Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Revisiting Cloud Security Issues and Challenges

Vaishali Singh*
Department of Computer Science,
St. Xavier's College, JAIPUR -302001, INDIA,

S. K. Pandey
Department of Information Technology, Board of Studies,
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament), NOIDA – 201309, INDIA,

Abstract*– There is no doubt to say that cloud computing appears to be one of the prominent ways as well as an evolution in the delivery of various computing services enabled by its key principle 'virtualization'. Like any other technology, along with several distinctive advantages, it has some challenges too. Security is one of the prime concerns/challenges among these. There seems to be a slow Cloud adoption rate due to these security issues and challenges associated with Cloud. The paper highlights major issues relating to Cloud computing and challenges that have been originated due to the nature and deployment of different models in use for service delivery. The aim of this paper is to render a more elaborated and complete understanding of the issues and challenges related to Cloud security and provide major research directions for future to the researchers in concerned area/s.

Keywords: Information Technology Cloud Computing, Cloud Security, Challenges in Cloud Security, Issues in Cloud Security.

I. Introduction

Cloud Computing aims for virtual centralization of data and resources through internet. Cloud provides users the fast access to the best-of-breed business applications or drastically boosts their infrastructure resources, all at very low cost [1]. Yet, guaranteeing the security of the data in the Cloud is difficult. The emergence of Cloud computing has critical aspects of security that have been gathered from the published reports of various agencies [41]. Though, there is a need for new solutions in terms of specific mechanisms, but before that, exploring all the issues and challenges related to Cloud security is more important [1]. Enterprises face several challenges regarding virtualization where applications are not hardware peculiar. Self healing mechanism is having its own backup running programs during any failure of data storage or network applications. Data management is concerned with the distribution, security measures and synchronization of data. The Service Level Agreement (SLA) allows replication of instances of one application on multiple servers, also multi tenancy permits multiple clients, which use same hardware simultaneously with time possibly that causes conflicts and service oriented challenge of creating its own Cloud application etc. [42]. According to a research study carried out by IDC Enterprise Board, security is the most emerging issue for Cloud computing [1]. Several issues and challenges discussed in this paper tend to discuss the medium slowing the adoption rate and usage of Cloud. Therefore, issues and challenges related to Cloud security need to be addressed for the growth of Cloud computing at the earliest. Beyond this introduction on the background details, the remainder of this paper is organized as follows. Section II highlights Cloud computing security that is believed to have long-term significance for Cloud computing. Section III describes issues relating to cloud security. Ensued by, challenges have been described in the Section IV. Afterwards, Section V highlights the statistical perspective of the issues with reference to cloud security. Conclusion and future work is reported in the Section VI.

II. Cloud Computing Security

Cloud computing solutions have had a substantial impact on the way in which businesses are conducted, though data security in cloud has been a concern. The business professionals need information to make informed decisions and cloud facilitates this use of information. Information Security is of at most importance to a customer as well as the provider. Securing a cloud refers to the security principles applied to protect the data stored, applications in use, and the infrastructure associated with the Cloud Technology. When considering the data of the cloud provider, all three pillars of security i.e. "CIA" should be adequately covered keeping in view the criticalness of the relevant data. Hence, the Confidentiality, Integrity and Availability (CIA) of the data must be ensured. Confidentiality is the term used to prevent disclosure of information to unauthorized individuals or systems. When there is a requirement to hide the information from the public, who don't have the access permission. It ensures that the data is not disclosed to the unauthorized entity. Secondly, Integrity means that data cannot be modified undetectable. It refers to the quality of being able to perform the protection of data from deletion and modification by unauthorized entities. The sole purpose of any information system is to make information available when it is needed. It should be highly unavailable to the unauthorized entities and instantly

available to the required authorized user. Considerations of SLAs, backup demands, calamity recovery measures, and the power of the client to reconstruct data are a part of Availability. The CIA are a well known security elements that need to be guaranteed in any kind of secure organization. Cloud system recognizes the need for security, but they tend to leave large security gaps that must be filled by the providers and the customers. Cloud has been like a black box to the clients and the providers may be negligent about the data or application handling. This might result in serious security breaches. When these breaches go unnoticed, they result in security vulnerabilities that attackers can easily leverage [2]. There are various cloud service providers but data privacy and security has always been a roadblock to adoption [3].

III. Issues Relating to Cloud Security

There are many issues, which show an adverse impact on cloud computing with reference to security [4]. The security issues on cloud computing primarily focus on data safety, data privacy, data confidentiality and network security [5]**.** The literature reveals various issues relating to Cloud adoption, which are given as follows and also shown in Fig.3.1 [6]:

- **Confidentiality**

Prevention of the unauthorized disclosure of the data is referred as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control) [7].

- **Integrity**

Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be insured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage [10].

- **Availability**

Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete from Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability [8]. One of the major Cloud service provider, AWS had a breakdown for several hours, which lead to data loss and access issues with multiple Web 2.0 services [9].

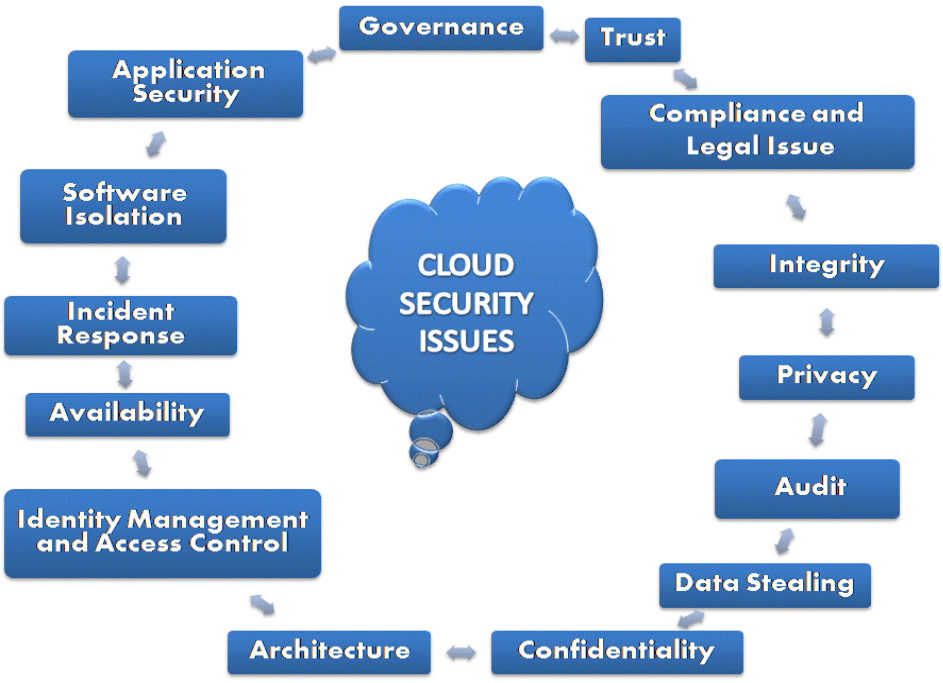

Fig. 3.1 Cloud Security Issues

- **Governance**

Due to the lack of control over the employees and services, it creates problems relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization. The organization gains computational resources as capital expenditures. These actions should be looked by the organization under governance through legal regulation, policies, privacy and security. Recent study has been done relating to the problems of governance, risk and compliance of Cloud computing [11]. Auditing and risk management programs are some way to verify the policy, which can shift the risk landscape.

- **Trust**

Deployment model provided a trust to the Cloud environment. An organization has direct control over security aspects as well as the federal agencies even have responsibility to protect the information system from the risk. Trust is an important issue in Cloud. Various clients' oriented studies reveal that Cloud has still failed to build trust between the client and service provider. Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time [8].

- **Legal Issues and Compliance**

There are various requirements relating to legal, privacy and data security laws that need to be studied in Cloud system. One of the major troubles with laws is that they vary from place to place, and users have no assurance of where the data is located physically [22]. There is a need to understand various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements [8]. An approach to monitor and compliance that helps to prepare Cloud Service Provider (CSP) and users to address emerging requirements and the evolution of Cloud models. To achieve efficiency, risk management, and compliance, CSPs need to implement an internal control monitoring function coupled with external audit process [12]. To increase the comfort of Cloud activities, Cloud user define control requirements, internal control monitoring processes, examine applicable external audit reports, and accomplish their responsibilities as CSP users [13]. It is the responsibility of the cloud suppliers that they are protecting the data and supplying to the customer in a very secure and legal way [14].

- **Privacy**

Privacy is also considered as one of the important issues in Cloud. The privacy issues are embedded in each phase of the Cloud design. It should include both the legal compliance and trusting maturity. The Cloud should be designed in such a way that it decreases the privacy risk. Some tips has been recommended for the Cloud engineers including that one should ensure to send minimum information stored in Cloud, protection of personal information, maximize user control, allowing user choice, limitation and specification of data usage and providing feedback [15].

- **Audit**

Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'. Its security is stronger than the one built in software and application. But, still it consumes more time, insistent across customers, pricy and motivational debilitate for everyone. The context of use of Cloud, time consuming audits seriously detains a key gain of Cloud agility [16].

- **Data Stealing**

In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing. Some of the Cloud providers do not use their own server, instead. They use server/s from other service providers. In that case, there is a probability that the data is less secure and is more prone to the loss from external server. If the external server is shutdown due to any legal problem, financial crisis, natural disaster, and fire creates loss for the user. In that case, data protection is an important mechanism to secure the data. Back up policies such as Continuous Data Protection (CDP) should be implemented in order to avoid issues with data recovery in case of a sudden attack [17].

- **Architecture**

In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model. Its reliable and scalable infrastructure is dependent on the design and implementation to support the overall framework. Through application programming interfaces, multiple Cloud components integrate to build a specific application, which is internet accessible. The deployment of IaaS is handled by virtual machines. It is loosely coupled with the Cloud storage architecture. Adequate and secure network communications infrastructure architecture must be in place. An architecture ontology approach for secure Cloud computing is to be defined [18].

- **Identity Management and Access control**

The key critical success factor for Cloud providers is to have a robust federated identity management architecture and strategy internal in the organization [19]. Using Cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with Cloud providers

[20]. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public Cloud and extending or changing the existing framework to support Cloud services may prove difficult [20]. Identity Management and Access control provides a secure authentication and authorization to an organization. The identity management provides a trust and share the digital attributes between the Cloud provider and organization ensuring the protection against attackers. Some technique used for it is Security Assertion Markup Language (SAML) standard or the OpenID standard [8].

- **Incident Response**

It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident [8]. Affected networks measures, determined systems, and applications, exposed intrusion vector helps to understand an incident response and the activities carried out must be remodelled [21].

- **Software Isolation**

Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture, and evaluate the risks required for the organization [8].

- **Application Security**

Security issues relating to application security still apply when applications move to a cloud platform.
To prevent Cloud computing, service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server [23]. Infected applications need to be monitored and recovered by the Cloud security drivers.

IV. Challenges Relating To Cloud Security

Security is one of the major issues, which requires proper attention. Despite of these advantages gained by Cloud computing, it's difficult to accomplish Cloud solutions due to the challenges associated with the models. Major challenges towards cloud security with respect to its different models are given as follows and shown in Fig. 4.1:

4.1 Deployment Model Challenges

Deployment of Cloud services can be done in different ways, depending on the organizational structure and location. Public, Private, Community and Hybrid Cloud are the key deployment models. These models face several challenges such as cloning, which deals with the duplication and replication of data etc. Major deployment challenges have been given as follows:

- Resource pooling implies unauthorized access due to sharing through the same network. The provider's computing resources are combined into a common fund to serve multiple consumers with physical and virtual resources using a multi-tenant, depending on consumer demand. This implies that there is no sense of location; the customer has no control over the exact location of the resources but may be able to be specific about location at a higher degree of abstraction [24].
- In case of mobility of data, the data is left back when data is moved from one place to another and is being used by unauthorized users. There is also an ongoing concern about the safety of moving data between the enterprise and the Cloud, as well as how to ensure that no residual data remnants remain upon moving to another Cloud service provider.
- Various service providers and users throughout the organization allow sharing of different resources to increase facility of access but unfortunately lead to data breach problems, which create elastic perimeter.
- In the public Cloud environment, the shared multi-tenant is prone to security challenges where illegal access of data is done using same hardware. When multiple tenants are supported by a cloud, then the scope of any breach is not contained to a single tenant. The breach of an application in a shared hosted cloud could result in the breach of other applications that use the same pool of resources in that cloud. Applications connected via the cloud may allow for unintended connections and unauthorized access [25].
- One of the threats in encryption is that it limits the efficiency of the cloud services because large data is expensive and time consuming to get encrypted as well as need to be stored before encryption then decrypted in the mean while one can manipulate the data, which will lead to violation of data integrity. The unencrypted data is the weakness for the Cloud models that can be easily accessed by unauthorized users.
- A key issue, concerned with Identity Management (IDM), is the disadvantage of interoperability resulting from different identity tokens and identity negotiation protocols as well as the architectural pattern [26].

4.2 Service Model Challenges

Cloud Models can be broadly sectioned into (SaaS), (PaaS) and (IaaS). The variety of the service models presents different security challenges depending on the model and consumers' Quality of Service (QoS) requirements. IaaS serves as the cornerstone layer for the other delivery models. But lack of security in Iaas layer affect the other delivery models. Considering PaaS, the primary focus of this model is on protecting data. PaaS can be a trapped because of uneven support for platform characteristics, that some PaaS providers lay greater risks than others. These service models have several challenges, which are given as follows:

- In Service hijacking, with the stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the CIA of those services. They may gain the power of reputation to launch subsequent attacks.
- The threat of malicious attackers is augmented for customers of cloud services by the use of various IT services, which lacks the lucidity between the procedure and process relating to service providers. Malicious users may gain access to certain confidential data and thus leading to data breaches.
- Multi-tenancy makes the impact of a VM (Virtual Machine) hopping attack larger than in a conventional IT environment. Because quite a few VMs can run at the same time and on the same host, there is a possibility of all of them becoming a victim VMs. VM hopping is thus a critical vulnerability for IaaS and PaaS infrastructures [27].
- Data leakage and data deletion lead to data related problems like security, locality, breaches, and integrity and so on. Data are stored in an organization in servers. Some time, it happens that after deletion of information from the cloud by the user, the data residual is left, which can be misused. Many a times, it has been seen that the record is not altered or deleted properly as well as there is no backup of data which leads to permanent loss of data. It can be stolen or leaked by the unauthorized user.
- The contents of VM virtual disks are saved as files such that VMs can be copied from one host to another host over the system or via moveable storage devices with no physically pilfering a hard drive. VM mobility might offer quick use but could show the way to security problems likewise, the rapid spread of susceptible configurations that an attacker could make use of to endanger the security of a novel host.
- DoS attack in virtualization takes place when one VM occupies all the obtainable physical resources such that the hypervisor cannot hold up more VMs and accessibility is endangered [28]. Malicious users may gain access to certain confidential data and thus leading to data breaches.
- The backup data is generally found in unencrypted form leading to misuse of the data by unauthorized parties leads to security threats [27].

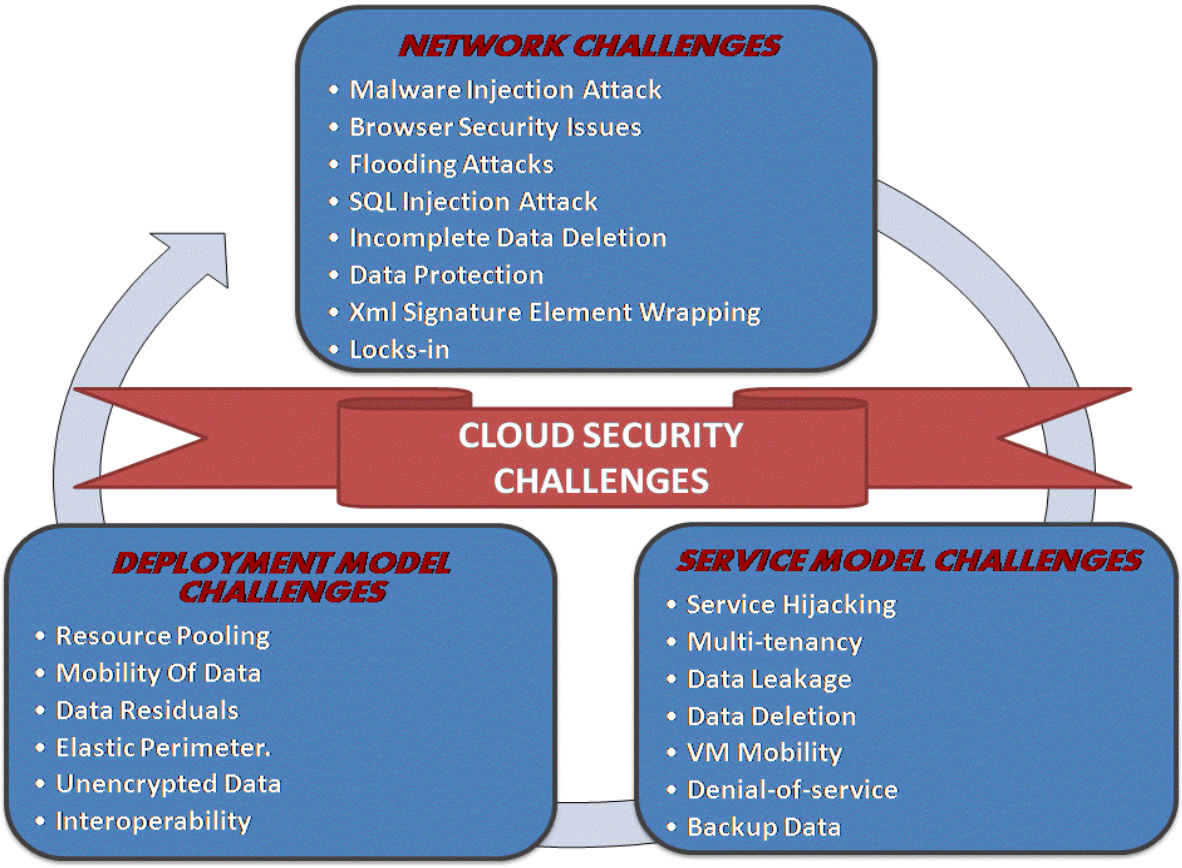

Fig. 4.1 Overview of Cloud Security Challenges

4.3 Network Challenges

One of the renowned service providers faced a severe degradation for about 22 hours due to networking issues related to an upgrade [29]. A lightning storm caused a partial outage of an IaaS Cloud that affected some users for four hours, and a network upgrade attempt caused a serious outage lasting more than twenty-four hours [30] [31] [32]. The technical security issues that are arising from adopting the Cloud computing model are such as XML-attacks, Browsers related attacks, and flooding attacks [33]. The network structure of Cloud faces various attacks and security issues, which ARE given as follows [27]:

- Malware injection attack aims at injecting a malicious service implementation or virtual machine into the Cloud system. An attacker uploads a modified copy of a victim's service instance so that some service requests to the victim service are processed within that malicious instance.
- Cloud computing actually depends on remote servers for each and every computational tasks to be done. Client machine is only used with I/O devices to access any software applications. In this case, browser in client machine is the gateway to access the cloud servers. So, browser security is crucial on total cloud security, because if the gateway is attacked by malware, then total cloud security becomes a problem [34].
- Flooding attack is the one where huge amount of requests to a specific service or large amount of data in the form of small messages are sent blocking the entire service or the session. This may also cause the loss of availability for more time due to processing delays [34].
- Cloud providers offer numerous tools, applications, standard data formats to their customers. But these services face problems when a customer tries to move to some other cloud provider, because mostly cloud providers are not compatible with one another. So, customers are forced to stick with same cloud provider and cannot migrate to another cloud operator's services. This problem creates a dependency issue on those cloud operators to get continued service [34].
- Data is not deleted completely even after the data erased from their physical machine. Clients are not able to know, whether their data is fully wiped out from all the virtual machines once after the delete command is applied. This problem leads to unsecured data on cloud. In addition, there may be a risk of this stolen data being used by unauthorized persons or hackers from the cloud [34].
- Data protection in cloud computing is very important factor. It could be complicated for the cloud customer to efficiently check the behaviour of the cloud supplier. Data moves freely around the globe via the internet, it is not clear which data-protection authorities at which location are responsible for ensuring the observance of the principles of data protection. For example, the XML Signature wrapping attack changes simply the content of the signed part of a message without tampering the signature [35]. SQL Injection Attacks are malicious act on the Cloud computing in which a spiteful code is inserted into a model SQL code [35].

V. Statistical Perspective

Cloud security is obviously of high interest to security professionals. Based on a recent survey conducted by AccelOps, about two-thirds companies are using some or other form of cloud services for critical applications and their data. 29 percent are utilizing hybrid clouds in their organizations. 19 percent are using private cloud infrastructure, and 17 percent are public cloud services. 35 are not using any cloud services at this time [36].

Various surveys conducted in 2012 indicated different immature state and challenges being faced by the cloud. 88% of IT professionals believed that, their data hosted in the cloud could be accessed by unauthorized individuals. 86% of survey respondents preferred to keep their data on their organization's network, instead of keeping in the cloud while 51% do not trust their personal data to the cloud. 48% thought of government or legal action discourages them from keeping data in the cloud [37]. One of the biggest concerns that the consumers around the world have is of security. Major security concerns relating to cloud and their statistical data is given in the following graph as reported in one of the major finding Fig.5.1 [26].

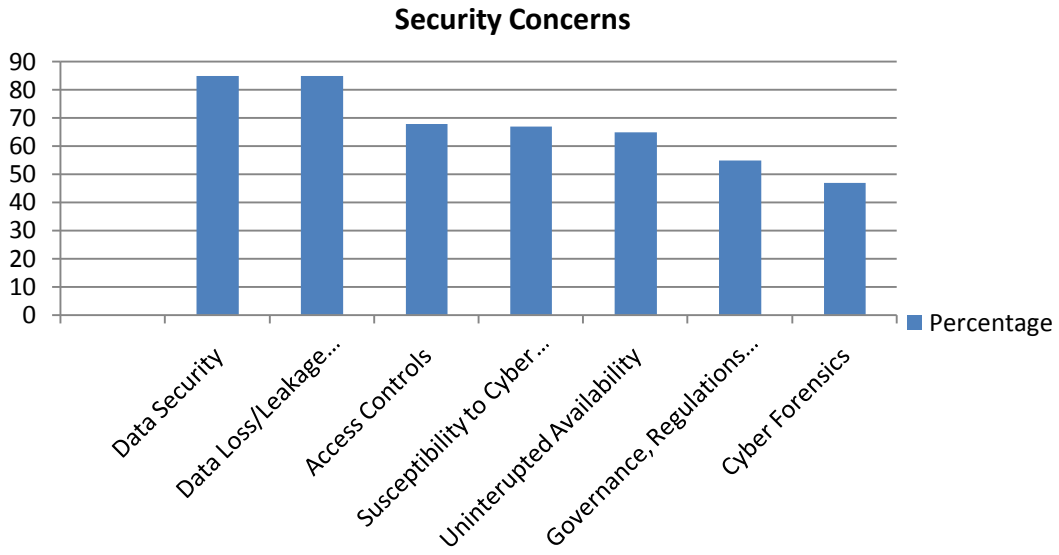

Fig. 5.1 STATISTICAL DATA (I)

Another major survey sponsored by Microsoft conducted in EARLIER 2013, has found that sixty percent still said that, they had viewed cloud as insecure, 45% said that they believe that it would result in the deprivation of control over the privacy of the data and 42% were concerned about the cloud's reliability [38]. Based on another global survey of more than 4,000 organizations conducted by Thales in June 2013 revealed that more than half of all respondents (53%) feel that their organizations currently transfer sensitive or confidential data to the cloud, yet only 30% say that they know 'how their cloud provider protects their data' [39]. The results of many other surveys also found privacy, reliability and security of cloud to be the top in list of challenges faced by IT managers. While security fears decrease to a degree, there is some evidence that concerns over performance and contractual issues actually increase. The following graph shows such issues in concerned clear way Fig. 5.2 [40]:

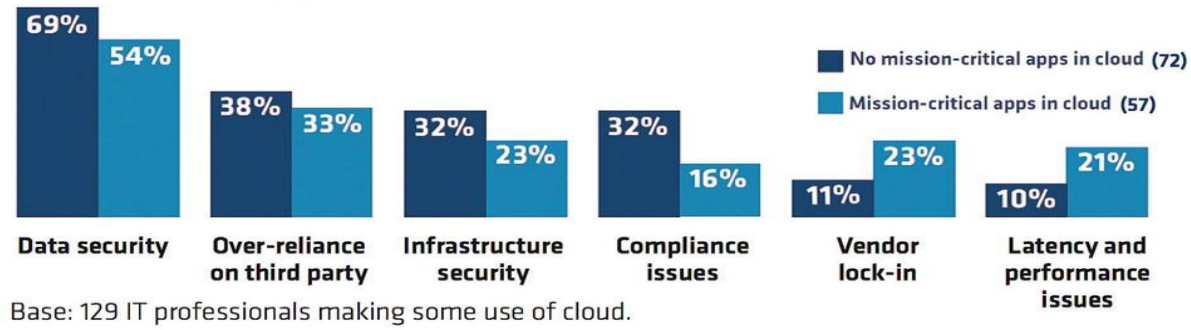

Fig. 5.2 STATISTICAL DATA (II)

In spite of all these aforementioned issues and challenges, researchers are continuously working with many fronts to come with solution/s. Security is a wide area of research with respect to Cloud Computing [41]. Researchers have done a significant work in the area/s but there is still a need to work further to address all the aforementioned issues and challenges. Researchers may select any issues/challenges and may work further to evolve some new techniques to address the same.

VI. Conclusion and Future Work

Cloud computing has emerged as an evolving technique for managing the computing services, delivered over the internet. There are astonishing advantages to adopt the same such as fast processing power, less spending on technology infrastructure, increased flexibility, decreased capital costs, and increased accessibility. But despite of these benefits, Cloud computing have several issues and challenges too, particularly relating to Cloud security, which decreases its adoption rate. Cloud system should adapt right security practices to overcome these problems relating to adoption of Cloud so that the users can fully enjoy the benefits of Cloud services. In this paper, issues and challenges relating to Cloud security have been highlighted. The focus is to understand these issues and challenges relating to the nature and deployment of Cloud services. It is evident from the discussion that the security threats relating to cloud computing has emerged as one of the very plausible topics. Future work may be to identify the specific threats with reference to cloud security based on these already identified issues and challenges and propose their suitable countermeasures to mitigate the risk up to desirable level.

References

[1] Behl, A., & Behl, K. "An Analysis of Cloud Computing Security Issues", Information and Communication Technologies (WICT), IEEE, Oct. 30-Nov. 2, 2012, pp.109-114.

[2] Ken Presti, "Halfway Approach to Cloud Security Leaves Huge Channel Play", May 03, 2013, pp.1, http://www.crn.com/news/cloud/240154180/halfway-approach-to-cloud-security-leaves-huge-channel-play.htm. [Accessed: 20-Jun-2013]

[3] Alistair Barr, "Data mining puts cloud security back on agenda", Jun 19, 2013, http://www.reuters.com/article/2013/06/20/us-summit-cloud-idUSBRE95J01720130620. [Accessed: 22-Jun-2013]

[4] Rajesh Piplode, Umesh Kumar Singh, "An Overview and Study of Security Issues & Challenges in Cloud Computing", IJARCSSE, Vol. 2, Issue 9, September 2012, pp.115

[5] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", Cloud Security Alliance, 2009, [Accessed: 22-Jun-2013] https://Cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[6] "Cloud computing: A new era of IT opportunity and challenges". ZDNet. March 3rd, 2009. pp.261, [Accessed: 23-Jun-2013], http://blogs.zdnet.com/Hinchcliffe/?

[7] Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z, "Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), Nov. 1-3 ,2010, pp. 105.

[8] JansenWayne, GranceTimothy, "Guidelines on security and privacy in public Cloud computing", NIST, Special Publication 800-144, Dec 2011, pp.35

[9] Kashif Munir, Sellapan Palaniappan, "Secure Cloud Architecture", Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013, pp.13.

[10] Yumerefendi, A.R., Chase, J.S., "Strong accountability for network storage". ACM Trans. Storage (TOS), Volume 3 Issue 3, October 2007, pp.382-401.

[11] R. Farrell, "Securing the Cloud-governance, risk, and compliance issues reign supreme", Information Security Journal: A Global Perspective, Volume 19, Number 6, 2010, pp.310-319.

[12] Vahid Ashktora, Seyed Reza Taghizadeh, "Security Threats and Countermeasures in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 1, Issue 2, October 2012, pp. 234-242.

[13] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance", 2009, pp.61-70.

[14] M. Christodorescu, R. Sailer, D. L. Schales, D.Sgandurra, D. Zamboni. Cloud Security is not (just) Virtualization Security, CCSW'09, Nov. 13, 2009, Chicago, Illinois, USA./.

[15] Siani Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", CLOUD '09: Proceedings of the 2009, ICSE Workshop on Software Engineering Challenges of Cloud Computing, May 2009, pp. 44-52.

[16] Craig Balding, "Stop the Madness! Cloud On boarding Audits - An Open Question", June 16, 2009, [Accessed: 20-Jun-2013] ,http://Cloudsecurity.org/blog/2009/06/16/stop-the-madness-Cloud-onboarding-audits-an-open-question.html

[17] Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network", IEEE Network, vol. 25, no. 4, July-August, 2011, pp. 28-33.

[18] Kevin Jackson, "Secure Cloud Computing: An Architecture Ontology Approach", DataLine, 2009, [Accessed: 24-Jun-2013], http://sunset.usc.edu/gsaw/gsaw2009/s12b/jackson.pdf.

[19] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. "A view of Cloud computing. Communications of the ACM", Vol. 53, Issue 4, April 2010, pp. 50-58.

[20] Richard Chow, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", ACM Workshop on Cloud Computing Security, Chicago, Illinois, November 2009, [Accessed: 25-Jun-2013], http://www2.parc.com/csl/members/eshi/docs/ccsw.pdf.

[21] Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication 800-144, December 2011, pp.14-33.

[22] Joshua Kissoon, "Cloud Computing Security Issues and Solutions", [Accessed: 26-Jun-2013], http://cleverlogic.net/articles/Cloud-computing-security-issues-and-solutions

[23] C.N.Hofer and G. Karagiannis, "Cloud computing services: taxonomy and comparison", Internet Serv Appl, September 2011, Volume 2, Issue 2, pp 81-94.

[24] Resource Pooling, [Accessed: 27-Jun-2013], http://Cloudcomputingvocabulary.com/resource-pooling/#

[25] Mano Paul, "Security in the Skies Cloud computing security concerns, threats, and controls", (ISC), pp.3

[26] Rosa Sánchez, Florina Almenares, Patricia Arias, Daniel Díaz-Sánchez and Andrés Marín, "Enhancing Privacy and Dynamic Federation IdM for Consumer Cloud Computing", vol.58 , Issue 1, February 2012, pp. 95-103.

[27] Disha H. Parekh, R. Sridaran, "An Analysis of Security Challenges in Cloud Computing", International Journal of Advanced Computer Science and Applications, vol. 4, No.1, February 2013, pp.1-9

[28] Perez R, van Doorn L, Sailer R. "Virtualization and hardware-based security". IEEE Security and Privacy 2008, vol. 6, Issue 5, pp. 24–31.

[29] G. Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009, [Accessed: 28-Jun-2013], http://www.theregister.co.uk /2009/03/16/azure_Cloud_crash/

[30] Cade Metz, Amazon Cloud Fell from Sky after Botched Network Upgrade, The Register, April 29, 2011, [Accessed: 27-Jun-2013] http://www.theregister.co.uk/2011/04/29/amazon_ec2_outage_post_mortem/.

[31] Rich Miller, Lightning Strike Triggers Amazon EC2 Outage, Data Center Knowledge, June 11, 2009, [Accessed: 27-Jun-2013],http://www.datacenterknowledge.com/archives/2009/06/11/lightning-strike-triggers-amazon-ec2-outage/

[32] Julianne Pepitone, Amazon EC2 Outage Downs Reddit, Quora, CNN Money, April 22, 2011, [Accessed: 27-Jun-2013], http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm.

[33] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109-116.

[34] Gunasekar Kumar, Anirudh Chelikani, "Analysis of security issues in cloud based e-learning", 2011, [Accessed: 27-Jun-2013], http://bada.hb.se/bitstream/2320/9271/1/2011MAGI23.pdf

[35] Lee Garber, "Serious Security Flaws identified in Cloud Systems", News Briefs, IEEE, December, 2011, pp. 21 – 23

[36] "AccelOps. Cloud Security Survey 2013", [Accessed: 28-Jun-2013], http://www.accelops.com/pdf/Cloud%20Security%20Survey%20Report.pdf

[37] Lieberman Software's 2012 Cloud Security Survey, conducted at the 2012 Cloud Security Alliance Congress. Last Accessed: 26-6-2013, http://www.liebsoft.com/cloud_security_survey/

[38] Charles Babcock, "Microsoft: SMB Cloud Security Worries Easing", June 11, 2013, Last Accessed: 26-6-2013, http://www.informationweek.com/cloud-computing/infrastructure/microsoft-smb-cloud-security-worries-eas/240156402

[39] Warwick Ashford, "Cloud adoption immature, shows security survey", Monday 24 June 2013, [Accessed: 28-Jun-2013], http://www.computerweekly.com/news/2240186784/Cloud-adoption-immature-shows-security-survey

[40] John Leonard, "Cloud computing: the lessons learned", 12 Dec 2012, [Accessed: 29-Jun-2013] http://www.computing.co.uk/ctg/analysis/2230812/cloud-computing-the-lessons-learned#ixzz2XRZb8ov5

[41] Vaishali Singh, S. K. Pandey, "Recent Advances in Cloud Security" Submitted at Elsevier Morgan Kaufman ICT, 06/15/2013

[42] S. Subashini ,V. Kavitha , "A survey on security issues in service delivery models of Cloud computing," Journal of Network and Computer Applications, 2011, pp.1-11.

AUTHORS

Vaishali Singh is presently working as an Assistant Professor in the Department of Computer Science, St. Xavier's College, Jaipur, India. She has an excellent academic background right from the school level. Under the Institute-Industry linkage program, she delivers expert lectures on various areas of Computer Science. She has contributed many research papers in the conferences of national repute. Her research interest includes: Cloud Security, Cloud Security vulnerabilities, threats and countermeasures, Access control, Identity measurement etc.

Dr. Santosh K. Pandey is presently working as a Faculty of Information Technology with Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament) New Delhi. Prior to this, he worked with the Department of Computer Science, Jamia Millia Islamia (A Central University) New Delhi and Directorate of Education, Govt. of NCT of Delhi. He has a rich Academics & Research experience in various areas of Computer Science. His research interest includes: Software Security, Requirements Engineering, Security Policies and Standards, Formal Methods, Cloud Computing, Security Metrics, Vulnerability Assessment etc. He has published around 46 high quality research papers and articles in various acclaimed International/National Journals (including IEEE, ACM, CSI) and Proceedings of the reputed International/ National Conferences (including Springer). Out of these publications, most of them have good citation records. He has been nominated in the board of editors/reviewers of various peer-reviewed and refereed Journals. In addition, he has also served as a Program Committee Member of several reputed conferences in India as well as abroad. He has also been designated in various academic/research committees by the government organizations as well as software companies as a subject expert.

