ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

AN EVALUATION OF PROTECTION PROBLEMS FOR CLOUD COMPUTING

R.Arun*, Ram Kumar
Saveetha School of Engineering, Saveetha University, Chennai.

Received on 10-08-2016 *Accepted on 06-09-2016*

Abstract

Cloud Computing is a flexible, fee-effective, and verified shipping platform for providing business or customer IT offerings over the internet. however, cloud Computing offers an delivered level of chance because important services are often outsourced to a 3rd party, which makes it more hard to protect records security and security, bolster truths and supplier accessibility, and display consistence. Distributed computing influences numerous innovation sit additionally acquires their security issues, which we examine right here, distinguishing the essential vulnerabilities in this sort of frameworks and the most basic dangers found in the writing connected with Cloud Computing and its surroundings and in addition to end up mindful of and relate vulnerabilities and dangers with conceivable answers. The incomplete data we consider incorporates amassed portrayal of sub networks, and neighbourhood states from wavelength converters. We cast the light-way evaluation as a choice issue, and characterize the execution as the hood of incorrect choice. Cloud storage has quickly turned into a foundation of numerous IT frameworks, constituting a consistent answer for the reinforcement, synchronization, and sharing of a lot of information. Putting client information in the immediate control of cloud administration suppliers, be that as it may, raises security and protection concerns related to the uprightness of outsourced information.

Keywords

Cloud Computing, Cloud Backup, Cloud Database, Distributed Computing, Cloud Management.

Introduction

The importance of Cloud Computing is expanding and it is getting a creating enthusiasm inside the clinical and mechanical gatherings. An observe by method for Gartner contemplated Cloud Computing as the main a large number of the main 10 most crucial innovation and with a superior prospect in progressive years with the guide of organizations and associations. Distributed computing permits omnipresent, handy, on-call for group motivate admission to a mutual pool of configurable processing sources (e.g., systems, servers, carport, bundles, and

administrations) that can be hurriedly provisioned and discharged with least administration exertion or supplier guarantor interaction. Cloud Computing appears as a computational worldview not withstanding a dispersion structure and its principal objective is to give secure, short, helpful data stockpiling and web registering bearer, with all figuring sources imagined as offerings and presented over the web. The cloud supplements cooperation, readiness, versatility, accessibility, ability to fit in with vacillations with regards to request, support up advancement works of art, and presents capacity for value lessening through streamlined and green figuring .Cloud Computing joins some of processing ideas and advances, for example, bearer situated design (SOA), web 2.zero, virtualization and other innovation with dependence at the web, giving ordinary business programs on-line through net programs to satisfy the registering goals of clients, in the meantime as their product program and records are saved money on the servers. In a few regards, Cloud Computing speaks to the developing of those innovations and is a promoting term to speak to that adulthood and the administrations they offer. Despite the fact that there are numerous preferences to receiving Cloud Computing, there additionally are a couple of sizable constraints to reception. One of the most extreme tremendous hindrances to appropriation is wellbeing, joined by issues concerning consistence, security and lawful offense points. Because of the reality Cloud Computing speaks to an outstandingly new registering adaptation, there might be a fabulous arrangement of vulnerability about how security at all extents (e.g., system, host, application, and measurements levels) should be possible and the way programs assurance is moved to Cloud Computing. That instability has continually driven data officials to nation that wellbeing is their main test with Cloud Computing security issues identify with danger districts comprehensive of outside data stockpiling, reliance at "general society" web, absence of oversee, multi-occupancy and joining with inward security. In contrast with customary innovations, the cloud has numerous exact capacities, together with its monstrous scale and the truth that advantages having a place with cloud merchants are totally dispersed, heterogeneous and total virtualized. Customary security instruments together with recognizable proof, confirmation, and approval are insufficient for billows of their present structure. Insurance controls in Cloud Computing are, for the most component, the same than security controls in any IT environment. Be that as it may, as a result of the cloud supplier models procured, the operational models, and the innovation used to permit cloud offerings, Cloud Computing may likewise blessing exceptional dangers to an organization than routine IT arrangements. Tragically, coordinating security into those arrangements is oftentimes seen as making them additional firm. Exchanging vital projects and sensitive data to open cloud situations is of wonderful trouble for those organizations that are moving past their actualities centre’s system under their oversee. to

mitigate these issues, a cloud answer organization ought to ensure that customers will hold to have the indistinguishable security and protection controls over their projects and administrations, offer confirmation to customers that their endeavour are secure and they could meet their administration level assentation's, and that they can demonstrate consistence to inspectors.

Systematic review of protection issues for cloud computing

We have finished a precise appraisal of the present writing concerning insurance in Cloud Computing, now not best so one can abridge the current vulnerabilities and dangers concerning this topic however also to find and analyze the bleeding edge country and the most critical security issues for Cloud Computing.

Query for malization

The question acknowledgment changed into to distinguish the most important issues in Cloud Computing which bear in mind vulnerabilities, dangers, dangers, necessities and arrangements of security for Cloud Computing. This inquiry must be connected with the objective of this work; this is to choose and relate vulnerabilities and dangers with conceivable answers. Thus, the examination question tended to by means of our studies turn into the accompanying: What wellbeing vulnerabilities and dangers are the most extreme basic in Cloud Computing which must be contemplated top to bottom with the reason of managing them. The watchwords and related ideas that make up this inquiry and that had been utilized at some phase as a part of the audit execution are: quiet Cloud frameworks, Cloud wellbeing, shipping models security, SPI insurance, SaaS assurance, Pa as security, IaaS safety, Cloud dangers, Cloud vulnerabilities, Cloud rules, top notch rehearses in Cloud.

Three selection of resources

The decision models through which we assessed watch resources got to be founded on the studies experience of the writers of this compositions, and with an end goal to choose these advantages we have mulled over specific requirements: research ensured in the picked sources should be composed in English and those assets should be net-to be had. the accompanying rundown of assets has been mulled over: Science Direct, ACM advanced library, IEEE computerized library, understudy Google and DBLP .Later, the experts will refine the outcomes and could incorporate fundamental works that had now not been recouped in those sources and will upgrade these work examining different imperatives which incorporate effect viewpoint, got refers to, crucial diaries, prestigious creators, and so forth when the assets were characterized, it get to be vital to depict the method and the benchmarks for watch choice and assessment. The incorporation and rejection criteria of this take a gander at have been construct absolutely

in light of the examination question. We subsequently settled that the studies need to incorporate issues and subjects which check security on Cloud Computing, and that those exploration must depict dangers, vulnerabilities, countermeasures, and threats.

Four evaluate execution

At some point of this section, the search within the defined assets should be done and the received studies have to be evaluated according to the installed standards. After executing the seek chain on the selected sources we acquired a set of approximately a hundred and twenty results which were filtered with the inclusion criteria to give a set of about 40 relevant research. This set of applicable research was once more filtered with the exclusion criteria to give a fixed of studies which corresponds with 15 number one proposals.

Effects and discussion

The consequences of the systematic assessment are summarized in desk 1 which suggests a precis of the topics and ideas taken into consideration for every approach. As it is proven in desk 1, most of the techniques discussed become aware of, classify, analyze, and listing some of vulnerabilities and threats targeted on Cloud Computing. The studies analyze the risks and threats, frequently deliver guidelines on how they can be prevented or blanketed, resulting in a direct courting among vulnerability or threats and viable answers and mechanisms to clear up them. In addition, we will see that in our search, a lot of the approaches, further to speaking about threats and vulnerabilities, also discuss other problems associated with security in the Cloud including the information safety, trust, or protection suggestions and mechanisms for any of the problems encountered in these environments.

Security inside the SPI version: The cloud version affords three forms of offerings:

1. Software as a service (SaaS).

The functionality supplied to the customer is to use the provider's programs jogging on a cloud infrastructure. The programs are on hand from numerous purchaser gadgets through a thin consumer interface inclusive of an internet browser (e.g., web-based totally electronic mail).

2. Platform as a provider (PaaS).

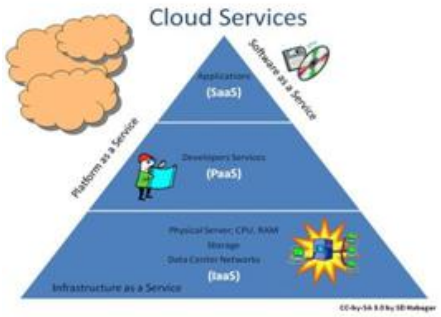
The capability furnished to the purchaser is to deploy onto the cloud infrastructure his very own programs without installing any platform or equipment on their nearby machines. PaaS refers to imparting platform layer sources, inclusive of running device aid and software program improvement frameworks that can be used to build better-stage services.

3. Infrastructure as a carrier (IaaS).

The functionality provided to the customer is to provision processing, storage, networks, and other fundamental computing sources in which the customer is capable of deploy and run arbitrary software program, which could include operating structures and applications. With SaaS, the burden of security lies with the cloud provider. In part, that is due to the degree of abstraction, the SaaS version is based totally on an excessive diploma of incorporated functionality with minimal patron manage or extensibility. by means of comparison, the PaaS version gives extra extensibility and more purchaser manage. Largely because of the notably lower degree of abstraction, IaaS offers greater tenant or client control over protection than do PaaS or SaaS .Before studying protection challenges in Cloud Computing, we need to understand the relationships and dependencies between those cloud carrier models. PaaS as well as SaaS are hosted on pinnacle of IaaS; as a consequence, any breach in IaaS will affect the safety of both PaaS and SaaS offerings, however also it can be true on the other manner around. However, we must remember the fact that PaaS gives a platform to build and installation SaaS applications, which increases the safety dependency between them. As a result of these deep dependencies, any attack to any cloud provider layer can compromise the top layers. Every cloud carrier version comprises its personal inherent security flaws; however, additionally they proportion a few challenges that have an effect on them all. Those relationships and dependencies among cloud models might also be a source of safety risks. A SaaS issuer might also lease a improvement surroundings from a PaaS provider, which may also hire an infrastructure from an IaaS company. Every issuer is chargeable for securing his personal offerings, which can also result in an inconsistent mixture of security fashions. It also creates confusion over which Provider Company is accountable as soon as an assault occurs.

Software-as-a-carrier (SaaS) security troubles

SaaS affords application offerings on demand which includes e mail, conferencing software program, and business packages along with ERP, CRM, and SCM. SaaS customers have much less manage over protection most of the three fundamentaldelivery models in the cloud. The adoption of SaaS packages may improve a few security issues.



Software protection

Those applications are typically introduced thru the net thru a web browser. However, flaws in net packages may additionally create vulnerabilities for the SaaS programs. Attackers have been the usage of the internet to compromise user's computers and perform malicious sports such as thief's sensitive data. Safety demanding situations in SaaS packages aren't exclusive from any internet software generation; however conventional security solutions do now not successfully protect it from attacks, so new processes are essential. The Open net utility protection project (OWASP) has recognized the 10 most critical net packages security threats. There are extra security troubles, but it is a superb start for securing net applications.

Data protection

Facts safety is a common challenge for any era, however it turns into a chief venture when SaaS users have to depend upon their companies for correct security .In SaaS, organizational data is frequently processed in plaintext and stored inside the cloud. The SaaS issuer is the one liable for the safety of the information at the same time as is being processed and saved. Additionally, records backup is a essential thing in an effort to facilitate restoration in case of catastrophe, however it introduces protection worries as well .also cloud companies can subcontract different offerings such as backup from third-birthday celebration carrier vendors, which may additionally boost worries. Furthermore, maximum compliance standards do now not envision compliance with rules in a international of Cloud Computing . inside the world of SaaS, the method of compliance is complex because information is placed within the company's datacenters, which may additionally introduce regulatory compliance troubles along with statistics privatives, segregation, and security, that ought to be enforced with the aid of the company.

Accessibility: Getting access to applications over the internet thru web browser makes access from any network device easier, such as public computer systems and cell gadgets. however, it additional exposes the carrier to additional security risks. The Cloud protection Alliance has launched a document that describes the present day state of cellular computing and the top threats on this location which include records stealing cell malware, insecure networks (Wi-Fi), vulnerabilities determined inside the tool OS and legitimate applications, insecure marketplaces, and proximity-primarily based hacking.

Platform-as-a-provider (PaaS) security issues

PaaS helps deployment of cloud-primarily based packages without the fee of buying and retaining the underlying hardware and software program layers . As with SaaS and IaaS, PaaS depends on a relaxed and dependable network

and relaxed internet browser. PaaS utility security incorporates two software program layers: safety of the PaaS platform itself (i.e., runtime engine), and safety of consumer programs deployed on a PaaS platform. PaaS companies are accountable for securing the platform software program stack that includes the runtime engine that runs the client packages. Equal as SaaS, PaaS also brings records security issues and other challenges which are described as follows:

1/3-birthday celebration relationships

Moreover, PaaS does not best offer traditional programming languages, however additionally does it provide 0.33-celebration web services additives inclusive of mashups. Mashups integrate multiple source elements into a single integrated unit. Accordingly, PaaS models additionally inherit protection \problems associated with mashups which include information and community protection. Also PaaS customers need to rely on both the security of internet-hosted development equipment and 1/3-birthday party services.

Improvement lifestyles Cycle

From the angle of the application development, builders face the complexity of constructing copy applications that can be hosted within the cloud. The speed at which Packages will change in the cloud will affect each the system improvement lifestyles Cycle (SDLC) and safety. Developers have to remember that PaaS packages have to be upgraded frequently, so that they must make sure that their software improvement tactics are bendy enough to preserve up with modifications. However, builders also should remember that any adjustments in PaaS additives can compromise the protection in their packages. Besides at ease development techniques, developers need to be knowledgeable about facts criminal problems as nicely, so that statistics isn't saved in beside the point locations. Information may be saved on specific locations with special prison regimes that may compromise its privacy and security.

Infrastructure-as-a-provider (IaaS) protection problems

IaaS offers a pool of assets such as servers, garage, networks, and other computing assets in the shape of virtualized systems, which are accessed through the internet. Users are entitled to run any software with full manage and control on the resources allotted to them. With IaaS, cloud customers have better manipulate over the safety as compared to the other fashions as long there may be no protection hole inside the digital gadget Reveal. They manage the software running in their virtual machines, and they're responsible to configure protection regulations successfully. However, the underlying compute, community, and storage infrastructure is controlled through cloud providers. IaaS vendors

should undertake a sizable effort to comfortable their structures which will reduce those threats that result from advent, conversation, monitoring, modification, and mobility. Right here are some of the security problems related to IaaS.

Virtualization

Virtualization permits customers to create, replica, share, migrate, and roll lower back digital machines, which can also allow them to run a diffusion of applications. However, it also introduces new possibilities for attackers due to the greater layer that must be secured. Digital system security becomes as crucial as bodily system security, and any flaw in both one may have an effect on the opposite. Virtualized environments are vulnerable to all kinds of assaults for everyday infrastructures; but, safety is a greater mission as virtualization provides greater points of entry and extra interconnection complexity. Unlike physical servers, VMs have barriers: physical and virtual.

Virtual machine motor

The virtual machine reveals (VMM) or hypervisor is accountable for digital machines isolation; therefore, if the VMM is compromised, its virtual machines may additionally doubtlessly be compromised as properly. The VMM is a low-level software that controls and video display units its digital machines, so as any traditional software program it involves protection flaws. Reserving the VMM as easy and small as feasible reduces the danger of security vulnerabilities, when you consider that it is going to be less complicated to discover and attach any vulnerability. Furthermore, virtualization introduces the capacity to migrate virtual machines between physical servers for fault tolerance, load balancing or maintenance. This useful feature also can increase security issues. An attacker can compromise the migration module in the VMM and transfer a victim digital gadget to a malicious server. additionally, it is clean that VM migration exposes the content of the VM to the community, which could compromise its information integrity and confidentiality. A malicious digital device may be migrated to another host (with another VMM) compromising it.

Evaluation of safety troubles in cloud computing

We systematically examine now present safety vulnerabilities and threats of Cloud Computing. For every vulnerability and threat, we discover what cloud carrier version or models are suffering from those protection problems. an evaluation of vulnerabilities in Cloud Computing. This evaluation gives a brief description of the vulnerabilities, and suggests what cloud service fashions (SPI) may be tormented by them. For this evaluation, we cognizance especially on technology-based totally vulnerabilities; however, there are other vulnerabilities which can

be not unusual to any business enterprise, but they ought to be taken in consideration for the reason that they can negatively impact the security of the cloud and its underlying platform. a few of those vulnerabilities are the subsequent:

1. Lack of worker screening and negative hiring practices

Some cloud companies may not perform heritage screening in their personnel or carriers. Privileged customers such as cloud administrators normally have unlimited get admission to the cloud records.

2 .Lack of customer historical past exams

Most cloud providers do now not test their purchaser's historical past, and almost all people can open an account with a valid credit score card and e-mail. Apocryphal debts can allow attackers carry out any malicious activity without being identified.

3. Loss of protection training

Humans continue to be a susceptible point in records security. That is true in any type of enterprise; but, inside the cloud, it has a bigger effect due to the fact there are greater human beings that have interaction with the cloud: cloud providers, third party carriers, providers, organizational clients, and cease-users. Cloud Computing leverages many existing technologies inclusive of web services, net Browsers, and virtualization, which contributes to the evolution of cloud environments. Consequently, any vulnerability related to those technologies also influences the cloud, and it can actually have a significant effect. the connection between threats and vulnerabilities is illustrated in desk four, which describes how a risk can take gain of a few vulnerability to compromise the device. The aim of this analysis is likewise to identify some present defences that may defeat those threats. This statistics can be expressed in a extra precise way the usage of misuse patterns. Misuse styles describe how a misuse is finished from the point of view of the attacker. as an instance, in risk T10, an attacker can examine or tamper with the contents of the VM nation files all through live migration. this may be possible due to the fact VM migration transfer the facts over network channels which are frequently insecure, which includes the net. Insecure VM migration may be mitigated by using the subsequent proposed techniques: TCCP gives private execution of VMs and comfortable migration operations as properly. PALM proposes a comfy migration gadget that gives VM live migration abilities beneath the condition that a VMM-blanketed gadget is present and active. Hazard eleven is every other cloud chance in which an attacker creates malicious VM photograph containing any kind of virus or malware. This risk is possible due to the fact any valid consumer can create a VM photo and submit it at the issuer's repository in which other customers can retrieve

them. If the malicious VM photograph consists of malware, it's going to infect different VMs instantiated with this malicious VM photograph. in order to triumph over this hazard, an image management gadget become proposed, Mirage. It provides the subsequent protection control capabilities: get right of entry to manipulate framework, photo filters, provenance tracking system, and repository maintenance services

Homomorphism encryption

The 3 simple operations for cloud facts are switch, keep, and system. Encryption strategies can be used to at ease statistics while it's far being transferred inside and out of the cloud or saved in the company's premises. Cloud vendors need to decrypt cipher information with a purpose to method it, which raises privatives worries. In, they advocate a technique primarily based on the application of completely homomorphic encryption to the security of clouds. Absolutely homomorphic encryption permits acting arbitrary computation on cipher texts without being decrypted. Modern-day homomorphic encryption schemes assist confined quantity of homomorphic operations which include addition and multiplication. The authors in provided some real-world cloud applications where some simple homomorphic operations are wished. But, it requires massive processing electricity which can also effect on user reaction time and energy intake. Net utility scanners web applications can be an easy goal due to the fact they're exposed to the public consisting of ability attackers. Internet utility scanners are software which scans net programs via the internet front-cease in order to discover security vulnerabilities. There also is different internet software security equipment including net software firewall. Internet utility firewall routes all net visitors via the internet software firewall which inspects specific threats.

Countermeasures for T06: VM escape

Hyper Safe it's far an approach that offers hypervisor control-flow integrity. Hyper Safe's intention is to defend kind I hypervisors the use of strategies: non by passable reminiscence lockdown which protects write protected reminiscence pages from being changed, and constrained pointed indexing that converts control data into pointer indexes. a good way to evaluate the effectiveness of this technique, they have conducted 4 styles of attacks together with adjust the hypervisor code, execute the injected code, alter the page desk, and tamper from a go back table. They concluded that Hyper Safe efficiently averted these kinds of attacks, and that the performance overhead is low. Relied on cloud computing platform TCCP enables carriers to provide closed container execution environments, and lets in customers to determine if the environment is relaxed before launching their VMs. The TCCP provides fundamental elements: a depended on virtual system screen (TVMM) and a depended on coordinator (TC). The TC manages a set

of depended on nodes that run TVMMs, and it is maintained but a relied on 0.33 party. The TC participates within the manner of launching or migrating a VM, which verifies that a VM is running in a trusted platform. The authors in claimed that TCCP has a widespread disadvantage because of the fact that each one the transactions must verify with the TC which creates an overload. They proposed to apply Direct anonymous Attestation (DAA) and privacy CA scheme to tackle this difficulty.

Virtual network security

Wu and ET al.presents a virtual community framework that secures the communique among digital machines. This framework is primarily based on Xen which offers configuration modes for digital networks: "bridged" and "routed". The digital community model is composed of three layers: routing layers, firewall, and shared networks, that could save you VMs from sniffing and spoofing. An assessment of this technique turned into not achieved when this booklet turned into posted. Furthermore, web offerings are the biggest implementation era in cloud environments. However, internet offerings additionally cause numerous challenges that want to be addressed. Security internet services standards describe how to relaxed communique between applications thru integrity, confidentiality, authentication and authorization.

There are several protection standard specifications such as security assertion Mark up Language (SAML), WS Security, Extensible get entry to control Mark up (XACML), XML digital Signature, XML Encryption, Key management Specification (XKMS), WS-Federation, WS-relaxed verbal exchange, WS-safety policy and WS-accept as true with. The NIST Cloud Computing requirements Roadmap running institution has accumulated excessive stage standards which can be applicable for Cloud Computing.

Conclusion

Cloud Computing is an exceptionally new concept that offers an amazing range of blessings for its users; however, it also increases a few protection troubles which can also gradual down its use. Understanding what vulnerabilities exist in Cloud Computing will assist groups to make the shift towards the Cloud. On account that Cloud Computing leverages many technologies, it also inherits their security troubles.

Traditional web packages, statistics web hosting, and virtualization were regarded over; however some of the solutions provided are immature or inexistent. We've offered protection issues for cloud models: IaaS, PaaS, and IaaS, which range depending at the version. As defined in this paper, storage, virtualization, and networks are the largest protection worries in Cloud Computing. Virtualization which permits a couple of users to percentage a bodily

server is one of the essential concerns for cloud customers. Additionally, every other task is that there are exclusive styles of virtualization technology, and every kind cans also technique protection mechanisms in extraordinary approaches. Digital networks also are target for some assaults especially while communicating with far flung digital machines.

Acknowledgments

This paintings became supported in part by the NSF (presents OISE-0730065). Any critiques, findings, and conclusions or hints expressed on this fabric are the ones of the author(s) and do not necessarily reflect the ones of the NSF. We additionally need to thank the GSyA research group at the University of Castilla-Los Angeles Mancha, in Ciudad actual, Spain for taking part with us on this project**.**

References

1. 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
2. Wang Z, Jiang X (2010) Hyper Safe: 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
3. Fernandez EB, Yoshioka N, Washizaki H (2009) Modelling 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
4. 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
5. Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology
6. 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, Sa

7. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.
8. Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.
9. Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.. 2011. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.
10. Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.
11. Centre for the Protection of National Infrastructure: Information Security Briefing 01/2010 Cloud Computing. 2010. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf.
12. Khalid A: Cloud Computing: applying issues in Small Business. International Conference on Signal Acquisition and Processing (ICSAP'10) 2010, 278–281.
13. KPMG: From hype to future: KPMG's 2010 Cloud Computing survey.. 2010. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291.
14. Rosado DG, Gómez R, Mellado D, Fernández-Medina E: Security analysis in the migration to cloud environments. Future Internet 2012, 4(2):469–487.
15. Mather T, Kumaraswamy S, Latif S: Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.; 2009.
16. Li W, Ping L: Trust model to enhance Security and interoperability of Cloud environment. In Proceedings of the 1st International conference on Cloud Computing. Beijing, China: Springer Berlin Heidelberg; 2009:69–79.
17. Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.
18. Kitchenham B: Procedures for perfoming systematic review, software engineering group. Australia: Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd; 2004. TR/SE-0401

19. Kitchenham B, Charters S: 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. UK: Department of Computer Science; 2007.
20. Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M: Lessons from applying the systematic literature review process within the software engineering domain. J Syst Softw 2007, 80(4):571–583. 10.1016/j.jss.2006.07.009.
21. Cloud Security Alliance: Top Threats to Cloud Computing V1.0. 2010. Available: https://cloudsecurityalliance.org/research/top-threats.
22. ENISA: Cloud Computing: benefits, risks and recommendations for information Security. 2009. Available: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.
23. Dahbur K, Mohammad B, Tarakji AB: A survey of risks, threats and vulnerabilities in Cloud Computing. In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. Jordan: Amman; 2011:1–6.
24. Ertaul L, Singhal S, Gökay S: Security challenges in Cloud Computing. In Proceedings of the 2010 International conference on Security and Management SAM'10. Las Vegas, US: CSREA Press; 2010:36–42.
25. Grobauer B, Walloschek T, Stocker E: Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 2011, 9(2):50–57.
26. Subashini S, Kavitha V: A survey on Security issues in service delivery models of Cloud Computing. J Newt Comput Appl 2011, 34(1):1–11. 10.1016/j.jnca.2010.07.006.
27. Jensen M, Schwenk J, Gruschka N, Iacono LL: On technical Security issues in Cloud Computing. In IEEE International conference on Cloud Computing (CLOUD'09). 116: 116; 2009:109–116.
28. Onwubiko C: Security issues to Cloud Computing. In Cloud Computing: principles, systems & applications. Edited by: Antonopoulos N, Gillam L. Springer-Verlag: 2010; 2010.r
29. Morsy MA, Grundy J, Müller I: An analysis of the Cloud Computing Security problem. In Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC; 2010.
30. Jansen WA: Cloud Hooks: Security and Privacy Issues in Cloud Computing. In Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI. Washington, DC, USA: IEEE Computer Society; 2011:1–10.

31. Zissis D, Lekkas D: Addressing Cloud Computing Security issues. Futur Gener Comput Syst 2012, 28(3):583–592. 10.1016/j.future.2010.12.006.
32. Jansen W, Grance T: Guidelines on Security and privacy in public Cloud Computing. Gaithersburg, MD: NIST, Special Publication 800–144; 2011.
33. Mell P, Grance T: The NIST definition of Cloud Computing. Gaithersburg, MD: NIST, Special Publication 800–145; 2011.
34. Zhang Q, Cheng L, Boutaba R: Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications 2010, 1(1):7–18. 10.1007/s13174-010-0007-6.
35. Ju J, Wang Y, Fu J, Wu J, Lin Z: Research on Key Technology in SaaS. In International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. Washington, DC, USA: IEEE Computer Society; 2010:384–387.