International Journal of Engineering & Technology, 7 (2.20) (2018) 236-242

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Two Way Validation Framework for Cloud Storage Security

Anantula Jyothi[1]*, Baddam Indira[2]

[1]Asst.Prof., Anurag Group of Institutions.
[2]Assoc.Prof., Kasturba Gandhi Degree and PG College.
E-mail:Indira.baddam@gmail.com
**Corresponding author E-mail:jyothianantula@gmail.com*

Abstract

High Performance Computing (HPC) has become one of the predominant techniques for processing the large scale applications. Cloud environment has been chosen to provide the required services and to process these high demand applications. Management of such applications challenges us on three major things i.e. network feasibility, computational feasibility and data security. Several research endeavours are focused on network load and computing cloud date and provided better outcomes. Still those approaches are not able to provide standard mechanisms in view of data security. On the other side, research towards enabling the auditing features on the cloud based data by various researchers has been addressed but their performance is poor. However, the complexity of the audit process proven to be the bottleneck in improving performance of the application as it consumes the computational resources of the same application. Henceforth, this work proposes a novel framework for cloud data auditing at multiple levels to audit the access requests and upon validating the conditions of one level, the connection request will be moved to the further complex levels in order to reduce the computational loads. The proposed framework determines a substantial reduction in the computational load on the cloud server, thus improves the application performance leveraging the infrastructure use.

Keywords: *Cloud storage, cost reduction, data auditing, Data security, framework.*

1. Introduction

In the recent development, the growth in cloud computing in technical, business and research prospective is the point of focus. The majority of the organizations have adopted benefits from cloud computing such as efficient deployment and management of the services, agility of the business cases for DCO oriented cases, uptime of the services and customer satisfaction. The work of Marston et al. [1] has demonstrated the benefits to be achieved for business cases and the work of M. A. Vouk et al. [2] has proven the research significance of cloud computing. The massive growth is been observed in case of software as a service scenarios. Thus the evaluation of healthcare as a service as demonstrated by A. K. Jha et al. [3] and also finance as a service as demonstrated by H. T. Peng et al. [4] showcased the modernization of the regular software on cloud away from the contemporary usages. Not alone for the business or commercial spaces, the benefits have also reached to the education domain as well. The case study by the M. Mircea et al. [5] has shown the new paradigm of education as a service. Nevertheless, this growth in the cloud computing has made the industry, consumers and the researchers to think about the contingency of these adoptions of cloud computing. Various researchers have expressed their researches and works in order to decide the best possible security features of the cloud computing.

However, the challenge in deploying the security protocols on cloud is to identify the accurate abode. Multiple opinions from research attempts have shown multiple benefits and flaws of deploying the cloud security at service providers' end or at consumers end or the end of cloud data centres.

The work by M. Armbrust et al. [6] presented a decent survey of the existing security measures and the work by L. Liu et al. [7] contributed significantly in identifying the security policies to be adopted for social applications. In the other hand the findings by T. Mather et al. [8] proven that the security expectations for enterprise applications are different from the other aspects.

As realized the deployment of cloud security protocols can only be justified by considering the fundamental purpose of the application. Nonetheless, the focus of this work is to analyse and propose the security measures for data on cloud computing. Thus this work proposes the security deployments on cloud data centres. The primary challenge of the data centres are the continuous growth in the data in gigantic and exponential rate as showcased by M. Pop et al. [9] and M V Narayana et.al[23]. The elaboration of this issue is highly analysed and also forecasted in the work by A. Greenberg et al. [10] and Q. Zhang et al. [11].

Henceforth, the challenges identified as

- The inclusion of the security policies must not be done in the application level as the in order to estimate the performance of the cloud services must be carried out separately and specifically.
- The traditional security policies for verification must be revamped as the existing policies can be vulnerable to the hackers.
- Access of the data is provided to the data centre owners or the consumers or the service providers or the data auditors. The specific access policies by be rooted in the security policies.
- Finally, the inclusion of the security policies from the data centre end must incorporate the verifications of the access requests from data centre controllers, service owners, consumers and most importantly the data auditors.

This proposed framework provides the solutions to these mentioned popular problems.

2. Related work

In this section of the work, the articulations of the parallel research outcomes are furnished as part of the survey for problem identification and enhancements. Only the significant ones are elaborated here.

The field of cloud security is none to first in the place for adoption for research and a significant amount of work is carried out. The existing methodologies have proposed various security mandates for different application domains ranging from business to financial to healthcare. The demonstration by V. Chang et al. [12] has demonstrated the contingencies for Cloud Storage and Bioinformatics on cloud based data centres. Again, V. Chang et al. [13] contributed in identifying the security demands for business intelligence applications. The recommendations for business process optimized algorithm based algorithms are provided in the work by G. M. Cimino et al. [14].

Having the major focus on the security as service, the work of V. Vardharajan et al. [15] has shown the recommendations and road map for security as a service.

The concluding contribution as on date is given by N. Antunes et al. [16] for comparing various security protocols for cloud computing.

This work also summarizes the security recommendations from various research attempts [Table – 1]

Table 1: Security Recommendations

Application Type	Security Deployment Recommendations	Security Protocol Recommendations
Business Intelligence [17]	Service Owner	Business Action Validation
Education [18]	Service Owner	Data Protection
IoT and Sensors [19]	Client Devices	User Access / Device Access Verification
Data Management [20]	Data Centre	User Access Validation

3. Problem formulation

In general, the data in Cloud will be created or shared by the data owner. Data consumers are the persons; they may be the customers of the data owner, third party auditors and cloud service providers. Data owner deploys the information by trusting the Cloud service provider. The responsibility of the cloud service provider is to ensure the data security while being accessed by the consumers.

However, the third party auditor and the cloud service providers have an authorization to access the data, while being partially trusted by the data owner. In such situations, the data being accessed by any invader in terms of audit information and statistical information of the cloud service provider. Thus making this model challenged by the researchers and demands improvements.

Secondly, analysis of the computational capacity of the cloud servers is other considerable challenge. The cloud server is configured to supply the consumer and data owner demands for higher loads, but the further computational processing for the security and auditing always tend to reduce the performance.

Standard cloud security model

The above discussed, Cloud security model is the standard and most popular existing framework [Figure 1] in spite of the arguments for security.

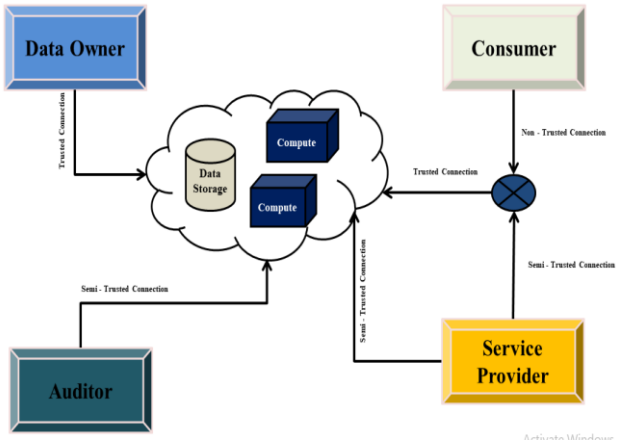

Figure 1: Three party verification and cloud data security model–as existing

The standard framework is an associated model which consists of the data owner, data consumer, third party auditor and service provider. The data owner always deploys the data and expecting to establish the secure and trusted connection to the data. In the other side, Auditor and Service Provider can also establish the connection to the data but those connections and access requests are considered to be the semi-trusted connections.

Finally, the connections from the data consumers are completely untrusted and it is the responsibility of the cloud service provider to reduce the risk of unauthorized access by verifying the connections.

Problem identification

With the detail understanding of the existing framework, this section discusses about the following challenges to be addressed.

Initially, the data access and auditing requests from the third party auditor and the consumer of the data are to be confirmed. In terms of the data processing and data security of cloud server; the allocation of computational loads to be optimised.

Next, the reduced mechanism for verification is to be enabled without compromising the security challenges. The auditing and statistical data collection process is to be enabled for enhancements of the research and improvement of the performance.

Henceforth, this work proposes a novel two way verification framework in the next section of this work considering the problems identified in this section.

4. Proposed framework

The existing systems for cloud security are always challenged by the partially trusted access by the third party data auditors. The auditing process cannot be ignored in order to maintain the industry and other standards. Nevertheless, this access can be viewed as compromise in the security of the data. Also imposing the additional security protocol increases the computational load on the server.

Thus this work motivates the novel framework proposed in this work. The fundamental idea is to provide a two way security on the cloud based data for data consumers and the data auditors.

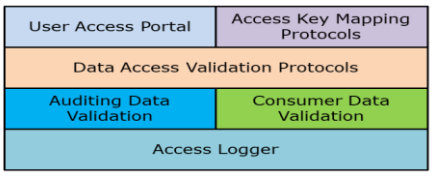

Figure 2: Proposed two way cloud data security framework

The proposed model

The proposed model algorithm is divided into four parts as generate the keys, upload the files with key based encryption, access request validation and finally the data decryption.

Algorithm – 1: Key Generation Algorithm	
Step -1.	Accept two prime number where first number > second number
Step -2.	Calculate the product for both numbers
Step -3.	Consider any random polynomial
Step -4.	Calculate the constant of the polynomial as (first number - 1) X (second number - 1)
Step -5.	Calculate the primary component as GCD(polynomial, E) = 1
Step -6.	Generate the public key as PK = (E, polynomial)
Step -7.	Generate the file descriptor private key, FDPRK = (first const. of the polynomial, polynomial)
Step -8.	Generate the file content private key, FCPRK = (second const. of the polynomial, polynomial)

Nevertheless, the key generation algorithm can be replaced by any proprietary algorithm and the modified algorithm will not change the performance of this proposed framework. The algorithm is visualized graphically [Figure 3].

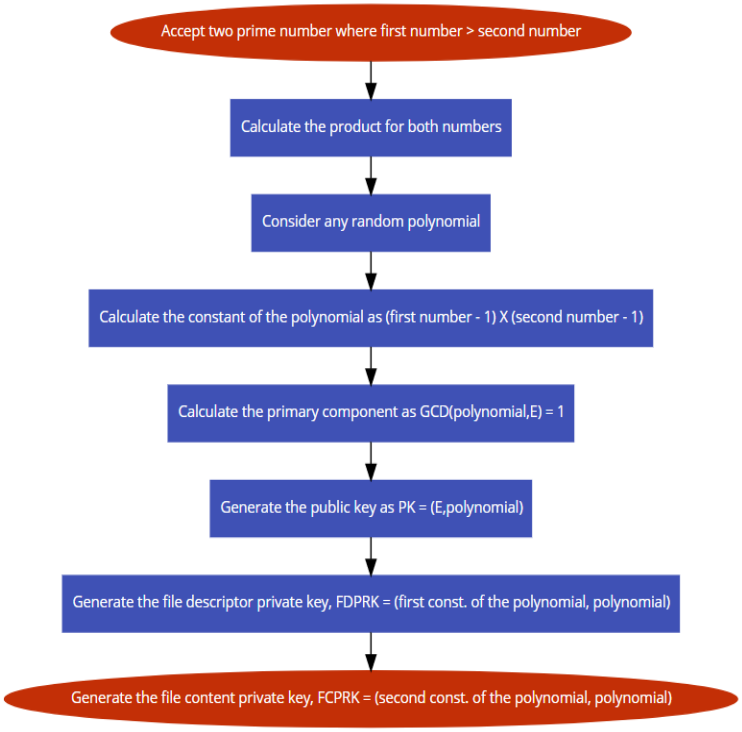

Figure 3: Key generator algorithm flow

Algorithm – 2: Encryption Algorithm	
Step -1.	Divide any file on cloud as descriptor and content
Step -2.	Encrypt the file descriptor
Step -3.	Encrypt the file content
Step -4.	Once the complete file is encrypted, provide the access

The algorithm is visualized graphically [Figure 4]

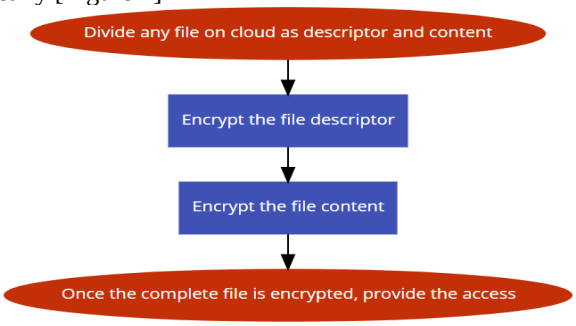

Figure 4: File encryption algorithm flow

Algorithm – 3: Request Validation
1. If the access request contains public key and file descriptor private key
a. Then provide access to file descriptor data
2. If the access request contains public key and file content private key

a. Then provide access to file content data
3. Else
a. Reject the request.

This phase is expected to reduce the computational load on the server. The algorithm is visualized graphically [Figure 5].

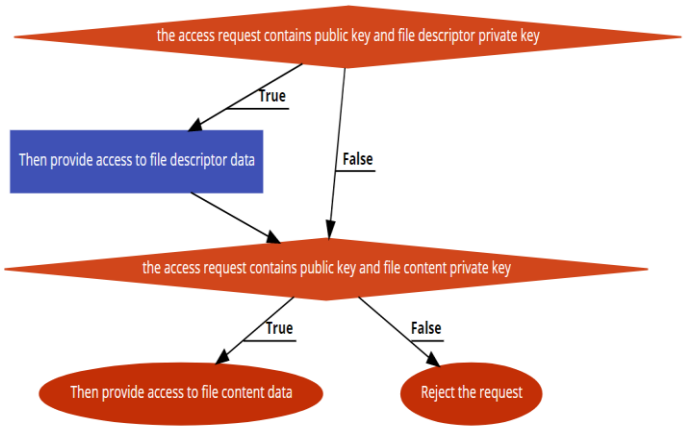

Figure 5: Request validation algorithm flow

5. Results and discussion

Firstly, the experimental setup is discussed [Table – 2]

Table 2: Experimental Setup

SNO	Component	Records
1	Number of Physical Host	1
2	Number of Virtual Machines	110
3	Simulation Time in Secs	120000 Seconds
4	Number of Cloudlets	125

Further the simulation of file management over cloud is carried out and the duration of the tasks are furnished here [Table 3].Also, the computational load of the existing encryption scheme is evaluated. The existing system proposes the complete execution time for encrypting the file. The simulation result is furnished here [Table 4].

Table 3: Standard Response Time for File Access Cloud Lets

ID number of the Cloud -Let	Task Completion Status	ID of the data centre	Virtual Machine ID Number	Duration (sec)	Request Start Time (sec)	Response End Time (sec)
0	Successfully Completed	3	0	320	0.11	320.11
5	Successfully Completed	3	0	320	0.11	320.11
1	Successfully Completed	3	1	320	0.11	320.11
6	Successfully Completed	3	1	320	0.11	320.11
2	Successfully Completed	3	2	320	0.11	320.11
7	Successfully Completed	3	2	320	0.11	320.11
4	Successfully Completed	3	4	320	0.11	320.11
9	Successfully Completed	3	4	320	0.11	320.11
3	Successfully Completed	3	3	320	0.11	320.11
8	Successfully Completed	3	3	320	0.11	320.11
101	Successfully Completed	3	101	320	200.1	520.1
106	Successfully Completed	3	101	320	200.1	520.1
103	Successfully Completed	3	103	320	200.1	520.1
108	Successfully Completed	3	103	320	200.1	520.1
100	Successfully Completed	3	100	320	200.1	520.1
105	Successfully Completed	3	100	320	200.1	520.1
102	Successfully Completed	3	102	320	200.1	520.1
107	Successfully Completed	3	102	320	200.1	520.1
104	Successfully Completed	3	104	320	200.1	520.1
109	Successfully Completed	3	104	320	200.1	520.1

Table 4: Standard Access Time for Encryption Cloud Lets

ID number of the Cloud -Let	Task Completion Status	ID of the data centre	Virtual Machine ID Number	Duration (sec)	Request Start Time (sec)	Response End Time (sec)
4	Successfully Completed	2	4	3	0.2	3.2

16	Success-fully Completed	2	4	3	0.2	3.2
28	Success-fully Completed	2	4	3	0.2	3.2
5	Success-fully Completed	2	5	3	0.2	3.2
17	Success-fully Completed	2	5	3	0.2	3.2
29	Success-fully Completed	2	5	3	0.2	3.2
6	Success-fully Completed	3	6	3	0.2	3.2
18	Success-fully Completed	3	6	3	0.2	3.2
30	Success-fully Completed	3	6	3	0.2	3.2
7	Success-fully Completed	3	7	3	0.2	3.2
19	Success-fully Completed	3	7	3	0.2	3.2
31	Success-fully Completed	3	7	3	0.2	3.2
8	Success-fully Completed	3	8	3	0.2	3.2
20	Success-fully Completed	3	8	3	0.2	3.2
32	Success-fully Completed	3	8	3	0.2	3.2
10	Success-fully Completed	3	10	3	0.2	3.2
22	Success-fully Completed	3	10	3	0.2	3.2
34	Success-fully Completed	3	10	3	0.2	3.2
9	Success-fully Completed	3	9	3	0.2	3.2
21	Success-fully Completed	3	9	3	0.2	3.2

The results are validated graphically for access time [Figure 6] and encryption time [Figure 7].

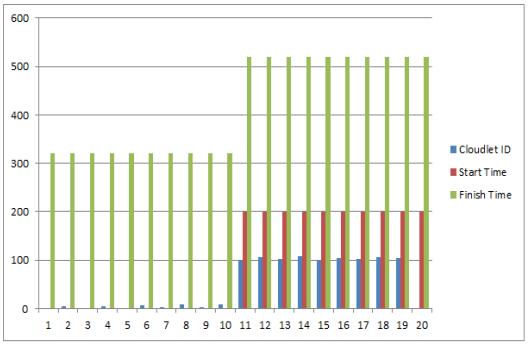

Figure 6: Access time analysis

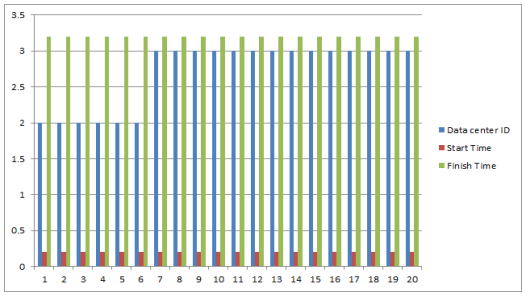

Figure 7: Encryption time analysis

Further, this work analyses the total time for the file access and file encryption [Table 5].

Table 5: Total Access Time

Average File Access Time (sec)	Average File Encryption Time (sec)	Total Average Response Time (Sec)
320.1	3.2	323.3

Next, the response time for the proposed algorithm is analysed [Table 6].

Table 6I: Standard Access Time for Access & Encryption Cloud Lets

ID number of the Cloud-Let	Task Completion Status	ID of the data centre	Virtual Machine ID Number	Duration (sec)	Request Start Time (sec)	Response End Time (sec)
0	Success-fully Completed	2	0	320	0.11	320.11
5	Success-fully Completed	2	0	320	0.11	320.11
1	Success-fully Completed	2	1	320	0.11	320.11
6	Success-fully Completed	2	1	320	0.11	320.11
2	Success-fully Completed	2	2	320	0.11	320.11
7	Success-fully Completed	2	2	320	0.11	320.11
4	Success-fully Completed	2	4	320	0.11	320.11
9	Success-fully Completed	2	4	320	0.11	320.11
3	Success-fully Completed	2	3	320	0.11	320.11
8	Success-fully Completed	2	3	320	0.11	320.11

It is natural to understand that the same cloud let is performing the access and encryption process, thus the time consumption is less. Hence the total average access time [Table 7] is less.

Table 7II: Total Access Time

Average File Access Time (sec)	Average File Encryption Time (sec)	Total Average Response Time (Sec)
320.1	0	320.1

Finally considering the improvements over the existing system [Table 8], the improvement of average response time is 3.2 sec for each cloud lets.

Table 8: Total Access Time Comparison

Total Average Response Time for Existing Framework (Sec)	Total Average Response Time for Proposed Framework (Sec)	Improvement (Sec)
323.3	320.1	3.2

6. Comparative analysis

In this section of the work, the comparative analysis of the access or the response time and the structural complexities are compared with the parallel research outcomes.

Structural complexity

Firstly this work compares the structural complexity of the proposed framework with the existing methods [Table 9].

Table 9: Structural Complexity Analysis

Model Name	Encryption & Decryption Complexity	Structural Complexity
ePass J. Su et al. [23]	$2N_C + T_P$	Security at Service Owner
Decentralized Access S. Ruj et al. [24]	$2N_C + T_P$	Security at Service Owner
CCA C. Zuo et al. [25]	T_E	Security at Service Owner
Access Control P. Zhang et al. [26]	T_P	Security at Data Centre
Proposed Method	T_P^N	Security at Data Centre

In order to normalise the parameters for comparison the following ranking description table is proposed [Table 10].

Table 10: Ranking Description Table

Parameters	**Ranking Value (As low as Good)**
$2N_C + T_P$	4
T_E	3
T_P	1
T_P^N	2

The assumptions and the descriptions are elaborated here.

T_P denotes the time for passkey generation and N_C denotes the number of cypher operation to be undertaken for this model. Natural to understand that the number of cypher operation depends on the amount of the data stored and which is likely to be very high on the cloud. Also, the passkey generation is likely to be depending on the algorithm for encryption which is a polynomial in majority of the research attempts. Hence this method is to be considered as less time efficient.

Also, it is to be realized that T_E and T_P^N are the model complexity where E denotes the number of connection request and N denotes a higher order polynomial for passkey generation. Hence, the situations where the model complexity depends on the number of connections will decay on long response situations. In the other hand, the higher order polynomial will decay the performance but in comparison with the first model, the complexity is less.

Further, the ranking analysis is considered for structural complexity [Table 11].

Table 11: Ranking Description Table

Parameters	Description	Ranking Value (As low as Good)
Security at Service Owner	The complexity for the application / service increases	2
Security at Data Centre	The complexity of the manageability of the service alone decreases	1

Thus, the final ranking analysis is considered here [Table 12].

Table 12: Ranking Analysis

Model Name	Encryption & Decryption Complexity (A)	Structural Complexity (B)	Ranking (As low as Good)(A + B)
ePass J. Su et al. [23]	4	2	6
Decentralized Access S. Ruj et al. [24]	4	2	6
CCA C. Zuo et al. [25]	3	2	5
Access Control P. Zhang et al. [26]	1	1	2
Proposed Method	2	1	3

The results are visualized graphically here [Figure – 8].

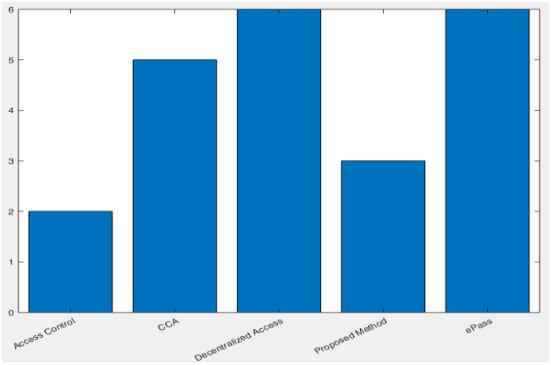

Figure 8: Structural complexity comparative analysis

Time complexity

Lastly, this work compares the response time complexity for the proposed method with the outcomes of the proposed method [Table 13].

Table 13: Ranking Analysis

Number of CloudLets (Range)	Response Time (Sec)				
	ePass J. Su et al. [23]	Decentralized Access S. Ruj et al. [24]	CCA C. Zuo et al. [25]	Access Control P. Zhang et al. [26]	Proposed Method
100 – 200	267	343	279	273	257
200 – 250	363	313	299	275	305
250 – 300	388	382	333	285	322
300 – 500	469	363	374	290	324
500+	487	340	389	292	328

The comparative results are also analysed visually [Figure 9].

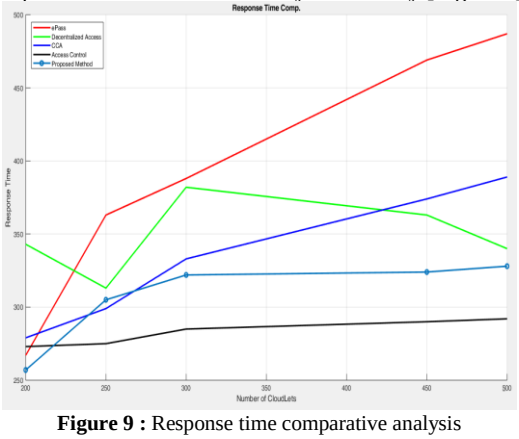

Figure 9 : Response time comparative analysis

Thus, it is natural to understand that the proposed, two way validation method is performing better than the 60% of the existing algorithms. In the next section of the work, the overall conclusion is presented.

7. Conclusion

The cloud computing is becoming the highest popular technology for consumers and the service provider. Thus the demand for further improvements is continuous. Hence, cloud computing is attracting attention from huge research community. One of the challenging problems of cloud computing is the data or information security for the information stored on the cloud. One of the purposes of adopting cloud computing by the consumers is time efficiency. However, the security is also a prime concern for the service providers and the consumers of the cloud based data and services. Imposing the cloud security is a computational over load, which compromises on the time efficiency. Thus it is the demand of the recent research progresses. Hence, this work proposes a two way security for the cloud based data and demonstrated significant improvements over response time reduction.

References

[1] Marston S, Li Z, Bandyopadhyay S, Zhang J & Ghalsasi A, "Cloud computing—The business perspective", *Decision support systems*, Vol.51,l No.1,(2011), pp.176-189.

[2] Vouk MA, "Cloud computing—issues research and implementations", *Jrnl of Comp. Inf. Tech-CIT*, Vol.4, (2008), pp.235-246.

[3] Jha AK, DesRoches CM, Campbell EG, Donelan K, Rao SR, Ferris TG, Shields A, Rosenbaum S & Blumenthal D, "Use of electronic health records in US hospitals", *New England Journal of Medicine*, Vol.360, No.16,(2009), pp.1628-1638.

[4] Peng HT, Hsu WW, Chen CH, Lai F & Ho JM, "FinancialCloud: Open cloud framework of derivative pricing", *International Conference on Social Computing (SocialCom)*, (2013), pp.782-789.

[5] Mircea M & Andreescu AI, "Using cloud computing in higher education: A strategy to improve agility in the current financial crisis", *Commun. IBIMA*, (2011).

[6] Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I & Zaharia M, "Above the clouds: A Berkeley view of cloud computing", *Commun. ACM*, Vol.53, No.4,(2010), pp.50-58.

[7] Liu L, Yu E & Mylopoulos J, "Security and privacy requirements analysis within a social setting", *11th IEEE Conf. Requirements Eng. Conf*., (2003), pp.151-161.

[8] Mather T, Kumaraswamy S & Latif S, C*loud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, Sebastopol, CA, USA:O'Reilly Media, (2009).

[9] Pop M & Salzberg SL, "Bioinformatics challenges of new sequencing technology", *Trends Genetics*, Vol.24, No.3, (2008), pp.142-149.

[10] Greenberg A, Hamilton AJ, Maltz DA & Patel P, "The cost of a cloud: Research problems in data center networks", *ACM SIGCOMM Comput. Commun. Rev.*, Vol.39, No.1, (2008), pp.68-73.

[11] Zhang Q, Cheng L & Boutaba R, "Cloud computing: state-of-the-art and research challenges", *J. Internet Services Appl.*, Vol.1, No.1, (2010), pp.7-18.

[12] Chang V, Walters RJ & Wills G, *Cloud Storage and Bioinformatics in a Private Cloud Deployment: Lessons for Data Intensive Research*, New York, NY, USA:Springer, (2013), pp.245-264.

[13] Chang V, "Business intelligence as service in the cloud", *Future Gener. Comput. Syst.*, Vol.37,(2014), pp.512-534.

[14] Cimino GM & Vaglini G, "An interval-valued approach to business process simulation based on genetic algorithms and the BPMN", *Information*, Vol.5, (2014), pp.319-356.

[15] Vardharajan V & Tupakula U, "Security as a service model for cloud environment", *IEEE Trans. Netw. Service Manage.*, Vol.11, No.1, (2014), pp.60-75.

[16] Antunes N & Vieira M, "Assessing and comparing vulnerability detection tools for web services: Benchmarking approach and examples", *IEEE Trans. Services Comput.*, Vol.8, No.2, (2015), pp.269-283.

[17] Yang K & Jia X, "An efcient and secure dynamic auditing protocol for data storage in cloud computing", IEEE Trans. Prll Distrib. Syst.,Vol.24, No.9, (2013), pp.1717-1726.

[18] Wang C, Chow SSM, Wang Q, Ren K & Lou W, "Privacy preserving public auditing for secure cloud storage", *IEEE Trans. Comput.*, Vol.62, No.2, (2013), pp.362-375.

[19] Zhu Y, Hu H, Ahn GJ & Yu M, "Cooperative provable data possession for integrity verication in multicloud storage", *IEEE Trans. Parallel Distrib. Syst*., Vol.23, No.12, (2012), pp.2231-2244.

[20] Boneh D, Gentry C, Lynn B & Shacham H, "Aggregate and verably encrypted signatures from bilinear maps", *Adv. Cryptograph Eurocrypt_ Int. Confer. Thy Appl. Cryptograph. Techn.*, (2003).

[21] Sookhak M, Gania A, Khanb MK & Buyyac R, "Dynamic remote data auditing for securing big data storage in cloud computing", *Inf. Sci.*, (2015).

[22] Jia Y, Kui R, Cong W & Varadharajan V, "Enabling cloud storage auditing with key-exposure resistance", *IEEE Trans. Inf. Forensics Securit*y, Vol.10, No.6, (2015), pp.1167-1179.

[23] Narayana MV, Narsimha G & Sarma SSVN, "Secure- ZHLS: Secure Zone Based Hierarchical Link State Routing Protocol using Digital Signature", *International Journal of Applied Engineering Research*, Vol.10, No.9, (2015), pp.22927-22940.