Available online at www.worldscientificnews.com

World Scientific News

WSN 86(3) (2017) 242-253 EISSN 2392-2192

Cloud Computing – Architecture, Platform and Security Issues: A Survey

Md. Sakib Bin Alam

Department of Computer Science and Engineering, Faculty of Science and Engineering, International Islamic University Chittagong, Chittagong - 4318, Bangladesh

Email address: sakibsba@gmail.com

ABSTRACT

Cloud computing system delivers computing resources as a service over the network. During the last few years clod computing technology has gained attention due to its autonomous and cost effective services. It is responsible for the growth of IT industry. But cloud computing has various security challenges that hinder the rapid adoption of this computing paradigm. Efficient steps should be taken to make cloud computing more secure and reliable. This paper works on overview of clod computing as well as related security issues.

***Keywords*:** Cloud Computing, Service Models, Deployment Models, Security Issues

1. INTRODUCTION

According to National Institute of Standards and Technology (NIST) [1]: *"Cloud Computing is a model for enabling ubiquitous, convenient on demand access to a shared pool of configurable computing resources (e.g., network servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".* The cloud computing market is increasing significantly. According to a survey [2] a user runs at least four cloud based applications where at any point in time is running another four. The survey also found that 41% of commercial entities run significant tasks on public cloud. But the growth of cloud computing has brought some

security challenges. These security issues should be identified and analyzed in order to make cloud computing services more secured and reliable. This paper describes cloud computing architecture, platform, main security issues and their potential solutions.

1. 1. Characteristics of Cloud Computing

According to the NIST cloud computing contains following five essential characteristics [1]:

A. On-demand self-service: Provision computer services such as email, network, application and computer capabilities. It also provision server service without human interaction from each service provider.

B. Broad network access: Computing capabilities are available over the network and can be accessed through standard mechanisms that promote the use of heterogeneous thin or thick client platform.

C. Resource pooling: The computing resources of the providers are pooled to support multiple consumers using a multi-tenant model with different virtual and physical resources dynamically assigned and reassigned according to consumer demand. The consumer has no idea or knowledge over the exact location of the resources but can access and use data at any time from any location.

D. Rapid elasticity: Computing capabilities can be rapidly and elastically provisioned. The resource pooling and self-service make it possible. The provider can automatically distribute more or less resources from available pool.

E. Measured Service: Cloud systems, in this case, automatically control and manage resource use by leveraging a metering capability at some level of abstraction as it seen appropriate to the type of service.

1. 2. Advantages of Cloud Computing

Some major advantages of cloud computing are given below:

- **Greater Mobility:** Information can be accessed at anytime from anywhere unlike traditional system (storing information in personal computer and accessing only when near it).
- **Cost Reduction:** Reduced costs due to more rapid deployment services and operational efficiencies.
- **Increased Storage:** At the point when compared to private computer systems, large amount of data can be stored than usual.
- **Elasticity:** Elastic nature of the infrastructure allows to swiftly allocate and de-allocate vastly scalable resources to business services on a demand basis.

2. CLOUD ARCHITECTURE

In order to analyze cloud security issues it is important to understand cloud architecture. According to NIST's cloud reference architecture [3], there are five most important factors

that have an effect on and are impacted by cloud computing, along with its security implications.

- **Cloud Consumer:** An individual or organization that keeps up a business association with, and uses services from cloud provider.
- **Cloud Provider:** An individual or organization for creating a service accessible to interested parties.
- **Cloud Auditor:** A party that can conduct autonomous appraisal of cloud administrations, data framework operations, performance and security of the cloud usage.
- **Cloud Broker:** An entity that deals with utilization, performance and delivery of cloud services and negotiates relationships between cloud consumers and providers.
- **Cloud Carrier:** A medium that provides network and transport of cloud services from cloud providers to cloud consumers.

Figure 1 shows the architecture of cloud computing. The figure represents an end-to-end reference architecture that represents the layers of Open Systems Interconnection Model (OSI). As it is apparent, cloud computing is a complex arrangements with numerous areas of vulnerabilities.

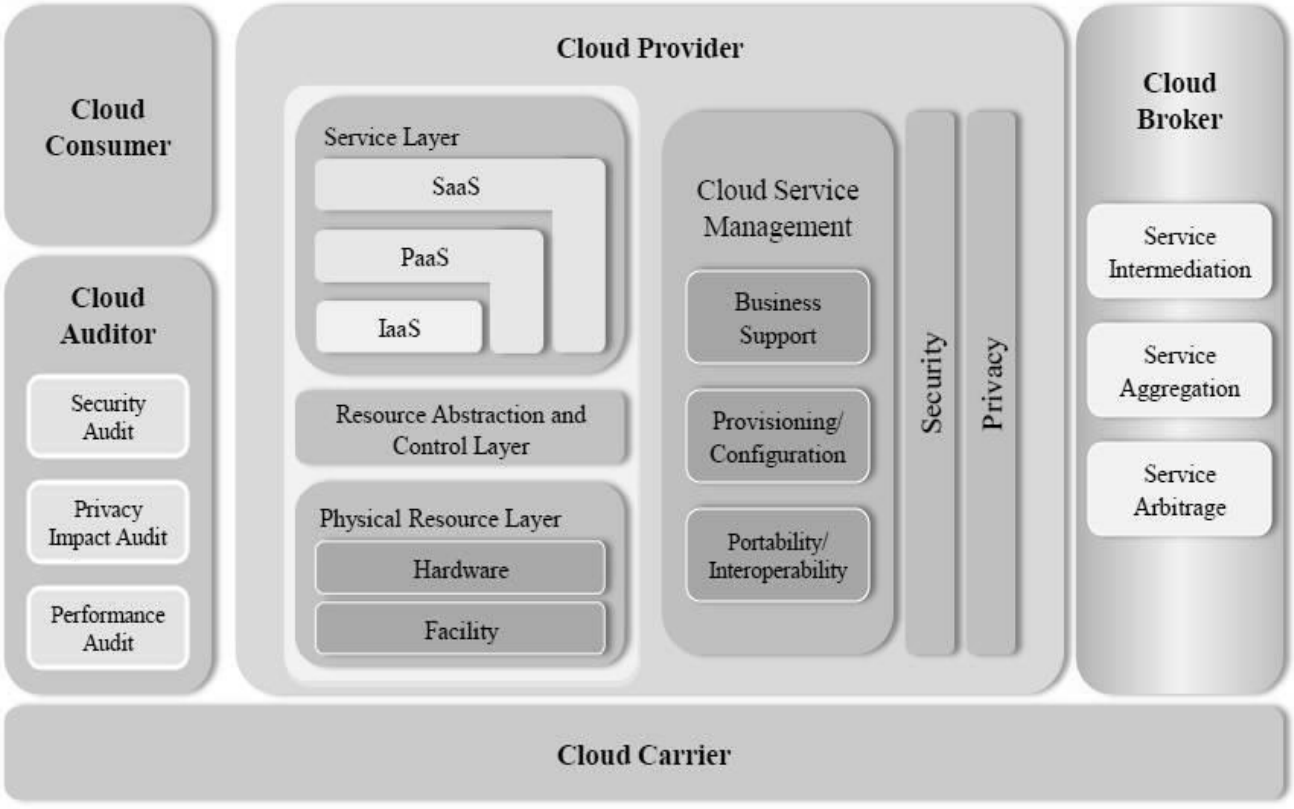

Figure 1. NIST Cloud Computing Reference Architecture [3]

3. CLOUD COMPUTING SERVICE MODELS

As big data cloud computing and internet technology grow, they raise a new concept of services. This services can interconnect huge number of online activities. As per a review from Cisco, the Internet of Things (IoT) is dynamically expanding the abilities of the cloud [4]. The major three service models are Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

A. Software as a Service (SaaS): A Software as a Service (SaaS) cloud framework enables clients to access applications and settings that have been conveyed by the supplier. The customers can access these cloud applications using a simple browser. In SaaS, the cloud provider is only authorized to control the application level. The subscriber does not control or manage middleware, hardware or operating system. Figure 2 shows the control responsibilities of cloud provider and cloud subscriber in SaaS model. The SaaS model has some unique characteristics [5]:

- In spite of the fact that the consumers loses some level of control, the SaaS model moves the burden of getting and keeping a venture application up and running from the customer to the vendor. It allows users to use the software functionality without the burden of managing the software themselves.
- Generally rather than authorizing, installing and maintaining software on consumers' personal computers or servers, the SaaS model gives users access to the software via the internet on a pay-as-you-use basis.
- The SaaS model enables every customers to benefit from the vendor's most recent technological elements without the disturbances and costs associated with software updates and upgrades.
- The SaaS model disposes of the additional expenses and complexities of conveying extra hardware and software, to help an enterprise application on a continuous basis.
- Every customer can pick either to share access to the software to different customers (multi-tenancy), in this way empowering shared aggregate expenses and making economies of scale, or choose to be a single tenant, accordingly giving more prominent control and security.

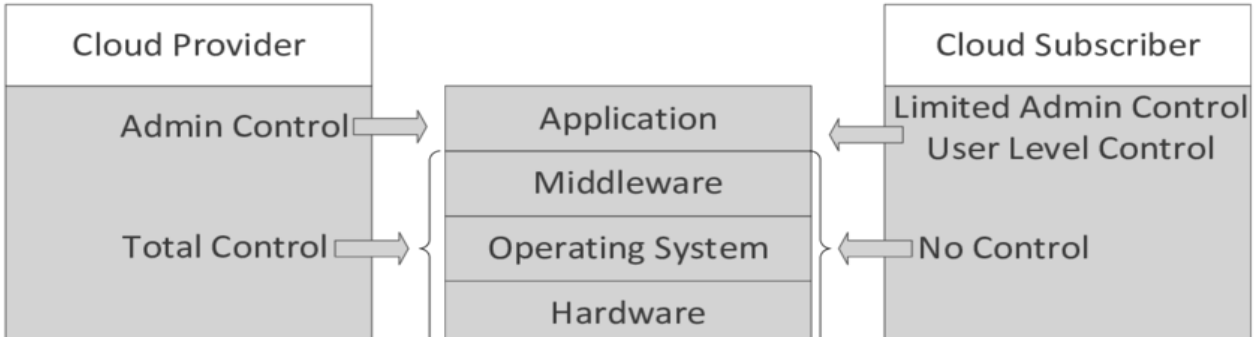

Figure 2. SaaS provider/subscriber control responsibilities [2]

B. Platform as a Service: To permit consumers full control of applications and configurations according to their specific requirements, a PaaS arrangement can be used [2]. PaaS offers to create and modify applications where in SaaS application is typically possessed by the cloud provider. In PaaS model, the consumer is permitted to write applications that run on the provider's specific surroundings. A PaaS provider gives its consumers an extra Application Programming Interface (API) for dynamically adjusting the computational resources (e.g. memory, storage disk) according to client's requirements. The platforms offered by PaaS providers drive their applications to be coded in a particular language, following their own API. This makes tremendous troubles to move legacy applications to another PaaS environment.

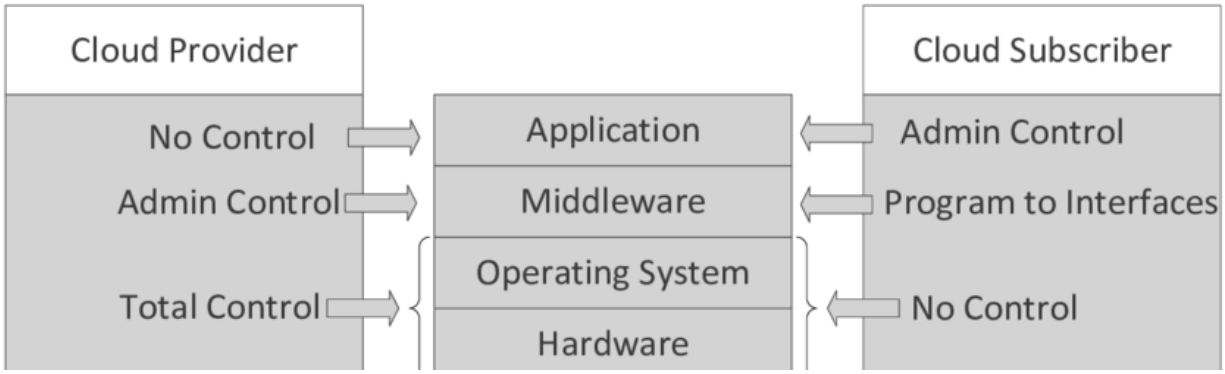

Figure 3. PaaS provider/subscriber control responsibilities [2]

C. Infrastructure as a Service: The ability gave to the customer is to arrangement processing, networks, storage, and other computing resources where the customer can convey and run arbitrary software, which can incorporate operating systems and applications. The customer does not oversee or control the basic cloud framework but rather has control over storage, operating systems, deployed applications, and limited control of networking parts [5]. With the development of technology in communications, computing, and storage devices, IaaS has emerged as a highly effective platform to construct SaaS and PaaS layer on top of it. Figure 4 shows the control responsibilities of cloud provider and cloud subscriber in IaaS model. In the present case, the virtualization should be utilized to ensure to each cloud subscriber a machine with a full operating system that is totally free from the remaining operating systems related with other subscribers, disregarding all these operating systems running over the same hardware [2]. Figure 4 outlines, simply over the hardware, the layer assigned by the Virtual Machine Monitor (VMM), or normally the 'hypervisor'. The hypervisor uses the same hardware and shares its computational resources among assorted Virtual Machines (VMs). Each VM works like a genuine machine in any case, is totally confined from the rest of the VMs. For this situation, the VM shows up to the subscriber like an independent machine that can be totally configured by that subscriber in different viewpoints, specifically: i) switch on/off the VM; ii) install any guest operating system, iii) install a complete set of desired applications/offerings; iv) change computational assets, such as, CPU cores, network interfaces or data storage [2].

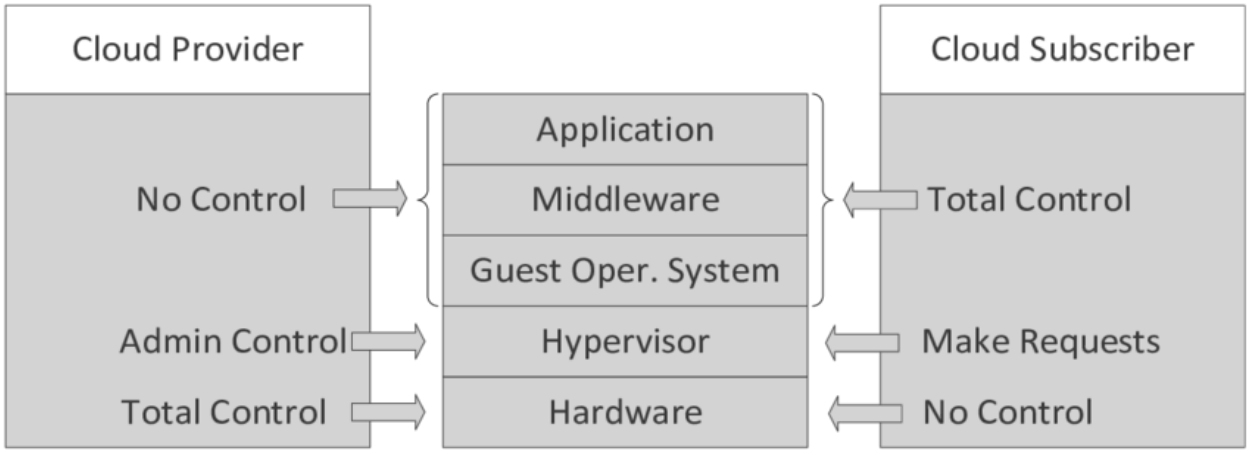

Figure 4. IaaS provider/subscriber control responsibilities [2]

4. CLOUD COMPUTING DEPLOYMENT MODELS

Choosing the suitable type of cloud computing deployment model is very important for an institution. Institutions must analyze their data precisely before deciding which type of model to choose in order to avoid failure of implementation. There are four common cloud deployment models, namely, private cloud, public cloud, hybrid cloud, community cloud.

A. Private Cloud: The cloud infrastructure is operated exclusively for an organization. It may be controlled by the organization or a third party and might exist on premise or off premise [5]. Cloud computing services is not accessible by the public but to use it within the organization. A private cloud gives more security than public clouds, and cost saving in case it makes use of unused capacities in an already existing data center. Making such un-used capacities available through cloud interfaces allows to utilize the same tools as when working with public clouds and to benefit the capabilities inherent in cloud management software, like a self-service interface, automated control of computing resources, and the potential to sell current over capacities to partner corporations [5]. Some characteristics of private cloud are listed below [6]:

- **Enhanced security measures:** In IT sector is one of the requirements. Almost all institutions seek for security particularly financial institutions. Private cloud model ensures security against illegal usage, such as hacking by providing strong security tools.
- **Dedicated Resources:** Like a supporter of private cloud, enterprises have their own committed resources, for instance, the time of processor and the data buses that assure ideal execution.
- **Better Customization:** The private cloud model is customizable as it could be constructed to outfit the perfect requests of a commercial enterprise. This in turns permits the commercial enterprise to take additional manage over their own data to ensure security.

B. Public Cloud: The public cloud model offers data storages, applications and other services to its users and owned by the service provider. This is based on the characteristics of pay-per-usage model. Users can scale their use on demand and do not have to buy hardware for the service. Public clouds are available to the general public or organizations, and are owned by a third party service provider that offers the cloud service [5]. Public cloud users are normally residential users and connect to the general public internet through an internet service provider's network.

The advantages of public cloud include [5]:

- On demand scalability.
- Continuous uptime and data availability.
- No dissipated resources.
- Easy and flexible setup.

Public clouds have some drawbacks also including data security and privacy. Another issue is that users don't know where the data is stored.

Characteristics of public clouds are listed below [6]:

- **Flexible and elastic environment:** Public cloud provides an elastic environment to its users. It allows customers to share and store information on their demand.
- **Freedom of self-service:** The public cloud conjures up it customers in making a cloud all on my own exceptional of taking anybody's assistance. That is called because the pre-configured clouds, which exist on the internet. The main factor is that organizations that preference to select the public cloud need to do is to visit the portals of the public cloud begin with it. They do not need to depend on any third-party support in making or running kind of cloud.
- **Pay-Per-Use:** This unique function empowers the era of cloud to be greater reachable by organizations to operate in a synchronized manner. The further organization uses the services of cloud, the well progressive the future business could be.
- **Availability and Reliability:** The fact that the public cloud is out there to all and believes in agility is one of the many other characteristics if the public cloud. The users have the opportunity to time their work from anywhere in the glob and at any time. No longer just consumers come to be being free to run simple assignments of the business but they're additionally more productive in reinforcing purchaser relationships over the globe.

C. Hybrid Cloud: Hybrid cloud is made from lots of both public or private cloud that is shared among the institutions that have similar interests and necessities, it is can be internally managed and it may also be managed by the third-party which is inner or outside hosted. Hybrid cloud infrastructure is a composition of two or more clouds which can be unique entities and are bound collectively by using standardized or proprietary technology that permits data and application portability [5]. A hybrid cloud is normally supplied in considered one of two methods: a vendor has a private cloud and makes a partnership with a public cloud provider, or a public cloud provider makes a partnership with a vendor that provides private cloud systems [5]. The characteristics of hybrid cloud include [6]:

- **Optimal Use:** The typical centres of data in the server resources are used from 5 to 20%. The cause behind that is the crest masses, which are ten times higher than that of the typical burden. On this manner, servers are generally sitting still - making unnecessary costs. Hybrid cloud could expand server use with the aid of scaling out the open assets to take care of the hosts.
- **Availability:** The accessibility in the corporate server is troublesome in addition to expensive, as it necessitates data reinforcements, data redundancy and geographical scattering. Especially inside the corporations where information technology is not the point of interest corporate, the ability round there is incredibly restrained. In a hybrid cloud, the general public cloud would possibly scale up or completely overtake operations if the organization's server is not available due to some failures.
- **Risk Transfer:** Organizations personally are managing and running their server and private cloud. The provider of the public cloud must ensures an intense uptime for their service. Using the hybrid cloud, the danger of misestimating workload is relocated to the cloud dealer from the service operator**.**

D. Community Cloud: The community cloud is supervised and utilized by a different number of institutions that have the identical core business, initiatives or shareable needs infrastructures which include software program and hardware so that the running can be reduced [6]. It aspires to combine distributed resource provision from grid computing, distributed manipulate from virtual ecosystems and sustainability from green computing, with the use instances of cloud computing, at the same time as making greater use of self-management advances from autonomic computing. The advantages of community cloud include [5]:

- Cost of establishing a communal cloud versus personal private cloud can be cheaper because of the distribution of costs among all participants.
- Tools located inside the community cloud can be used to leverage the information stored to serve consumers and the supply chain.
- Management of the community cloud can be outsourced to a cloud provider. The benefit right here is that the provider would be an independent third party that is bound by way of agreement and that has no desire to any of the customers involved aside from what's contractually mandated.

Drawbacks of community cloud [5]:

- More costly than public cloud.
- Fixed amount of data storage and bandwidth is shared among all community members.

5. CLOUD SECURITY ISSUES AND EXISTING SOLUTIONS

This section discusses the specific security issues and existing solutions to secure cloud computing environment. Top seven security threats to cloud computing analyzed by Cloud Security Alliance (CSA) [7] are described below:

(I) Abuse and Nefarious Use of Cloud Computing: Abuse and nefarious use of cloud computing is one of the major threat identified by the CSA. An example of that is the usage of botnets to spread spam and malware. Attackers can access a public cloud, for instance, and discover a way to upload malware to thousands of computers and use the power of the cloud infrastructure to assault other machines. Suggested remedies by the CSA:

- Stricter initial registration and validation procedures
- Enhanced credit score card fraud tracking and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

(II) Insecure Application Programming Interfaces: As software interfaces or APIs are what customers use to have interaction with cloud services, those must have extraordinarily secure authentication, access control, encryption and activity monitoring mechanisms - specifically when third parties begin to construct on them. Suggested remedies by CSA:

- Analyze the safety version of cloud provider interfaces.
- Ensure best authentication and access controls are carried out in concert with encrypted transmission.
- Recognize the dependency chain associated with the API.

(III) Malicious Insiders: The malicious insider danger is one that is important as many providers don't reveal how they hire people, how they provide them access to assets or how they monitor them. Suggested remedies by CSA:

- Enforce strict supply chain management and operate a comprehensive supplier evaluation.
- Specify human resource necessities as a part of legal contracts.
- Require transparency into entire information security and management practices, as well as compliance reporting.
- Identify security breach notification techniques.

(IV) Shared Technology Vulnerabilities: IaaS providers usually share infrastructure. Unfortunately, the components on which this infrastructure is primarily based were not designed for that. To make sure that consumers do not thread on each different's "territory", monitoring and robust compartmentalization is required. Suggested remedies by CSA:

- Implement security best practices for installation/configuration.
- Observe surroundings for unauthorized adjustments/activity.
- Promote robust authentication access control for administrative access and operations.
- Enforce service level contracts for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

(V) Data Loss/Leakage: Without a backup or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top threats for companies as the nay lose their reputation. Suggested remedies by CSA:

- Implement robust API access control.
- Encrypt and protect integrity of data in transit.

- Analyze data protection at each layout and run time.
- Implement strong key generation, management and storage, and destruction practices.
- Contractually call for providers to wipe persistent media earlier than it is released into the pool.
- Contractually specify provider backup and retention techniques.

(VI) Account, Service & Traffic Hijacking: Account, service and traffic hijacking is another trouble that cloud users should be aware of. These threats variety from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of-service attacks. Suggested remedies by CSA:

- Prohibit the sharing of account credentials among customers and services.
- Leverage robust two-factor authentication strategies where possible.
- Employ proactive monitoring to identify unauthorized activity.
- Understand cloud provider safety policies and service level agreements (SLA).

(VII) Unknown Risk Profile: Security have to continually within the top part of the concern list. Code updates, vulnerability profiles, security practices, intrusion tries - all things that must continually be kept in mind. Suggested remedies by CSA:

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details.
- Monitoring and alerting on vital records.

General Risks [8]:

- **Social Engineering:** This threat is one of the most omitted because most technical personnel attention at the nonhuman elements of their structures. The exploitation of this risk has caused loss of popularity for cloud service provider. This risk can be minimized by proper user provisioning, resource isolation, data encryption, and strong physical security procedures.
- **Backup Loss:** This risk affects company reputation, all backed up data, and service delivery. It also occurs due to improper physical security strategies, and access management vulnerabilities.
- **Natural Disasters:** This risk is often neglected however will have a high impact on the businesses concerned in the event of its occurrence. If an enterprise has a bad or untested continuity and disaster recovery plan or lacks one, their recognition, data, and service delivery can be seriously compromised.

6. CONCLUSION

This paper presents various aspects of cloud computing and its security issues. There are several cloud platforms. How to recognize and use these platforms is a big issue. As cloud computing is enhancing more and more it brings with it many problems and challenges which include many security threads. Cloud computing has essential ability to protect these challenges and grow to be a leader in resource sharing technologies.

References

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, Special Publication 800-145, 2011

[2] Jose Moura, David Hutchison, Review and Analysis of Networking Challenges in Cloud Computing, *Journal of Network and Computer Applications,* 60, 2015 http://dx.doi.org/10.1016/j.jnca.2015.11.015

[3] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, A Comprehensive Survey on Security in Cloud Computing, *Procedia Computer Science*, Volume 110, 2017, 465-472, http://dx.doi.org/10.1016/j.procs.2017.06.124

[4] Saurabh Singh, Young-Sik Jeong and Jong Hyuk park, A Survey on Cloud Computing Security: Issues, Threats, and Solutions, *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2016.09.002

[5] Sumit Goyal, Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. *I. J. Computer Network and Information Security,* 2014, 3, 20-29, DOI:10.5815/ijcnis.2014.03.03

[6] Tinankoria Diaby, Babak Bashari Rad, Cloud Computing: A review of the Concepts and Deployment Models, *I.J. Information Technology and Computer Science,* 2017, 6, 50-58, DOI:10.5815/ijitcs.2017.06.07

[7] Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[8] Gurkok, Cem. (2017). Securing Cloud Computing Systems. Chapter 63. http://dx.doi.org/10.1016/B978-0-12-803843-7.00063-6

[9] Yuhong Liu, Yan (Lindsay) Sun, Jungwoo Ryoo and Syed Rizvi, Athanasios V. Vasilakos. A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. *Journal of Computing Science and Engineering,* Vol. 9, No. 3, September 2015, pp. 119-133

[10] C. Prakash and S. Dasgupta. Cloud computing security analysis: Challenges and possible solutions. *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 54-57.

[11] Rajani Sharma, Rajender Kumar Trivedi, Literature review: Cloud Computing – Security Issues, Solution and Technologies. *International Journal of Engineering Research,* Volume No.3, Issue No.4, pp. 221-225

[12] Jose Moura and David Hutchison. Review and Analysis of Networking Challenges in Cloud Computing. *Journal of Network and Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2015.11.015

[13] Himanshu Raj, Ripal Nathuji, Abhishek Singh, Paul England-Microsoft Corporation, Resource Management for Isolation Enhanced Cloud Services, *CCSW'09,* November 13, 2009, Chicago, Illinois, USA. Available at: http://www.cs.jhu.edu/~sdoshi/jhuisi650/papers/spimacs/SPIMACS_CD/ccsw/p77.pdf

[14] S. Pearson and A. Benameur, Privacy, Security and trust issues arising from cloud computing, *IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom)*, Indianapolis, IN, 2010, pp. 693-702

[15] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, Controlling data in the cloud: outsourcing computation without outsourcing control, *ACM Workshop on Cloud Computing Security*, Chicago, IL, 2009, pp. 85-90.

[16] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., Scientific Cloud Computing: Early Definition and Experience, *10th IEEE Int. Conference on High Performance Computing and Communications*, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0

[17] Sanjoli Singla, Jasmeet Singh, Cloud Data Security using Authentication and Encryption Technique. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, Volume 2, Issue 7, July 2013

[18] Tehrani, S.R. and F. Shirazi, Factors influencing the adoption of cloud computing by small and medium size enterprises (SMEs). *International Conference on Human Interface and the Management of Information*. 2014. Springer

[19] Hashemi, S.M. and A.K. Bardsiri, Cloud computing Vs. grid computing. *ARPN Journal of Systems and Software*, 2(5), 2012, 188-194

[20] Chiang Ku Fan, Chen-Mei Fan Chiang, Tong Liang Kao, Risk Management Strategies for the Use of Cloud Computing, *I. J. Computer Network and Information Security*, 12 2012, 50-58

[21] M. Monsef, N. Gidado, Trust and privacy concern in the Cloud, 2011 European Cup, *IT Security for the Next Generation*, 2011, p. 1-15

[22] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, *International Journal of Engineering Science and Technology*, Vol. 3, No. 4, 2011, pp. 2672-2676

(Received 21 August 2017; accepted 09 September 2017)