Cloud based E-Learning, Security Threats and Security Measures

Abdul Rahman[1]*, Shahzad Sarfraz[1], Umar Shoaib[1], Ghulam Abbas[2] and Muhammad Atif Sattar[1]

[1]Faculty of Computing and Information Technology, University of Gujrat, Gujrat - 50700, Pakistan;
malik.rahman@uog.edu.pk, Shahzad.sarfraz@uog.edu.pk, Shoaib.umar@gmail.com
[2]Department of Chemical Engineering and Technology, University of Gujrat, Gujrat - 50700, Pakistan;
Abbasg110@yahoo.com, Atif.sattar@uog.edu.pk

Abstract

Objective: The purpose of this paper is to rectify the aspects that leads the acceptance of cloud based E-learning services and why it is plagued by security issues despite its numerous advantages and find out the possible solutions to the problems. So this study highlights the security threats with cloud based e-learning and the precaution acquired recently on those problems. **Method**: This paper used both theoretical and empirical studies. Empirical study is done by the information congregated using numerous cloud based e-learning solution vendors websites. On the other hand, theoretical study is made by examining several research articles linked to our theme areas. Based on this analysis it identify different security threats in cloud service delivery model through the object to recommend a solution in the procedure of security measures related to the cloud based e-learning. Projected practice certifies data availability and offers solution to secure essential data from the invaders. **Findings:** The project edupshot of this study is to highlight the vital security threats and concerns occupied on when executing the cloud computing for e-learning systems. We do attempt to exploit the security concerns that e-learners and the end-users of cloud based e-learning solutions desire to acquire it from the cloud based e-learning solution vendors. This study finds diverse security issues in cloud service by an object to advocate a resolution in the form of security dealings linked to the cloud based e-learning. Traditional E-Learning approaches are merged with cloud computing technology to give enormous benefits to the academic users but it compromises on security facets. This study of E-Learning advocate's users to acquire the data in the cloud via a secured layer using the internet. Cloud based E-Learning is a way to lessen cost and density of data retrieving, which are handled by third party services. **Improvements:** The study does not explore negative aspects that may deject acceptance of cloud-based services. However, we have just discussed cloud computing and its service and have presented ways by which the present security issues in cloud computing can be resolved.

Keywords: Cloud Service, Data Availability, Measures, Security Risk, Solution, Threats

1. Introduction

E-learning is one of the widespread technologies, which recompense the scarcity of well-informed teachers in universities and several institutes, so cloud computing makes its fortune by giving cloud strength to the functionality of E-learning solutions[1]. It is a vital pattern, with note worthy potential for dipping charges via optimization and growing economic efficiency, which can meaning-fully, increase collaboration, agility and scalability[2]. Cloud computing enables expedient access to networks and applications, common set of configurable computing resources such as networks, servers and applications that can be provided and unconfined straight away by slight effort or involvement[3,4].

The portable cloud computing is helpful in finding e-learning solutions for cells and other alike node such as Tablet PCs, smart phones, PDAs. Cloud based E-learning

solutions lessen the cost in the traditional E- learning technology by its widespread cloud source. Due to infinite vulnerabilities related to web sources, people are very conscious about the security features of the technology and cloud based E-Learning technology is no way an exception from such security vulnerabilities. The software of E-learning that is provided by the educational services is accessible through the Internet and Website. It provides network system and the result is a cloud-based service that is obtained through computing and the Internet. However, in order to maintain an effective and successful E-learning, we need to identify and resolve security cloud-based E-learning products. Through this work, an effort is made to explore the merits of this emerging technology, with a focus on security concerns, and with possible outcome to ensure the safety of the cloud-based E-learning products and the safety of handlers and information stored on the server.

2. Cloud Systems

The basic theme of this technology is to make virtual pool with its main concern on large-scale computing resources link to the network resources, plus allowing Consumers can share hardware resources, software dynamic and data, and based on actual usage, pay. Therefore, we can easily purchase and vend this technology through the network in order to lower prices of commodities, such as water, sale of natural gas and electricity[5]. Now, you acknowledge and admit the key features of it, we have to aware the development model, and what is right way to enjoy the service, plus how protection[6]. There is five main characteristics of it Calculated[7,8] and the Figure 1 illustrates the key models and key characteristic.
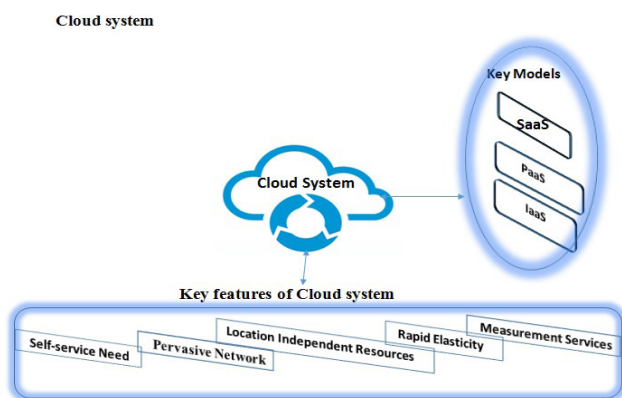

Figure 1. Cloud system.

2.1 Self-Service Needs

Through this, customers do directly and automatically access online learning cloud computing and more in any computer emphasizes safety facilities, such as servers, network storage supplier in no time.

2.2 Pervasive Network Entrance

It means the device accessible on the network, and do follow the standard approaches. This approach is useful for both professional and non-professional client, such as laptops plus cell phones.

2.3 Location-Independent Resource Pool

The value Resource pools for the need of various customers in dynamic place provider. Such resources indulged memory, storage, network bandwidth, and virtual machines.

2.4 Rapid Elasticity

With this function, the facility does set quickly and through great flexibility, it must Enlarge or quickly discharge. Similarly, the service may be continuously being updated and improved by visiting users.

2.5 Measurement Services

This feature allows the monitor, Monitoring and report age of such resources, and can obviously, regulate plus echo on the number and amount of Resources and customer use infrastructure providers.

Similarly, all of these feature, including consistency and Presence cloud[7].

There are some models of cloud: public, private and group and hybrid cloud[6,7]. Public cloud providers public can by different tenants, including access resources, network applications and services by providing the Internet can provide the necessary infrastructure, its implementation, by organizing help[9]. Although the second type of cloud is just an Institute, so that each person do interact inside the institute, Services and applications, on the other side no one from outside can interact with it. Cloud Infrastructure Organizations[10]. Therefore, private cloud Management organizations maintain user protection entirely by tissue[7]. Similarly, the group clouded signed for customers of a particular set of[6] some organizations sharing infrastructure, Group support specific security needs, but share among multiple organizations involved in atten-

tion[10]. The latest model hybrid cloud must be a mixture of two or more clouds. This is the reality that its Atmosphere through inner and outer cloud services several vendors using[9].

There are three models of several cloud computing services this is[6,7]: Software as a Service (SaaS), Platform as a service (PaaS) and Infrastructure as a Service (IaaS).

3. E-Learning Environment

Through this, students over and done with online learning applications and by related tools Study. Virtualization and personal learning environments, learning environment is the most important environmental, this presents a variety of E-learning environment through E-learning applications allow students the opportunity to Study[10]. Key benefit of Virtual Learning Environment (VLE) is stored parallel a plurality of threads, it offers a very convenient environ for teachers plus Students who want to shift from one area to another also VLE offer many other opportunities Such as[11]

- Notice of the latest information about the courses page Problems.
- Students in any course required in your account Time plus it do interact from anywhere.
- Allow students which have any distinct demand plus constraints for such of e-learning systems.
- Provide preparation in a great geographical range.
- Through Internet (due to flexibility and cost Effective in helping students) to facilitate learning.
- There is no big choice to use of virtual learning environments curricular more selective provided to students for tiny schools.
- For contact among students and Teachers.

PLE is a user-network learning System that give the permission to students to handle and progress their learning process. PLE supports many features, for most users[10,12].

The Figure 2 highlights the overall pros and cons of cloud based E-learning environment.

4. Cloud-based E-learning Advantages

It is a part of cloud computing, through which It involves the education system and E-learning fields. Traditional cloud-based e-learning resources include all the necessary hardware and software infrastructure to improve network learning[10].
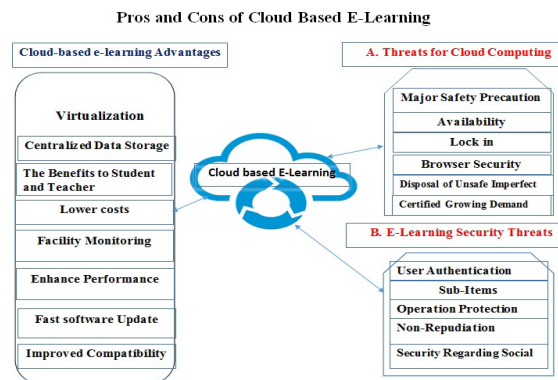

Figure 2. Pros and cons of cloud based e-learning.

4.1 Virtualization

It rapidly replaces the server in the cloud guilty, no significant costs or losses. Lower cloud greatly anticipated time the reason is that it is simple creating a virtual machine[13,14] clones.

4.2 Centralized Data Storage

This is the most vital aspect of the application, while its information is saved in cloud, lose serious incidents customer cloud is not a cloud in the Calculations. Therefore, newcomer will link to that system[13,14].

4.3 The Benefits to Students

cloud is become a helping hand for a no of students. It provide platform for student to take participate in online course, testing and get feedback in Teacher training plus send their project and works online to relevant teachers[15].

4.4 Benefit of Teachers

Teachers specially get more and more E-learning based on the benefits of cloud computing. Teachers have best facility to Online test for students to prepare; they can prepare Students from the best content resources CMS can assess plus reply to their work, project and queries in timely manner because they communicate their students to online forums[10,15].

4.5 Facilitate Watching

There should be one central place of monitoring Instead of a computer monitor is one hundred thousand a univer-

sity to control data access Easier. In addition, security can be changed testing and implementation deprived of any trouble Cloud computing represents a single point for all Customers entering[13].

4.6 Lower Costs

User E-learning is not need a PC hardware specification of powerful electronic learning application. You can deploy the application running Cloud from your PC, Cell phone, tablet PCs and Internet connectivity through least configuration. User no need to pay any extra charge if they want to saved more date on cloud then local machine. So companies will rent an empty Cloud-based demand[16].

4.7 Enhance Performance

The application E-learning is based on cloud computing and there are plans applicator in cloud computing in many processes, so any problems can be Occurs, the client[17] is activated.

4.8 Fast Software Update

Since the application of cloud-based E-learning implemented, their software will be routinely upgrades cloud sources. Then, the user will always be updated online learning Software[10,17].

4.9 Improved Compatibility

Due Format and source files make the appropriate computer/phone, so all sizes cloud network learning Applications, so there is nothing to worry. Since e-learning applications, cloud-based, open files through cloud environment[10,17].

5. Concerns in Term of Security in Cloud based E-Learning

In the security issues due to latest technology, it is vital to sort out issues if you your users will want it as a surety of security. Since when this technology through web-based resources are not safe, so that many threats in cloud computing is mostly Internet-based which is faced by E-learning users. Although the cloud E-learning still has carried a lot of benefits, though uncertainty in cloud computing security has not been fully met, there is still security challenges plus problems in the digital world[17].

5.1 Threats for Cloud Computing

5.1.1 Major Safety Precautions

Required Including knowledge or control of the standard Resource utility, as they are being shared Third-party client system. Therefore, encountered some difficulties in the spell when it transfers of utility services Cloud computing system, altered[13] systems. In Cloud service it has to keep encryption/decryption Keys through official person[17].

5.1.2 Availability

As we know cloud has a no of application and data which is accessed through different method and provide such services to its clients without any disturbance is a critical. Both DOS attacks and DDOS attacks are the most famous attacks which compromise the availability of the service 24/7[10].

5.1.3 Lock Information

Today, cloud service providers provide a lot of tools, applications, and standard data pattern to your clients. Then again the problem faced by these services when the service client tries to use other suppliers[10,17]. There is a compatible with the cloud providers. Therefore, client easily shifts from one side to another service. This issue has difficulty to obtain cloud service providers[18].

5.1.4 Browser Security

Remote server task is related to cloud computing. The client machine is simply used by the device access to any application. In such scenario, through browser any user uses the gateway to access the cloud server[10]. Therefore, the whole browser security if the attack criminal's gateway software is very important, because Global cloud security will become a problem. It's required both security certificate and authentication policy for secure browser. XM Signature and XML Encryption also help to ensure that security issues[19].

5.1.5 Disposal of Unsafe Imperfect Data

In most operations System, there is a chance to not fully remove the data, even if it is removed from physically. Clients have no idea, if your data is completely eliminated from after a delete command from all virtual machines

Applications. This problem leads to unsafe cloud data. And the risk of the ft is possible to use the data Unauthorized persons or hacker cloud[10,18].

5.1.6 Certified Growing Demand

The providers have a no of advantages for its clients; first of all it is providing software and access to applications in line. There is no need for a client to install all software to get fully utilized it every aspects. No worry for the customers to care about the privacy of software, because they are monitored by a centralized server through the cloud. The service providers should be cautious to give verifies its customer's access through certified personnel People. If the cloud operators cannot provide these the authentication process, which may result in increased Phishing or other vulnerabilities by threatening unauthorized access to these cloud applications[10,16].

5.2 E-Learning Security Threats

Online learning technology concerns in general, basic safety when we use it in traditional teaching applications Equipment. These problems give the following[10,20]:

5.2.1 User Authentication plus License

User enter into e-learning environment is a main Necessary permit. In overall, e-learning clients have various places, away from the user ID and password should be provided. Apprentice or student according to Permissions define the account can be accessed Installation. Billing on the way he/she can make the foundation under the rules of access to the level of Learning (learning regulations), or not[21].

5.2.2 Sub-items

Tickets, a lot of terminals mean that there is a chance of security breach can happen in passive mode the case of e-learning. Because the number of clients, Use of e-learning servers in remote areas, makes Enter the two inputs will lead to security threats.

5.2.3 Operation Protection

Protection Processing is the most important tasks necessary Applied on e-learning environment. Prevent other users through the use of such technology Digital signatures, firewalls and other several similar measures should be taken to prevent tampering registered users.

5.2.4 Non-repudiation

At this level, information security, the pattern of data is damaged, or destroyed by a virus. The system should provide multi-Capacity change data is not attacked.

5.2.5 Security Regarding Social Aspect

Online E-learning varied from traditional learning environment. The main differ in the event of Assigned to the student teachers raised. In Traditional learning environment, students Teachers directly in the print job in the classroom. The online e-learning Environment, students must upload a soft copy of their task[22].

6. Proposed Solution

Figure 3illustrates, the solution provides a cloud-based system, in order to secure E-learning environment. Security awareness, mechanisms, methods and Hacker techniques were discussed to strengthen this model.
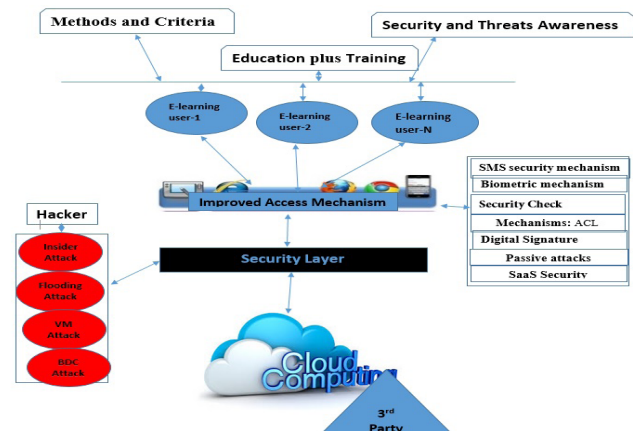

Figure 3. Secure model of cloud based e-learning.

6.1 The Security and Safety Awareness

With the formation of the Organization for Security Committee Provide guidance and care for safety purposes, the company's development strategy. The Commission will clearly define the roles and responsibilities safety Function. Safety cognizance is a key Work to be done[23].

6.2 Education plus Training

This portion indulged some basic training of security issues and crisis management capabilities (Risk), these issues for security teams and local partners. Yes Definition have basic introduction or safety Providing skills training

and mentoring team members Can be used as the basis of a certificate (Home Basic security) security, it is also refer to Data and Knowledge Management confidentiality.

6.3 Methods and Criteria

Do check the source Patterns and develop methods and standards cloud the computer system is an upright method. Firstly and the most importantly safety device should be considered is Data security and business needs[24,25].

6.4 Hacker

Hackers who represent the failure observed computer or computer network authorized/unauthorized access. There are a number of reasons, not the computer, such as benefits, protest or challenge pirates. The hackers different classification is white hat, black hat, gray hat, hackers elite Kiddi writing, Neophyt, blue lids.

6.5 E-Learning

Usually it means using computers to provide part or entirely, of course, whether at school, part of the mandatory business training or complete the course distance education. As it is already discussed.

6.6 Flooding Attack

In the system approach cloud computing all servers is service-oriented. If the server is overloaded or the maximum load, which shares some of his works to the nearby computer servers. This allocation method produces a cloud of skillful and fast execution. When the server receives an unauthorized request for a huge number, the service[26] will not be able to use a legitimate user. This attack is called a denial-of-service attack, which was requested by the floods. No legitimate application can be identified by examining the use of CPU, memory and hardware. In order to prevent server floods, organize all servers in the cloud, and assign specific tasks to each server, for example: one for the file system, the other is the memory management as well.

6.7 Backdoor Channel Attack

Backdoor Attack channel is a passive attack, to prevent the traditional authentication methods to get to the detriment of legitimate users to access confidential. Resources and possibly intrusion control needs of the target system,

trying to DDoS attacks, when the attacks were happened in back door channels.

6.8 VM Attack

Virtualization is a key infrastructure is a cloud technology services. This is a very difficult task for cloud service providers to ensure their customers virtual machine. In this typical platform, available to users of the resource is virtual and physical. These resources are limited, related to real needs. In cloud system, multi-tenant shared resources, so that various virtual resources can be attached to the same physical resources. If there is a cloud security vulnerability virtualization software platform, user data can be accessed by other users.

6.9 Insider Attacks

have been, because they been allowed access to the system, you may be familiar with the structure of the network and system policy/external attackers program has obvious advantages.

6.10 3rd Party Provider

Third party service provider is responsible for transactions cloud security services, because some cloud service providers from outside sources. Prior to the adoption of cloud services, we must be aware of the roles of provider cloud third and clearly addressed in the contract responsibilities. Data owners should know if you outsource to cloud vendors another cloud provider or not. For example, data stored in the storage box (SaaS) Amazon Web Services (IaaS) data center. At this stage, the customer can be detrimental to your privacy in the cloud, poverty contract[27]. To avoid this risk, cloud providers should consider the following recommendations:

It is clear that third parties mentioned names and identify their function.

Other suppliers to follow security policies and procedures • this is followed by the cloud provider. If there is any fault, cloud providers need only responsible • direct support in all aspects of customer data.

6.11 Enhance Security Mechanisms

The listed below methods should be improved and make it more user friendly.
- SMS security mechanism
- Biometric mechanism

- Security Check
- Mechanisms: ACL Access Control List or Process is used to access the server or user-specific resources you can customize elements of the access mechanism.
- Digital Signatures
- Security due to passive attacks
- SaaS Security

7. Conclusions

The main theme of E-learning is to facilitate and enhance the educational services using latest techniques and novel methods such as cloud-based technology. However, issues and challenges ongoing process in the field of security. Any kind of threat is noted immediately and effort is made to resolve it as soon as possible. The reason of which is the security issue of cloud applications as all the data can be transmitted over the Internet.

Due to security concerns and slow resolutions of problems, the customers are doubtful about new technology. The customers access all their data through internet in cloud. These issues served as barrier and to some extent stopped the rapid growth of such technologies, especially in the field of cloud-based E-learning. In research views, questions, suggestions, service providers and the government should strive for the new protocol and data transfer mechanism. Technical data of who is the user of insurance is the most important Benefit from cloud-based online learning users. In addition, one needs to consider the security infrastructure, such as Servers and firewalls that can play an important role in it. Because the main concern this model is in the technical consumer server security the data server based on the server security than it looks Necessary. To reduce these threats to the security of the server, disaster recovery, safety and management standards of personal safety, you can use Security measures. A listed security challenge/proposed solution is a valuable new management and future design methods of the Security of cloud-based e-learning. This work contributes to cloud computing data centers around the clock data availability and development of e-learning and e-learning methodology.

8. Acknowledgements

9. References

1. Kadam Y. Security issues in cloud computing a transparent view. International Journal of Computer Science & Emerging Technologies. 2011; 2(5):316-22.
2. Lal P, Bharadwaj SS. Understanding the impact of cloud-based services adoption on organizational flexibility. Journal of Enterprise Information Management. 2016; 29(4):566-88.
3. Kadam Y. Security issues in cloud computing a transparent view. International Journal of Computer Science & Emerging Technologies. 2011; 2(5):316-22.
4. Morsy MA, Grundy J, Muller I. An analysis of the cloud computing security problem. Proceedings of APSEC Cloud Workshop; Sydney, Australia. 2010.
5. Che J, Duan Y, Zhang T, Fan J. Study on the security models and strategies of cloud computing. Procedia Engineering. 2011; 23:586-93.
6. Gharehchopogh FS, Hashemi S. Security challenges in cloud computing with more emphasis on trust and privacy. International Journal of Scientific & Technology Research. 2012; 1(6):49-54.
7. Jamil D, Zaki H. Security issues in cloud computing and counter measures. International Journal of Engineering Science and Technology. 2011; 3(4):2672-6.
8. Al-Fares M. A scalable, commodity data center network architecture. Proceedings of SIGCOMM; 2008.
9. Takabi H, Joshi JBD, Ahn G. Security and privacy challenges in cloud computing environments. IEEE Security Privacy Magazine. IEEE Computer Society. 2010; 8:24-31.
10. Monsef M, Gidado N. Trust and privacy concern in the Cloud European Cup. IT Security for the Next Generation; UK. 2011. p. 1-15.
11. Qaisar S, Khawaja KF. Cloud computing: Network/security threats and counter measures. Inter Disciplinary Journal of Contemporary Research in Business. 2012; 3(9):1323-9.
12. Vic JR, Winkler W. Securing the Cloud: Cloud Computer Security Techniques and Tactics. Elsevier Publishing; 2011.
13. Kumar G, Chelikani A. Analysis of security issues in cloud based e-learning [Master's thesis]. Sweden: University of BORAS; 2011.
14. Harmelen VM. Personal learning environments. 6th IEEE International Conference on Advanced Learning Technologies ICALT; 2006. p. 815-6.
15. Pocatilu P. Cloud Computing Benefits for E-learning Solutions. O-Economics Of Knowledge. 2010; 2(1):1-6.
16. Hameetha Begum S, Sheeba T, Nisha Rani SN. Security in cloud based e-learning. International Journal of Advanced

Research in Computer Science and Software Engineering. 2013; 3(1):1- 6.

17. Begum SH, Sheeba TSN, Rani N. Security in cloud based e-Learning. International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(1):1-6.

18. Al-Jumeily D, Williams D, Hussain A, Griffiths P. Can we truly learn from a cloud or is it just a lot of thunder. Developments in E-Systems Engineering (DESE); USA. 2010. p. 131-9.

19. Rao NM, Sasidhar C, Kumar VS. Cloud Computing Through Mobile-Learning. India; 2011. p. 1-6.

20. Jamil D, Zaki H. Cloud computing security. IJEST. 2011; 3(4):3478-83.

21. Jensen M, Schwenk J, Gruschka N, Iacono LL. On technical security issues in cloud computing. IEEE International Conference on Cloud Computing, CLOUD '09; Bangalore. 2009. p. 109–16.

22. Ahmed S, Buragga K, Ramani AK. Security issues concern for E-Learning by Saudi universities. IEEE 13th International Conference on Advanced Communication Technology (ICACT); Seoul-Korea. 2011. p. 1579-82.

23. Kambatla K. Towards optimizing Hadoop provisioning in the cloud. Proceedings of the Hot Cloud; 2009. p. 1-5.

24. Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J. Controlling data in the cloud: Outsourcing computation without outsourcing control. Proceedings of the ACM Workshop on Cloud Computing Security; Chicago. 2009. p. 85-90.

25. Durairaj M, Manimaran A. A study on security issues in cloud based e-learning. Indian Journal of Science and Technology. 2015 Apr; 8(8):1-9.

26. Angel S, Rodrigues P. Estimating the size of e-learning system using learning object points method. Indian Journal of Science and Technology. 2016 Aug; 9(33):1-12.

27. Auxilia M, Raja K. Ontology centric access control mechanism for enabling data protection in cloud. Indian Journal of Science and Technology. 2016 Jun; 9(23):1-7.

28. Ryan MD. Cloud computing security: The scientific challenge and a survey of solutions. Journal of Systems and Software. 2013; 86(9):2263-8.

29. Batra M, Arora A. Cloud computing security: A review. International Journal of Advance Research in Computer Science and Management Studies. 2016 May; 4(5):1-6.