Cloud Computing: Study on Cloud Computing and its Security Threats

Niranjanamurth M
Research Scholar Dept. of Computer Science Engg, JJTU, RAJASTHAN,
niruhsd@gmail.com

Sharavan N S
Student of MCA
MSRIT
BANGALORE
Shravana4000@gmail.com

Kavya K
Student of MCA, MSRIT, Bangalore,
kavya892@gmail.com

Mithun U
Student of MCA, MSRIT, Bangalore,
mithunfire25@gmail.com

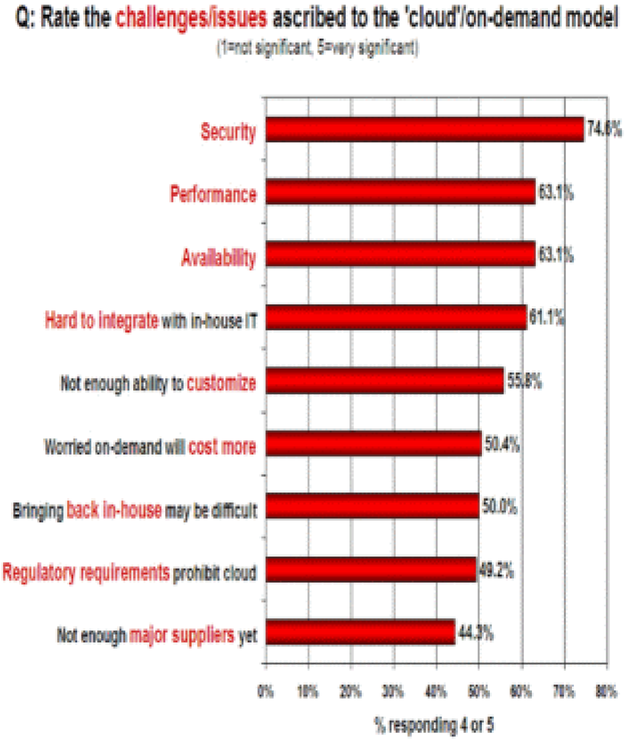
***Abstract* -- Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. In this paper we have discussed cloud computing and its Deployment models, Security threats, security risk, Solution of Security threats of cloud computing**

Keywords: Cloud Computing, Deployment models, Security threats, security risk, Solution of Security threats

I. Introduction

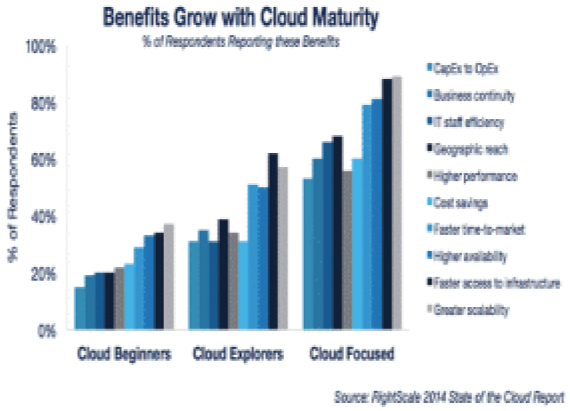
Security is a primary concern when organizations are ready to develop using cloud based technologies and can even inhibit cloud adoption. Some of the common issues cited include the perceived lack of control using a public cloud, visibility into the cloud or data compliance requirements. For those with compliance or regulatory requirements, it`s absolutely necessary to maintain this control in-house. We find that these organizations set up a private cloud infrastructure as the best way to deal with this. However, cloud security is an issue at every layer of the stack, not just the infrastructure layer. Organizations need to review the security associated with the platform-as-a-service (PaaS) used to build their applications because it is equally important.

For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology`s (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted in figure 1



Source: IDC Enterprise Panel, August 2008 n=244

Fig. 1. Challenges and issues in Cloud Computing



Source: RightScale 2014 State of the Cloud Report

Fig 2: Benefits grow with Cloud Maturity

II. AIM OF THE STUDY

The aim of the paper:

- To know what is Cloud computing.
- To know the types of cloud computing
- To know deployment model
- To understand the security threats of cloud computing
- To know security risk in cloud computing
- Understand the Solution of Security threats sin cloud computing

III. RELATED WORKS

A. Cloud Deployments Models:

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. The Cloud Computing model has three main deployment models which are:

1) Private cloud

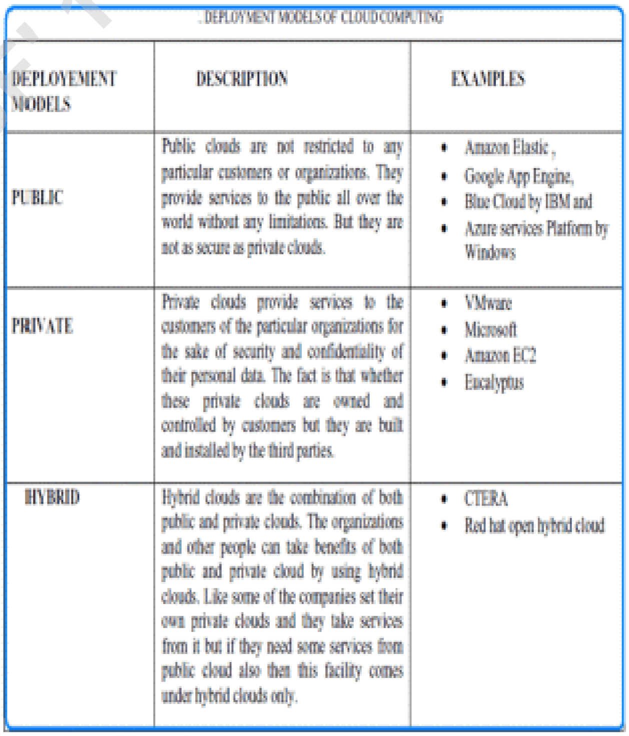
Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

2) Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

3) Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.



. DEPLOYMENT MODELS OF CLOUD COMPUTING

DEPLOYEMENT MODELS	DESCRIPTION	EXAMPLES
PUBLIC	Public clouds are not restricted to any particular customers or organizations. They provide services to the public all over the world without any limitations. But they are not as secure as private clouds.	• Amazon Elastic , • Google App Engine, • Blue Cloud by IBM and • Azure services Platform by Windows
PRIVATE	Private clouds provide services to the customers of the particular organizations for the sake of security and confidentiality of their personal data. The fact is that whether these private clouds are owned and controlled by customers but they are built and installed by the third parties.	• VMware • Microsoft • Amazon EC2 • Eucalyptus
HYBRID	Hybrid clouds are the combination of both public and private clouds. The organizations and other people can take benefits of both public and private cloud by using hybrid clouds. Like some of the companies set their own private clouds and they take services from it but if they need some services from public cloud also then this facility comes under hybrid clouds only.	• CTERA • Red hat open hybrid cloud

Fig. 3. Deployment models of cloud computing

B. Cloud Computing Service Delivery Models

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service(SaaS).

1) Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service. IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security providedat the host.

2) Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channelsis fundamental.

3) Software as a Service (SaaS)

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over theInternet.

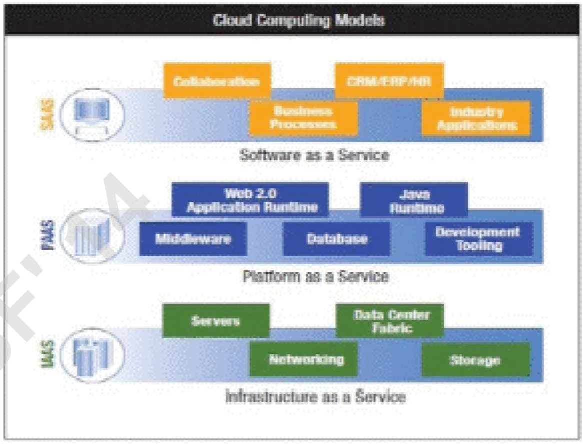


Fig. 4. Cloud Computing Models

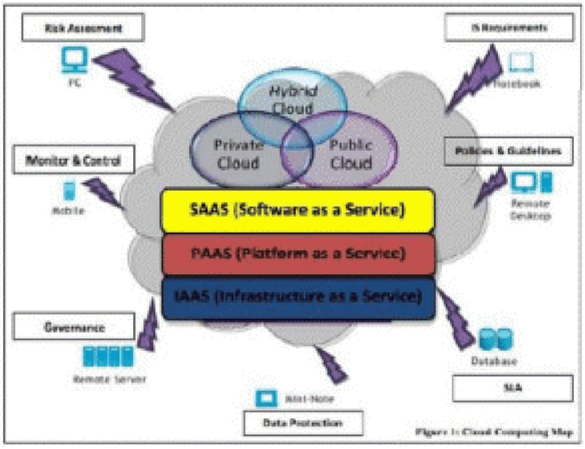


Fig. 5. Cloud Computing Map

C. Security Issues with Cloud models

1) Software-as-a-service (SaaS) security issues:

SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM. SaaS users have lesscontrol over security among the three fundamentaldelivery models in the cloud. The adoption of SaaS applications may raise some security concerns as listed below.

Application security

These applications are typically delivered via the Internet through a Web browser. However, flaws in web applications may create vulnerabilities for the SaaS applications. Attackers have been using the web to compromise user's computers and perform malicious activities such as steal sensitive data. Security challenges in SaaS applications are not different from any web application technology, but traditional security solutions do not effectively protect it from attacks, so new approaches are necessary.

Accessibility

Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks. The Cloud Security Alliance has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (Wi-Fi), vulnerabilities found in the device OS and official applications, insecuremarketplaces, and proximity-based hacking.

2) Platform-as-a-service (PaaS) security issues

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers. As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. Same as SaaS, PaaS also brings data security issues and other challenges that aredescribed as follows:

Third-party relationships

Moreover, PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups. Mashups combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network security. Also, PaaS users have to depend on both the security of web-hosted development tools andthird-party services.

Development Life Cycle

From the perspective of the application development, developers face the complexity of building secure applications that may be hosted in the cloud. The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security. Developers have to keep in mind the PaaS applications should be upgraded frequently, so theyhave to ensure that their application developmentprocesses are flexible enough to keep up with changes. However, developers also have to understand that any changes in PaaS components can compromise this purity of their applications. Besides secure development techniques, developers need to be educated about data legal issues as well, so that data is not stored in inappropriatelocations.

3) Infrastructure-as-a-service (IaaS) security issues

IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to them. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor. They control the software running in their virtual machines, and they are responsible to configure security policies correctly. However, the underlying compute, network, and storage infrastructure is controlled by cloud providers. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility. Here aresome of the security issues associated to IaaS.

4) Security Concerns of Cloud Service Consumers

Many people are wary of using cloud services because of concerns about service outages, data loss, privacy issues, hacker compromising their access accounts, and compliance with legislation. For IT savvy enterprises, they are likely to have skills and resources to monitor the service level of their service provider, assess the service provider's security compliance, or implement their own additional security safeguards to protect their data. On the other hand, for average cloud service consumers and SMEs, they may overlook their own rights and responsibilities, be confused about how to choose a cloud service provider that is trustworthy, and hesitant on whether their data has sufficient protection when using a cloud service.

5) What Cloud Service Consumers Should Be Aware Of?

Data processed or stored by cloud service consumers in a cloud service may contain valuable, sensitive and personal information. Knowing only the security measures applied by the cloud service provider is not sufficient to protect this data. For SMEs, they need to know what needs to be considered when selecting a cloud service provider, as well as what needs to be considered when using cloud services. All cloud service consumers, both responsible parties of businesses and individuals, are advised to have an in-depth understanding of the issues and concerns for protecting their data in the cloud environment.

IV. SECURITY ISSUES IN CLOUD COMPUTING

Security in the cloud is achieved, in part, through third party controls and assurance much like in traditional outsourcing arrangements. But since there is no common cloud computing security standard, there are additional challenges associated with this. Many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated on their own merits. In a vendor cloud model, it is ultimately down to adopting customer organizations to ensure that security in the cloud meets their own security polices through requirements gathering provider risk assessments, due diligence, and assurance activities (CPNI Security Briefing, 2010).

Thus, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependent on their own in-house managed enterprises. The same internal and external threats are present and require risk mitigation or risk acceptance. In the following, we examine the information security challenges that adopting organizations will need to consider, either through assurance activities on the vendor or public cloud providers or directly, through designing and

implementing security control in a privately owned cloud. In particular, examine the following issues:

- The treats against information assets residing in cloud computing environments.
- The types of attackers and their capability of attacking the cloud.
- The security risks associated with the cloud, and where relevant considerations of attacks and Counter measures.
- Emerging cloud security risks.

A. List of security risks in cloud computing

Privileged user access -- Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data.

Data location and segregation - - Customers may not know where their data is being stored and there may be a risk of data being stored along side other customers' information.

Data disposal - - Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during decommissioning is enhanced within the cloud.

E-investigations and Protective monitoring - -The ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model in use, and the access and complexity of the cloud architecture. Customers cannot effectively deploy monitoring systems on infrastructure they do not own; they must rely on the systems in use by the cloud service provider to support investigations.

Assuring cloud security - - Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements.

V CLOUD SECURITY THREATS

A . Solution of Security threats

6.1 Find Key Cloud Provider First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

6.2 Clear Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

6.3 Recovery Facilities Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

6.4 Better Enterprise Infrastructure Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber-attacks.

6.5 Use of Data Encryption for security purpose Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor. IT leaders must define strategy and key security elements to know where the data encryption is needed.

6. 6 Prepare chart regarding data flow

There should be a chart regarding the flow of data. So the IT managers can have idea where the data is for all the times, where it is being stored and where it is being shared. There should be total analysis of data.

B. List of cloud security threats

Threat
Confidentiality
Insider user threats: * Malicious cloud provider user * Malicious cloud customer user * Malicious third party user (Supporting either the cloud provider or customer organizations)
External attacker threats: * Remote software attack of cloud infrastructure * Remote software attack of cloud applications * Remote hardware attack against the cloud * Remote software and hardware attack against cloud user organizations' endpoint software and hardware * Social engineering of cloud provider users, and cloud customer users.
Data leakage: * Failure of security access rights across multiple domains * Failure of electronic and physical transport systems for cloud data and backups
Integrity
Data segregation: * Incorrectly defined security perimeters * Incorrect configuration of virtual machines and hypervisors
User access: * Poor identity and access management procedures
Data quality: * Introduction of faulty application or infrastructure components
Availability
Change management: * Customer penetration testing impacting other cloud customers * Infrastructure changes upon cloud provider, customer and third party systems impacting cloud customers
Denial of service threat:
* Network bandwidth distributed denial of service * Network DNS denial of service * Application and data denial of service
Physical disruption: * Disruption of cloud provider IT services through physical access * Disruption of cloud customer IT services through physical access * Disruption of third party WAN providers services
Exploiting weak recovery procedures: * Invocation of inadequate disaster recovery or business continuity processes

The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the flowing major threats:

* Failures in Provider Security
* Attacks by Other Customers
* Availability and Reliability Issues
* Legal and Regulatory Issues
* Perimeter Security Model Broken
* Integrating Provider and Customer Security Systems
* Abuse and Nefarious Use of Cloud Computing
* Insecure Application Programming Interfaces
* Malicious Insiders
* Shared Technology Vulnerabilities
* Data Loss/Leakage
* Account, Service & Traffic Hijacking
* Unknown Risk Profile

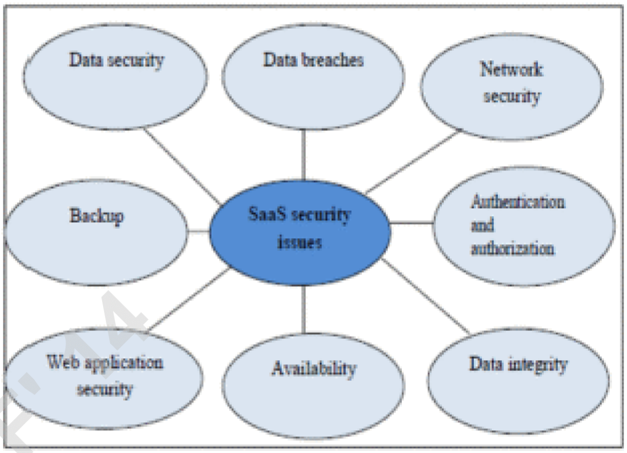


Fig : Security issues in SaaS

Fig. 6. Security issues in SaaS

VI. CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down issues. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtualmachines.

In the process of adopting cloud based services companies and IT organizations should evaluate the business benefits and risks. The cloud's economies of scale and flexibility are both a friend and aloe from a security point of view. The management of security risk involves users, the technology itself, the cloud service providers, and the legal aspects of the data and services being used. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective than traditional ones. To help reduce the threat, cloud computing stakeholders should investing implementing security measures to ensure that the data is being kept secure and private throughout its lifecycle.

VII. ACKNOWLEDGEMENT

We thank Dr. T. V. Suresh Kumar, Prof. and Head, Dept. of MCA, MSRIT, Bangalore-54. For his continuous support and encouragement for completing this research paper and also thanks to MSRIT management.

We thank Mr. S. Jagannatha , Associate Professor. Dept. of MCA, MSRIT, Bangalore-54.for his constant support and motivation.

REFERENCES

[1] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges",IDC Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

[2] Cloud Computing Use Case Discussion Group. "Cloud Computing Use Cases Version 3.0," 2010.

[3] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.

[4] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[5] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.

[6] Florin OGIGAU-NEAMTIU - "CLOUD COMPUTING SECURITY ISSUES" The Regional Department of Defense Resources Management Studies, Brasov, Romania - 2013.

[7] Jaydip Sen - "Security and Privacy Issues in Cloud Computing" - Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[8] [8]Kuyoro S. O. Ibikunle F. "Cloud Computing Security Issues and Challenges" - International Journal of Computer Networks (IJCN), Volume (3): Issue (5): 2011

[9] Kevin Hamlen, Murat Kantarcioglu - "Security Issues for Cloud Computing" - International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010

[10] Wayne A. Jansen, NIST - "Cloud Hooks: Security and Privacy Issues in Cloud Computing" -Proceedings of the 44th Hawaii International Conference on System Sciences – 2011

[11] Mohammad Sajid, Zahid Raza - "Cloud Computing: Issues & Challenges" - International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV

[12] Keiko Hashizume, David G Rosado, "An analysis of security issues for cloud computing" SPRINGER -Hashizume et al. Journal of Internet Services and Applications 2013

[13] Pradeep Kumar Tiwari, Dr. Bharat Mishra - "Cloud Computing Security Issues, Challenges and Solution" - International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 8, August 2012)

[14] Rajesh Piplode, Umesh Kumar Singh "An Overview and Study of Security Issues & Challenges in Cloud Computing" -2012, IJARCSSE, Volume 2, Issue 9, September 2012 ISSN: 2277 128X