



# Strong Storage and Security Policy for Cloud Servers with Hybrid Secure Replication

Megha Singh<sup>1</sup>, Dr. Sunita Gond<sup>2</sup>

1Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore, India

Corresponding author: Megha Singh  
maggii.megha@gmail.com

## Abstract

Cloud computing technology enables users to deploy shared infrastructure and services. The internet and other public networks must be used in order to build up a public cloud. The system is very vulnerable to a variety of security vulnerabilities because to its reliance on open routes of communication. This has implications for authentication and data access security. In order to address security concerns during authentication, prior research built a RADIUS system with two-factor authentication approaches, TPA techniques, and different security over storage measures. Current works suffer from poor access control and confidentiality problems. Hence, this study proposed a security architecture that implements the RBAC method of access control and the ECC and MD5 algorithms of secrecy in order to improve storage and security. The strong storage is achieved through replica copies of data. The entire work tested on a range of datasets of varying file sizes to determine its effectiveness.

**Keywords:** Cloud computing, storage, security, ECC, MD5, ,

DOI Number: 10.14704/nq.2021.19.4.NQ21043

NeuroQuantology2021;19(4): 99-107

## 1. Introduction

Cloud security consists of a set of policies, controls, procedures and technologies. These all are work together to protect cloud-based system. These securities also protect customer's privacy. Data security is a major concern in the cloud because all data is transmitted via the internet. The data must be stored in an encrypted form in the cloud. This constrains the client from directly accessing the shared data. For this reason, it is appropriate to employ proxy and brokerage services. Encryption helps protect the data transferred and the data stored in the cloud as well. Encryption also helps protect data from unauthorized access but does not prevent loss of data.

### Principles of cloud security

Lack of Visibility & Shadow IT: It is easy in cloud computing technology to subscribe or even turn new instances and ecosystems into a SaaS program for anyone. Users should adhere to strict appropriate usage policies to receive authorization for new cloud services or to create new instances and to subscribe.



**Lack of Control:** It presents the availability of public cloud service to an organization who does not own the hardware, apps or software that the cloud services run on. It also makes sure that the approach of the cloud vendor understands the importance of those assets.

**Transmitting and Receiving Data:** The data is shared among various cloud apps which is integrated and interfaced with other applications which are achieved by the Application programming interface (API).

**Embedded/Default Credentials & Secrets:** The feature of embedded credentials and default credentials are the important aspects of cloud computing. It has to be dealt with so as to handle the risk associated with the unauthorized access.

**Incompatibilities:** Various architectures are been used in the IT domain among different environments which are incompatible to each other. It results into mis-configuration, data leakage, access control and compliance issues.

**Multi-tenancy:** The shared resources benefits in cloud are generally attained through Multi-tenancy but it also raises concerns about data isolation and privacy.

**Scalability Cuts Both Ways:** Main advantages of Cloud computing includes automation and quick scalability, but there are concerns like vulnerabilities, misconfigurations, and other security issues too, which can also breed at both speed and scale.

**Malware and External Attackers:** Attackers can make a living by harnessing compromisable aspects in the cloud. Fast detection and a multi-level approach to security can help in reducing the risk while preparing to respond to an attack.

**Insider Threats-Privileges:** In-house threats in an organization usually take the longest time to detect and resolve and assumed to be the most harmful potential. A clear individuality and entrance protection system along with appropriate dispensation management tools is important to remove these threats and reduce damage when they arise (such as preventing lateral movement and privilege escalation).

## **2. Related work**

The potential which cloud computing has offered to various services and customers also brought the challenges along with it. The security and privacy of the data stored and processed over the cloud environment have attracted many researchers to address this issue over the last decade. Various solutions have been proposed to deal with the malicious attacks for cloud computing environment. Some of the notable contributions in this field are discussed as below:

Emna Guerhazi et al. [15] have introduced a versatile security solution for sensitive information in cloud-based data centers. They addressed the security concerns for the cloud computing warehouse where multiple stakeholders have the access to the data. The authors proposed a data sensitive security framework to offer the authentication in the cloud computing environment.



The proposed model offered a multi-tier security level depending upon the level of sensitivity of the data stored in the warehouse.

Krithikashree. L et al. [16] presented an audit based security framework in cloud for mobile devices. They have proposed a restricted query technique using Homomorphic Cryptography with Provable Data Possession (PDP) and Proof of Retrievability (POR). Third party auditor scheme was augmented in this work to address the data manipulation problem. The study and experimental analysis resulted into effective outcome.

Nan Zhang et al. [17] addressed the time complexity and amount of overhead associated with the security model in cloud computing. They identified that the level of security is proportional to the amount of overhead added to the information. The other network parameters like throughput, channel capacity and latency got compromised with the increase in the size of overhead. The authors presented a lightweight solution to the problem of security attack. The authenticated and authorized solution was also proposed by authors using Kerberos algorithm.

Anshukirar et al. [18] identified that the data security in cloud based services is often compromised due to the interfaces defined for the ubiquitous, on-demand and resource based services. Data security with cloud is prone to attacks due to physical security control approach which is extremely valuable. The authors found that the information outsourcing is also an issue because of protection and privacy of data in multi-tenant environment. They proposed multi-factor technique for the authentication of multiple users and also preventing illegal cloud access to any unauthorized user.

Xiong et al. [19] proposed a cryptography based security models in the virtualization mode. They have used the RSA algorithm for the encryption and decryption. The public and private keys for the encryption and decryption in the proposed work is derived and incorporated for both physical and virtual mode. This technique has extended the region of operations through the virtual mode.

Algarni et al. [20] presented an advanced encryption standard (AES) based authentication framework for the cloud computing environment. The author has presented the symmetric as well as asymmetric algorithms to manage the security patches in the model. It could be installed whenever the user needs the updates. The range of applications which this model could provide effective security support is larger than the other models.

Ali et al. [21] proposed a novel security framework named as secure data sharing in clouds (SeDaSC). This model concentrated on the access control aspect of security framework and offered a data sharing model without using compute-intensive re-encryption. They have also incorporated data integrity and confidentiality, forward and backward access control, and insider threat security. This technique was based on two keys generation for each user, one of which is with the user and other is with the server. However the complexity and trust deficit are the drawbacks of this technique.

### 3. Problem Statement

It is evident from a survey of the literature that no one algorithm can simultaneously satisfy the needs of many security kinds, such as integrity, secrecy,



and authenticity. However, they can all be achieved by using diverse techniques on a single model. Our research mostly supports the widely held view that adding an additional layer of security necessitates much more time and money.

Applications for cloud computing were discovered to be dependent on bandwidth and storage provided by cloud servers. An excessive strain on the resources of a security system could lead to slower performance and greater unnecessary costs. The cost of using one of these servers changes significantly depending on how much data is kept, processed, and transported through the connection, as can be shown if we use Amazon's web servers as an actual-world example.

The study comes to the conclusion that if security algorithms are used in server traffic to ensure content originality and personal information security, a severe issue will arise. Even though numerous programmes have been created, it is still unknown which algorithms work best in various situations. Although each system uses a unique collection of security settings to operate in its intended context, it is unclear which set of parameters is best for a given application. This issue can be resolved by comparing algorithms in the same environment to determine which one performs the best. The results of this study have led researchers to the conclusion that a dynamic security algorithm must be developed in order to lower the ongoing cost of security overhead by dynamically building a security algorithm based on the need for security as it is learned.

As noted in the problem description above, all security measures offer authentication, confidentiality, authorization, integrity, access control, and availability. Algorithms do provide all security measures, but they do not classify which ones are most suited for various applications.

Due to its focus on message authentication, RC6 is a well-known example of an algorithm that performs well in private networks but poorly in public ones. We can reduce data transport prices and save time by using the quick method RC6. There is no requirement to exchange keys before beginning a chat because each party can generate their own. ECC requires a public certificate for access and requires the exchange of a key between the sender and the recipient. This is particularly clear in the situation of the loop bandwidth application, where network resources are limited and numerous users are utilising it at once. With this impulsive security, overloading the server is a possible problem.

Examining several elementary publications that describe the solution to the issue and the security-achieving techniques while each strategy has its own unique style of carrying out tasks, they all work to reduce bandwidth usage and unsecured computing.

Security measures should be flexible, just like the looks and themes of an application. To suit the specific requirements of the organisation, the settings allow for adjustment of the security level. Utilizing customised security settings, the security degree of the previous data will be evaluated. If we apply ML to it, we'll be able to determine whether it will always recommend higher degrees of security and whether it will adapt to meet those demands as they change.

The system will evaluate the existing environment to choose the proper security level when it is set to automate. In order to achieve this, we'll use a self-learning algorithm, make use of every symmetric and asymmetric cryptographic approach available, and research numerous authentication strategies. The top time wise will be used to compare all metrics, such as reaction time, computation time, and total time spent on the activity at hand.



### 4. Methodology

A single document file must be divided into multiple smaller files, or "chunks," according to this study. It may be possible to reduce downtime and speed up transfers by using an ECC approach to encrypt each chunk and dividing it into several copies to create replicas of each piece.

The security solution has suggested splitting the content into multiple files, creating a message digest, and encrypting each portion separately. Multiple backups of each chunk file are kept on different servers figure.1 and figure.2 depicts whole situation:

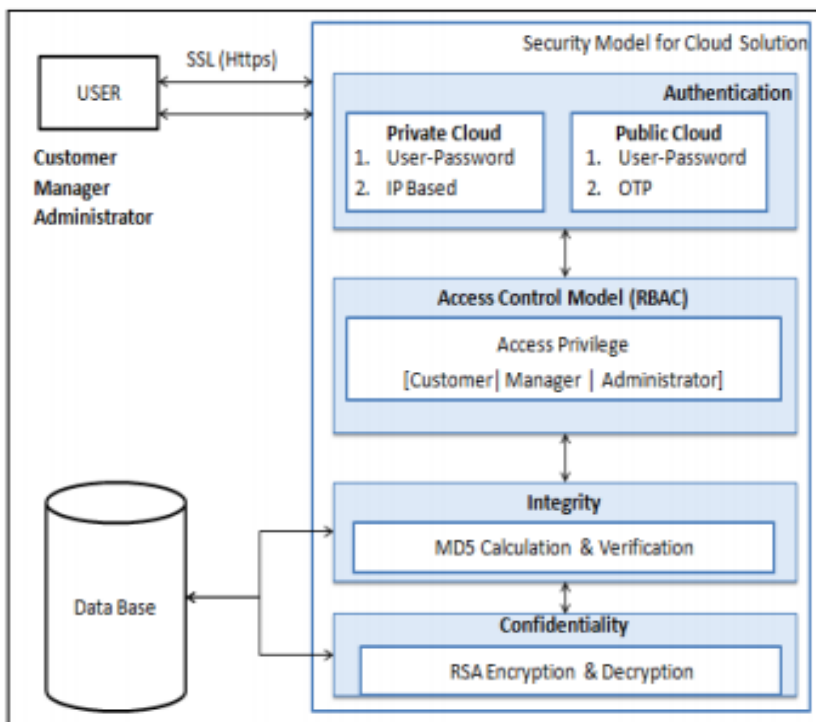


Fig.1 Security model for cloud solution

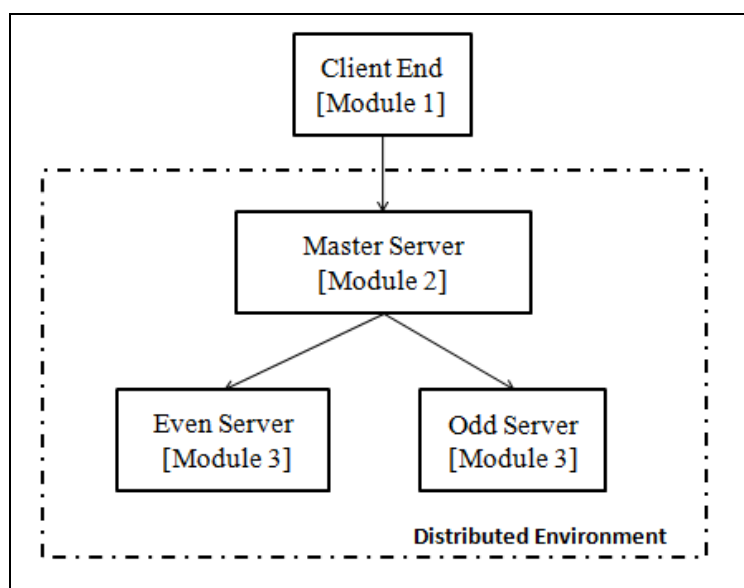


Fig.2 Modules



The complete scenarios are developed into three modules which are listed below:

**Module 1: Client End**

**Module 2: Master Server / Distributed Server**

**Module 3: Replication**

A block representation of all above modules is shown in figure 3.

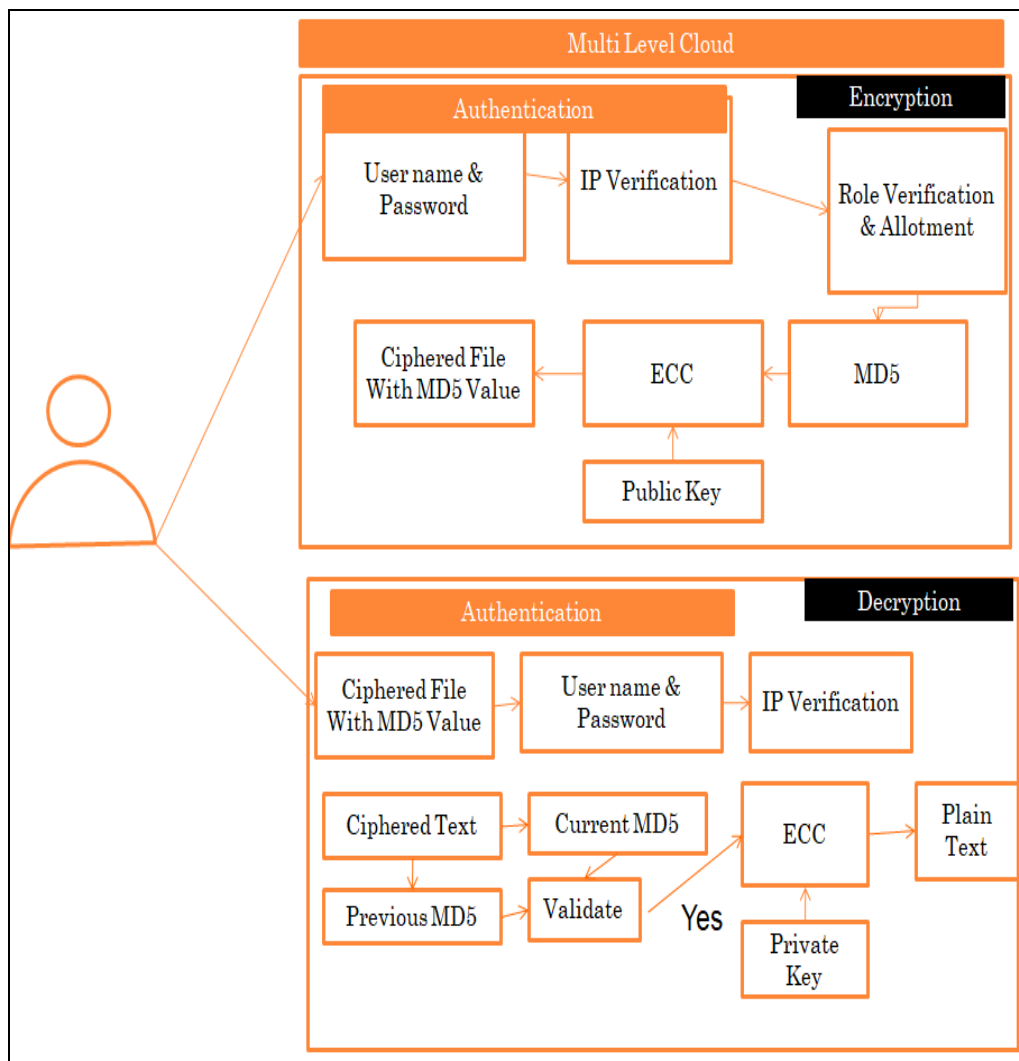


Fig. 3 Block representation of all above modules

### 5. Experimental Analysis

The complete work has been implemented using java technology. To develop cloud based software as a service model, servlet Api has been developed. Proposed implementation uses MySql technology as a database, java servlet api for business logic development and html, css, bootstrap and java script for front end development.



Table.1 Computation time for varying file size

Plain Text Size (KB)	MD5 Time	ECC Encryption	Chunking Time	Total Time
10	0.87	496	27	524
100	1.8	3188	16.81	32.6
200	7	6294	948	7248
300	9.2	9219	1157	10385
400	12	11947	1521	13480
500	7	18531	1667	20206

The efficiency of the proposed method has been assessed by analysing the input of varying file sizes and measuring the resultant computation time. Each proposed approach has been evaluated independently with regards to how long it takes to generate a message digest, an ECC, a chunk, and an overall. The overall evaluation suggests that a rise in file size may cause a rise in computation time but not in chunking time. It's possible that replication will make the upload take longer but will speed up the download, all while ensuring the safety of the data. This study demonstrates that storage and security assurances may be provided with replication, authentication, and ECC integration, with just a little increase in encryption time.

## 6. Conclusion

According to the study's findings, pairing authentication with encryption is an effective strategy to protect data both during the login process and in any subsequent conversations. Therefore, maintaining security even as the data is being stored is made possible by copies and methods for chunk-level encryption.

According to implementation studies, larger files result in longer encryption times but only a minor increase in chunking durations. Replication therefore results in a minor increase in calculation times but offers strong storage and security assurances.

## References

1. X. Sun, "Critical Security Issues in Cloud Computing: A Survey," 2018 IEEE 4th International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Omaha, NE, 2018, pp. 216-221.
2. Y. AlHumaidan, L. AlAjmi, M. Aljamea and M. Mahmud, "Analysis Of Cloud Computing Security In Perspective Of Saudi Arabia," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-4.



3. R. L. Paikrao and V. H. Patil, "Security as a Service Model for Virtualization Vulnerabilities in Cloud Computing," 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), Sangamner, 2018, pp. 559-562.
4. R. A. R. Shaikh and M. M. Modak, "Measuring Data Security for a Cloud Computing Service," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, 2017, pp. 1-5.
5. D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," 2017 IEEE 3rd international conference on big data security on cloud (big data security), IEEE international conference on high performance and smart computing (hpsc), and IEEE international conference on intelligent data and security (ids), Beijing, 2017, pp. 145-149.
6. Vijay Varadharajan, Department of Computing, Macquarie University, Sydney, Australia, Security and trust in the web, Proceeding APWeb'12 Proceedings of the 14th Asia-Pacific international conference on Web Technologies and Applications
7. B.Prasanalakshmi, A.Kannammal, Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics, International Journal of Computer Applications (0975 – 8887) Volume 53– No.18, September 2012
8. D.E. Popescu, A.M. Lonea, An Hybrid Text-Image Based Authentication for Cloud Services, INT J COMPUT COMMUN, ISSN 1841-9836 8(2):263-274, April, 2013.
9. Jin-Mook Kim and Jeong-Kyung Moon, Secure Authentication system for hybrid cloud service in mobile communication environment, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 828092, 7 pages <http://dx.doi.org/10.1155/2014/828092>
10. Sang-Ho Na, Jun-Young Park, Eui-Nam Huh, Personal Cloud Computing Security Framework, Proceeding APSCC '10 Proceedings of the 2010 IEEE Asia-Pacific Services Computing Conference, Pages 671-675
11. Hsing-Chung (Jack) Chen, Marsha Anjanette Violetta, Cheng-Ying Yang, Contract RBAC in cloud computing, The Journal of Supercomputing archive Volume 66 Issue 2, Nov 2013 Page 1111-1131 Kluwer Academic Publisher Hingham,MA, USA
12. John Linkous, Don't Let Hybrid Clouds Rain on Your Security, ECC Conference | Where the world talks security, 4th Sep 2014 <http://www.ECCconference.com/blogs/dont-let-hybrid-clouds-rain-on-your-security>
13. T. H. Kim, I. H. Kim, C.W.Min, and Y. I. Yeom, Security technical trend of cloud computing, Computer Science Managing, vol. 30, no. 1, pp. 30–38, 2012
14. Y. H. Bang, S. J. Jeong, and S. M. Hwang, Security requirement development tools of mobile cloud system, Information and Communications, vol. 28, no. 10, pp.19–29, 2011
15. E. Guerhazi, M. Ben Ayed and H. Ben-bdallah,"Adaptive security for Cloud data warehouse as a service," 2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, NV, 2015, pp. 647-650.



16. Krithikashree.L, S. Manisha, Dr.Sujithra.M. Audit Cloud: Ensuring Data Integrity for Mobile Devices in Cloud Storage. 9th ICCCNT, IISC, Bengaluru India, July 10-12, 2018.
17. Nan Zhangl, Xiaoyu Wul, Cheng Yangl, Yinghua Shenl, Yingye Chengl, “A lightweight authentication and authorization solution based on Kerberos”. Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). 3<sup>rd</sup>, 5<sup>th</sup> October, 2016 IEEE.
18. Anshu Kirar, Arun Kumar Yadav and Supriya Maheswari, “An Efficient Architecture and Algorithm to Prevent Data Leakage in Cloud Computing using Multi-tier Security Approach”, Proceedings of the SMART -2016, IEEE, 5th International Conference on System Modeling & Advancement in Research Trends , 25th \_27'h November, 2016.
19. Xiong H, Zhang H, Sun J (2018) Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. IEEE Syst J.
20. Algarni A (2019) A survey and classification of security and privacy research in smart healthcare systems. IEEE Access
21. Ali M, Dhamotharan R, Khan E, Khan SU, Vasilakos AV, Li K et al (2015) SeDaSC: secure data sharing in clouds. IEEE Syst 11:395–404.

