IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 8, April 2024

A Review of Security Issues in Cloud Computing Systems

Anjaney Shukla[1] and Dr. Narender Kumar[2]
Research Scholar, Department of Computer Science[1]
Research Guide, Department of Computer Science[2]
NIILM University, Kaithal, Haryana, India

Abstract: *Cloud computing delivers commercial or consumer IT services via the Internet in a proven, adaptive, and cost-effective manner. Due to the frequent outsourcing of vital functions, cloud computing increases risk. This behavior makes data security, privacy, availability, and compliance harder. This article examines cloud computing's security issues, which stem from SOA, virtualization, and Web 2.0. Our goal is to find and correlate solutions to the biggest Cloud Computing and its environment risks and vulnerabilities in the literature.*

Keywords: Cloud computing, Security, Vulnerabilities.

I. INTRODUCTION

Cloud computing is gaining popularity in science and industry. Cloud computing is the first of the ten most important technologies, and its adoption by companies and organizations is improving, according to Gartner [1].

Cloud computing provides simple, wherever, and anytime network connection to customizable computer resources including servers, storage, apps, and services. Service providers and management may easily provide and cancel these resources.

Cloud computing is a distribution architecture and computational paradigm that provides safe, efficient, and easy computing and data storage. This context treats all computer resources as Internet-delivered services [2,3]. Improved cooperation, agility, scalability, availability, demand adaptability, expedited development work, and cost savings via effective and optimal computing are all advantages of the cloud [4–7].

Cloud computing combines SOA, Web 2.0, virtualization, and more. It provides web-based business applications via web browsers. Software and data are stored on servers to meet user computing needs [5]. Cloud computing is a marketing phrase for technological advancements and services [6]. In this way, cloud computing matures these technologies. Cloud Computing has many benefits, but it faces several barriers to adoption. Compliance, privacy, and legal difficulties are major adoption barriers, followed by security [8]. The novelty of Cloud Computing raises questions about the possibility of establishing security measures across all tiers (e.g., network, host, application, and data) and migrating application security to Cloud Computing [9]. Information executives have consistently cited cloud computing security as their top issue due to uncertainty [10].

Vulnerabilities include external data storage, "public" internet use, lack of control, multi-tenancy, and internal security integration. The cloud's wide breadth and completely dispersed, heterogeneous, and virtualized resources set it apart from traditional technology. Traditional cloud security measures including identity verification, authentication, and permission are insufficient [11]. Most cloud computing security policies are similar to those in traditional IT settings. Cloud computing may bring different risks than traditional IT solutions owing to its operational structures, cloud service models, and supporting technologies. Unfortunately, security often makes these solutions more inflexible [4].

Organizations growing outside their data center worry about migrating key apps and sensitive data to public cloud environments. To address these concerns, a cloud solution provider must ensure that clients retain the same security and privacy controls across their services and applications, provide customers with proof that their organizations are secure and can meet service-level agreements, and allow auditors to verify compliance [12].

DOI: 10.48175/568

The SPI model (SaaS, PaaS, and IaaS) is used to classify Cloud Computing security threats in this article. We highlight the main system flaws and highest-level dangers in Cloud Computing and its surrounds literature. A threat is a potential attack that might misuse resources or information, whereas a vulnerability is a system flaw that allows an attack. Some polls focus on a specific service type, while others discuss cloud security risks without distinguishing vulnerabilities and attacks. This paper lists vulnerabilities, threats, and cloud service models that may be affected. We also explain the relationship between these vulnerabilities and threats, explain how these vulnerabilities can be used to launch an attack, and suggest countermeasures to fix or improve the identified issues.

Structure of the paper's succeeding sections: We provide our systematic review results in Section 2. In Section 3, we outline the most important security considerations for each Cloud model stratum. Next, we'll examine cloud computing's security issues to identify the biggest risks and vulnerabilities and every effective defense. In conclusion, we draw some conclusions.

Systematic Review of Security Issues For CloudComputing

A comprehensive review [13-15] examined Cloud Computing security literature. This study sought to identify and evaluate Cloud Computing security concerns and risks and give a full security overview.

Question Formalization

The question sought the most important Cloud Computing security challenges, threats, vulnerabilities, and solutions. This question has to be relevant to this study's goal of identifying vulnerabilities and risks and linking remedies. Our study explored the following research question: Which Cloud Computing security risks and vulnerabilities are most important and demand the most thorough study to manage? Secure cloud systems, cloud security, delivery model security, SPI security, SaaS, PaaS, and IaaS security, threats and vulnerabilities in the cloud, and cloud recommendations and best practices were used to write this question during the review process.

Selection of Sources

The writers used their research expertise to pick study sources. The source selection approach required English-language, internet-accessible research. ScienceDirect, the ACM and IEEE digital libraries, Scholar Google, and DBLP were considered. Specialists will next add major works that were not recovered from these sources and adjust the results to account for other restrictions such impact factor, received citations, prominent journals, authors, etc.

After identifying sources, the study selection and evaluation process had to be defined. The research question determined inclusion and exclusion in this study. The study must address cloud computing security challenges and describe possible threats, vulnerabilities, responses, and hazards.

Review Execution

During this step, search the given sources and evaluate the collected research using preset criteria. After running the search chain on the selected sources, we filtered 120 results using the inclusion criteria to find 40 relevant papers. The exclusion criteria were applied again to this collection of relevant research, yielding a subset that matches fifteen major suggestions [4, 6, 10, 16-27].

II. RESULTS AND DISCUSSION

Table 1 summarizes the systematic review's principles and topics for each technique.

Table 1 shows that most methodologies detect, classify, analyze, and list Cloud Computing-specific vulnerabilities and risks. The studies analyze hazards and dangers and provide prevention or mitigation advice. Consequently, vulnerabilities or dangers and possible remedies and methods are linked. Our analysis shows that several techniques handle threats, vulnerabilities, trust, data security, and security recommendations and processes for cloud environment difficulties.

Security in the Spi Model

The cloud model offers three services [21, 28, 29]:Software as a service is SaaS. The consumer may use the provider's cloud-based apps. The programs are available from various client devices via a thin client interface (e.g., web browser for web-based email).

Platform as a Service. Users may deploy their own apps to the cloud without installing platforms or tools. PaaS provides platform-layer resources like software development frameworks and operating system support for higher-level services.

IaaS is infrastructure-as-a-service. Consumers may provide processing, storage, networks, and other computer resources. These tools allow consumers to run any software, including operating systems and apps.

Cloud providers are responsible for SaaS security. Due to abstraction, the SaaS model has high integrated functionality and low client control or expansion needs. However, PaaS gives consumers more control and flexibility. IaaS gives customers or renters more security control than PaaS and SaaS due to its lower abstraction level [10].

Understanding the linkages and reliances across cloud service models is essential before evaluating cloud computing security issues [4]. PaaS and SaaS are housed on IaaS, therefore any security event there affects them. However, the opposite may be true. PaaS offers a platform for designing and deploying SaaS applications, increasing their security dependency. Any attack on a cloud service tier might damage upper levels due to their interdependencies. Every cloud service architecture has its unique security concerns, but certain difficulties are common. The interdependencies and linkages across cloud models might create security risks. A SaaS provider may rent a development environment from a PaaS provider, which may rent infrastructure from an IaaS provider. Individual service providers must secure their own offers, therefore security approaches may vary. It also makes determining service provider liability in an assault more difficult.

Software-As-A-Service (Saas) Security Issues

Conference software, email, and corporate programs like ERP, CRM, and SCM are available on demand via SaaS [30]. SaaS users have the least security control of the three fundamentals.

Application Security

These apps are usually provided via a browser [12,22]. However, web application shortcomings may make SaaS applications vulnerable. Cybercriminals utilize the internet to hack consumers' devices and steal sensitive data [31]. SaaS apps suffer the same security concerns as traditional online applications, but standard security solutions are inadequate to protect them [21]. The Open online Application Security Project (OWASP) recognized the top 10 online application security threats [32]. While security issues persist, this is a respectable first step toward online application security.

Multi-Tenancy

Scalability, metadata configurability, and multi-tenancy determine SaaS application maturity [30,33]. Each client receives a customized software instance in the first maturity model. This paradigm has several drawbacks, but security issues are lower than with others. In the second paradigm, the vendor provides unique application instances to each customer, but the application code is constant. This type allows customers to choose setup choices. The third maturation paradigm includes multitenancy so one instance may serve all clients [34]. This strategy optimizes resource use but has limited scalability. The chance that many renters' data would be kept in the same database increases the danger of data leakage. Segregating client data requires security rules [35]. Applications for the final model may be moved to a more powerful server to boost scalability.

Data Security

All technologies struggle with data security, but SaaS consumers rely on their suppliers to secure them [12,21,36]. SaaS often processes and stores organizational data in raw text. SaaS providers must secure data throughout processing and storage [30]. Data storage is vital for disaster recovery, but it also poses security issues [21]. Cloud

ISSN 2581-9429 IJARSCT

DOI: 10.48175/568

service providers may outsource backup and other services to other parties, which is concerning. Most cloud computing compliance guidelines do not foresee regulatory compliance [12]. SaaS compliance is complicated since data is kept in provider datacenters. The supplier must implement data privacy, segregation, and security regulations, which may arise.

Accessibility

Web browsers provide access to internet applications from mobile devices and public workstations. However, this undermines service security. The Cloud Security Alliance produced a report on mobile computing and its top dangers [37]. Mobile malware that steals data, unsecured WiFi networks, weaknesses in the OS system and official apps, insecure marketplaces, and proximity-based hacking are the risks.

Platform-As-A-Service (Paas) Security Issues

PaaS lets you deploy cloud-based apps without buying and maintaining the software and hardware [21]. PaaS needs a reliable browser and network like SaaS and IaaS. Customer applications deployed on a PaaS platform have two software layers: runtime engine security and application security [10]. PaaS providers must secure the platform software architecture, which includes the runtime engine used to run client applications. Similar to SaaS, PaaS poses data security problems and extra challenges:

Third-Party Relationships

PaaS offers third-party online services, including mashups, together with traditional programming languages [10,38]. Mashups combine source components. Thus, PaaS models inherit mashup security problems, including data and network security [39]. PaaS users must also use third-party services and web-hosted development tools for security.

Development Life Cycle

Secure cloud-hosted application development is difficult. Cloud application growth will affect security and SDLC [12,24]. Developers must adjust their application development techniques since PaaS apps should be regularly updated [19]. Developers must understand that tampering with PaaS components might compromise application security. Developers must know data legislation and safe development approaches to avoid storing data in improper places. Data held in several legal systems may endanger its security and privacy.

Underlying Infrastructure Security

As PaaS limits developer access to the underlying layers, suppliers must protect both the application services and infrastructure [40]. Developers distrust PaaS development environment technologies despite having control over application security.

To conclude, PaaS security literature is scarce. SaaS is web-delivered software, whereas PaaS provides development tools. However, both may leverage multi-tenant designs to let numerous users use the same program. As indicated above, cloud servers hold PaaS applications and user data, which may constitute a security concern. Both PaaS and SaaS connect data to cloud apps. The supplier must protect this data throughout transmission, storage, and processing.

Infrastructure-As-A-Service (Iaas) Security Issues

IaaS delivers virtualized servers, storage, networks, and other computer services via the Internet [24]. Users may execute any program with complete resource management [18]. As long as the virtual machine monitor has no security holes, IaaS gives cloud consumers stronger security control than other methods [21]. They manage virtual machine software and establish security rules [41]. The computation, network, and storage infrastructure is managed by cloud providers. IaaS providers must protect their systems to reduce vulnerabilities from creation, communication, monitoring, modification, and mobility [42]. IaaS security problems include these.

Virtualization

Virtualization lets users build, clone, distribute, move, and roll back virtual computers to execute various applications [43,44]. Due to the additional layer to secure, attackers have greater options [31]. Both physical and virtual machine security are critical, because flaws in one may impact the other [19]. All sorts of assaults may target virtualized infrastructures, but security is harder since virtualization introduces additional ports of entry and connectivity complexity [45]. Unlike traditional servers, VMs have physical and virtual limits [24].

Virtual Machine Monitor

The Virtual Machine Monitor (VMM) or hypervisor isolates virtual machines, thus if it's compromised, so may its virtual machines. Low-level VMM software manages and monitors virtual machines, hence it has security weaknesses like any other program [45]. Since vulnerabilities are simpler to identify and correct, keeping the VMM simple and small minimizes security risks.

Virtualization allows virtual machine migration between physical servers for fault tolerance, load balancing, and maintenance [16,46]. This handy feature might cause security issues [42,43,47]. An attacker may exploit the VMM migration module and move a victim virtual machine to a hostile server. Since VM migration exposes VM material to the network, data integrity and confidentiality may be compromised. Migrating a malicious virtual machine to another host (with another VMM) compromises it.

The same server may host shared resource VMs that share CPU, memory, I/O, and more. Sharing resources may reduce VM security. A rogue VM may infer information about other VMs from shared memory or other resources without compromising the hypervisor [46]. Using covert channels, two VMs may evade all VMM security module restrictions [48]. Thus, a malicious Virtual Machine may monitor shared resources without its VMM noticing, allowing the attacker to deduce information about other virtual machines.

Public VM Image Repository

In IaaS setups, VM images are prepackaged software templates with VM configuration files. Thus, these photos are crucial to cloud security [46,49]. One may make her own VM image or utilize one from the provider's repository. For instance, Amazon provides a public repository for lawful users to download or publish VM images. malevolent people may store photos with malicious code in public repositories, compromising other users or the cloud [20,24,25]. An attacker with a legitimate account may generate a Trojan horse picture. This picture will infect another customer's virtual computer with concealed spyware. Additionally, VM replication might mistakenly disclose data [20]. Passwords and cryptographic keys may be recorded during picture creation. If the picture is not "cleaned," other users might see sensitive information. Dormant VM images are challenging to fix offline [50].

Virtual Machine Rollback

If a mistake occurs, virtual machines may be reverted. However, rolling back virtual machines might expose them to corrected security vulnerabilities or enable disabled accounts or passwords. We must produce a “copy” (snapshot) of the virtual machine to offer rollbacks, which might propagate configuration problems and other vulnerabilities [12,44].

Virtual Machine Life Cycle

Understanding the lifespan of VMs and their state changes in the environment is also crucial. VMs might be on, off, or suspended, making virus detection difficult. Even offline virtual computers may be susceptible [24]; a picture with malicious code can start a virtual machine. These bad pictures may spread malware by inserting code into other virtual machines during construction.

Virtual Networks

Tenants share network components owing to resource pooling. Sharing resources enables cross-tenant assaults [20]. Virtual Networks enhance VM connectivity, a Cloud Computing security issue [51]. Dedicated physical channels are the safest approach to connect VMs to hosts. Virtual networks connect VMs to interact more directly and effectively in most hypervisors. Most virtualization technologies like Xen provide bridged and routed virtual network configurations, however these methods raise the risk of spying and spoofing [45,52].

Analysis of Security Issues In Cloud Computing

We study current Cloud Computing security vulnerabilities and threats. We determine which cloud service models are impacted by each vulnerability and threat.Cloud computing vulnerabilities are examined. This research briefly describes the vulnerabilities and which cloud service models (SPI) are vulnerable. We concentrate on technology-based vulnerabilities in our research, but additional weaknesses that are common to every company might severely influence cloud and platform security. The following vulnerabilities exist:

Poor recruiting and staff screening [16] — some cloud providers do not screen their workers or vendors. User privileges like cloud administrators normally provide limitless data access. Most cloud providers do not verify customer backgrounds, so anybody with a credit card and email may sign up. Apocryphal accounts allow attackers to do any crime undetected [16]. Without security education, humans remain a weakness in information security [53]. This is true in any organization, but in the cloud, it has a stronger influence since more individuals engage with it: cloud providers, third-party providers, suppliers, organizational clients, and end-users.

Cloud computing uses online services, browsers, and virtualization to evolve cloud environments. Thus, any weakness in these technologies impacts the cloud and might be significant.

Data storage and virtualization are the most important and may be most damaged by an attack. Lower layer attacks affect other levels more. Cloud Computing Threats Overview. It also covers cloud technology dangers and which cloud service models are vulnerable. We prioritize dangers from distant data storage and processing, resource sharing, and virtualization.

Threats may exploit flaws to compromise systems. This research also seeks to discover defenses against these dangers. Misuse patterns may clarify this [62]. Attacker misuse patterns illustrate how misuses are committed. Threat T10 allows attackers to view or modify VM state files during live migration. This is conceivable because VM migration transfers data via unsecure network channels like the Internet. The following methods may prevent insecure VM migration: TCCP [63] secures VM execution and migration. PALM [64] suggests a safe migration mechanism for VM live migration, requiring an active VMM-protected system. The 11th cloud danger involves an attacker creating a malicious VM image with any virus or malware. This vulnerability is possible because any valid user may post VM images in the provider's repository for other users to download. Malware in the malicious VM image will infect other VMs. Mirage, an image management system, addresses this problem [49]. Access control, picture filters, provenance tracking, and repository maintenance are its security features.

Countermeasures for T01: Account or Service Hijacking

ID/access management advice Cloud Security Alliance (CSA) is a non-profit that supports cloud security best practices. CSA's Identity and Access Management Guidance [65] recommends best practices for identity and access management. Centralized directory, access management, identity management, role-based access control, user access certifications, privileged user and access management, separation of roles, and identity and access reporting are covered in this paper.

A dynamic credentials technique for mobile cloud computing systems is presented [66]. The dynamic credential updates when a user moves or exchanges a certain amount of data packets.

Countermeasures for T03: Data Leakage

Intrusion tolerance and safe storage are the goals of fragmentation-redundancy-scattering (FRS) [67]. This method initially breaks sensitive data into inconsequential pieces so each fragment has no meaningful information. Fragments are then redundantly disseminated among distributed system locations. Digital signatures [68] suggest utilizing RSA algorithm to safeguard Internet data transfers. They stated that RSA, the most famous algorithm, can safeguard cloud data.

The homomorphic encryption In the cloud, data is sent, stored, and processed. Data transported in and out of the cloud or kept at the provider may be encrypted. Cloud providers must decrypt encrypted data to handle it, raising privacy issues. In [70], they propose cloud security using fully homomorphic encryption. Fully homomorphic encryption lets ciphertexts be computed without decryption. Some homomorphic encryption algorithms offer addition and multiplication. The authors [77] described real-world cloud applications that need fundamental homomorphic computations. Its massive computing power may slow user reaction time and electricity usage.

Encryption Encryption has historically protected sensitive data. Cloud storage of encrypted data ensures data security. This is true if encryption techniques are powerful. Some popular encryption techniques include AES. SSL may also safeguard data in transit. Encryption may prevent side channel attacks on cloud storage de-duplication, but it may allow offline dictionary attacks that reveal personal keys [69].

Countermeasures for T05: Customer Data Manipulation

Web app scanners Web apps are vulnerable to attackers since they are public. Web application scanners [71] examine web applications' front-ends for security flaws. Other web application security techniques include firewalls. All web traffic passes via the web application firewall, which checks for risks.

DOI: 10.48175/568

Countermeasures for T06: VM Escape

HyperSafe [60] This method ensures hypervisor control-flow integrity. HyperSafe safeguards type I hypervisors using non-bypassable memory lockup and restricted pointed indexing, which turns control data into pointer indexes. This strategy was tested by modifying the hypervisor code, executing the injected code, modifying the page table, and tampering with a return table. They found that HyperSafe stopped all these attacks and had negligible performance overhead.

Trusted Cloud Computing Platform Tccp

Allows providers to deliver closed box execution environments and lets consumers check for security before starting VMs. TCCP adds a trusted virtual machine monitor (TVMM) and a trusted coordinator. A trustworthy third party maintains the TC managed list of trusted nodes running TVMMs. The TC checks VMs operating on trustworthy platforms before starting or transferring them. The authors [78] suggested that TCCP has a major drawback since all transactions must check with the TC, causing an overload. The proposed solution was Direct Anonymous Attestation (DAA) and Privacy CA.

The trusted virtual datacenter TVDc [73,74] ensures cloud isolation and integrity. It organizes virtual computers with similar goals into Trusted Virtual Domains. Through obligatory access control, hypervisor-based isolation, and secured communication routes like VLANs, TVDc isolates workloads. TVDc verifies system integrity via load-time attestation.

Countermeasures for T08: Malicious Virtual Machine Creation

Mirage A cloud-based virtual machine image management system is proposed in [49]. This method incorporates access control, picture filters, provenance tracking, and repository maintenance. However, filters may not detect all viruses or erase all sensitive data from photos. Running these filters may pose privacy issues since they may access picture content, which may include customer data.

Countermeasures for T09: Insecure Virtual Machine Migration

PALM [64] presents a secure live migration architecture that protects integrity and privacy during and after migration. The prototype was developed using Xen and GNU Linux, and the evaluation indicated that encryption and decryption only adds modest downtime and migration time.

VNSS [52] introduces a security architecture that customizes security settings for each virtual machine and provides continuous protection during live migration. A prototype system combining stateful firewall technologies and userspace tools like iptables, xm commands, and conntrack-tools was developed on Xen hypervisors. The authors tested their framework and found that security controls are in place during live migration.

Countermeasures for T010: Sniffing/Spoofing Virtual Networks

Virtual network security Wu and et al. [51] provide a virtual network architecture that protects virtual machine communication. This framework uses Xen's “bridged” and “routed” virtual network configurations. Routing layers, firewalls, and shared networks prohibit VM spying and spoofing in the virtual network concept. The technique was not evaluated when this paper was released.

Web services also dominate cloud implementations. Web services provide various issues that must be handled. Security web services standards protect application communication with integrity, secrecy, authentication, and permission. SAML, WS-Security, XACML, XML Digital Signature, XML Encryption, XKMS, WS-Federation, WS-Secure Conver-sation, WS-Security Policy, and WS-Trust are security standards [79]. NIST Cloud Computing Standards Roadmap Working Group has gathered high-level Cloud Computing standards.

III. CONCLUSION

Cloud computing is a novel idea with many advantages, but security issues may impede its usage. Understanding Cloud Computing vulnerabilities can help firms go to the Cloud. Because Cloud Computing uses various technologies, it inherits their security vulnerabilities. Web applications, data hosting, and virtualization have been examined, however some solutions are immature or nonexistent. We discussed security challenges for IaaS, PaaS, and IaaS cloud models, which differ. Storage, virtualization, and networks are Cloud Computing's major security risks, according to this report. Cloud users worry about virtualization, which lets several users share a physical server. Another issue is that various virtualization systems handle security procedures differently. Some attacks target virtual networks, particularly when connecting with distant virtual computers.

Some polls have examined cloud security without distinguishing vulnerabilities and threats. We examined this difference to better comprehend these challenges. It was not enough to list these security concerns; we also created a link between threats and vulnerabilities to discover the weaknesses that contributed to their execution and make the system more resistant. Some existing remedies were presented to minimize these dangers. The cloud architecture requires new security methods and reworked existing solutions. Traditional security techniques may not operate effectively in cloud settings due to their complicated design and mix of technologies.

REFERENCES

[1]. Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011

[2]. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358

[3]. Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93–97

[4]. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf

[5]. Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg

[6]. Centre for the Protection of National Infrastructure (2010) Information Security Briefing 01/2010 Cloud Computing. Available: http://www.cpni.gov. uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

[7]. Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10), pp 278–281

[8]. KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey.. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future- kpmgs-2010-cloud-computing-survey/2384291

[9]. Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487

[10]. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA

[11]. Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69–79

[12]. Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press

[13]. Kitchenham B (2004) Procedures for perfoming systematic review, software engineering group. Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd, Australia. TR/SE-0401

[14]. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering. Version 2.3 University of keele (software engineering group, school of computer science and mathematics) and Durham. Department of Conputer Science, UK

[15]. Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M (2007) Lessons from applying the systematic literature review process within the software engineering domain. J Syst Softw 80(4):571–583

[16]. Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats

[17]. ENISA (2009) Cloud Computing: benefits, risks and recommendations for information Security. Available: http://www.enisa.europa.eu/activities/risk- management/files/deliverables/cloud-computing-risk-assessment

[18]. Dahbur K, Mohammad B, Tarakji AB (2011) A survey of risks, threats and vulnerabilities in Cloud Computing. In: Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. Amman, Jordan, pp 1–6

[19]. Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42

[20]. Grobauer B, Walloschek T, Stocker E (2011) Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 9(2):50–57

[21]. Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1–11

[22]. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical Security issues in Cloud Computing. In: IEEE International conference on Cloud Computing (CLOUD'09). 116, 116, pp 109–116

[23]. Onwubiko C (2010) Security issues to Cloud Computing. In: Antonopoulos N, Gillam L (ed) Cloud Computing: principles, systems & applications. 2010, Springer-Verlag

[24]. Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia

[25]. Jansen WA (2011) Cloud Hooks: Security and Privacy Issues in Cloud Computing. In: Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI. IEEE Computer Society, Washington, DC, USA, pp 1–10

[26]. Zissis D, Lekkas D (2012) Addressing Cloud Computing Security issues. Futur Gener Comput Syst 28(3):583–592

[27]. Jansen W, Grance T (2011) Guidelines on Security and privacy in public Cloud Computing. NIST, Special Publication 800–144, Gaithersburg, MD

[28]. Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD

[29]. Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications 1(1):7–18

[30]. Ju J, Wang Y, Fu J, Wu J, Lin Z (2010) Research on Key Technology in SaaS. In: International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp 384–387

[31]. Owens D (2010) Securing elasticity in the Cloud. Commun ACM 53(6):46–51

[32]. OWASP (2010) The Ten most critical Web application Security risks. Available: https://www.owasp.org/index.php/Category: OWASP_Top_Ten_Project

[33]. Zhang Y, Liu S, Meng X (2009) Towards high level SaaS maturity model: methods and case study. In: Services Computing conference. APSCC, IEEE Asia-Pacific, pp 273–278

[34]. Chong F, Carraro G, Wolter R (2006) Multi-tenant data architecture. Online. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx. Accessed: 05-Jun-201

[35]. Bezemer C-P, Zaidman A (2010) Multi-tenant SaaS applications: maintenance dream or nightmare? In: Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), Antwerp, Belgium. ACM New York, NY, USA, pp 88–92

[36]. Viega J (2009) Cloud Computing and the common Man. Computer 42 (8):106–108 Cloud Security Alliance (2012) Security guidance for critical areas of Mobile Computing. Available: https://downloads.cloudsecurityalliance.org/initiatives/ mobile/Mobile_Guidance_v1.pdf

[37]. Keene C (2009) The Keene View on Cloud Computing. Online. Available: http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html. Accessed: 16-Jul-2011

[38]. Xu K, Zhang X, Song M, Song J (2009) Mobile Mashup: Architecture, Challenges and Suggestions. In: International Conference on Management and Service Science. MASS'09. IEEE Computer Society, Washington, DC, USA, pp 1–4

[39]. Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16 (3):23–25

[40]. Jaeger T, Schiffman J (2010) Outlook: cloudy with a chance of Security challenges and improvements. IEEE Security Privacy 8(1):77–80

[41]. Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. In: the 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany. IEEE Computer Society, Washington, DC, USA, pp 1–8

[42]. Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35–41

[43]. Garfinkel T, Rosenblum M (2005) When virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. USENIX Association Berkeley, CA, USA, pp 227–229

[44]. Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007

[45]. Hashizume K, Yoshioka N, Fernandez EB (2013) Three misuse patterns for Cloud Computing. In: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M (ed) Security engineering for Cloud Computing: approaches and Tools. IGI Global, Pennsylvania, United States, pp 36–53

[46]. Venkatesha S, Sadhu S, Kintali S (2009) Survey of virtual machine migration techniques., Technical report, Dept. of Computer Science, University of California, Santa Barbara. http://www.academia.edu/760613/

[47]. Ranjith P, Chandran P, Kaleeswaran S (2012) On covert channels between virtual machines. Journal in Computer Virology Springer 8:85–97

[48]. Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp 91–96

[49]. Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21

[50]. Xiaopeng G, Sumei W, Xianqin C (2010) VNSS: a Network Security sandbox for virtual Computing environment. In: IEEE youth conference on information Computing and telecommunications (YC-ICT). IEEE Computer Society, Washington DC, USA, pp 395–398

[51]. Popovic K, Hocenski Z (2010) Cloud Computing Security issues and challenges. In: Proceedings of the 33rd International convention MIPRO. IEEE Computer Society Washington DC, USA, pp 344–349

[52]. Carlin S, Curran K (2011) Cloud Computing Security. International Journal of Ambient Computing and Intelligence 3(1):38–46

[53]. Bisong A, Rahman S (2011) An overview of the Security concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications (IJNSA) 3(1):30–45

[54]. Townsend M (2009) Managing a security program in a cloud computing environment. In: Information Security Curriculum Development Conference, Kennesaw, Georgia. ACM New York, NY, USA, pp 128–133

[55]. Winkler V (2011) Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier Inc, Waltham, MA

[56]. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA. ACM New York, NY, USA, pp 199–212

[57]. Zhang Y, Juels A, Reiter MK, Ristenpart T (2012) Cross-VM side channels and their use to extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security, New York, NY, USA. ACM New York, NY, USA, pp 305–316

[58]. Wang Z, Jiang X (2010) HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity. In: Proceedings of the IEEE symposium on Security and privacy. IEEE Computer Society, Washington, DC, USA, pp 380–395

[59]. Wang C, Wang Q, Ren K, Lou W (2009) Ensuring data Storage Security in Cloud Computing. In: The 17th International workshop on quality of service. IEEE Computer Society, Washington, DC, USA, pp 1–9

[60]. Fernandez EB, Yoshioka N, Washizaki H (2009) Modeling Misuse Patterns. In: Proceedings of the 4th Int. Workshop on Dependability Aspects of Data Warehousing and Mining Applications (DAWAM 2009), in conjunction with the 4th Int.Conf. on Availability, Reliability, and Security (ARES 2009), Fukuoka, Japan. IEEE Computer Society, Washington, DC, USA, pp 566–571

[61]. Santos N, Gummadi KP, Rodrigues R (2009) Towards Trusted Cloud Computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California. USENIX Association Berkeley, CA, USA

[62]. Zhang F, Huang Y, Wang H, Chen H, Zang B (2008) PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In: Trusted Infrastructure Technologies Conference, 2008. APTC'08, Third Asia- Pacific. IEEE Computer Society, Washington, DC, USA, pp 9–18

[63]. Xiao S, Gong W (2010) Mobility Can help: protect user identity with dynamic credential. In: Eleventh International conference on Mobile data Management (MDM). IEEE Computer Society, Washington, DC, USA, pp 378–380

[64]. Wylie J, Bakkaloglu M, Pandurangan V, Bigrigg M, Oguz S, Tew K, Williams C, Ganger G, Khosla P (2001) Selecting the right data distribution scheme for a survivable Storage system. CMU-CS-01-120, Pittsburgh, PA

[65]. Somani U, Lakhani K, Mundra M (2010) Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In: 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, pp 211–216

DOI: 10.48175/568