www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-3, June 2018
Survey Paper

Int. J. Sc. Res. in Network Security and Communication

E-ISSN:2321-3256

Vulnerabilities and Countermeasures on Cloud: A Survey

Kamal Bunkar[1*], Chhaya Arya[2]

[1]Institute of Computer Science, Vikram University Ujjain
[2]Research Scholar Pt. JNIBM, Vikram University, Ujjain

Received: 26/May/2018, Revised: 08/Jun/2018, Accepted: 21/Jun/2018, Published: 30/Jun/2018

Abstract- A system, programme, or process that has a vulnerability or flaw that could be used by bad actors to undermine the security or integrity of that system is said to be vulnerable. Organisations must establish a complete cybersecurity strategy that includes routine security assessments, vulnerability scanning, patch management, employee training, and incident response planning in order to reduce vulnerabilities. Protecting systems and data from potential exploitation requires staying up to date on the newest security threats and best practises. Misconfigurations, software defects, insecure APIs (Application Programming Interfaces), and insufficient access controls are only a few of the causes of cloud vulnerabilities. This review paper reviewed different related studies published from 2010 to 2017 from the academia and industry. They classified the security issues as per defined taxonomy with real-life examples that provided a rationale for discussion and highlighted the related impact of the security issues. Security and privacy were cited as important obstacles to the cloud's rapid rise in earlier research. However, the narrative evaluation offered in this study offers an integrationist end-to-end mapping of cloud security requirements, detected threats, known vulnerabilities, and recommended responses, which appears to be a first-time presentation of this information in one location.

Keywords- Attack Classification; Cloud Computing; Threats Classification; Threat Identification; Vulnerabilities.

1. INTRODUCTION

The way applications are created and made available has been completely transformed by the emerging computing paradigm known as cloud computing. In order to enhance application provisioning, it encourages the usage of computational and networked resources on demand. As a result, cloud providers are used to manage resources, which enables a decrease in operational and management costs. The development of cloud computing has also resulted in a rise in abstraction level due to the availability of additional service kinds over and above infrastructure-related ones. To ease the complexity of setting up and administering the execution environments within the leashed resources, platform services are specifically provided. The range of these services has also been expanded to make it easier to build and develop cloud applications. Most of the security challenges are inherited from the vulnerabilities in cloud architectural components and technologies used, like, vulnerabilities in Internet communication, web services, service oriented architecture, web-browsers, virtualization, hypervisors, multi-tenancy, software, virtual machines, self-service management interfaces. Existing applications were moved to the cloud as a result of the use of infrastructure as a service (IaaS) and platform as a service (PaaS) services, and new ones appeared as a result, showcasing the benefit that they can indefinitely scale to manage the ever-increasing workloads. The abundance of software-level services (SaaS) makes it possible to combine these services to produce sophisticated functionality with added value. As a result, software companies may now purchase a wide range of tools and services to quickly develop their apps and sell them in a market that is ever-competitive.

2. RELATED WORK

According to Akhil D. More et al.[1], cloud computing is a modern technology that provides a variety of services over the internet. The ability to store information on the cloud is provided by cloud services for the users. Without giving the accuracy and dependability of the information any thought. According to Aized Amin Soofi et al.[2], cloud computing is an internet-based computing technology that is the future of computing. Although it has received a lot of attention recently, safety concerns pose the biggest threat to the system's development. It basically conveys customer information over which the customers have no control, and information preservation does not provide the highest level of security. Automated security provisioning, virtual machine migration, hardware server consolidation, energy management, software framework, data security, storage technologies, and related security aspects are highlighted as the challenges for the cloud. According to Takabi et al. [3], the outsourcing of data and applications, virtualization and hypervisors, heterogeneity, extensibility and shared responsibility, service level agreements (SLAs), compliance and regulation all have special security and privacy issues in the cloud. Their suggested security solution paradigm

revolves around managing user authentication, identity, access control, and accounting, along with unified organisational security management. It also includes management of trust, secured services, and security policy. The challenges of building an unidentifiable medical database out of various supplies were discussed by Alevtina Dubovitskaya et al. [4]. The developed design illustrates how to collect data in non-identical networks for various scientific organisations where it is necessary to preserve daily information. The author is involved in creating a secure, scalable cloud-based health platform for storing and exchanging patient data for therapeutic reasons. For the purpose of successfully combining the health-related data from various sources individually, an algorithm has been developed. Grobauer et al. [5] used risk factors to analyze the impact of cloud-specific vulnerabilities due to its characteristics and the underlying technology used. Based on risk factors, they also proposed indicators for cloud specific vulnerabilities. Their paper does explain in detail about vulnerabilities in the cloud. However, there is no specific mention about trust mechanism. Security concerns pertaining to SaaS, PasS, and IaaS cloud service delivery models were examined by Subashini and Kavitha [6]. They discovered fourteen security problems with the SaaS delivery model, including vulnerabilities in virtualization and issues with data security, data integrity, data access, web application security, network security, identity management & sign-on process, authentication & authorization, data locality, data segregation, confidentiality, and data breaches. For PaaS, they suggested to define and use security specific metrics to measure vulnerability scores of applications being developed and deployed by the PasS cloud users. They advocated for shared responsibilities of both provider and consumer to implement security measures in case of IaaS. According to Anantha Lakshmi and Shaik Muhammad Rasheed [7], hosting cloud data is a key component of popular autonomous software cloud applications. Thus, enabling public inspection capabilities for cloud storage is dangerously valuable so that users can select potential inspection strategies for information security. The system's security and the consumers' online load should not be increased by any additional hazards that a third party auditor (TPA) introduces for security reasons. The third party auditors (TPA) conduct concurrent inspections for a number of users. The developed methods are safer and extremely useful, according to the extensive safety and performance estimation. The authors suggested a dispersed erase coded information and identical tokens-based hosted inspection approach. Security, trust, privacy, and their interrelationships were defined by Pearson [8]. Furthermore, Pearson examined the difficulties in resolving the security, trust, and privacy issues unique to the cloud and emphasised that old procedures are no longer adaptable or dynamic enough to do so. Phaphoom et al. [9] consider cloud computing as an amalgam of existing technologies, primarily, based on the established concepts and solution for virtualization, distributed systems, and web services. They described four major focus areas — cloud architecture, virtualization, data management, and security issues and solutions. They presented a five-layer cloud architecture for service delivery. They recommended robust solutions for virtualization and data management based on the analysis of different solutions proposed in related literature. In their pertinent work, they have explained vulnerabilities associated with components of each of five layers of cloud architecture and the associated solution approach. Their work includes a mapping of the identified security issues and their suggested solution in a very precise and concise way.

Table 1. Comparative analysis of the related works with this survey.

Survey	Year	Major Area discussed	A	B	C	D	E	F	G	H	I	J	K	L
Coppolino et al. [13]	2017	Cloud security issues, attack vectors, current solutions for attacks along with examples of industry used solutions	Y				Y	Y	Y				Y	Y
Singh et al. [14]	2016	Cloud security threats, issues, challenges and proposal for a three-tier security architecture					Y						Y	Y
Khan and Al-Yasiri [15]	2016	Current and future challenges for cloud security and a cloud adoption framework					Y						Y	Y
Huang et al. [16]	2015	Cloud security mechanisms used in the IaaS industry and security problems and solution from academia		Y			Y	Y	Y					Y
Ali et al. [17]	2015	Cloud security issues and existing solution analysis, vulnerabilities in mobile cloud computing					Y			Y			Y	Y
Khalil et al. [18]	2014	Cloud vulnerabilities, security threats, attacks, and comparative analysis of available solutions		Y			Y	Y		Y			Y	Y
Fernandes et al. [19]	2014	Cloud computing architecture, underlying technologies, threats, vulnerabilities, attacks, cloud security issues taxonomy		Y			Y			Y			Y	Y

Xiao and Xiao [20]	2013	Cloud architecture, characteristics, security challenges, supporting techniques, cloud security and privacy attributes, suggested security solution				Y	Y		Y					Y
Pearson [8]	2013	Cloud computing concepts, cloud security, trust and privacy issues				Y	Y	Y					Y	Y
Zissis and Lekkas [21]	2012	Cloud security requirements, associated potential threats and trusted third party based security solution recommendations			Y		Y	Y	Y		Y			Y
Vaquero et al. [22]	2011	Cloud security issues, attack vectors, current solutions for attacks along with examples of industry used solutions			Y			Y			Y			Y
Morsy et al. [23]	2010	Security issues from the perspective of cloud architecture, characteristics, service delivery model and stakeholders, and the recommended security solution				Y	Y	Y			Y		Y	Y
Zhang et al. [24]	2010	Design challenges of cloud computing and commercial solution used with example cloud provider	Y			Y	Y							Y
Takabi et al. [3]	2010	Cloud computing definition and features, unique security and privacy implications, security and privacy challenges, and solution approaches	Y			Y	Y						Y	Y
This Paper	2017	Cloud overview, architecture, cloud security model and taxonomy, security requirements, threats, vulnerabilities, countermeasures and their mappings, trust based solutions, privacy preservation and impact on the emerging applications and technologies	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

A: Privacy; B: Trust mechanism; C: Security analysis and mappings; D: Security Countermeasures; E: Security Vulnerabilities; F: Security Threats; G: Security Requirements; H: Security Taxonomy; I: Architecture; J: Overview; K: Cloud Computing;

Hashizume et al. [10] described cloud-related threats, vulnerabilities, and countermeasures in their comprehensive work. The most important aspect of their work is about the service level security view from the end user perspective. They very well explained about different threats, vulnerabilities, and possible countermeasures along with their inter-related mapping. Ankush et al. [11] explained that using cloud services frees consumers from the hassle of local data storage and preservation by enabling them to host their information arbitrarily on-demand from high-quality apps and services from a distributed collection of computer resources. Cloud computing enables the hosting and sharing of information, but there is disagreement over how to guarantee the privacy and accuracy of data while it is being viewed by the public. According to Modi et al. [12], the cloud environment may be thought of as a layered model with security concerns in each layer and supporting technologies. The privacy-related concerns and solutions, particularly with regard to data storage management strategies and life cycle management, should have been improved, though.

Presented a comprehensive study on security issues in the cloud, using a taxonomy for vulnerabilities, threats, and attack. They reviewed different related studies published from 2010 to 2017 from the academia and industry. They classified the security issues as per defined taxonomy with real-life examples that provided a rationale for discussion and highlighted the related impact of the security issues. They provide practical recommendations for addressing these security issues.

2.1 Cloud computing delivery models:

Cloud computing delivery models refer to different ways in which cloud services are made available to users. These models define the level of control, management, and responsibility that both the cloud service provider and the customer have. The three primary cloud computing delivery models are Infrastructure as a Service (IaaS). In the IaaS model, the cloud provider offers virtualized computing resources over the internet. Users can rent virtual machines, storage, and networking components on a pay-as-you-go basis. Platform as a Service (PaaS) provides a platform and environment for developers to build, deploy, and manage applications without needing to worry about the underlying infrastructure. The cloud provider manages the infrastructure, including networking, storage, and operating systems, while the customer focuses on coding and deploying their applications.

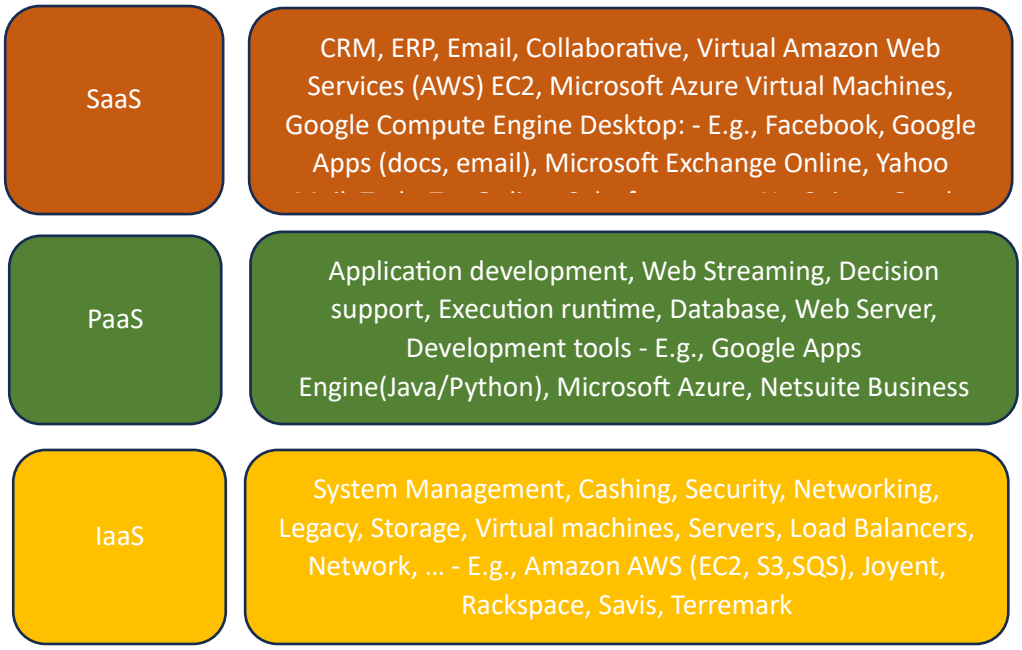

Fig.1 Cloud Computing delivery module and services

Software as a Service (SaaS) delivers software applications over the internet on a subscription basis. Users can access these applications through a web browser without needing to install or maintain any software on their local devices. The cloud provider handles everything, including infrastructure, maintenance, updates, and security.

2.2 Cloud Development Models

Cloud deployment models refer to the ways in which cloud computing resources are hosted and made available to users. These models define how the cloud infrastructure is structured and who has access to it.

Public Cloud: In a public cloud deployment, cloud resources are owned and operated by a third-party cloud service provider and are made available to the general public over the internet. These resources are shared among multiple customers, and users can access services and applications on a pay-as-you-go basis.

Private Cloud: A private cloud is a cloud infrastructure that is dedicated to a single organization. It can be hosted internally within the organization's data center or externally by a third-party provider. Private clouds offer more control, security, and customization compared to public clouds.

Hybrid Cloud: A hybrid cloud deployment combines elements of both public and private clouds. It allows data and applications to be shared between on-premises infrastructure and cloud resources. Organizations can use the public cloud for tasks that require scalability and flexibility while keeping sensitive or critical workloads in a private environment.

Multi-Cloud: Multi-cloud refers to using services from multiple cloud providers to meet specific business needs. This approach can help mitigate vendor lock-in and provide access to specialized services from different providers. Each cloud service can be chosen based on its strengths and suitability for different applications.

2.3 Security challenges of the cloud:

Security challenges in the cloud can arise due to the unique nature of cloud computing environments, where data, applications, and resources are stored and accessed remotely over the internet. While cloud computing offers numerous benefits, it also introduces several security concerns that organizations must address.

Table 2 Cloud computing top 12 threats.

Rank	Threat	Threat description
1.	Data breaches	It means releasing, viewing, stealing or using of sensitive, protected or confidential information by any party for any purpose which was not authorized to do so. Any information leaked that was not intended for public release may come under the purview of data breaches like personal health information, personally identifiable information (PII), etc. The extent of damage due to data breaches could be determined based on the sensitivity of the breached information
2.	Weak identity, Credential and Access Management	It results in attackers masquerading as legitimate users and getting unauthorized access to data resulting into data breaches which potentially damaging to the owner of data and associated stakeholders.
3.	Insecure APIs	For monitoring, provisioning, orchestration, and managing the allocated resources, cloud consumers are provided with application programming interfaces (APIs) and/or user interfaces (UIs) which exposes the cloud computing environment to the external world and potentially to attackers. These UIs and APIs are generally designed and implemented using web services which have inherent vulnerabilities. These APIs can be further used to build value-added services which might further dilute the user's credentials to the third party
4.	System and Application Vulnerabilities	This threat appears due to bugs in the system and application software which could be exploited by the attackers to steal data and take control of the systems' operation. Vulnerabilities in libraries, kernel and application tools of an operating system put all services and data at the security risk. The feature like multi-tenancy creates yet another attack surface as it needs usage of shared memory and resources among different systems of organizations, hosted in the same cloud environment
5.	Account Hijacking	This is the traditional threat of any computer system and so is in the cloud computing environment which means gaining access to a system by hacking credentials and password of a legitimate user. From the cloud perspective, if attackers hijacked a user's account, they can redirect clients to illegitimate sites, manipulate data, return falsified information, and eavesdrop on activities and transactions.
6.	Malicious Insiders	A malicious insider is a current or former employee or any business partner that has or had authorized access to information system creates threat if he or she intentionally misused that access to negatively impact the security and privacy aspects of the information system
7.	Advanced Persistent Threats	APTs refer to a higher degree of sophisticated attack which is of very much of specific purpose and aimed to specific target. These attacks are difficult to eliminate as they adapt to deployed security measures while pursuing their goals over an extended period.
8.	Data loss	Data can be lost other than malicious attacks as well, like accidental deletion or unfortunate damage or physical catastrophe like fire, earthquake, flood, etc., which may lead to permanent loss of stored outsourced data unless it is backed up to some alternate safe location which can be made accessible to the legitimate consumer
9.	Insufficient Due Diligence	While making a choice and decision for selection for cloud technology to use and cloud provider to provide services to host business functions the selection committee must consider many factors. Lack of proper approach and plan for conducting due diligence leads to security risks
10.	Abuse and Nefarious Use of Cloud Services	It is potentially caused due to unaccounted, mismanaged, fraudulent, free trails user accounts and poorly secured cloud deployments that allows attackers to access the computing resources and misuses it to target victims. Launching distributed email spam, denial-of-service attacks, and phishing campaigns are some of the examples of misuse of cloud-based resources
11.	Denial of Service	It simply means legitimate users are prevented from accessing their data and application due to slow response or simply no availability of the cloud resources. An attacker causes system slowdown by forcing the target cloud service to consume more than allocated finite system resources and virtually resulting in no access to legitimate users.
12.	Shared Technology Vulnerabilities	Sharing technology, either for infrastructure, platforms or applications, is the basic characteristics of the cloud computing system. The components which facilitate sharing of technology are, generally, not designed to offer an effective isolation property for a multi-tenant environment where applications of multiple customers are hosted together. This potentially can lead to shared technology vulnerabilities like flaws in hypervisors.

To mitigate these challenges, implement a robust cloud security strategy that includes Thorough risk assessments and regular security audits, Strong access controls and identity management, Data encryption at rest and in transit, Monitoring and logging of cloud environments for suspicious activities, Regular patching and updates of software and applications

2.4 Threat Identification in the Cloud

To determine which attacks can take advantage of the recently identified vulnerabilities of the cloud components and what hazards they offer, we apply our classification of threats from the tables described in Section 3.1. The suggested threat identification method consists of the three steps shown in figure 2: Identification of cloud components, identification of vulnerabilities, and identification of threats.

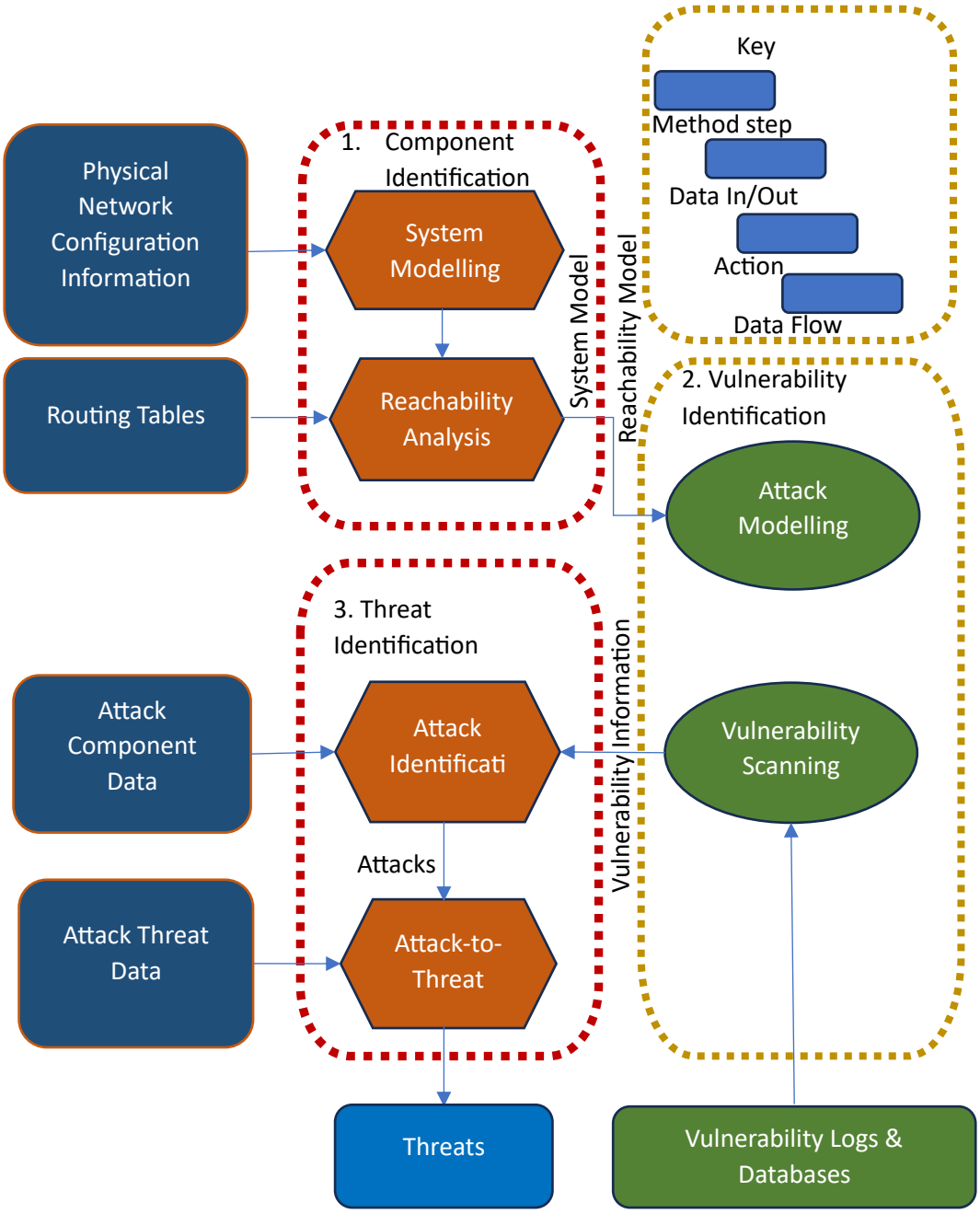

Fig 2 Threat Identification Method Steps and Actions

2.5 Vulnerability Analysis of Cloud Frameworks: A vulnerability analysis of various existing cloud frameworks against different identified security attacks is presented in table 3

Table 3 Vulnerability analysis of different cloud frameworks.

S. No.	Framework	Zombie Attack	Service Injection	Attack Man-in Middle Attack	Metadata Spoofing Attack	Phishing Attack	Backdoor Channel Attack	Replay Attack	Relay Attack
1.	Data integrity proof	Y	Y	N	Y	Y	Y	N	N
2.	Secure and	Y	Y	N	Y	Y	Y	N	N

	dependable storage service								
3.	Secure overlay storage with deletion	Y	N	N	Y	Y	Y	N	N
4.	Adaptive attribute based trust with SLA	N	Y	N	N	Y	N	N	N
5.	Secure role-based access control	Y	N	N	Y	Y	Y	N	N
6.	Cloud information accountability	Y	Y	N	Y	N	Y	N	N
7.	Privacy-preserving auditing system	Y	Y	N	Y	Y	Y	N	N
8.	Collaboration based security	N	Y	N	Y	Y	Y	N	N
9.	Public auditability with dynamic data storage	Y	Y	N	Y	Y	Y	N	N
10.	Dynamic indirect mutual trust	Y	N	Y	Y	N	Y	Y	N
11.	Data retention policy management	N	Y	Y	Y	N	Y	Y	N
12.	Secure cloud computing	N	Y	Y	Y	N	Y	Y	N

During this literature review, numerous security requirements, risks, threats, attacks and concerns associated with the expansion of cloud infrastructure are studied. Both cloud providers and businesses must give their full support to establish a safe, secure, and sound environment. The analysis of the literature revealed that no single research work offers comprehensive information on how various predicted models created by different researchers are impacted by various cloud events. Ultimately, proactive security measures, constant vigilance, and a comprehensive understanding of the cloud environment are essential to addressing the security challenges of cloud computing.

3. CONCLUSIONS AND FUTURE WORK

Cloud computing is in continual development in order to make different levels of on-demand services available to customers. While people enjoy benefits cloud computing brings, security in clouds is a key challenge. In this paper, we examined the security vulnerabilities in clouds from different perspective that included related real-world exploits, and introduced countermeasures to those security breaches. The review of the literature found that no single study provides full information on the effects of distinct cloud events on different anticipated models developed by different scholars. This study examines several cloud representations in an effort to shed light on how cloud events impact cloud models and potential fixes. In the future, we will continue to contribute to the efforts in studying cloud security risks and the countermeasures to cloud security breaches.

REFERENCES

[1] Akhil D More, Shailesh Nelwade, Avinash Chhabra, Nachiket Bhosale and Abha Pathak, Jan. 2016, „A Review on Privacy Preserving Public Auditing for Data Storage Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, No. 1, pp. 50 - 56.

[2] Aized Amin Soofi, Irfan Khan, M and Fazal – e – Amin , May 2014, „A Review on Data Security in Cloud Computing", International Journal of Computer Applications, Vol. 94, No. 5, pp. 26 – 35

[3] H. Takabi, J.B.D. Joshi, G.-J. Ahn, Security and privacy challenges in cloud computing environments, IEEE Secur. Priv. (ISSN: 1540-7993) 8 (6) (2010) 24–31.

[4] Alevitina Dubovitskaya, Visara Urovi, Matteo Vasirani, Karl Aberer and Michael I. Schumacher, 2015, „A Cloud Based eHealth Architecture for Privacy Preserving Data Integration, IFIP, pp. 585 – 598.

[5] B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Secur. Priv. (ISSN: 1540-7993) 9 (2) (2011) 50–57.

[6] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. (ISSN: 1084-8045) 34 (1) (2011) 1–11.

[7] Anantha Lakshmi, M and Shaik Mahammad Rasheed, April 2016, "Integrity Constraints for Cloud Auditing Services Using Third Party Services", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, No. 4, pp. 32 – 38

[8] S. Pearson, Privacy, security and trust in cloud computing, in: S. Pearson, G. Yee (Eds.), Privacy and Security for Cloud Computing, Springer, London, UK, ISBN: 978-1-4471-4189-1, 2013, pp. 3–42.

[9] N. Phaphoom, X. Wang, S. Samuel, S. Helmer, P. Abrahamsson, A survey study on major technical barriers affecting the decision to adopt cloud services, J. Syst. Softw. (ISSN: 0164-1212) 103 (2015) 167–181.

[10] K. Hashizume, D.G. Rosado, E. Fernández-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Serv. Appl. (ISSN: 1869-0238) 4 (1) (2013) 1–13.
[11] Ankush R. Nistane, Shubhangi Sapkal and Deshmukh, R.R, Feb. 2016, „Privacy Preserving Public Auditing and Data Integrity for Secure Cloud Storage Using Cloud Third Party Auditor", International Journal of Advanced Engineering, Management and Science, Vol. 2, No. 2, pp. 50 - 56.
[12] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, A survey on security issues and solutions at different layers of cloud computing, J. Supercomput. (ISSN: 1573-0484) 63 (2) (2013) 561–592.
[13] L. Coppolino, S. DAntonio, G. Mazzeo, L. Romano, Cloud security: Emerging threats and current solutions, Comput. Electr. Eng. (ISSN: 0045-7906) 59 (2017) 126–140.
[14] S. Singh, Y.-S. Jeong, J.H. Park, A survey on cloud computing security: Issues, threats, and solutions, J. Netw. Comput. Appl. 75 (2016) 200–222.
[15] [36] N. Khan, A. Al-Yasiri, Identifying cloud security threats to strengthen cloud computing adoption framework, Procedia Comput. Sci. (ISSN: 1877-0509) 94 (2016) 485–490.
[16] W. Huang, A. Ganjali, B.H. Kim, S. Oh, D. Lie, The state of public infrastructure-as-a-service cloud security, ACM Comput. Surv. (ISSN: 0360-0300) 47 (4) (2015) 1–31.
[17] M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: Opportunities and challenges, Inform. Sci. (ISSN: 0020-0255) 305 (2015) 357–383.
[18] I.M. Khalil, A. Khreishah, M. Azeem, Cloud computing security: A survey, Computers (ISSN: 2073-431X) 3 (1) (2014) 1–35.
[19] D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M. Freire, P.R.M. Inácio, Security issues in cloud environments: a survey, Int. J. Inf. Secur. (ISSN: 1615-5270) 13 (2) (2014) 113–170.
[20] Z. Xiao, Y. Xiao, Security and privacy in cloud computing, IEEE Commun. Surv. Tutor. (ISSN: 1553-877X) 15 (2) (2013) 843–859.
[21] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst. (ISSN: 0167-739X) 28 (3) (2012) 583–592.
[22] L.M. Vaquero, L. Rodero-Merino, D. Morán, Locking the sky: a survey on IaaS cloud security, Computing (ISSN: 1436-5057) 91 (1) (2011) 93–118.
[23] M.A. Morsy, J. Grundy, I. Müller, An analysis of the cloud computing security problem, in: Proceedings of APSEC 2010 Cloud Workshop, 2010, pp. 1–6.
[24] Q. Zhang, L. Cheng, R. Boutaba, Cloud computing: state-of-the-art and research challenges, J. Internet Serv. Appl. (ISSN: 1869-0238) 1 (1) (2010) 7–18.
[25] M. Avram, Advantages and challenges of adopting cloud computing from an enterprise perspective, Procedia Technol. (ISSN: 2212-0173) 12 (2014) 529–534.
[26] C.-L. Hsu, J.C.-C. Lin, Factors affecting the adoption of cloud services in enterprises, Inf. Syst. E-bus. Manag. (ISSN: 1617-9846) 14 (4) (2016) 791–822.
[27] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf, NIST Cloud Computing Reference Architecture (SP 500-292), National Institute of Standards & Technology, Gaithersburg, MD 20899-8930, USA, 2011.
[28] E. Aguiar, Y. Zhang, M. Blanton, An overview of issues and recent developments in cloud computing and storage security, in: K.J. Han, B.-Y. Choi, S. Song (Eds.), High Performance Cloud Auditing and Applications, Springer, New York, NY, USA, ISBN: 978-1-4614-3296-8, 2014, pp. 3–33.
[29] C.A. Ardagna, R. Asal, E. Damiani, Q.H. Vu, From security to assurance in the cloud: A survey, ACM Comput. Surv. (ISSN: 0360-0300) 48 (1) (2015) 1–50.

