication

In order to provide secure and authorized data access from cloud systems, following components needs to be secured:
1. Data Privacy & Data Security:
For achieving data privacy and security, we have proposed to use following Encryption algorithms:

- AES (Advanced Encryption Standard)
- Blowfish Encryption Algorithm
- Hybrid Encryption Algorithm (Combination of AES & Blowfish)

Data/document to be uploaded will be encrypted by a different algorithm based on the security level of the document.
2. User Authentication:
For providing a strong user authentication process, we have proposed to use two-level authentication process.

- **Level #1 - Password based Authentication:** In this level, user will be authenticated using the generic password based authentication
- **Level #2: CHAP Authentication:** Once user successfully gets authenticated with level-1, he/she has to go through CHAP authentication process as part of level-2 authentication.

V Hybrid Encryption Algorithm

Hybrid Encryption Algorithm is a two-phase process. In the principal stage the report (in plain content) is scrambled with AES calculation and after that in the second stage the figure content produced from stage 1, is again encoded utilizing Blowfish calculation to create the last figure content, which makes it about unimaginable for any programmer/assailant to interpret. Following flow-chart shows the working of Hybrid Encryption process:

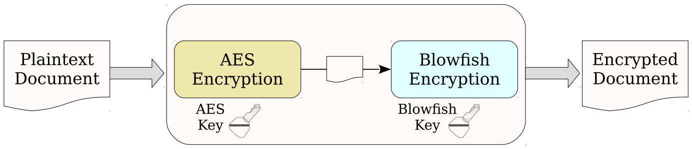


Figure 2: Hybrid Encryption Process

And following flow-chart shows of decryption using Hybrid algorithm:

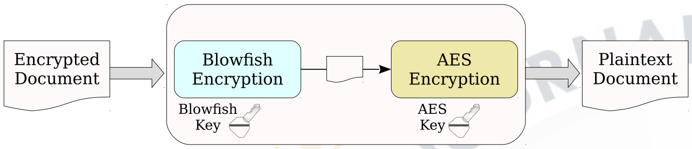


Figure 3: Hybrid Decryption Process

This process provides highly secure mechanism for document encryption/decryption.

5.1 Increased Availability of Authentication Process

Step I: Hence in the proposed work, instead of a single CHAP server, we will use N servers (where $N > 1$), and each of the CHAP server will use unique hashing algorithm to authenticate against user request. And in addition to that there will be a success threshold limit S (where $S <= N$), which denotes the numbers of servers a user should successfully authenticate, in order to get the access to cloud system.
Step II: N =Number of CHAP servers ($N > 1$)

$$S = N/2 + 1$$

For an instance if $N = 5$, then
Step III: Security threshold limit $= (5/2) + 1 = 3$
Hence if any one (or two) of the servers goes down due to some issue, then also user will be able to login into the system if he successfully achieves the success threshold limit.

5.2 Increased Security of Authentication Process

As it is quite possible that a hacker can hack a single authentication server, however it is very difficult for him to crack all the involved servers, where all of them are configured to use a different hashing algorithm.

Following Figure shows the quick view of authentication process and access to cloud system:

VI Result Analysis

In the proposed work, we have attempted to enhance the security of a cloud system execution by using definitely known and broadly utilized advances. We can condense the resultant advantages of utilizing the proposed approach: We have looked at the execution of different encryption calculations for encryption/decryption process; we have recorded the time taken during process, CPU and memory usage.

6.1 Comparing the Time Taken by Various Encryption Algorithms

Analysis done for the encryption process of 5 algorithms, for file sizes from 1 MB to 20 MB, and the resultant value is the average of 5 iterations of each algorithm.

Table 1: Encryption Algorithm Comparison

File Size	**Encryption Time (in ms)**				
	AES	**Blowfish**	**DES**	**3-DES**	**Hybrid**
1 MB	368.2	334.8	381.5	541.4	429.4
3 MB	469	425.4	572.8	1030.2	577.6
5 MB	788.4	645.4	775.7	1582	801.8
10 MB	889.2	806.2	1283.8	2935.6	1266.2
15 MB	1439.2	1168.8	1687.6	4069.4	1658.7
20 MB	1546.4	1503.2	2355.6	5574.2	2269.4

6.2 Performance Graph of Encryption Algorithms

Horizontal Axis = File sizes in MB
Vertical Axis = Time taken by the algorithm during encryption (in ms)

6.3 Comparing the Average CPU and Memory Utilization

We can see that AES and Blowfish are the quickest algorithms. on the other hand Hybrid algorithm is likewise performing ideally well and is superior to DES and Triple-DES. Especially for higher file sizes Hybrid is performing way better than DES and Triple-DES. Result of this analysis shows that the average CPU and memory required for these algorithm for these calculation is likewise having indistinguishable example from past examination. Kindly observe the gathered information in the underneath table. Apart from this analysis, we have also taken the CPU and memory utilization report (using Windows Performance Monitor Tool) of these 5 algorithms, during the encryption of a 15 MB file.

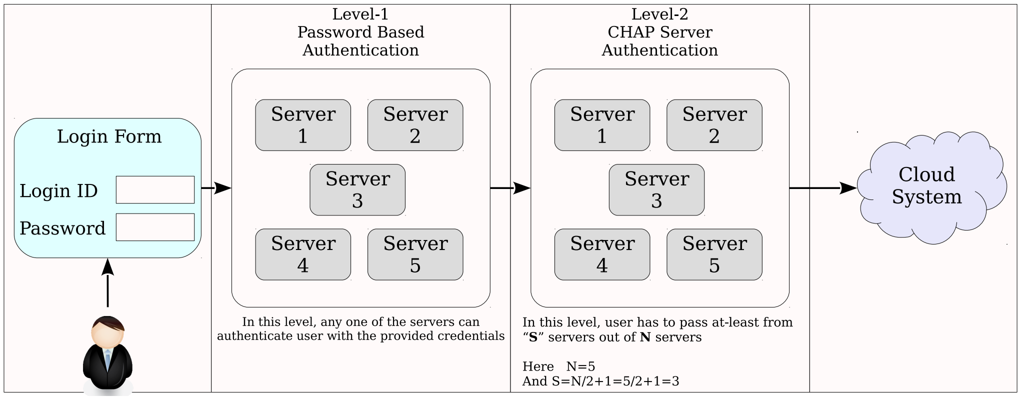


Figure 4: Two-level Authentication Process

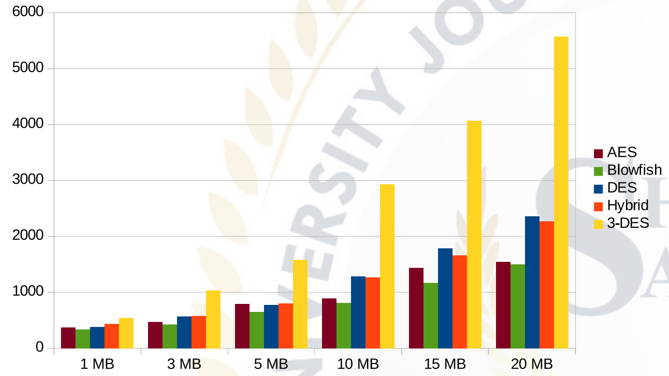
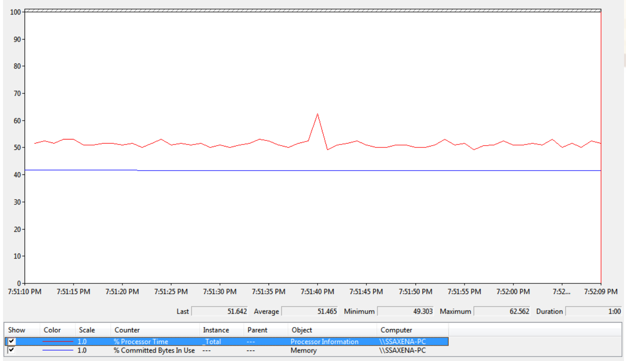


Figure 5: Comparative Analysis of Encryption Algorithms

Table 2: Performance Analysis of Encryption Algorithms

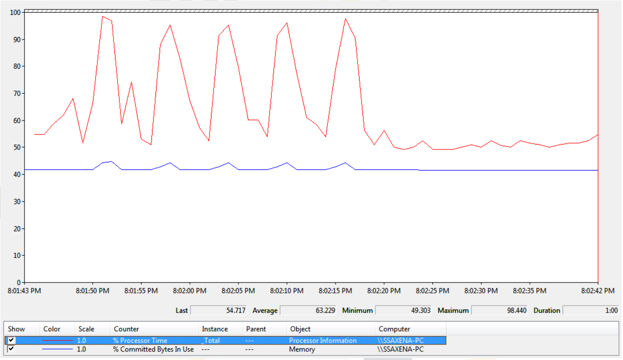
Metric	Encryption Algorithms				
	AES	Blowfish	DES	3-DES	Hybrid
Avg. CPU Utilization (%)	61.383	60.797	63.237	72.553	63.229
Avg. Memory Utilization (%)	46.073	45.573	46.378	46.931	46.38



Last 51.642 Average 51.465 Minimum 49.303 Maximum 62.562 Duration 1:00

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	—	1.0	% Processor Time	_Total	---	Processor Information	\\SSAXENA-PC
☑	—	1.0	% Committed Bytes In Use	---	---	Memory	\\SSAXENA-PC

Figure 6: System Performance in Idle State



Last 54.717 Average 63.229 Minimum 49.303 Maximum 98.440 Duration 1:00

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	—	1.0	% Processor Time	_Total	---	Processor Information	\\SSAXENA-PC
☑	—	1.0	% Committed Bytes In Use	---	---	Memory	\\SSAXENA-PC

Figure 7: System Performance while using Hybrid for 5 times (for encrypting 15 MB file)

VII Conclusion and Future Work

As we push forward with time in this registering world, we will positively observe numerous difficulties, changes, and improvement in distributed computing; anyway the security and administration accessibility angles are continually going to be the key for the accomplishment of Cloud situations. There have been numerous such proposed answers for battle with Security issues, having upgrades more than one or the other. This paper analyses the importance of the data security and availability in the cloud. Purpose behind picking mixture encryption calculations are proficient to deal with encryption for extensive measure of information availability and successful speed of security information in the cloud.

From the point of view of our answer, we have proposed systems to anchor cloud condition, up to a decent degree. This proposed work effectively conveys following changes for securing cloud systems:

1. Enhanced security for cloud system (using strong authentication and encryption)

2. Overall performance optimization

As a future improvement work of the arrangement proposed in this paper we can additionally make it more secure utilizing the SSL (Secured Socket Layer) or TLS (Transport Layer Security) features, which will certainly secure the data in transit as well. Another aspect for improvement will be to work on achieving better performance of the overall system.

REFERENCES

[1] M. Sugumaran, B. B. Murugan, and D. Kamalraj, "An architecture for data security in cloud computing," in *2014 World Congress on Computing and Communication Technologies*, Feb 2014, pp. 252–255. [Online]. Available: https://doi.org/10.1109/WCCCT.2014.53

[2] F. F. Moghaddam, S. D. Varnosfaderani, I. Ghavam, and S. Mobedi, "A client-based user authentication and encryption algorithm for secure accessing to cloud servers based on modified diffie-hellman and rsa small-e," in *2013 IEEE Student Conference on Research and Developement*, Dec 2013, pp. 175–180. [Online]. Available: https://doi.org/10.1109/SCOReD.2013.7002566

[3] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud computing: An overview," in *Cloud Computing*, M. G. Jaatun, G. Zhao, and C. Rong, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 626–631.

[4] B. Balamurugan and P. Krishna, "Extensive survey on usage of attribute based encryption in cloud," *Journal of Emerging Technologies in Web Intelligence*, vol. 6, no. 3, pp. 263–272, Jan 2014. [Online]. Available: http://www.jetwi.us/uploadfile/2014/1210/20141210112144224.pdf

[5] R. K. L. Ko, M. Kirchberg, and B. S. Lee, "From system-centric to data-centric logging - accountability, trust amp;amp; security in cloud computing," in *2011 Defense Science Research Conference and Expo (DSR)*, Aug 2011, pp. 1–4. [Online]. Available: https://doi.org/10.1109/DSR.2011.6026885

[6] F. F. Moghaddam, M. B. Rohani, M. Ahmadi, T. Khodadadi, and K. Madadipouya, "Cloud computing: Vision, architecture and characteristics," in *2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC)*, Aug 2015, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ICSGRC.2015.7412454

[7] A. Shukla and Y. Simmhan, "Toward reliable and rapid elasticity for streaming dataflows on clouds," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, July 2018, pp. 1096–1106. [Online]. Available: https://doi.org/10.1109/ICDCS.2018.00109

[8] D. M. Shawky and A. F. Ali, "Defining a measure of cloud computing elasticity," in *2012 1st International Conference on Systems and Computer Science (ICSCS)*, Aug 2012, pp. 1–5. [Online]. Available: https://doi.org/10.1109/IConSCS.2012.6502449

[9] T. K. Damenu and C. Balakrishna, "Cloud security risk management: A critical review," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, Sept 2015, pp. 370–375. [Online]. Available: https://doi.org/10.1109/NGMAST.2015.25

[10] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *International Journal of Information Security*, vol. 13, no. 2, pp. 113–170, Apr 2014. [Online]. Available: https://doi.org/10.1007/s10207-013-0208-7

[11] "Security in cloud computing," *International Journal of Information Security*, vol. 13, no. 2, pp. 95–96, Apr 2014. [Online]. Available: https://doi.org/10.1007/s10207-014-0232-2

[12] B. A. Sullivan, "Securing the cloud: Cloud computer security techniques and tactics," *Security Journal*, vol. 27, no. 3, pp. 338–340, Jul 2014. [Online]. Available: https://doi.org/10.1057/sj.2012.16