A Framework for Secure Cloud Based Computing in Higher Educational Institution

Moe Moe San, Khin May Win
University of Computer Studies (Pathein)
mmsan.swe@gmail.com,winn.km05@gmail.com

Abstract

The students are becoming more technology oriented and the classroom teaching is changing, therefore it's changing to enhance. Because of its vast advantages, one of the latest technologies of students' learning currently for education is cloud computing. By sharing IT services in the cloud, educational institution can offer the essential tools to students, teachers, faculty, and staff to help them succeed. However, there is several security challenges associated with cloud environment that inhibit the proper adoption of this technology. Mostly organization wants a framework to keep their data more secure over cloud. This paper focuses on the attacks and risks of cloud computing on the education system and how can provide the quality education by solving the security challenges of this technology. It presents proposed framework to avoid security risks efficiently when adopting cloud computing in institutions of higher educational services. The proposed system identifies security and privacy challenges, highlights cloud-specific attacks and threats and clearly illustrates how to mitigate these attacks and threats.

Keywords: *Cloud Computing, Risks, Security, Threats, Attacks, Higher Educational Institution*

1. Introduction

Cloud computing is as computing model based on networks, especially based on the Internet, whose task is to ensure that users can simply use the computing resources on demand and pay money according to their usage by a metering pattern. Therefore, a new business model is being created where the services it provides are becoming computing resources.

The use of cloud computing in institutions of higher learning has provided many benefits to universities and colleges. The cloud helps ensure that students, teachers, faculty, parents, and staff have on-demand access to critical information using any device from anywhere. Both public and private institutions can use the cloud to deliver better services, even as they work with fewer resources.

Higher educational institutions can certainly choose Private cloud rather than Public cloud for many reasons. A private cloud is a cloud computing infrastructure created by an organization for its own internal use which can give better security, than utilizing someone else's infrastructure. Since a private cloud is hosted on the organization's own servers and within their own network, users are free of cloud data security fear. The organizations have direct control over the whole information that is being stored in the infrastructure including hardware, networks, operating system etc.

Even through private cloud provide many IT services for higher educational institution, it is in fact facing many security and privacy new challenges, attacks, threats and risks on private cloud in higher educational institution. This paper reviews and proposes a framework for secure private cloud in higher educational institution.

The rest of the paper is organized as follows. The related work is mentioned in section 2. In section 3, it presents cloud computing infrastructure: cloud service models, cloud deployment models, cloud computing characteristics and challenges of private cloud in higher educational institutions. It proposes a secure framework for private cloud in higher educational institutions; discuss security and privacy requirements, Attacks on cloud, threats to cloud computing and risks & security concerns in section 4. Finally, methods to achieve security and privacy requirements and mitigation of threats and attacks are illustrated based on literature review.

2. Related Work

The security challenges and privacy issues are one of the main topics that recently researchers focus on for adopting cloud computing in education. Different authors have different point of views cloud technology in higher educational institution.

The work in [1] provided a framework gives guidelines on most of the aspects of secure clouds including: security and privacy requirements, attacks and threats that clouds are vulnerable to and risks and concerns about cloud security. The author proposed a generic security model for cloud computing that helps satisfy its security requirements.

The work in [2] discussed on Cloud technology is implementing everywhere so cloud technology is been implanted in education sector and presented the key benefits of cloud based E-learning system.

The authors in [3] proposed a framework aims to treat the security issues by establishing a relationship among the cloud service providers in which the data about possible threats can be generated based on the previous attacks on other providers.

Factors that have an effect on the cloud adoption by higher education were identified in [4].

The author in [5] discussed Private Cloud Setup in educational institutions using the open source software Ubuntu Enterprise Cloud (UEC) and detailed the various services offered using the private cloud in educational institution.

The [6] discussed possible threats\attacks present in cloud computing environment. The authors provided a framework for cloud security and privacy and proposed a security model and a security framework that identifies security challenges in cloud computing.

In [7] the authors reviewed the literature on challenges of adoption cloud computing in institutions and universities. It also presented an overview of the security issues in the cloud service models and discussed the security challenges and risks and then provides helpful recommendations to avoid security challenges efficiently for adopting cloud computing in higher educational institutions.

The [8] introduced the cloud education system and how it is beneficial for students, faculty and the educational instituted for providing.

In [9], how to set up E-learning system based on cloud in an educational institution and prove how cloud solutions may increase the utilization of resources, minimize risks, and improve data security.

The authors in [10] discussed and analyzed the concepts of cloud computing information, cloud computing models, cloud computing services, cloud computing architecture and the main objective of the authors is to how to use and applied cloud computing architecture within higher educational institutions in third world countries.

The [11] provided review of different security aspects of cloud data storage. This Review paper give a view or idea about the problems that can be occur in a cloud computing system at multiple security issues.

The authors in [13] presented advantages and disadvantages of the previous risk management frameworks on cloud computing.

In [14] the questionnaire was conducted to explore the views of students towards cloud applications and services utilized in education.

In [15], the authors described the framework of design and implementing a simple private cloud for education and research based on chip level virtualization with hypervisor to establish a simple model of Infrastructure as a service in cloud computing.

3. Cloud Computing Infrastructure

The National Institute of Standards and Technology (NIST) defined cloud computing as : “ a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

NIST also defines three service models, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (Iaas).

SaaS provider hosts and manages a given application in their data center and makes it available to multiple users over the Web. Oracles CRM on Demand, Salesforce.com are some of the well-known SaaS examples.

PaaS is an application development and deployment platform which delivered over the web to developers. PaaS facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure. All of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available through Internet. This platform includes a database, middleware, development tools and infrastructure software. Well-known PaaS service providers include Google App Engine, Engine Yard.

IaaS is the delivery of hardware and software as a service. It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand. Amazon Web Services Elastic ComputeCloud (EC2) and Secure Storage Service (S3) are examples of IaaS services [6].

Figure 1 shows the main stakeholders of cloud computing in higher educational institutions [7]. The stakeholder in the higher educational institutions anyone who has access to educational services, including students, lecturers, researchers, staff members, etc.

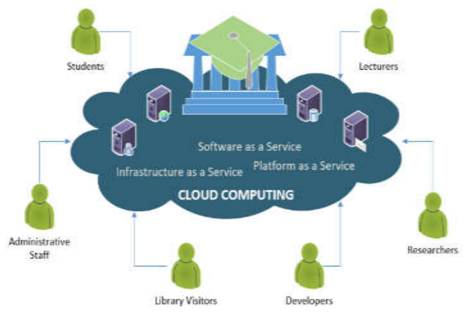

Figure 1. Stakeholders of cloud in an educational institution

3.1. Cloud Deployment Models

Cloud computing deployment models were defined by NIST and classified into four common modes; private, public, hybrid and community clouds [12].

Private cloud is deployed inside the boundary of the organization and is provisioned for exclusive use by specific consumers, its data and services cannot be accessed from outside of an organization.

Public cloud is owned and managed by a business, academic, or government organizations that provide cloud services for open use to the public.

The hybrid cloud is a composition of both public and private clouds characteristics.

In the community cloud, the infrastructure and services are provisioned for use by the specific community of consumers or among several organizations that have same mission or target. It can be operated and managed internally in the community or by a third party.

3.2. Cloud Computing Characteristics

According to the NIST definition, the cloud computing services require about five essential characteristics; on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Here, we will discuss in details the fundamental education-based characteristics of cloud computing:

On-demand self-service: The diversity of users in educational institutions leads to a variety of functionality and performed operations. Usually, the user online configures and manages resources under on-demand environment through a web-based self-service interface.

Broad network access: The cloud services and resources must be widely accessible from anywhere by heterogeneous platforms such as laptops, tablets, mobile phones, etc.

Resource Pooling: The cloud providers pool large-scale computing resources and services to serve multiple users separately on a logical level.

Rapid elasticity: The cloud services or resources provisioned to the user can be scaled up and down rapidly based on the user policy and requirements, with no impact on the application or any human interaction.

Measured services: The usage of cloud services or resources must be monitored, metered permanently by a performance with the pay-per-use feature.

Figure 2 below shows the NIST visual model for cloud computing [4].

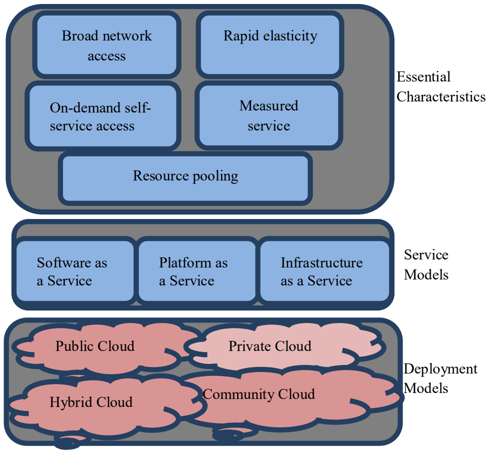

Figure 2. NIST visual model for cloud computing

3.3. Private Cloud in Higher Educational Institutions

A private cloud, also called as an “internal cloud” resides within the organizational boundary. The access to this internal cloud is restricted to internal users according to their role. In order to overcome the challenges faced in Public cloud, organizations are looking at enterprise private cloud offerings.

Most of higher educational institutions are using a private cloud, rather than public or hybrid cloud. Private clouds are built exclusively for a single organization and are aimed to address concerns on better data control and better data security, which is lacking in a public cloud. Owning a private cloud, an organization becomes a single tenant with complete control over its dedicated data center. As the organization is the sole tenant, it is in charge of monitoring and maintaining the data. Also the organization can well control the performance and security of its infrastructure. The users of this private cloud access the cloud within the organization’s firewall, which seems to provide faster data-transfer rates due to the internal network structure [5].

The key benefits of cloud computing in education can be categorized according to stakeholders who use cloud resources and services in higher education institutions. Students can store anything electronically such as their schedule, class notes, reports and any other documents. Furthermore, they able to back up their files to the cloud and retrieve them when needed. Students can earn e-copy of textbooks and have access to quality learning materials of their courses.

Students have the opportunity to access the system easily at any time to get courses online, attend the online exam, and upload their assignments and projects through the cloud to the instructors [7].

3.4. Challenges of Private Cloud in Higher Educational institutions

Even though the great benefits of using private cloud in higher educational institutions, there are some challenges that hinder the wide scale adoption of this technology in various sectors of the university. In the current circumstances, it is not easy to track the variety security issues in cloud computing environments.

The security issues are related mainly to three key requirements: confidentiality, integrity, and availability. The confidentiality is defined as a set of rules that prevent unauthorized user from accessing sensitive information, while integrity is a way to protect data from being modified by unauthorized user and ensure that data are retrieved accurately and trustworthy, and the availability concerned with enabling authorized users to access data reliably when needed, especially during difficult circumstances and emergencies [7].

4. A Framework for Secure Private Cloud in Higher Educational Institution

Figure 3 below shows a framework for secure private cloud. It consists of four essential security components; each of them includes important challenges related to cloud security and privacy. These components are:

Security and privacy requirements: identifies security and privacy requirements for the cloud such as authentication, authorization, integrity, etc.

Threats to cloud computing: discuss some potential threats relevant to cloud.

Attacks on cloud computing: warns from different types of attacks and to which clouds are vulnerable.

Risks and Security concerns: pay attention to risks and security concerns about cloud computing. We discuss each guideline in detail in the following sub-sections.

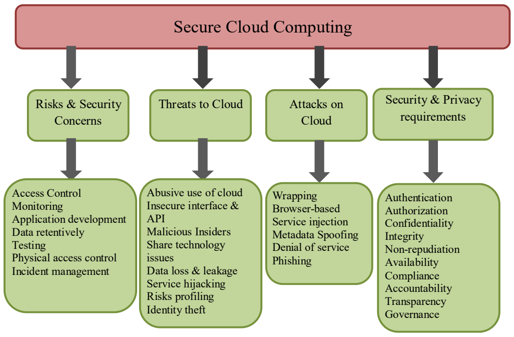

Figure 3. A framework for secure private cloud

4.1. Security and Privacy Requirements

To enhance the security in cloud computing, it is important to provide authentication, authorization and access control for data stored in cloud. The three main areas in data or information security are confidentiality, availability and integrity [11, 15]. On the other hand, privacy concerns the adherence to various legal and non-legal norms. It includes: consent, purpose restriction and legitimacy which all ensure that a cloud deployment meets the requirements imposed by law. It may also include transparency, governance and compliance. The International Standards Organization (ISO), in ISO7498-2 [1], suggested a number of information security requirements, they are

Identification and Authentication management: The authentication and identity management module is responsible for authenticating users and services based on credentials and characteristics [6]. In the cloud computing, with this security principle we must identify the client making requests and their access privileges. If any client is not assigned to any service then he is denied for that service. The client authentication by username and password are also validated before accessing to any cloud service. The identification and authentication is the essential security principle for all types of clouds [11]. A more efficient way for authentication is to use an additional authentication factor outside the browser such as two factor authentication (2FA), but this limits cloud scalability and usability [1].

Access control: Access Control includes important security issues such as authentication, identification, and authorization [7]. Authorization preserves referential integrity in cloud environment. With this rule only authorized person access the cloud resources. All the unauthorized persons are denied for cloud services and resources [11]. An important thing that helps resolve authorization issue in cloud environment is to establish a solid confidence between Cloud Service Providers (CSPs) and customers who should both trust cloud administrators as well [1].

Confidentiality: Confidentiality is a core requirement to maintain control over the data of many organizations that may be located across several distributed databases. Emphasizing confidentiality and protection of users' data and profiles at all levels will enforce information security principles at different levels of cloud applications [11].

Integrity: refers to protecting cloud data and software from unauthorized deletion, modification, theft or fabrication, this ensures that data has not been tampered with or abused. Integrity includes data accuracy, completeness and ensures Atomicity, Consistency, Isolation and Durability (ACID) [1].

Non-repudiation: With this principle security of cloud data is maintained by some Security protocols and token provisioning for transmission of data on cloud server to client and vice versa. To maintain non-repudiation different concepts are applied such as digital signatures, confirmation acknowledgement etc. [11].

Availability: Another cloud security principle is availability of cloud vender. It refers to cloud data, software and also hardware being available, usable and accessible to authorized users upon demand. CSPs should be able to continue providing customers with services even in case of the existence of security breaches, malicious activities or system faults. Availability is an important factor in choosing among various CSPs. We must choose cloud vender among public, private, or hybrid cloud vendors according to facility and security required for our data. If specific cloud vendor is currently not available then wait for some time or choose the vendors that provide maximum security of client's data and resources [1, 11].

Compliance and Audit: compliance with regulations and laws is a necessary privacy requirement to ensure that the cloud deployment meets the requirements of general legislation, sector-specific rules and contractual obligations [1].

Transparency: the operation of the cloud should be sufficiently clear to users and CSPs. Users must be able to get a clear overview of where and how their data will be handled. They also must be able to determine who the cloud provider is and where his responsibility ends [1].

Governance: data on the cloud is vulnerable since it is processed and stored remotely. Customers have concerns about why their personal information is requested and who will use it. There are also threats associated with virtualization and resource sharing. Policies and procedures should be applied to protect the cloud from attacks, threats and data loss. Governance ensures protecting data against various malicious activities and helps control cloud operations [1].

Accountability: implies that security and privacy gaps are correctly addressed [1]. Table 1 summarizes cloud security and privacy requirements and methods to achieve them based on literature review.

Table 1. A summary for security and privacy requirements and how to achieve them

Security and privacy req.	Achieved by
Authentication	Username, Password, 2FA
Authorization and access control	Restrict cloud admins hiring process- Monitor activities of authorized users- Build trust between CSPs, cloud customers and admin
Confidentiality	Employ strong authentication methods - Prevent unauthorized access-Use encryption techniques
Integrity	Use encryption and hash algorithms-Prevent unauthorized access
Non-repudiation	Digital signatures-Timestamps-Confirmation receipt services
Availability	Use backup and recovery schemes, fault tolerance and replication
Compliance and audit	Perform internal and external audits on a regular basis to monitor CSP's compliance to agreed terms, standards and regulations
Transparency	Provide customers with clear information on controls, security and operation of the cloud-Refer to Service Level Agreements (SLA)
Governance and accountability	Effective implementation and adherence of security policies and procedures to protect clouds from threats and data loss

4.2. Attacks on cloud computing

Before defining types of attacks in clouds, we must identify the attackers themselves and their impact on the security of cloud systems. Cloud attackers may be categorized as follows:

Random: the most common type of attackers uses simple techniques to randomly scan the internet in order to find vulnerable computers. They deploy well known tools that should be easily detected.

Weak: are semi-skilled attackers who target specific cloud providers by customizing publicly available tools for specific targets.

Strong: are organized, skilled and well financed groups of attackers who target particular applications and users of the cloud. Generally, they form criminal groups specialized in large scale attacks.

Substantial: are motivated highly skilled attackers who can't be easily detected either by the organizations they attack or by the law enforcement and investigative organizations specializing in e-Crime or cyber security. Attacks on cloud computing can be classified according to cloud service models and they are described below:

Wrapping attacks: these attacks occur between the web browser and the server by altering the Simple Object Access Protocol (SOAP) messages for two persons, the user and the attacker.

In PaaS there are some types of attack such as:

Cloud injection attacks: attempt to create malicious service implementation modules or virtual machine instances for the opponent to be executed against intention. Examples for these modules are SQL injection; OS command injection and cross site scripting.

Metadata spoofing attacks: include reengineering Web Services' metadata descriptions. To defend against this threat, verification techniques should be used.

In IaaS, the most important attack is the flooding attack that is represented as:

Denial of service attacks: occur when an attacker sends a lot of malicious requests to the server and consumes its available resources, CPU and memory. When the server reaches its maximum capacity, it offloads the received requests to another server. In cloud computing, due to the large number of cloud users (multi-tenancy) who share the cloud infrastructure, the problem of Distributed DoS (DDoS) attacks becomes of much greater impact than that in single tenant architecture.

Buffer overflow attacks: when buffer overflow occurs, the attacker is able to overwrite data specialist in program execution to execute his malicious program [1].

Phishing attack: Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data. In Cloud, it may be possible that an attacker use the cloud service to host a phishing attack site to hijack accounts and services of other users in the Cloud [6].

Table 2. Summary for attacks on cloud computing and their mitigations

Attacks on cloud computing	Mitigations
Wrapping attacks	Increase security during message passing from the web server to the web browser by using the SOAP
Cloud injection Attacks	Use hash algorithms
Metadata spoofing Attacks	Use verification techniques
Denial of Service (DoS)	Provide more computational power and resources
Phishing attacks	Better authentication and isolation between Virtual Machines (VMs) can provide protection against

4.3. Threats to cloud computing

At the Black Hat USA 2010 Conference, the Cloud Security Alliance (CSA), a non-profit organization formed to promote the use of best practices for providing security assurance within cloud computing, announced industry's first certification program on secure cloud computing. According to CSA the top seven threats in cloud computing are described as follows [1]:

Abuse and Nefarious Use of Cloud Computing: Cloud computing provides several utilities including bandwidth and storage capacities. Some vendors also give a predefined trial period to use their services. However, they do not have sufficient control over the attackers, malicious users or spammers that can take advantages of the trials. These can often allow an intruder to plant a malicious attack and prove to be a platform for serious attacks. Areas of concern include password and key cracking, etc. Such threats affect the IaaS and PaaS service models.

Mitigation: To remediate this, initial registration should be through proper validation/verification and through stronger authentication. In addition to this, the user's network traffic should be monitored comprehensively.

Insecure interfaces and API: Cloud providers often publish a set of APIs to allow their customers to design an interface for interacting with Cloud services. These interfaces often add a layer on top of the framework, which in turn would increase the complexity of Cloud. Such inter- faces allow vulnerabilities (in the existing API) to move to the Cloud environment. Improper use of such interfaces would often pose threats such as clear-text authentication, transmission of content, improper authorizations, etc.

Such type of threat may affect the IaaS, PaaS, and SaaS service models.

Mitigation: This can be avoided by using a proper security model for Cloud provider's interface and ensuring strong authentication and access control mechanism with encrypted transmission.

Malicious insiders: Most of the organizations hide their policies regarding the level of access to employees and their recruitment procedure for employees. However, using a higher level of access, an employee can gain access to confidential data and services. Due to lack of transparency in Cloud provider's process and procedure, insiders often have the privilege. Insider activities are often bypassed by a firewall or Intrusion Detection system (IDS) assuming it to be a legal activity. However, a trusted insider may turn into an adversary. In such a situation, insiders can cause a considerable effect on Cloud service offerings, for example, malicious insiders can access confidential data and gain control over the Cloud services with no risk of detection.

This type of threat may be relevant to SaaS, PaaS, and IaaS.

Mitigation: To avoid this risk, more transparency is required in security and management process including compliance reporting and breach notification.

Shared technology issues/multi-tenancy nature: In multi-tenant architecture, virtualization is used to offer shared on-demand services. The same application is shared among different users having access to the virtual machine. However, as highlighted earlier, vulnerabilities in a hypervisor allow a malicious user to gain access and control of the legitimate users' virtual machine. IaaS services are delivered using shared resources, which may not be designed to provide strong isolation for multi-tenant architectures. This may affect the overall architecture of Cloud by allowing one tenant to interfere in the other, and hence affecting its normal operation. This type of threat affects IaaS.

Mitigation: Implementation of SLA for patching, strong authentication, and access control to administrative tasks are some of the solutions to address this issue.

Data loss and leakage: Data may be compromised in many ways. This may include data compromise, deletion, or modification. Due to the dynamic and shared nature of the Cloud, such threat could prove to be a major issue leading to data theft. Examples of such threats are lack of authentication, authorization and audit control, weak encryption algorithms, weak keys, risk of association, unreliable data center, and lack of disaster recovery. This threat can applicable to SaaS, PaaS, and IaaS.

Mitigation: Solutions include security of API, data integrity, secure storage for used keys, data backup, and retention policies.

Service hijacking: Service hijacking may redirect the client to an illegitimate website. User accounts and service instances could in turn make a new base for attackers. Phishing attack, fraud, exploitation of software vulnerabilities, reused credentials, and passwords may pose service or account hijacking. This threat can affect IaaS, PaaS, and SaaS.

Mitigation: Some of the mitigation strategies to address this threat include security policies, strong authentication, and activity monitoring.

Account or Service Hijacking: there are several known methods for account hijacking such as phishing, fraud detection and man-in-the-middle attacks. Attackers can use stolen credentials or passwords to jeopardize the confidentiality, integrity and availability of cloud services. CSA suggested remedies to mitigate this threat such as: forbidding sharing of account credential between users, employing 2FA techniques and understanding CSPs security policies and SLAs.

Mitigation: Employ 2FA- Understand CSPs security policies and SLAs-Forbid sharing of account credential [1].

Risk profiling: Cloud offerings make organizations less involved with ownership and maintenance of hardware and software. This offers significant advantages. However, these makes them unaware of internal security procedures, security compliance, hardening, patching, auditing, and logging process and expose the organization to greater risk.

Mitigation: To avoid this Cloud provider should disclose partial infrastructure details, logs, and data. In addition to this, there should also be a monitoring and alerting system.

Identity theft: Identity theft is a form of fraud in which someone pretends to be someone else, to access resources or obtain credit and other benefits. The victim (of identity theft) can suffer adverse consequences and losses and held accountable for the perpetrator's actions. Relevant security risks include weak password recovery workflows, phishing attacks, key loggers, etc. This affects SaaS, PaaS, and IaaS.

Mitigation: The solution is to use strong authentication mechanisms [6].

4.4. Risks and security concern

The literature noted a number of concerns about managing security and privacy in cloud computing [1, 11]. In [1] some concerns are:

***Access control**:* how can cloud users govern access control risks when the levels and types of access control used by cloud providers are unknown?

Monitoring: how can accurate, timely and effective monitoring of security and privacy levels achieved in business-critical infrastructure when its providers are not prepared to share such information at SLA?

***Applications development**:* how to accomplish application development and maintenance in the cloud when CSPs are responsible to?

Data retentively: how can the cloud user achieve appropriate confidence that the data have been actually and securely removed from the system by the cloud provider and are not merely made inaccessible to him?

Testing: how can consumers test the effectiveness of security control when these tests may not be made available by CSPs?

Physical access control: how can the cloud user achieve requirements for physical access when its measures are established and fully controlled by CSPs?

Incident management: how can the cloud user determine appropriate thresholds and criteria in order to respond to incident?

According to [11] different security levels that an organization must have are explained below:

***Personnel Security**:* With personnel security an organization appoint authorized individual or group of individuals for accessing and allocating all the organization resources and data.

Eavesdropping: An unauthorized user can access the data because of interception in network traffic; it may result in failure of confidentiality. The Eavesdropper secretly listen the private conversation of others. This attack may be done over email, instant messaging.

Information Security: With information security an organization can safeguard and protect the confidentiality and correctness (integrity) and assets information for processing and storage.

Physical Security: With this security an organization can protect its physical assets and other essential properties from unauthorized access and misuse.

Network Level Security: With network security an organization protects its networking components & connections. It also protects organization contents that are transferred through networks.

Operations Security: With operational security an organization protects the information of all transactions and operations performed regularly.

Communications Security: With communication security an organization protects various technologies, communications media and their content from unauthorized access.

5. Conclusion

Cloud computing represents an opportunity for higher educational institution to take the enormous benefits of cloud services and resources in the educational process. However, the cloud users remain concerned about the major obstacle that may prohibit the adoption of cloud computing on a large scale. This will lead to many security issues such as privacy, confidentiality, integrity and availability etc. This paper focused on security challenges in private cloud computing and to have highly protected, safe and sound private cloud computing environment. It also provided a framework that identifies more accurately security and privacy requirements, attacks, threats, concerns and risks associated to the deployment of the clouds for secure private cloud in higher educational institution than other frameworks. In the final section, it addressed possible achievement for security issues in private cloud environment and proposed mitigations of threats and attacks on private cloud computing in higher educational institution.

References

[1] Ahmed E. Youssef, Manal Alageel, “A Framework for Secure Cloud Computing”, *International Journal*, International Journal of Computer Science, KSA, *July 2012*, *ISSN1694-0814*

[2] Atif Ishaq, M.N. Brohi., “Literature Review of Cloud Computing in Education -A Survey with Respect to Qatar”, *International Journal*, International Journal of Computer Applications (0975 – 8887), Germany, *December2015, Volume 132 – No.17,*

[3] Atif Ishaq, Muhammad Nawaz Brohi, “Cloud Computing in Education Sector with Security and Privacy Issue”, *International Journal*, International Journal of Advances in Engineering & Technology, UAE, *December 2015*, ISSN: 22311963

[4] Bayan Hashr Alamri, M. Rizwan Jameel Qureshi, “Usability of Cloud Computing to Improve Higher Education”, *International Journal*, International Journal of Informational Technology and Computer science, Saudi Arabia, *, Sep 2015*, *DOI:10.5815*

[5] D.Sudha Devi, L. Yamuna Devi, K. thilagavathy, “Private Cloud in Educational Institutions-An Implementation using UEC”, *International Journal*, International Journal of Computer Applications, India, *, Sep 2013*, *260549189*

[6] Kashif Munir, Prof Dr. Sellapan Palaniappan, “Framework Secure Cloud Computing”, *International Journal*, International Journal on Cloud Computing: Services and Architecture(IJCCSA), Malaysia, *, April 2013*, *Volume 3 – No 2*

[7] Khalil H. A. Al-Shqeerat, Faiz M. A. Al-Shrouf., “Cloud Computing Security Challenges in Higher Educational Institutions-A Survey”, *International Journal*, International Journal of Computer Applications (0975 – 8887), Germany, *, March 2017*, *Volume 161 – No 6*

[8] Kiran Yadav, “Role of Cloud Computing in Education”, *International Journal*, Innovative Research in Computer and Communication Engineering Vol. 2, Issue 2, India, February 2014, ISSN (Print): 2320-9798

[9] Mohd Salman Khan, Tanisha Chaudhary, “E-learning System Based on Cloud Approach”, *International Journal*, International Journal of Advance Research In Science And Engineering, India, *, May 2014*, *ISSN-2319-8354(E)*

[10] Mohmed Sirelkhtem Adrees, Majzoob Kamal Aldein Omer, “Cloud Computing Architecture for Higher Education in the Third World Countries”, *International Journal*, International Journal of Database Management Systems, Saudi Arabia, *June 2015*, *vol.7,No.3*

[11] Nidhi Dahiya, Sunita Rani, “Cloud Computing Security :A Review”, *International Journal*, International Journal of Engineering Development and Research (IJEDR), India, *, 2017*, *ISSN: 2321-9939*

[12] Peter Mell, Timothy Grance, “The NIST definition of Cloud Computing”, *Report* , The National Institute of Standard Technology, US, *, September 2011*, Special Publication 800-145

[13] Rana Alosaimi, Mohammad Alnuem, “Risk Management Frameworks for Cloud Computing: A Critical Review”, *International Journal*, International Journal of Computer Science & Information Technology , Saudi Arabia, *, August 2016*, *Volume 8 – No 4*

[14] Tanvi Desai, Rikita Patel, “Cloud Computing in Education Sector”, *International Journal*, International Journal for Innovative Research in Science &Technology, Anand, *March 2016*, *Volume 2 – Issue 10*

[15] Yuhong Liu,Yan Sun, Jungwoo Ryoo and Syed Rizvi “A Survey Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions”, *International Journal*, International Journal of Computing Science and Engineering, USA, *September 2015*, *pp119-133*