Indian Journal of Science and Technology, Vol 9(31), DOI: 10.17485/ijst/2016/v9i31/85785, August 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Forecasting Response Time in Elastic Cloud for Secure Resource Access in Transactional Database using Two Phase Authentication System

N. G. S. Parameswaran[1]* and M. Sumathi[2]

[1]Department of Computer Applications, VHNSN College, (Autonomous), Virudhunagar - 626001, Tamil Nadu, India; parameswar2003@gmail.com

[2]Department of Computer Science, Sri Meenakshi Government Arts College for Women, Madurai - 625002, Tamil Nadu, India; sumathivasagam@gmail.com

Abstract

The key factor of IaaS in cloud computing, deals with resource sharing and efficient utilization. Though, it was accessed only by legitimate user with cloud grant and revoke mechanism that depends on cloud data management. In this paper, a two way authentication method is proposed for accessing cloud data services with transactional database to provide resource access to legitimate user. The results show the comparison between single and two way authentication method for providing scalable and consistent performance for accessing cloud data store.

Keywords: Elastic Cloud Forecasting, Resource Sharing, Secure Resource Access, Transactional Database

1. Introduction

Cloud computing technology refers for sharing the resources over the internet. This will save the disk space instead of storing all the files. All the files store in cloud available globally and accessing can be done based on access rights. The implication rise in the aspect of accessing the resource by staying in a remote place and doing it so. The concept of Infrastructure as a Service in cloud allows outsourcing the services via multiple service access along with the existing one. Such model of IaaS includes commercial based on the information access based on time constraint.

The objective of accessing cloud service is on-demand and extended use of cloud service which can be accomplished using cloud elasticity[1]. The multi-tier environment of cloud was shown in Figure 2. When dealing multi-tier cloud approach it main focus is on orchestration. Orchestration[2] in cloud integrates all components of cloud and provides intergraded approach for accessing service.

The cloud user when accessing service, access via component store in the present layer and gets linked with the cloud application layer to enjoy uninterrupted service. To do so Cloud orchestration is included in the service. In particular all modules in cloud components that are stored in the application layer connect individually with the cloud orchestration and while dealing the service as a whole both the presentation and application combines unanimously to make the task accomplished using cloud services. In such case individual accessing of components is restricted.

The best aspect of cloud orchestration is its uninterrupted service and most of the cloud IaaS are commercial where the users have to pay depends on their access time. If the resource access time to be infinite then along with orchestration elasticity of cloud is also included. Such approach will make the user pay only for the service accessed by them and it doesn't include the other service payment. The tradeoff between multitier and single tier cloud architecture is that the predecessor combine different cloud accessing approaches into a single application

*Author for correspondence

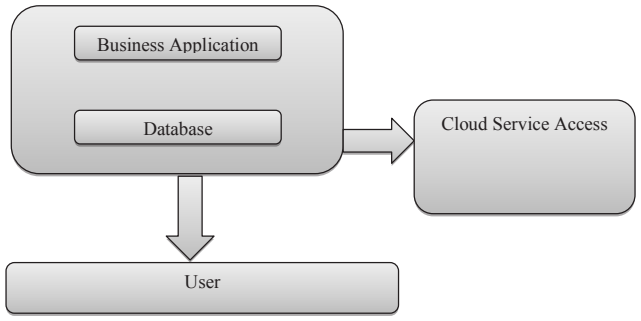

Figure 1. Cloud single tier architecture.

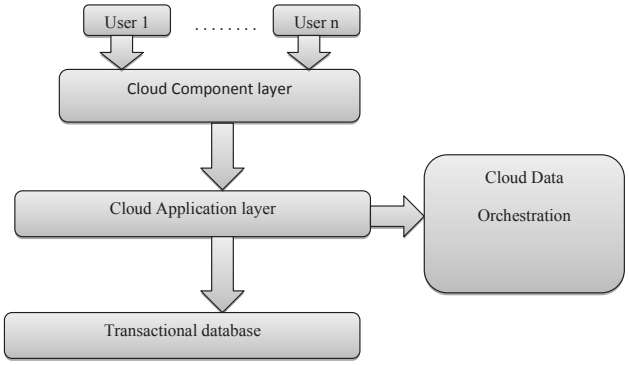

Figure 2. Cloud orchestration with transactional database.

whereas the successor makes the combination of data and business logic as a part of cloud and it won't extend itself for accessing other services when a service accessing is in process. Figure 1 depicts cloud single tier architecture where the combination of two different services paves the way for access cloud data service access.

The point is how to make a cloud service highly scalable for accessing service infinitely? In order to access the cloud service infinitely the following parameters have to be considered

1.1 Pay to the Utilized Service

The support of third party service assists cloud to get accessed to it by making the payment depends on the service accessed and the time utilized[3]. This further enhances the commercial aspect of cloud service like Amazon, Windows azure, Google. Most of service act as public cloud and few are purely commercial.

1.2 Service Accessed Infinitely

In contrast from pay for service utilization, another aspect of cloud is accessing their services indefinitely. Such mechanism also focuses on public cloud that makes the commercial as one-time payment to enjoy uninterrupted service.

1.3 Secure Access

The most challenging part of cloud is security. Cloud Security[4] deals with the following measures like

Computer or system security: It is meant to protect the computer system used as a client for accessing cloud resources or services. The system used for accessing cloud service has to adhere secure policies for continuing cloud access.

Network security: It focus on ensuring security in cloud connectivity via internet access. All the security flaws occurs in cloud happens in network connectivity and strict secure policies has to be implemented to protect the cloud accessed via internet services and this proposed concept is not address the secure policies but to ensure security in cloud services.

Information security: Combining the two secure measures as mentioned above the cloud information is secured. It addresses the way to protect the information in secure cloud models and to extend the following security which was also mentioned in information security.

Securing cloud software: Accomplished by cloud authentication process

Securing cloud platform: Accomplished by cloud model framework and its components

Securing the infrastructure (as its deployed in IaaS): Accomplished by virtual and shared cloud storage

2. Survey

2.1 Cloud Data Security and Secure Policies

Ensuring cloud data service policies resembles traditional data security by which secure algorithm is used for protecting the data between users. As cloud lies open to all users to make it utilized, security measures have to be leveled up. The data security in cloud addresses the user authentication factor and its policies refer the way to access it. User access control mechanism underlines the measures taken with identifying authentication, its confederacy and finally data management.

2.2 Cloud Elasticity

The most flexible part of cloud is it elasticity[5]. This also focuses on consistency and scalable cloud service access.

The entire traditional databases will never use the concept of elasticity and this is because of the fact that cloud infrastructure supports transactional database rather than using traditional database access. Transactional database has huge threat against data availability as it replicates the data for consistency and scalable access[6]. Our previous work address this issues ensuring consistency and reliability gap in elastic cloud.

2.3 Cloud Storage: IaaS and PaaS, SaaS

Generally cloud data storage is differentiated into IaaS store and PasS, SaaS store. It makes the broad classification between these two stores as the cloud transactional database access the information based on the cloud model it's proposed to deal with. The concept of virtual IP was given to every system accessing cloud in transactional database and the corresponding data store was given access to every virtual IP for storing and accessing the data. In Figure 3 first level authentication will ensure system consistency based valid authentication check and once through it will process the second level authentication for getting the query done with the cloud data store.

2.4 Transactional Storage

The purpose of transactional data store[7] is to emphasis on data consistency and while adhering to this it leads to data replication problem which is also a part of implying secure policies[8]. To get rid of these issues the concept of elasticity is introduced and to extend this will avoid data replication problem. This problem was addressed in single tier cloud architecture and still bottleneck remains as an issue.

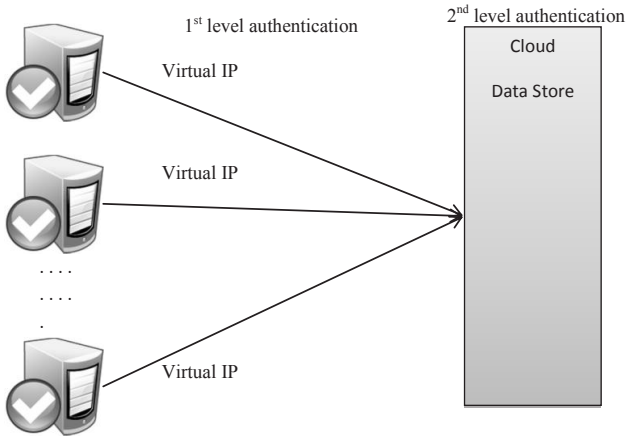

Figure 3. Two phase authentication for accessing cloud data store.

Further addressing this problem to get rid of it completely the database authentication mechanism is used. The way how the authentication mechanism was followed when the data is accessed using transactional database implies on two methods. 1. Single way authentication. 2. Two way authentication.

Single level authentication: Checks for user and system consistency by valid authentication check

Two level authentication: Process the query with the data store send by the user to the cloud store

3. Existing System

The existing system of cloud data store using transactional database works as mentioned in the Figure 4. When a user or a system sends a request to the DB it then receives a response in the form of acknowledgement. Such acknowledgement also ensures the first level of authentication is success. The condition when the first level authentication might be success is either the authentication phase is success or connection establishment is success as per policy term. The first level authentication sends an authentication message to the cloud stores to proceed with the second level of authentication process that is with the cloud data store. The authentication process ensures a flag value send by the first level phase to do the job. The flag value may be either 0 or 1 or in terms of True or False.

Figure 5 shows the comparison between the user/system authentication processing phases. The system which passes the first level of authentication will receive an acknowledgement and progress to the next phase and the system that fails will try to succeed the first level of authentication.

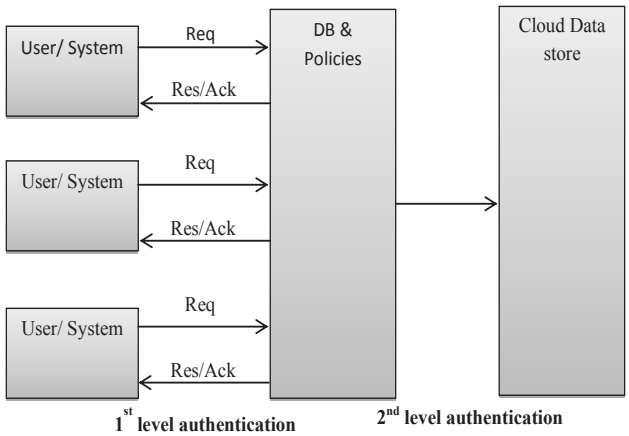

Figure 4. Level based authentication based on user access.

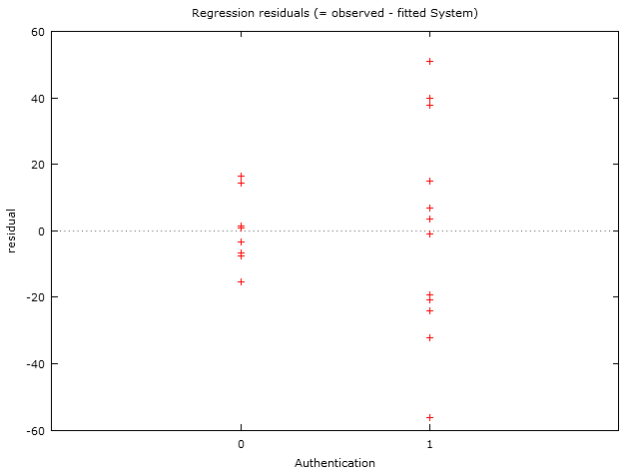

Figure 5. Observation based on authentication (single level authentication).

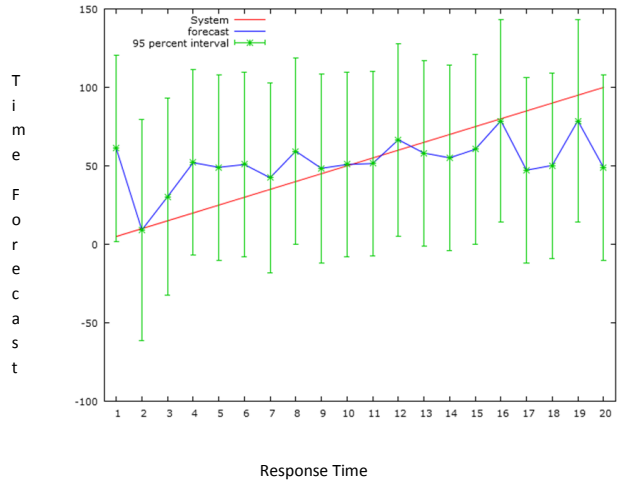

Figure 7. Observation based on response time (single level authentication).

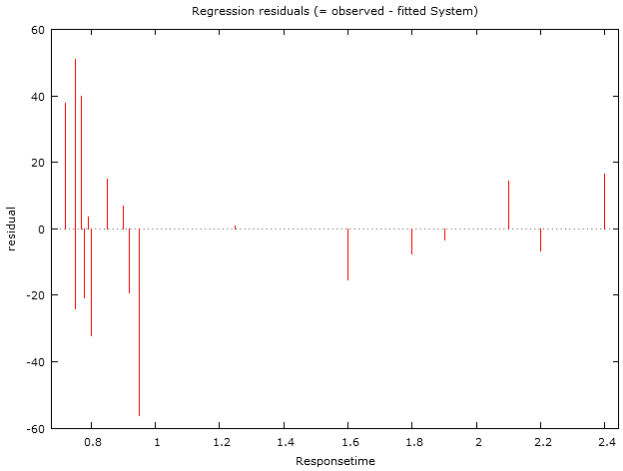

Figure 6. Observation based on response time (single level authentication).

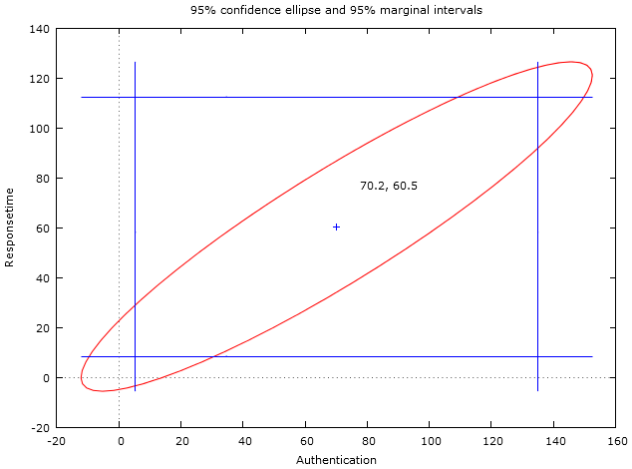

Figure 8. Confidence level for 1st level authentication.

Figure 6 shows the process in terms of response time and it should be kept low based on authentication process level. If the response time increase there will be delay in receiving the message between the phase and 95% of the confidence level fails. When Response time is 0 then it fails.

Figure 7 gives the total figure based on single authentication level that will forecast to make the response time as 95%. More the confidence level faster the access which in turns increase scalable performance of the system for accessing data store.

Figure 8 shows the confidence level marked in eclipse boundary and setting its parameter with respect to authentication and response time.

Table 1 shows the cloud forecasting[9] for measuring its scalability towards accessing resource and its response time.

4. Proposed System

The proposed system works with two phase authentication process[10] that ensures scalable and consistent performance for accessing cloud data store. In tradeoff with the existing system the proposed system addresses all these issues by making both the authentication phases[11] consistent for letting the query executed in the data store.

In phase I of the authentication process, it authenticates the user/system and sends the request value as 1

to the cloud data policies. On receiving the request, it sends back an acknowledgement in the form of response that validates the first level of authentication process. By holding the value 1 received from the previous process the phase two of the authentication process checks for query transaction that to be executed by the cloud data store. Such process is given to transactional data store for checking both the consistency result (1 in this case) for executing the result.

5. Experiment Result

In Figure 9, it tries to narrow done both the values of response time and authentication as it will proceed when both the value is send to 1. (i.e.,) authentication 1 and authentication 2 has the value 1 means the process is successful.

Table 1. Forecasting the response time based on authentication phase

	Coefficient	Std. error	t-ratio	p-value
Const	−66.4559	49.1607	−1.352	0.1941
Authentication	70.1751	30.7334	2.283	0.0355 **
Responsetime	60.4886	24.6564	2.453	0.0252 **
Mean dependent	var 52.50000		S.D. dependent	var 29.58040
Sum squared	resid 12274.31		S.E. of regression	26.87040
R-squared	0.261695		Adjusted R-squared	0.174836
F(2, 17)	3.012864		P-value(F)	0.075858
Log-likelihood	−92.57409		Akaike criterion	191.1482

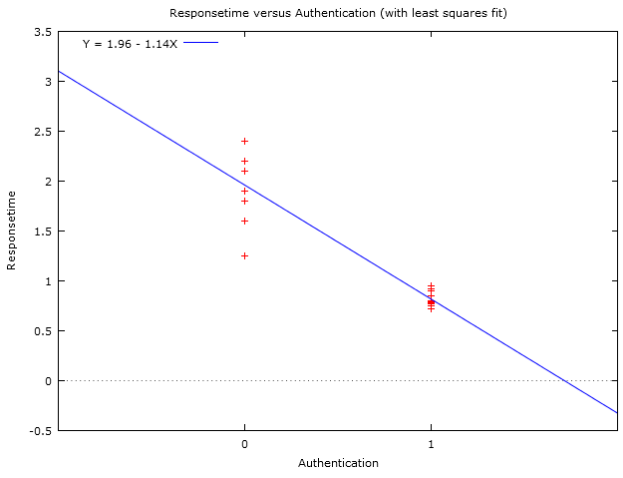

Figure 9. Response time vs authentication in two phase process.

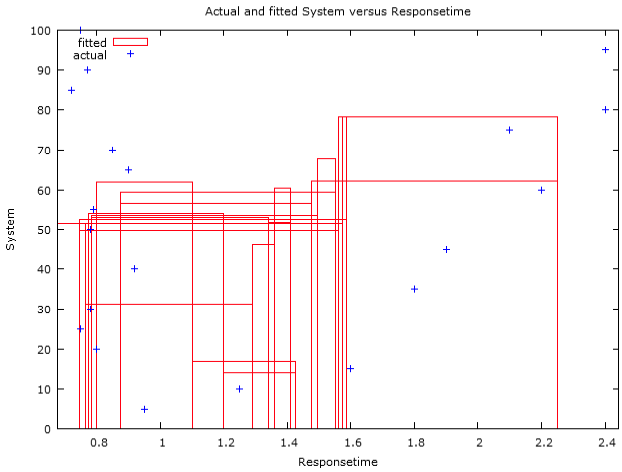

Figure 10. Actual fitted system based on response time.

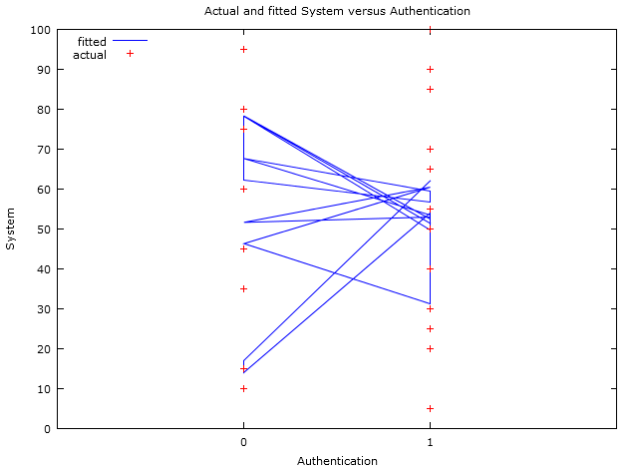

Figure 11. Reducing authentication gap vs systems in two phase authentication.

Table 2. Confidence level of two phase authentication

Variable	Coefficient	90% Confidence	Interval
const	-71.5353	-157.533	14.4625
Authentication	61.1054	5.51172	116.699
Authentication1	21.7723	14.4914	58.0360
Responsetime	53.3467	8.80619	97.8873

Figure 10 shows the actual fitted systems that are efficient towards response time.

Figure 11 minimizes the gap between actual systems with the system poised with authentication mechanism. The study is to reduce the number of systems that are not deployed with authentication standards and procedures.

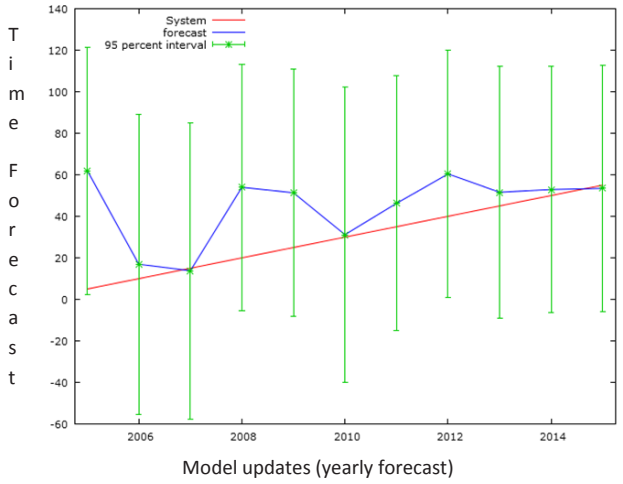

Figure 12. Reducing failure percentage with two phase authentication.

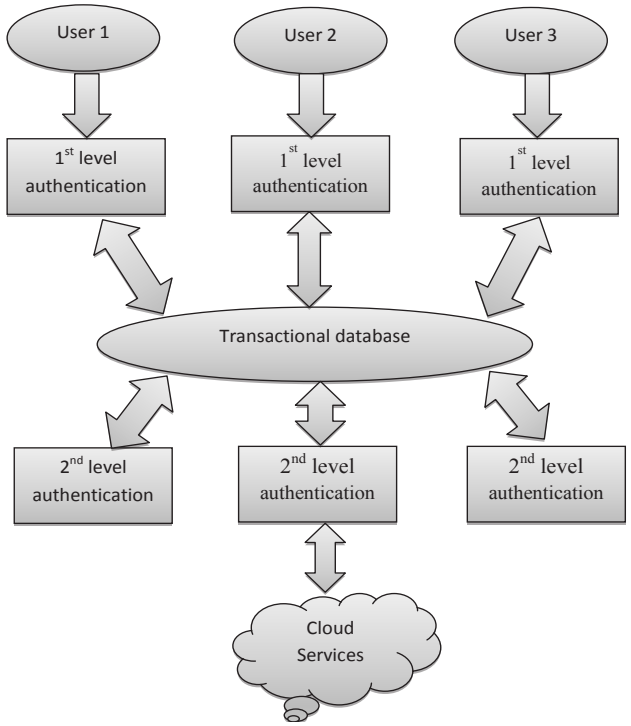

Figure 13. Proposed model.

Figure 12 shows the proposed system approach for reducing the system failure with authentication standards and 95% towards two phase authentication as the confidence level set is 90% with single phase authentication.

Figure 13 represents proposed cloud model using two phase authentication process for accessing the cloud service in secure channel. It also paves the way for accessing the cloud transaction database that is dually protected with secure cloud service access.

6. Conclusion

In this work, the secured cloud authentication using two phase authentication mechanism for ensuring scalable and consistent transactional database is achieved with 95% success rate. The secure policies set the secure cloud standard and it works consistent in two phase authentication mechanism. The results shown in the Table 2 represent the confidence factors achieved with two phase authentication. The response time also referred as interval time period which is also reduced in this process. The confidence level of two phase authentication process is checked with single phase authentication process and efficient result is achieved. Thus, the scalable performance of cloud transaction database is entirely dependent on its authentication process which is well balanced using two phase authentication.

7. References

1. Fito JO, Goiri I, Guitart J. SLA-driven elastic cloud hosting provider. 18th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP); 2010. p. 111–8.
2. Baldine I, Yufeng X, Mandal A, Renci CH. Networked cloud orchestration: A geni perspective. 2010 IEEE GLOBECOM Workshops; Miami, FL. 2010. p. 573–8.
3. Patel A, Seyfi A, Tew Y, Jaradat A. Comparative study and review of grid, cloud, utility computing and software as a service for use by libraries. Library Hi Tech News. 2011; 28(3):25–32.
4. Manjusha R, Ramachandran R. Secure authentication and access system for cloud computing auditing services using associated digital certificate. Indian Journal of Science and Technology. 2015 Apr; 8(S7). DOI: 10.17485/ijst/2015/v8iS7/71223.
5. Brebner PC. Is your cloud elastic enough? Performance modelling the elasticity of infrastructure as a service (iaas)

cloud applications. Proceedings of the 3rd ACM/SPEC International Conference on Performance Engineering, ICPE; 2012. p. 263–6.
6. Das S, Agrawal D, El Abbadi A. ElasTraS: An elastic transactional data store in the cloud. USENIX HotCloud. 2009. p. 1–5.
7. Vo HT, Chen C, Ooi BC. Towards elastic transactional cloud storage with range query support. Proceedings of the VLDB Endowment. 2010; 3(1-2):506–14.
8. Wobber T, Rodeheffer TL, Terry DB. Policy-based access control for weakly consistent replication. Proceedings of the 5th European Conference on Computer Systems, eUROsYS; 2010. p. 296–306.
9. Roy N, Dubey A, Gokhale A. Efficient autoscaling in the cloud using predictive models for workload forecasting. 2011 IEEE International Conference on Cloud Computing (CLOUD); Washington, DC. 2011. p. 500–7.
10. Wang C, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for data storage security in cloud computing. 2010 Proceedings IEEE INFOCOM; 2010. p. 1–9.
11. Park J-K, Lee H-S, Kim S-J, Park J-P. A study on secure authentication system using integrated user authentication service. Indian Journal of Science and Technology. 2015 Sep; 8(23). DOI: 10.17485/ijst/2015/v8i23/79284.