Indian Journal of Science and Technology, *Vol 8(8), 757–765, April 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
DOI: 10.17485/ijst/2015/v8i8/69307

A Study on Security Issues in Cloud based E-Learning

M. Durairaj and A. Manimaran*

School of Computer Science Engineering & Applications, Bharathidasan University, Trichy-620023, India; durairaj.m@csbdu.in, manimaranbdu@gmail.com

Abstract

Cloud based E-Learning is the method to reduce cost and complexity of data accessing, which are controlled by third party services. Traditional E-Learning methods are incorporated with cloud computing technology to provide massive advantages to the academic users but it compromises in security aspects. Proposed methodology ensures data availability and provides solution to protect indispensable data from the attackers. This study identifies different security issues in cloud service delivery model with an aim to suggest a solution in the form of security measures related to the cloud based e-learning. Different types of attacks in service delivery models of e-learning proposed by different researchers are discussed. Threats, security requirements, and challenges involved are also taken into consideration. This study of e-Learning models advocates users to access their data in the cloud through a secured layer using the internet.

Keywords: Cloud Security, Cloud Service Delivery Models, Cloud Security Attacks, E-Learning, Data Availability, Cloud Security Challenges and Threats

1. Introduction

E-Learning is one of the most significant technologies which help institutions to create a good learning environment. With the help of internet, it is possible to adopt e-learning system at low cost with minimum expenditure. Problems related to the security issues render greater constraints for cloud vendors and users. Various combinations of signal transmission techniques, advanced web technologies and other hardware developments which establishes secure e-learning[1,2]. The introduction of cloud computing technology in e-learning shows many advantages over the existing e-learning methodologies in infrastructure and cost wise[3]. This cloud e-learning technology is considered to be a proper replacement technology over traditional e-learning. The security is the major issue in the cloud computing or on demand cloud computing model. In a survey conducted by IDC on 224 IT executives, the security is marked as 74.6% which is as shown in Figure 1.

In this paper, we provide a brief but well-rounded survey on cloud security trends. We recognize that there are three cloud service delivery models 1. SaaS, e.g. Google apps, salesforce.com, zoho.com 2. PaaS, e.g. Google App engine, force.com, Microsoft Azure 3. IaaS, e.g. Amazon, IBM, Rackspace Cloud in which cloud security is involved. This paper tried to map security concerns and obligations of each of these groups. We observe that data, platform, user access and physical security issues; although emphasized in cloud computing; are generally applicable in other enterprise computing scenario as well. For example, hypervisor related threats such as cross channel attacks are present in any virtualized environment and it is not specific to cloud computing[4,5]. Two of the great virtues of cloud computing are service abstraction and location transparency. However, from security point of view these two points in conjunction with third-party control of data can create challenging security implications. The paper outlines how secure cloud environment, impact of security threats, and comparative study on security threats.

*Author for correspondence

Figure 1. IDC's survey report.

2. Cloud System

Cloud computing employs three service delivery models as listed below through which different types of services are delivered to the end user. Each service model has different levels of security requirement in the cloud environment. They are,

A. Software as a Service (SaaS)
B. Platform as a Service (PaaS)
C. Infrastructure as a Service (IaaS)

These models provide Software, application platform and infrastructure resources as a service to the users. The Figure 2 shows the different types of attacks involved in these service delivery models.

2.1 Security Issues in SaaS

In SaaS, the client has to depend on the provider for proper security measures. The provider must do the work to keep multiple users' from seeing each other's data. So it becomes difficult for the user to ensure that right security measures are in place and it is also complicated to get assurance that the application will be available when needed[6] to avoid the risks of maintaining high availability problems by having multiple copies of the data at several locations throughout the country.

2.1.1 Data Security

Data plays vital role in the cloud services, because many of cloud service providers store customers' data on large data centers. There is no guarantee for customers' data during transition operations. Data corruption may occur, when multiple devices are synchronized by one user. Data security can be classified into two ways. First, data owner must be satisfied that the cloud service provider will only process the data according to the customer instructions. Second, data owner must be satisfied that the cloud service provider has taken appropriate actions, when unauthorized data access, data modification, destruction of data by intruders.

Cloud providers are instructed to give assurance for the following data security key issues.

- Take preventive mechanism for unauthorized data access
- Allow data owners to take backup frequently
- Give legitimate authority to the data owners to data removal, data modification, and moving data to the other cloud provider

2.1.2 Network Security

Enterprises store sensitive data in the cloud server and SaaS vendor can manipulate it. To protect data from leakage of sensitive information, apply tough network traffic encryption techniques to manage data flow over the net-

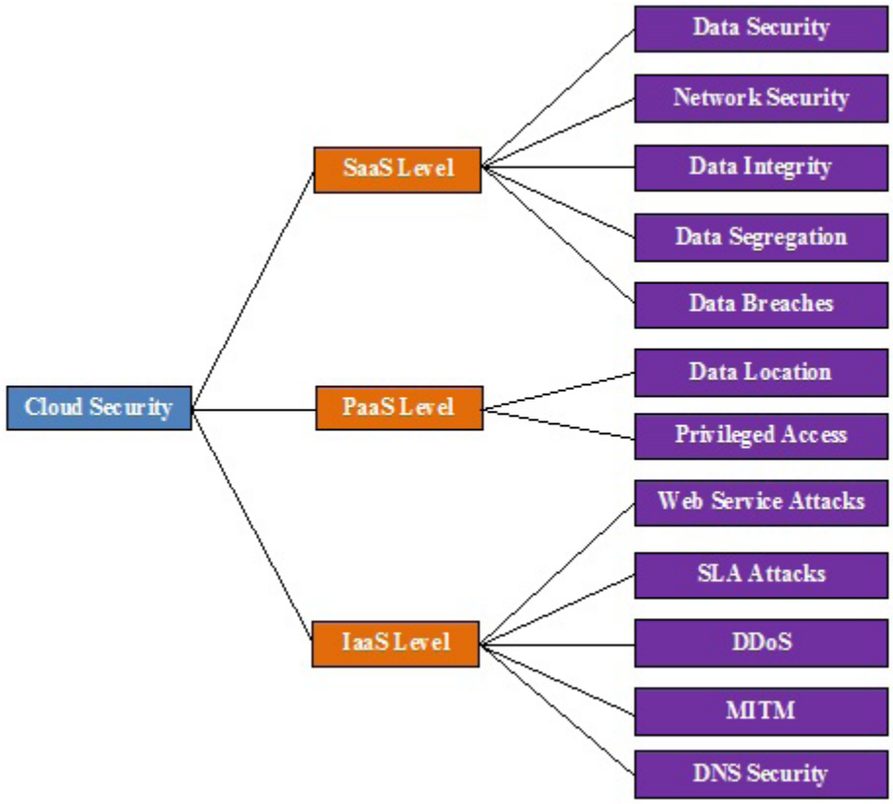

Figure 2. Types of Security attacks in Cloud based E-Learning.

work example: Secure Socket Layer (SSL) and Transport Layer Security (TLS). Survey report says Amazon web services network layer provides significant security opposed to traditional network security issues, such as MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, packet sniffing, etc. Amazon yields maximum security using SSL.

The following assessments inspect and validate the network security of the SaaS vendor:

- Network penetration and packet analysis
- Session management weakness
- Insecure SSL trust configuration.

2.1.3 Data Integrity

Data integrity defines the correctness, accessibility, high quality, and reliability of stored data. Cloud provides integrity of data storages for customer privacy. In order to defeat the risks of data integrity, get assistance of Third Party Auditor (TPA). The TPA has capability of verifying any threats in online storage services that are presented in the cloud server. In a distributed environment, many data resources are concerned in database transactions to achieve data integrity[7]. SaaS application needs multi-tenant environment for processing data and more numbers of third parties are involved. According to survey[8], it reveals the information that, Encryption techniques are not sufficient to ensure the data integrity due to multiple sources. To achieve integrity of data, Hashing techniques, message authentication, and digital signatures are taking into consideration.

2.1.4 Data Segregation

Data is residing in the cloud in a shared environment; there multiple tenants are sharing single location, so one customer's data is stored along with another customer's data, which effects difficulty in data segregation. Customer should examine the cloud provider's architecture to make sure proper data segregation and also customer should aware of protocols and implementation methods of the encryption system. Therefore each user's data limit should be considered by SaaS model[9]. To segregate the data prop-

erly from different users, fix limit to the physical level and application level.

By applying the following validation test, SaaS service provider separates the data in a multi-tenant environment.

- SQL injection flaws
- Data validation
- Insecure storage

2.1.5 Data Breaches

Ever since data from a different users and business concerns exist collectively in a cloud environment, break the data laws of cloud environment will certainly attack and damage the data of all the users. Therefore the cloud becomes a most elevated worth target[10]. In the Verizon Business[11], report says that external criminals create the maximum threat (73%), but accomplish the very lowest impact, resultant value of Pseudo Risk Score of 67,500. Collaborators are middle in both (73.39% and 187,500) resultant value of Pseudo Risk Score of 73,125. However SaaS advocates declare that SaaS providers can provide improved security to customers' data than by conservative means, still insiders have rights to use the data in a different way. The SaaS providers' employees have access to a lot more information and a single event could represent information from many customers. SaaS application providers can submit their complaints with PCI DSS (Payment Card Industry—Data Security Standards)[12] so that cloud users must meet the terms with PCI DSS.

2.2 Security Issues in PaaS

In Platform as a service, cloud computing provides computing platform and system software as a service. Cloud users create an application by controlling software deployment and configuration settings from the providers. When we look at security point of view, host based, and network based intrusions are challenging factors of PaaS Providers[13]. The major PaaS level security threats are in Data Location and Privileged access.

2.2.1 Data Location

PaaS vendors provide services for application design, application development, deployment, team collaboration, web service integration, and testing. In this statement, the PaaS cloud users access the applications of SaaS providers to get service. So that, the customer does not know where the data is stored and processed, which makes vulnerability to the system. According to survey report[14], many countries established universal security standards and data privacy laws for data location issues. For example, South America and many EU countries, they never allow sensitive data to move out of the countries. Based on data location, PaaS model provides reliability to its customers.

2.2.2 Privileged Access

The cloud provider has full rights to access data (including other users of the cloud and other third party suppliers), once data is stored in the cloud environment. There is no confidentiality of data in this cloud environment. So maintain the privileged user access can be accomplished by at least any one or two approaches by the data owner[14]. First one is to choose strong encryption method for store data and use another encryption method for data access; second one is to maintain high standard confidentiality of data, legally imposing the requirements of the cloud provider through contractual responsibilities and assurance mechanisms. The cloud provider must have provable security access control policies, technical solutions, and frequent auditing of user actions to prevent unauthorized user access, and support the segregation of duties principle for privileged users in order to prevent and detect malicious insider activity.

There are two challenges, when store encrypted data in the cloud storage. First challenge is that the decryption keys must be disintegrated securely from the cloud environment to ensure that only an authorized party can decrypt data. To attain that, store keys on disintegrated systems in house or store keys on second provider. Second challenge is that in the cloud environment, additional task about encryption is to prevent manipulations of encrypted data such that plain text, or any other meaningful data, can be recovered and be used to break the cipher.

Due to this condition in encryption technology means that cloud providers must not be conceded unlimited ability to store and archive encrypted data. If the cloud user system allows the cloud service provider to deal unencrypted data, then the cloud service provider must provide guarantee that the data will be protected from unauthorized access, both internally and externally.

2.3 Security Issues in IaaS

Infrastructure as a service model allows for variety of resources such as servers, storage, networks, and other computing resources are as virtualized systems, which are getting access through internet. Users can run any

software with security on the allocated resources, so IaaS provides full control and management on the resources. Hence, cloud providers are only the responsible for configuring security policies. Some of the security issues associated to IaaS are: Web service attack, SLA Attack, DDoS Attack, MITM Attack and DNS Attack.

2.3.1 Web Service Attack

Web service protocols are used by cloud users for getting service. SOAP is the most suspended protocol in web services; many SOAP-based security solutions are researched, developed, and implemented. A standard extension for security in SOAP is web service security, addresses the security for web services. It defines a SOAP header (Security) that carries the Web Service Security extensions and determines how the existing XML security standards like XML Signature and XML Encryption are applied to SOAP messages. Well known attacks on protocols using XML signature for authentication or integrity protection[15] would be applied to web services consequently affecting the cloud services. Finally, an extreme scenario showed the possibility of breaking the security between the browser and the clouds, and followed by proposal to enhance the current browsers security. Indeed, these attacks belong more to the web services world, but as a technology used in Cloud Computing, web services' security strongly influences the Cloud services' security.

2.3.2 SLA Attack

When customers have transferred their core business functions onto their committed cloud environment, they should be ensured the quality, availability, reliability, and performance of these resources, because cloud users do not have control over these computing resources. Cloud users are expected to get guarantees from cloud providers on service delivery, which are rendered through Service Level Agreements (SLAs) to manage among cloud providers and cloud users. The most important consequence is the definition of SLA specifications in such a way that it has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness[16]. This can fulfill most of the cloud user expectations and is comparatively simple to be weighted, verified, assessed, and imposed by the resource allocation mechanism on the cloud. Also different cloud service models (IaaS, PaaS, and SaaS) need to determine different SLA meta specifications. This also leads to number of implementation problems for the cloud providers. Finally advanced SLA mechanisms need to invariably integrate user feedback and customization features into the SLA assessment framework.

2.3.3 DDoS Attack

Distributed Denial of Service (DDoS) attack is advanced version of denial of service in terms of denying the important services by giving large number of request, which is not handled by target server. In DDoS, the attack is communicated with different dynamic networks which have already been compromised unlike the DoS attack. The attackers only have the full control of targeted system to access. Three functional units are used in DDoS attack, A Master, A Slave and A Victim. Master is handling the work of launching attack; Slave is acting as a launching platform in a network, where master can launch the attack on the victim[17]. Therefore it is also called as co-ordinated attack. Normally DDoS attack uses two different stages to operate functional units, first one is intrusion phase, where master check the possibilities of loopholes and secondly, installing DDoS attack tools attacking the victim server or machine. Purpose of DDoS attack is to make the service unavailable to the authorized user, where working procedure is same as DoS attack and only the difference is the way it is launched.

2.3.4 MITM Attack

Man In The Middle (MITM) attack is encountering when an attacker directs himself between two legitimate users. This attack is also a class of eavesdropping. The attacker set up the connection between two user and tries to hear the communication or it reveals false information between them. To protect from these kinds of attacks, tools have developed like, Dsniff, Cain, Ettercap, Wsniff, Airjack etc.

2.3.5 DNS Attack

IaaS Cloud environment deals with risky attack vector known as DNS Attack, which translates the domain name to an IP address. The user using IP address is not realistic because it has been routed to some other cloud virtual machine instead of original address one who expects. The cloud user and a cloud server get rerouted through some wicked connection. Generally applications depend on appropriate running DNS (Domain Name System) according to achieve their functions as required and websites uses DNS in two ways, one is to handle their own DNS and another one is subcontract it to ISPs. So that the cloud service functionalities are too difficult due to

incorrect DNS. DNS security measures are taken, still the route selected between the sender and receiver cause security problems.

3. Proposed System

This diagram provides cloud based model to secure E-Learning Environment. The E-Learning users, Secured Layer and 3rd party provider are taken into consideration to design this model. The Hacker's techniques are also discussed to strengthen this model. The cloud based model to secure E-Learning environment is shown in Figure 3.

3.1 Hacker

Hacker denotes who observe defects in a computer or computer network to gain authorized/unauthorized access. There are some reasons to do hacking such as profit, protestation, or challenge. Different classifications of hackers are White Hat, Black Hat, Grey Hat, Elite Hacker, Script Kiddi, Neophyt, Blue Hat, etc.

3.2 E-Learning

E-learning is electronic learning, and typically this means using a computer to deliver part, or all of a course whether it is in a school, part of your mandatory business training or a full distance learning course. E-Learning has developed, and now we embrace Smartphone's and tablets in the classroom and office, as well as using a wealth of interactive designs that makes distance learning not only engaging for the users, but valuable as a lesson delivery medium. E-Learning user can access the data in Cloud by using the Secured layer.

3.3 Flooding Attack

In a cloud system all the servers approach is service oriented. If server overloaded or reaches the maximum load, it shares some of its job to a nearby computational server. This distribution approach produces the cloud more proficient and quicker executing. When huge numbers of unauthorized request is received by the server, then the service is unavailable to the legitimate users. Such an attack is called Denial of service attack, which is occurred by flood request. Non–legitimate request can be identified by checking CPU usage, Memory, and hardware usage. To prevent servers from flooding attack, organize all the servers in a cloud environment, and allocate particular job to each server, e.g. one for file system and another for memory management likewise.

3.4 Backdoor Channel Attack

Backdoor channel attack is a passive attack, which avoids the traditional authentication methods to gain access in

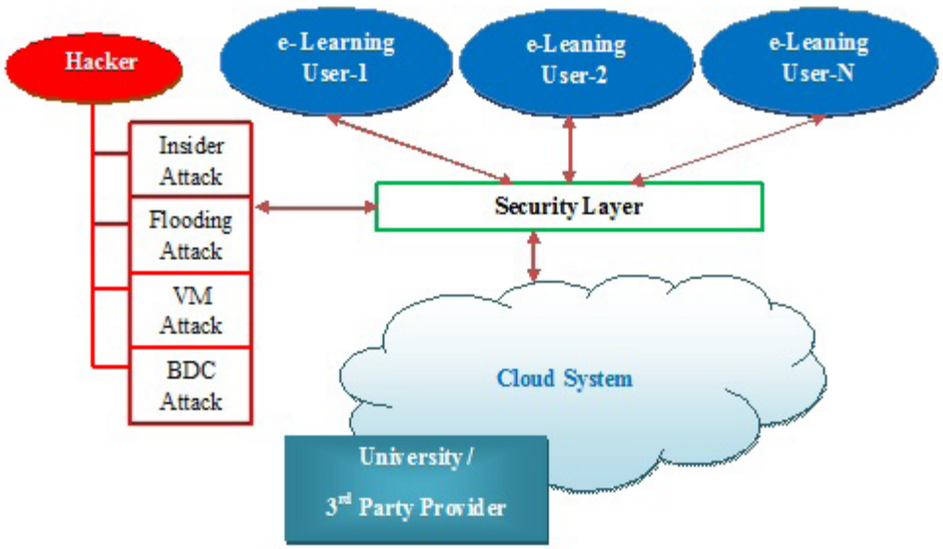

Figure 3. Cloud based model to secure E-Learning environment.

order to compromise legitimate users secrecy. An intruder takes control of target systems resources and possible to attempt DDoS attack, when backdoor channel attack is occurred. It can also be used to reveal confidential data of target user. In a cloud computing environment, this backdoor channel attack affects the Virtual Machine (VM) directly and make it as Zombie to start DoS/DDoS attack. To protect system from attacks on Hypervisor/VM, preferably anomaly based intrusion detection techniques can be used. Signature based or anomaly based technique is used for flooding and backdoor channel attacks.

3.5 VM Attack

Virtualization is one of the key technologies for the infrastructure as a service cloud. It is very difficult task for the cloud service provider to secure their customer virtual machines. In a typical cloud services platform, the resources provided to the user are to virtual and rented. These virtual resources and physical resources are bounded, according to the actually needs. In cloud computing, multi-tenants share resources, so multiple virtual resources are likely to be bound to the same physical resources. If exists security in the cloud platform virtualization software vulnerability, the user's data can be accessed by other users.

3.6 Insider Attacks

Insiders' attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies / procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks. Instances that malicious insiders working for cloud providers could impose security threat to cloud data. There are other insider threats that related to cloud computing. Employees of cloud providers with malicious intent are categorized as rogue administrator.

3.7 3rd Party Provider

Cloud Third party service providers are responsible for secure service transaction, because cloud vendors outsource some of the services. Before adopting a cloud service, we should be aware of third party cloud provider's role and responsibilities that are clearly addressed in the contract. Data owners must know, whether cloud vendors are themselves outsourcing to another cloud vendor or not. For example, Dropbox (SaaS) data stored in the Amazon web services (IaaS) data center. In this arena, the customers may be compromise their privacy in the cloud due to underprivileged contract. To prevent this risk, cloud vendor should consider the following proposal:

- Clearly mention the third party name and identify its functionality.
- Third party vendor should follow the security policies and procedures, which are followed by cloud vendor.
- If any failure, cloud vendor only takes direct responsibility for customers data in all aspects.

3.8 Security Layer

Security layer is a standard security technology designed to establish an encrypted link between a server and a client. It allows confidential information like credit card numbers, social security numbers, and login passwords to be transferred securely. Attacker can easily steal information when data transmitted between browsers and web servers as plain text. So, Security layer is a protocol which helps to deal with encryption techniques of both the link.

4. Challenges in Cloud Computing

The current acceptance of cloud computing is related with large number of challenges because users are still doubting about its authenticity.

4.1 Security

Absolute view of hindering cloud computing adoption is security issue. Running software on someone else's hard disk using their CPU looks scaring to many. Widely known security issues such as data loss, phishing attack, botnet (running remotely on a several machines) introduce serious threats to organization's data and software[18]. Furthermore, the multi-tenancy model and the shared computing resources in cloud computing has posed new security challenges that needs new techniques to handle with. For example, hackers can create cloud environment to attack others system using botnet.

4.2 Cost Effective Model

Compare to regular data centers, the elastic resource pool has made the cost analysis a lot more complicated and also data consumption cost is calculated in static computing model[19]. For example SaaS cloud providers; cost for producing multi-tenant environment is very signifi-

cant. Originally software was used for single-tenancy, if it requires redevelopment and redesign in multi-tenant environment, cost of providing these features that allow for intensive customization, performance, and security improvement are considered.

4.3 Service Level Agreement (SLA)

Service Level Agreement is most significant challenge in cloud computing for cloud users, because it is absolutely needed for consumers to receive guarantees from cloud providers. Though cloud consumers do not have control over the fundamental computing resources, they must ensure the quality, availability, reliability, and performance of these resources when consumers have shifted their core business functions onto their trusted cloud[20]. Finally, advanced SLA mechanisms require to invariably incorporating user feedback and customization features into the SLA evaluation framework.

4.4 Cloud Interoperability/Exchange Problem

The term interoperability denotes the potential to move data and workloads from one cloud vendor to another cloud vendor. Every cloud providers has their own style of unique interaction with clients/applications/users on the cloud environment. This seriously blocks the development of cloud ecosystems by forcing vendor locking, which forbids the power of users to select from alternative vendor/offering simultaneously in order to achieve maximum utilization of resources at different levels within an organization. More significantly, proprietary cloud APIs makes it very hard to integrate cloud services with an organization's own existing legacy systems (e.g. an on-premise data centre for highly interactive modeling applications in a pharmaceutical company). The main goal of interoperability is to recognize the unlined fluid data across clouds and between cloud and local applications[21]. Mainly two issues are discussed in the following section. First, to optimize the IT asset and computing resources, an organization often wants to keep in-house IT assets and capabilities associated with their core competencies when outsourcing marginal functions and activities on to the cloud. Second, for the purpose of optimization, an organization may necessitate to outsource a number of marginal functions to cloud services offered by different vendors. The solution to this interoperability problem is standardization. Even so, as cloud computing begins its

Table 1. Service level, type of users, security necessities, threats & security challenges in cloud environment

Service Level	Type of users	Security Necessities	Threats	Security Challenges
Software as a Service (Zoho planning, Google, Salesforce, Enterprise resource planning, Human Resource, customer Relationship management applications)	Who are in need of Application Services offered by cloud vendors	• Multi-tenant deployment • Data Consistency • Information defense • Application protection • Availability of Services	• Data Breaching • Data Correctness • Modification of stored data • Session Hijacking • Network traffic investigation	• Governance and Corporate Risk Management • Legal Issues: Contracts and Electronic findings • Auditing compliance • Information organization and secure data • Portability and Exchangeability • conventional protection, Business Continuity and Disaster Recovery • Data Center Procedures • Confrontation Response, Notification and Remediation • Programming Security • Encryption and Key Management • Identity and Access Management • Virtualization • Security as a Service
Platform as a Service (Java Runtime, Middleware, DB)	Application Developers can develop their programs using PaaS Cloud Platform Service	Secure the Data in data transfer, data in idle Secure Images Hypervisor based Security Virtual Machine based Security	• Defects in set of coding • Coding Modification • Application Programming Deletion • Imitate the relevant programs	
Infrastructure as a Service (Network, Storage, CPU)	User needs to obtain Physical (Infrastructure) resources for their usage from Cloud Service.		• Flooding request to server • configuration mismatch in traffic route • Distributed Denial of Service • Breaking up the communication	

hunting, the interoperability issue has not seemed that much trouble to the major industry cloud vendors. The Table 1 depicts the comparative analysis of cloud computing service level attacks for e-learners.

5. Conclusion

Data availability issue is the major hindrance in accessing cloud data for E-Learners. Among all the Distributed environment attacks, Distributed Denial of service (DDoS) attack is the root attack for data unavailability. Literature study clearly reveals the risks in cloud based e-learning along with its service delivery models and concluded solutions for each attack in an efficient manner. Listed security challenges are valuable to manage and newly design methodology for secure cloud based E-learning in future. This work helps to achieve 24/7 data availability in the cloud data center and develop the e-learning methodology for e-learners betterment.

6. References

1. Arunachalam AR. Bringing out the effective learning process by analyzing of e-learning methodologies. Indian Journal of Science and Technology. 2014 Jun; 7(S5):41–3.
2. Hurwitz J, Bloor R, Kaufman M, Halper F. Cloud computing for dummies. Wiley; 2012.
3. Sugaraj Samuel R, Subhashini A. E-Learning, the next big name in education. Indian Journal of Science and Technology. 2011 Mar; 4(3):173–6.
4. Begum SH, Sheeba T, Rani SNN. Security in cloud based e-learning. Int J Adv Res Comput Sci Software Eng. 2013; 3(1).
5. 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.
6. Choudhary V. Software as a service: implications for investment in software development. International conference on system sciences; 2007. p. 209.
7. Firdhous M, Ghazali O, Hassan S. Trust and trust management in cloud computing – a survey. Inter Networks Research Group. University Utara Malaysia; 2011. Technical Report UUM/ CAS/ Internetworks/TR2011-01.
8. Gharehchopogh FS, Hashemi S. Security challenges in cloud computing with more emphasis on trust and privacy. International Journal of Scientific and Technology Research. 2012; 1(6):49–54.
9. Masud MAH, Huang X. An e-learning system architecture based on cloud computing. World Academy of Science, Engineering and Technology. 2012; 62. Available from; http://www.waset.org/journals/waset/v62-15.pdf
10. Golden B. Defining private clouds. 2009. Available from: http://www.cio.com/article/492695/Defining private clouds part ones [accessed on: 11 January 2010].
11. Cooper R. Verizon business data breach security blog. 2008. Available from: http://www.securityblog. verizonbusiness.com/2008/06/10/2008-data-breach-investigations-report/s [accessed on: 11 February 2010].
12. PCI DSS. Requirements and security assessment procedures. 2009. Available from: https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v 1-2.pdf [accessed on: 24 January 2010].
13. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013 Apr; 6(4):4396–401.
14. Piplode R, Singh UK. An overview and study of security issues and challenges in cloud computing. Int J Adv Res Comput Sci Software Eng. 2012 Sep; 2(9).
15. Jensen M, Schwenk J, Gruschka N, Iacono LL. On technical security issues in cloud computing. IEEE; 2009.
16. Krautheim FJ, Phatak DS. LoBot: locator bot for securing cloud computing environments. ACM Cloud Computing Security Workshop; 2009.
17. Sharif AM, Amorgholipour SK, Alirezanejad M, Askil BS, Ghiami M. Availability challenge of cloud system under DDOS attack. Indian Journal of Science and Technology. 2012 Jun; 5(6):2933–7.
18. Ramgovind S, Eloff MM, Smith E. The management of security in cloud computing. PROC 2010, IEEE International Conference on Cloud Computing; 2010.
19. Kresimir P, Zeljko H. Cloud computing security issues and challenges. MIPRO 2010; 2010 May 24-28; Opatija, Croatia.
20. Neela TJ, Saravanan N. Privacy preserving approaches in cloud: a survey. Indian Journal of Science and Technology. 2013 May; 6(5):4531–5.
21. Gens F. New IDC IT cloud services survey: top benefits and challenges. IDC eXchange; 2009 Feb. Available from: http://blogs.idc.com/ie/?p=730 [Accessed on 2010 Feb 18].