I J C T A, 9(11) 2016, pp. 4979-4992

CLOUD COMPUTING SECURITY AND PRIVACY ISSUES- A SYSTEMATIC REVIEW

Harshpreet Singh[#1], Promila Manhas[*2], Deep Maan[#3] and Nisha Sethi[4]**

Abstract: Cloud Computing has emerged as a computation technique in the computing paradigm. Progressing widely, it is appearing as a prominent computing miniature to increase the computing capacities without lending in new framework, practice or licensing for modern software. With the capability of seamlessly developing and delivering service over the internet and the probable benefits attained from the cloud computing, many institutions still hesitate to expand their business over the cloud. Various issues related to security and privacy need to be addressed before adopting cloud. This paper introduces a comprehensive reasoning of the cloud's security problems and explores the possible security and data privacy problems from the perspective of the cloud architecture, its delivery and deployment models.

Keywords: Cloud Computing, Cloud Security, Cloud Privacy, Data Security, Cloud Barriers, Adoption Risk

1. INTRODUCTION

Cloud computing brings new generation of an internet-based computing which is highly scalable, distributed and offers computing resources in form of a service. From initial notion frame to modern substantial formation, cloud computing is flourishing more and more sophisticatedly. Cloud computing has recently immerged as "Next-Best-Thing" in Information and Communications Technology. Cloud Computing comes out as a utility paradigm which is attaining momentum in industry and academia. It has rooted the traditional computing technology by adding contemporary beliefs and is acknowledged as next mutative step of distributive computing [1]. It commits the convincing cost reductions with modern business infrastructure to its users as well as to its providers[2].

With respect to the interpretation of cloud computing, the universally accepted definition of cloud computing is introduced by National Institute of Standards and Technology (NIST) as " Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configureurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider's interaction"[3].

The cloud computing model introduced by NIST has five essential characteristics which include On-demand self-service, Broad network access, resource pooling, rapid elasticity and measured service with three service models named as Software, Platform and Infrastructure, and four deployment models known as Private, Public, Community and Hybrid. The service models are also known as SPI model. From these three SPI models, IaaS is, affably, the most entrenched standard, providing an ample diversity of products and advanced capabilities like self-regulating scalability, pay-per-use and on demand provisioning[4][5].

Today many organizations are shifting their businesses over cloud to achieve quick entry in outstanding business applications and to expand their framework at trivial cost[6]. A cloud offers several benefits

School of Computer Science and Engineering, Lovely Professional University, Punjab, India
* Department of Information Technology, GNA Institute of Management & Technology, Punjab, India
** School of Computer Applications, Lovely Professional University, Punjab, India
[1]harshpreet.17478@lpu.co.in, [2]promilamanhas@gnaedu.in,
[3]deep.17474@lpu.co.in, [4]nisha.18349@lpu.co.in

which include rapid stationing, metered services, scalability, accelerated provisioning, adaptability, pervasive network access, prominent elasticity, low-cost catastrophic restoration, data storage solutions, fast reconstruction of services etc[7]. Multi-tenancy and Flexibility are two key components of the cloud model. Multi-tenancy empowers the sharing of same service instances among various tenants whereas elasticity is the capability of cloud for mounting up and down resources as current service demands.

All these benefits attract new users from industries and academy to leverage the use of cloud. The cloud while providing such services also offers many challenges in adapting to these services. Most of the challenges are discussed under the problem heading of cloud provider selection[8][9]. Many researchers have focused their research in this context which takes into consideration security consideration on various levels such as data storage, data transmission, application, user authentication, third party software, etc.

This paper provides an insight to various levels of security to be considered by the researcher and the user for accepting the service benefits offered by the cloud.

2. BARRIERS TO CLOUD COMPUTING

According to the survey of Forbes, CISCO predicts the global cloud index showing the global data center traffic in Exabyte for 2011 to 2020. Figure.1 shows the global cloud data center IP traffic by Type and by Segment of a data center (Source: Cisco Global Cloud Index, 2014–2019).

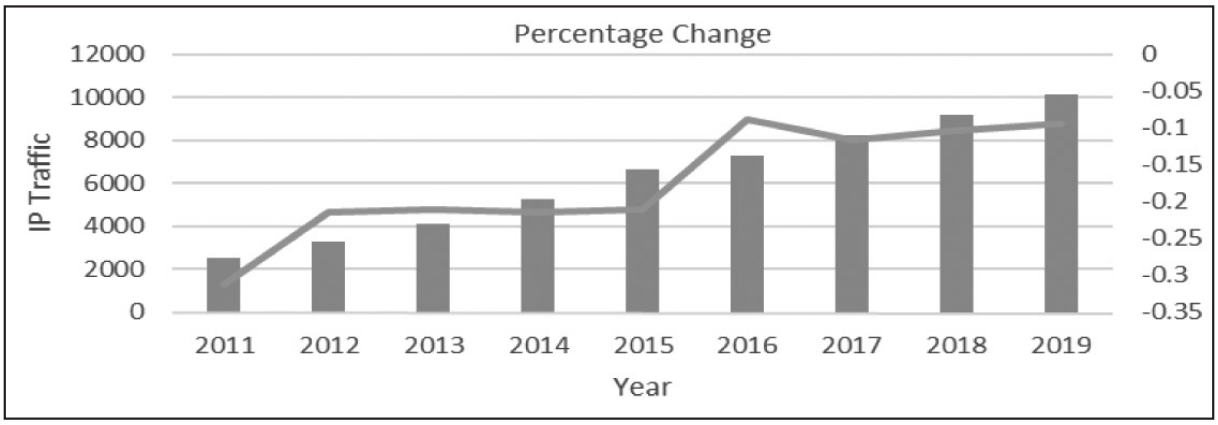

Figure. 1: Cloud Data Center IP Traffic, 2011-2020

The impact of cloud computing is going to dominate the internet traffic in the near future. This is waving a shift in the nature of traffic towards cloud applications, service and infrastructure. With its three service types each providing a varied type of control to the user. Cloud services provided globally account for huge collection of data, wherein 27.8 percent of users have uploaded sensitive data. Data breaches are estimated to rise and cost companies approximately $2.1 trillion by 2019[10].

Despite being a jargon, several convincing factors are allied with cloud computing, as a result of which 74% (IDC survey, 2010) of entrepreneurs are still not sure about shifting to the cloud, alleged security as the top challenge prohibiting their acceptance to cloud service model [11].

For few technical weaknesses in the architecture of cloud computing, it is sensitive to several privacy and security risks as the management of data and services associated with the application and databases migration from cloud to large data centers is not trustworthy [12][13]. It poses many security challenges along each level of service provided by cloud as depicted in Figure.2.

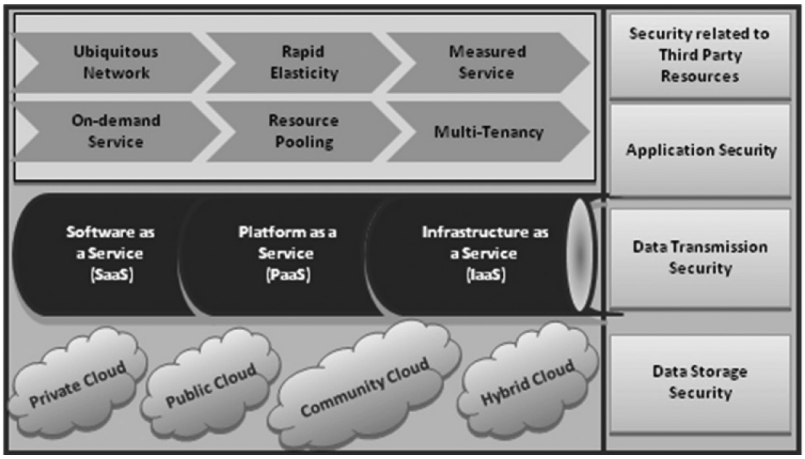

Figure. 2: Complexity of security in cloud architecture

These challenges are included but do not restrict any accountability to the accessibility, virtualization and web applications such as SQL injection and XSS, physical access controversies, privacy and control problems originating from third parties related to identity and credential management, concerns of data authentication, interposing, integrity, secrecy, data leakage and IP kidding [14][13][15][16][17].

There are some matters that limit the boundaries of this transformational computing as:

(a) **Security and Privacy Risks:** The success of any computing language can be determined from the level of security it provides to ensures how much secure it is [18][19][20]. Almost all the service providers assert that information sides in their servers is more secure and abundantly guarded from any kind of invasions and thefts than the data stored on innumerable personal computers or Laptops. But there have been many cases observed when the security provided by these providers is invaded and the complete system has been interrupted for several hours. Moreover, several security rifts found that bring crucial breaches in the security model of leading cloud service providers.

Privacy is the capability of an object to control the information that it acknowledges about itself to the service provider[21]. It has also the ability to regulate the approach to its information means that who has the privilege to use that information. Authors in [22] altercate the various guidelines concerned with the collection, sustenance and revelation of personal details of an object. Information requiring privacy needs the specific treatment as discussed in [23][24].

In case of deployment models, multiple security issues have been observed that also need to be inscribed in contrast of a public cloud to private cloud. A public cloud performs as a moderator for a myriad of virtual machines, VM auditors and supportive middleware [25]. The protection of a public cloud depends on the behaviour of all the entities and relationships between them. A public cloud provides distributive multi-tenant environment in which a group of users share a common software instance with specific privileges. As the users accumulate, security threats are assimilating more intensive and assorted. Thus it is essential to recognize the areas which are decumbent to security attacks and the necessary devices to ensure the protection of client-side as well as the server-side [19]. The existence of diverse security concerns in public cloud, idea of affirming a private cloud is safer with an option to choose the public cloud in future only if required[26].

Evolution of cloud computing be obligated to mash-up. A mash-up is a code, integrates data or functions from different web sources to create a new service. It uses the data or functions of multiple web sources in relation to a specific application by which security challenges become more multifarious and acute. On the basis of this conviction of mash-up, a secure component model has been proposed in[27][28].

(b) **Risks to the Performance, Reliability and Latency:** It is discovered that virtual machines are sharing processing units and main memory more efficiently as compare to network and disk I/O. One way to improve the performance of an I/O is to refine the architecture and operating system so that it may virtualizes the interrupts and I/O channels more effectively and efficiently. Another possibility to improve its performance is the usage of flash memory that conserves the information even when the system is powered off. It has no moving part, thus it accelerates the accessing speed and sustains more I/O operations than a disk[29].

Latency [30][31] is also a sensitive affair in cloud computing which deals with the flow of data throughout the different clouds. Some latency influencing determinants are:

- Data encryption and decryption when it switches over unsecured networks
- Congestion
- Windowing

Congestion leads to blockage when the amount of data flows through network channel are high and there are numerous requests that need concurrent access[32]. The conduct of system is a key element that should be taken into consideration, but, several times service providers face shortage either by permitting many VMs to access or getting its maximum throughput threshold, which hurts the performance of the system and increases the latency of the system[33][34].

(c) **Portability and Interoperability Risks:** Several scenarios have been noticed when organizations need to move their data and applications from existing cloud platform to some other cloud platform which is better than the existing one. When a customer is trying to migrate from one cloud platform to other cloud platform, faces many challenges which implicates multiple risks and disintegrate the system if it is not executed properly [35].

Sometimes, multiple cloud platforms are needed for a specific application for which platforms has to communicate with each other for the successful completion of a task. For smooth running of such tasks, the internal structure of the organization should be capable to manage the interoperability between multi-cloud platforms[36]. Cloud security model proposed in[35] act as a guideline for designing cloud security tools. The multi-folded feature provided by cloud is still an issue that is needed to be solved for a better functioning.

(d) **Risk of Data Breaching:** During the last few years, many security issues in data transitioning have been observed. Data transitioning includes multiple data centers and cloud deployment models. Leaving from one data enter to other data center is major security issue as it has been infringed several times[37].

Data transitioning through Fiber-Optic cables was advised a secure mode to transfer data until an illegal fiber wiretap device was detected by US security forces in Telco Verizon's optical network implanted at a Mutual Fund company[38]. It can tap the information without creating any disturbance.

(e) **Risks with Data Storage:** On-line data storage is becoming quite fashionable as it permits organizations to keep extensive blocks of data without mounting up the needed architecture.

In spite of many benefits of on-line data storage, still, there is a threat of data leakage. Some problems are noticed very frequently in dynamic data storage that remains continuous in the cloud. Depending on the level and category of storage provided, multiple risks are attached to them have been described in [18][12].

In addition to these barriers, many Mobile Cloud Computing (MCC) barriers has also been observed. From a Mobile cloud computing perspective, many additional challenges need to be inscribed to empower MCC to reach its utmost latent:

- *Accessible through Network:* Cloud computing is a Network-based computing technology. Hence, without having an internet connection, it is impossible to use mobile cloud applications.
- *Latency:* In contrast of dedicated wired local area network data transformation in remote networks in not as much rational. It is responsible for introducing lengthy intervals in data transformation at times.
- *Confidentiality:* Confidential data resides on a mobile device can become public if it uses cloud based mobile device. If the device is stolen or lost, due to hacked cloud, may provide access to highly confidential information of the user.
- *Problem with Identity Management:* Cloud providers use the concept of virtualization in which demand of user authentication and control beyond the cloud is high but the current schemes are not capable to manage the scenario of multi-clouds.

To avoid these barriers, quality scanners and malware protection software are to be initiated.

3. SECURITY RISKS IN CLOUD COMPUTING

All The main objective of cloud computing is to provide a secure environment around multi-tenancy and isolation[13]. It is necessary to secure the cloud model at all the levels i.e. at Network, Host and Application Level to retain the cloud up. In conformation to these levels, various security rifts may occur.

Basically, cloud computing employ three kinds of service delivery models to deliver distinct services to its users. The service models compass a diverse level of security requirement in the cloud model. SaaS is a software delivery model where different applications are remotely entertained and delivered to the customers on their demand. SaaS is rapidly become an assertive delivery model for fulfilling the IT requirements of enterprises. Web applications and SaaS are closely paired to provide assistance to the cloud users, thus most of the security risks to web applications are stiffed by SaaS model.

Few top-most security risks experienced by web applications are as:

- *SQL Injection:* SQL Injection is a type of attack, where intruder inject a vicious code into standard SQL code to obtain access to data and sensitive information stored in databases. The prevention treatment to SQL injection attacks is to avoid the usage of dynamically generated SQL in the code[39] [40].
- *XSS attacks*: It is also a type cross-site Scripting attack in which the attacker inserts the malicious script into the web content of a dynamic web-site. There are two methods to inject the malicious script. First one is known as Stored XSS in which intruder permanently store the malicious code into the properties of web application. The attack is introduced when victim demands dynamic page[41]. Secondly, Reflected XSS, the malicious coed is temporarily stored. It is immediately emulated to the user[41]. Many technologies have been proposed to prevent XSS attacks[42].
- *Man in the Middle (MITM) attacks:* Man in the Middle attacks are quite popular to SaaS model in which attacker try to interrupt an ongoing conversation between two users and insert false information to gain the knowledge of data transferred between them. MITM attack prevention schemes have been discussed in[43].

Hence, server security, Database security etc. is necessary considered to assure decent employment of cloud computing[12][16].

(a) **Security at Network Level:** Network systems are categorized in various categories as Shared and Non-Shared Networks, Public and Private Networks, restricted area and large area networks. Each one

of these networks has been victimized by a number of attacks. To assure the security at network level, one should consider some factors like confidentiality and integrity of data in network, proper data and network access controls and security maintenance mechanisms across third party threats.

Threats associated with network level security are as:

- *Domain Name System(DNS) attacks*–DNS is a key building block of internet which allows users to access websites and exchange emails. Domain Name System is a network (Internet) service that renders a domain name into IP address. Domain names are easier to remember. DNS attack is a type of attack in which the user has been routed to some nefarious cloud instead of the server called by user. Undoubtedly Domain Name System Security Extension minimizes the domain risks, but still many cases have been observed when these measures prove to be inadequate [44].
- *Sniffer attacks*– Sniffer attacks are placed by attackers to hack sensitive network information. A sniffer is a piece of code that grabs the packets flowing in a network. Sniffers are the real network troubleshooting tools. If the network packets are not encrypted, intruder can read their data through sniffer [45].
- *Reusability of IP Addresses* – Every node on the network has assigned an IP address and when a particular user moves out of network then same IP address is reassigned to a new user. It takes some time to changes IP address in DNS. During this lag time, there is a probability that the data may be accessed by some hacker as the address still lies in the DNS cache that can violates the privacy of the previous user[46].
- *Border Gateway Protocol (BGP) Prefix Hijacking* - It is a type of attack in which a wrong declaration to an IP address of Autonomous System (AS) is made which allows hijackers to trace the untraceable IP addresses and obtain control over them. ASs communicates via the BGP model. Sometimes a faulty AS may announce wrongly about the IP address affiliated to it, which routed the traffic to some other IP than the destined one. As a result, data is leaked and reaches to some unwanted source. Security system for AS is proposed in [47].

(b) **Security at Application Level:** Security at application level is concerned with the customization of software and hardware means to assure the security of all applications in such a manner that intruders cannot capture the control over them. Attacks at application level are launched by attackers as they appear to the system as a trusted user to obtain access and the system gets victimized. Thus, it is necessary to implement security checks to minimize the risks at this level. The threats to application level security are:

- *Denial of Service Attacks:* DoS makes the services assigned to authorized users unavailable. It causes the congestion by overloading the server by numerous requests that increases bandwidth consumption and make some portions of the cloud unapproachable to its users. Intrusion Detection System (IDS) is proposed to guard against DoS [42][48].
- *Cookie Poisoning:* It involves the modification of the elements of a cookie to provide unauthorized access to an application. Cookie basically includes the personal information of user. Once the cookie is available, its contents can be forged. This situation can be escaped either by carrying out the regular cookie clean-up or encoding the data of cookie [39].
- *Invisible Field Manipulation*: While using a web page, we find that certain fields are invisible as they have some information relating to page only for the use of its developers. These fields are extremely prostrate to attacks as they are modifiable. This is a severe security breach[42].

- *Backdoor and Debug Options*: The reason behind enabling the debug option is only to make developmental changes in the code. Sometimes, the debug options are unknowingly left enabled which may allow an attacker to make changes in code [49].
- *Distributed Denial of Service Attack:* DDoS targets the substantial services active on server. It overloads the server with numerous of packets so that it fails to handle them and obtain the control of information flowing at certain times[42]. Prevention treatment suggested against DDoS is to install IDS on all the machines[49].
- *CAPTCHA Breaking:* Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) was introduced to control spam and exploitation of the attached network components by bots. Recently, it has been observed that the spammers discovered a way to crack CAPTCHA, favoured by the service providers of Hotmail and Gmail as they introduce the audio systems to read CAPTCHA characters for the visually busted people[50].
- *Risk of Google Hacking:* Google has appeared as the best option for searching the information regarding anything on internet. Google hacking is a hacking technique in which intruder uses Google search engine to locate sensitive information from user's account. A Google hacking case was observed in 2010 in China when log on information of millions of Gmail users were abducted by a group of Chinese hackers [51].

(c) **Host Level Security:** From the perspective of security, the information regarding the host platforms, operating systems and process are publically not shared[52]. The host level security problems are related with hypervisor and virtual servers as:

- *Hypervisor Security:* Virtualization is one of the most important elements that plays an important role in the formation of cloud computing. Leading virtualization vendors are VMware, Xen and Microsoft. Virtual Machines and the hypervisor are two levels of virtualization. Virtual machine refers to a software computer that runs on operating system and applications like a physical computer. A hypervisor is a virtualization approach that permits different operating systems to run simultaneously on a host computer. A hypervisor becomes available at the boot time of the machine and act as a controlling agent of all the resources across the host machine, so they do not intersect each other. With increase of VMs, the security issues associated with them needs to be considered because it becomes difficult to maintain all systems[53][54].

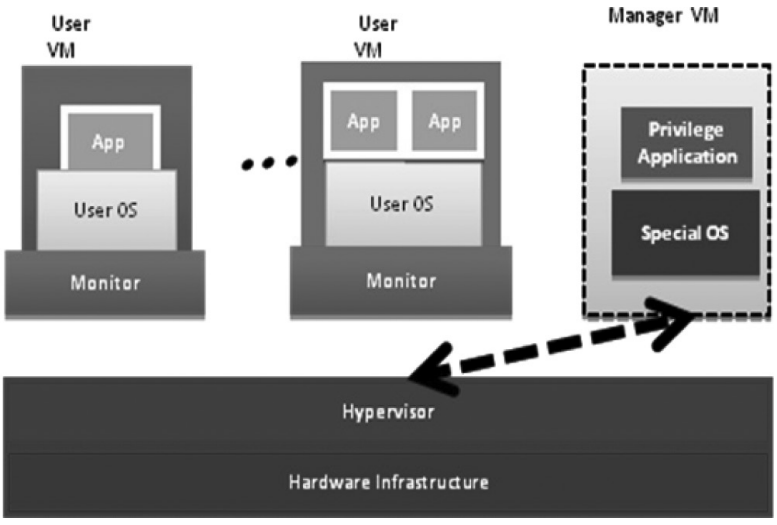

Figure. 3. Hypervisor Based Virtualization

Undoubtedly, there are many security zones but all exists within the same physical infrastructure. In case hypervisor crashes or the attacker obtains full control over hypervisor, all the systems and virtual machines gets affected

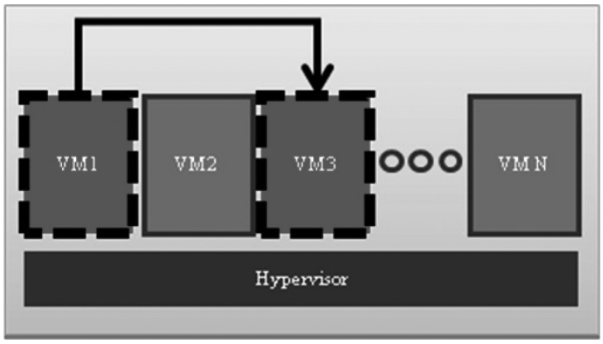

Figure. 4: Attack scenario within hypervisor

There is a need of more secure application interfaces (APIs) and careful network planning to minimize the hypervisor risks. By understanding the type, behaviour and association between the components of hypervisor architecture, cloud systems can be developed [57].

- ***Virtual Server Security:*** When a user is running his sensitive data on virtualized platforms, a lot of changes occurred like location, physical server, thus sensitive assets need to be secured all the time. IaaS users have full access to the guest virtual machine which is hosted and isolated by hypervisor technology. Virtual servers are approachable on the internet, thus the process of protecting the virtual server in cloud environment demands very strong security operations[58][59].

Some suggestions for virtual server security are given as:

1. Guard the integrity of images from unauthorized users.
2. Avoid password based access.
   - Allow Role based access password.
   - Keep the decoding key away from the cloud.
   - Facilitates system auditing and event logging.

(d) **Cloud Data Storage and Security:** It is a revolutionary storage method that service providers use to bring Storage as a Service[60]. From music files to pictures to sensitive data, they take the backup of the user's data and store them on the large data centers. It allows the users to access synchronize and access his data across multiple devices as long as internet is available[61]. The flow of data between the user, server and its storage in cloud is shown as Figure. 5.

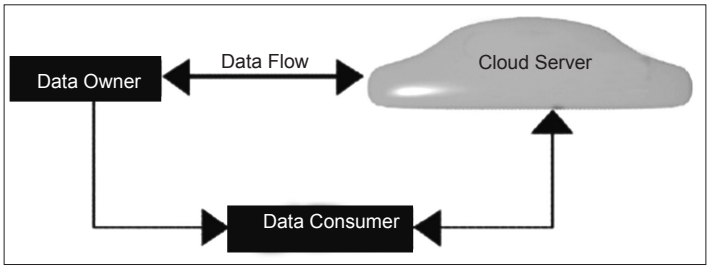

Figure. 5. Data flow been user and cloud server

Although, providers commit that their cloud is highly secure but many cases has been identified when their clouds have been modified and data leaked or lost due to security cracks or human error. No doubt, service providers are trying various technologies to ensure security of their cloud against any kind of security breach. Whether to store the data in cloud is secure or not is still a question for organizations.

The traditional environment of virtualized cloud storage is not suitable for controlling the security issues. The service providers' use various encryption and homo-morphic token techniques to secure the data resides in their cloud [62]. Domain based trust model is useful to handle interoperability in cross clouds where each domain has a specific agent dedicated for the purpose of trust management[63].

Neglected Data-Remanence is other major issue relates with the data storage security. Data-Remanence is the lingering representation of data which allow data reconstruction when data is removed, may cause minimal threat in private cloud computing offerings and severe security threats in case of public cloud offerings [64].

3. EXISTING SECURITY SCHEMES

Different techniques are adopted by the providers to secure cloud against various security threats.

TABLE 1
Existing security Schemes for Cloud

S. No.	*Scheme*	*Suggested Approach*	*Strengths*	*Limitations*
1.	Secure Data Storage [62]	Introduces homomorphism token with distributed verification of erasure-coded data against unauthorized data modification, Byzantine failures and also locate machine being attacked.	Providing dynamic data operations without any data loss and Efficient against byzantine failures	Issues related location of the fine-grained data errors are not addressed
2.	User Identity[65]	Suggest use of active bundle scheme where sensitive data is encrypted and upon arriving at the destination, bundle enables itself.	Trusted Third Party(TTP) verification is not needed	Personal identification information is decrypted before SP use it which may be prone to attacks
3.	Trust Model for interoperability in cross cloud	Introduces domain based approach which separates providers and users and proposes different trust methods for both.	Solve security problems in a multilayered cloud environment	Only help to achieve identity and behavioural authentication not the integrity
4.	Reputation- based trust management[66]	Uses pyramid of DHT based on overlay networks.	comprehensive use of virtualization for securing clouds	reproductions are required to verify the performance
5.	Virtualization [67]	Introduces Advanced Cloud Protection System (ACSP) to secure guest VMs, uses shared computing middleware and logging technique to audit the behaviour of cloud components and check the executable file system periodically.	Prone to different types of security attacks	System performance marginally degraded
6.	Secure Virtualized network	Suggest providers to hide the internal details of their services to lessen the chances of data leakage.	Identifies the attacking party	If attacker gets the address of any other VM, may harm VMs in between
7.	Pretty Border Gateway Protocol (PBGP)[68]	Suggest architecture to trace the cases where AS may announce wrongly about itself.	Prevent the routing to the wrong AS	Do not verify the path actually followed by traffic

To provide more secured environment to cloud customer, cloud service provider are continuously trying to implement each possible security measure in its offerings and its design [69].

4. CONCLUSION

Cloud computing has merged as today's most exciting technologies that is revolutionizing the computing world. Varied benefits have largely focused the industry in adopting this new computing paradigm. Researchers are focused on resolving the challenges in adoption of cloud as new technical prime. With reference to its service delivery models and deployment models, the paper's main focus is on the security and privacy problems that must be tackled and controlled for smooth functioning of this new computing paradigm. Problems related with confidentiality and integrity of data residing on cloud need to be examined before importing the cloud services. Moreover, investigation of the cloud needs to be done at regular intervals as safeguard to ensure that cloud is working properly and provides a protected environment against attacks. There is a need to analyze each and every element in cloud from the minimum level the hardware as well as at maximum level services offered by the cloud. A unified solution can be provided to customers; otherwise cloud environment will remain uncertain for its user.

References

[1] L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, "Scientific Cloud Computing: Early Definition and Experience.," in *HPCC*, 2008, vol. 8, pp. 825–830.

[2] L. Wang, G. Von Laszewski, A. Younge, X. He, M. Kunze, J. Tao, and C. Fu, "Cloud computing: a perspective study," *New Gener. Comput.*, vol. 28, no. 2, pp. 137–146, 2010.

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[4] Chappel David, "A Short Introduction To Cloud Platforms," *Microsoft Corp.*, no. August, pp. 3–13, 2008.

[5] P. Mell, T. Grance, and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology."

[6] H. Singh and R. Randhawa, "CPSEL : Cloud Provider Selection Framework For Ranking and Selection of Cloud Provider," vol. 10, no. 7, pp. 18787–18810, 2015.

[7] J. Q. Anderson and H. Rainie, *The future of cloud computing*. Pew Internet & American Life Project Washington, DC, 2010.

[8] S. Zhang, S. Zhang, X. Chen, and X. Huo, "Cloud computing research and development trend," in *Future Networks, 2010. ICFN'10. Second International Conference on*, 2010, pp. 93–97.

[9] H. Singh and R. Randhawa, "Evaluation Framework for Selection and Ranking of Cloud Providers ," vol. 7, no. July, pp. 31–37, 2015.

[10] W. Paper, "Cisco Global Cloud Index: Forecast and Methodology, 2013–2018," *Cisco Press*, pp. 2014–2019, 2014.

[11] K. Mualla and D. Jenkins, "Evaluating Cloud Computing Challenges for Non-Expert Decision-Makers," *IJDIWC*, p. 285, 2015.

[12] W. Paper, "Database Security in Virtualization and Cloud Computing Environments."

[13] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[14] Bhadauria and sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," *Int. J. Comput. Appl.*, pp. 47–66, 2012.

[15] S. M. S. Hashemi and M. Ardakani, "Taxonomy of the Security Aspects of Cloud Computing Systems-A Survey," *Networks*, vol. 4, no. 1, pp. 21–28, 2012.

[16] V. C. Bhagawat, "Survey on Data security Issues in Cloud Environment," vol. 2, no. 1, pp. 31–35, 2015.

[17] H. Saini and A. Saini, "Security Mechanisms at different Levels in Cloud Infrastructure," *Int. J. Comput. Appl.*, vol. 108, no. 2, 2014.

[18] C. S. Storage, "Security Considerations White Paper for Typical NAS Deployments in an IP Network," pp. 1–25.

[19] J. Wayne and G. Timothy, "NIST Guidelines on Security and Privacy in Public Cloud Computing," *Draft Spec. Publ.*, pp. 144–800, 2011.

[20] S. Pearson, "Taking account of privacy when designing cloud computing services," in *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009, pp. 44–52.

[21] H. C. Lim, S. Babu, J. S. Chase, and S. S. Parekh, "Automated control in cloud computing," *Proc. 1st Work. Autom. Control datacenters clouds - ACDC '09*, p. 13, 2009.

[22] R. Gellman, "Privacy in the clouds: risks to privacy and confidentiality from cloud computing.," in *Proceedings of the World privacy forum,* 2012.

[23] C.-C. Lo, C.-C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," in *Parallel processing workshops (ICPPW), 2010 39th international conference on*, 2010, pp. 280–284.

[24] H. R. Motahari-Nezhad, C. Bartolini, S. Graupner, S. Singhal, and S. Spence, "IT support conversation manager: A conversation-centered approach and tool for managing best practice IT processes," in *Enterprise Distributed Object Computing Conference (EDOC), 2010 14th IEEE International*, 2010, pp. 247–256.

[25] L.-J. Zhang and Q. Zhou, "CCOA: Cloud computing open architecture," in *Web Services, 2009. ICWS 2009. IEEE International Conference on*, 2009, pp. 607–616.

[26] B. Duncan and M. Whittington, "Company Management Approaches—Stewardship or Agency: Which Promotes Better Security in Cloud Ecosystems?," *CLOUD Comput. 2015*, p. 169, 2015.

[27] F. De Keukelaere, S. Bhola, M. Steiner, S. Chari, and S. Yoshihama, "SMash : Secure Component Model for Cross-Domain Mashups on Unmodified Browsers," pp. 535–544, 2008.

[28] A. Taivalsaari, "Mashware: The Future of Web Applications," Sun Microsystems, Inc., Mountain View, CA, USA, 2009.

[29] G. Casale, D. Ardagna, M. Artac, F. Barbier, E. Di Nitto, A. Henry, G. Iuhasz, C. Joubert, J. Merseguer, V. I. Munteanu, and others, "DICE: Quality Driven Development of Data Intensive Cloud Applications," 2015.

[30] N. Leavitt, "Is cloud computing really ready for prime time?," *Computer (Long. Beach. Calif).*, no. 1, pp. 15–20, 2009.

[31] R. Minnear, "Latency: The Achilles heel of cloud computing," *Cloud Comput. J.*, 2011.

[32] N. Bansal, K.-W. Lee, V. Nagarajan, and M. Zafer, "Minimum congestion mapping in a cloud," *SIAM J. Comput.*, vol. 44, no. 3, pp. 819–843, 2015.

[33] S. Kuppusamy, V. Kaniappan, and D. Thirupathi, "Switch Bandwidth Congestion Prediction in Cloud Environment," *Procedia Comput. Sci.*, vol. 50, pp. 235–243, 2015.

[34] P. Sreekumari, J. Jung, and M. Lee, "An early congestion feedback and rate adjustment schemes for many-to-one communication in cloud-based data center networks," *Photonic Netw. Commun.*, pp. 1–13, 2015.

[35] M. Kretzschmar and S. Hanigk, "Security management interoperability challenges for collaborative clouds," in *Systems and Virtualization Management (SVM), 2010 4th International DMTF Academic Alliance Workshop on*, 2010, pp. 43–49.

[36] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and A. Vakali, "Cloud computing: Distributed internet computing for IT and scientific research," *Internet Comput. IEEE*, vol. 13, no. 5, pp. 10–13, 2009.

[37] H. Intel Corp. OR, USA, "Monitoring and Managing the Data Center," *Data Cent. Effic. Optim. Data Cent. Manag. Monit.*, pp. 1–4, 2007.

[38] T. Jessica, "Connecting data centres over public networks. IPEXPO. ONLINE." 2011.

[39] D. Gollmann, "Securing Web Applications," *Inf. Secur. Tech. Rep.*, vol. 13, no. 1, pp. 1–9, Jan. 2008.

[40] A. A. Noureddine and M. Damodaran, "Security in Web 2.0 Application Development," in *Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services*, 2008, pp. 681–685.

[41] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis.," in *NDSS*, 2007.

[42] A. Bakshi and B. Yogesh, "Securing cloud from DDOS attacks using intrusion detection system in virtual machine," *2nd Int. Conf. Commun. Softw. Networks, ICCSN 2010*, vol. 1, no. 1, pp. 260–264, 2010.

[43] J. Katz, "Efficient Cryptographic Protocols Preventing 'Man-in-the-Middle' Attacks," COLUMBIA UNIVERSITY, 2002.

[44] D. E. Eastlake and others, "Domain name system security extensions," 1999.

[45] Z. Trabelsi, H. Rahmani, K. Kaouech, and M. Frikha, "Malicious sniffing systems detection platform," in Applications and the Internet, 2004. Proceedings. 2004 International Symposium on, 2004, pp. 201–207.

[46] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A Survey on Security Issues in Cloud Computing," arXiv Prepr. arXiv1109.5388, 2011.

[47] J. Karlin, S. Forrest, and J. Rexford, "Autonomous security for autonomous systems," Comput. Networks, vol. 52, no. 15, pp. 2908–2923, 2008.

[48] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," It Prof., no. 4, pp. 38–43, 2009.

[49] R. Lua and K. C. Yow, "Mitigating ddos attacks with transparent and intelligent fast-flux swarm network," Network, IEEE, vol. 25, no. 4, pp. 28–33, 2011.

[50] A. B. Jeng, C.-C. Tseng, D.-F. Tseng, and J.-C. Wang, "A study of CAPTCHA and its application to user authentication," in Computational Collective Intelligence. Technologies and Applications, Springer, 2010, pp. 433–440.

[51] T. Wang, "GOOGLIST REALISM: The Google-China saga and the free-information regimes as a new site of cultural imperialism and moral tensions," in The Eigth International Conference on New Directions in the Humanities. UCLA. Los Angeles, California, June, 2010, vol. 29.

[52] U. Jangid, N. Sharma, and K. Rathi, "A Survey on Secure the Cloud Environment using hypervisor-based virtualization technology," Int. J. Innov. Comput. Sci. Eng., vol. 1, no. 3, pp. 27–29, 2014.

[53] B. Kanoongo, P. Jagani, P. Mehta, and L. Kurup, "Exposition of Solutions to Hypervisor Vulnerabilities," 2014.

[54] L. M. Joshi, M. Kumar, and R. Bharti, "Understanding Threats in Hypervisor, its Forensics Mechanism and its Research Challenges," Int. J. Comput. Appl., vol. 119, no. 1, 2015.

[55] M. Jaiganesh, M. Aarthi, and A. V. A. Kumar, "Fuzzy ART-Based User Behavior Trust in Cloud Computing," in Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Springer, 2015, pp. 341–348.

[56] D. Jayarathna, U. Tupakula, and V. Varadharajan, "Hypervisor-based Security Architecture to Protect Web Applications," Inf. Secur. 2015, vol. 27, p. 15, 2015.

[57] F. Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology," Int. J. Mach. Learn. Comput., vol. 2, no. 1, pp. 39–45, 2012.

[58] T. Y. Win, H. Tianfield, and Q. Mair, "Virtualization Security Combining Mandatory Access Control and Virtual Machine Introspection," in Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014, pp. 1004–1009.

[59] Z. Yu, Q. Wang, W. Zhang, and H. Dai, "A Cloud Certificate Authority Architecture for Virtual Machines with Trusted Platform Module," in High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on, 2015, pp. 1377–1380.

[60] K. A. Kumar, S. Gnanadeepa, H. John, and G. K. Janani, "Survey on security and privacy preserving public auditing for content storage in cloud environment," in Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on, 2015, pp. 1–4.

[61] Q. H. Vu, M. Colombo, R. Asal, A. Sajjad, F. A. El-Moussa, and T. Dimitrakos, "Secure Cloud Storage: A framework for Data Protection as a Service in the multi-cloud environment," in Communications and Network Security (CNS), 2015 IEEE Conference on, 2015, pp. 638–642.

[62] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Netw., vol. 24, no. 4, pp. 19–24, 2010.

[63] M. Yang and H. Zhou, "New Scheme of Data Security Access For Cloud Computing Based on Hierarchical division.," Int. J. Digit. Content Technol. its Appl., vol. 9, no. 2, 2015.

[64] J. Bloomberg, "Data Remanence: Cloud Computing Shell Game," May 19, 2011. http//www. zapthink. com/2011/05/19/data-remanencecloud-computing-shell-game, 2011.

[65] R. M. Salih, "The Active Bundle Scheme for Protecting Electronic Medical Records," Trans. Int. Conf. Heal. Inf. Technol. Adv., vol. 1, no. 1, pp. 124 – 131, 2011.

[66] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," Internet Comput. IEEE, vol. 14, no. 5, pp. 14–22, 2010.

[67] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1113–1122, 2011.

[68] J. Karlin, S. Forrest, and J. Rexford, "Pretty good BGP: Improving BGP by cautiously adopting routes," Proc. - Int. Conf. Netw. Protoc. ICNP, pp. 290–299, 2006.

[69] S. Software, "SERENA SOFTWARE Serena Service Manager Security," 2014.