© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on Security Issues in Cloud Computing

Raghvendra Kumar, Arti Pandey
LNCT, Jabalpur, Madhya Pradesh, India

ABSTRACT

Cloud computing is a natural evolution for data and computation centers with automated systems management, workload balancing, and virtualization technologies. In this paper, the authors discuss security issues, privacy and control issues, accessibility issues, confidentiality, integrity of data and many more for cloud computing. Current solutions for these security risks are also discussed. In addition, we make a list of security items that all users should be aware of before opting to use cloud based services and discuss methods for allowing the user to select specific security levels of security for items. This paper aims to present a survey in cloud computing, which gives solutions for challenges faced by cloud .Further this helps to find out the solution for the drawbacks found in given methods and come up with new solution or method to secure the cloud.

Keywords : Cloud issues, Data issues, IaaS, PaaS, Security, SLA, SaaS, Virtual machine layer.

I. INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it.

The cloud is emerging as the latest way to approach alternative delivery models for IT capabilities. It is a way of delivering IT- enabled services in the form of software, infrastructure and more. This research examines the definition of cloud computing and how it will evolve.

Cloud computing can be defined as "A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing platforms on demand, which could be accessed in a simple and pervasive way"[1]. In simple words, Cloud computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Cloud computing aims to provide scalable and inexpensive on -demand computing infrastructures with good quality of service levels. Cloud Computing is the implementation of engineering principals to obtain high quality applications through Internet. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels [2].

Cloud computing provides the internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely used definition of the cloud computing model is introduced by NIST [3] as "a model for enabling convenient, on-demand network access to a shared pool of configurable

Computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter [4].

Cloud computing can be divided into two sections, the user and the cloud. In most scenarios, the user is connected to the cloud via the internet. It is also possible for an organization to have a private cloud in which a

user is connected via a intranet. However, both scenarios are identical other than the use of a private and public network or cloud [5]. The user sends requests to the cloud and the cloud provides the service.

Multi-tenancy and elasticity are two key characteristics of the cloud model. Multi-Tenancy enables sharing the same service instance among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics focus on improving resource utilization, cost and service availability.

Cloud computing products, also called cloud service delivery models, as in Fig 1., which are often roughly classified into a hierarchy of -as a service terms, presented here in order of increasing specialization:

Infrastructure-as-a-service (IaaS): where cloud providers deliver computation resources, storage and network as an internet-based services. This service model is based on the virtualization technology. Amazon EC2 is the most IaaS provider.

Platform-as-a-service (PaaS): where cloud providers deliver platforms, tools and other business services that enable customers to develop, deploy, and manage their own applications, without installing any of these platforms or support tools on their local be hosted on top of IaaS model or on top of the cloud infrastructures directly. Google Apps and Microsoft Windows Azure are the most known.

Software-as-a-service (SaaS) applications hosted on the cloud infrastructure as internet based service for end users, applications on the customers' computers be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. SalesForce CRM is an example of the provider.

Each service delivery model has dif implementations, as in Fig 1, which development of standard security model for each service delivery model. Moreover, these coexist in one cloud platform the security management process. Each service delivery model has different possible implementations, as in Fig 1, which complicates development of standard security model for each service delivery model. Moreover, these service delivery models coexist in one cloud platform the security management process.

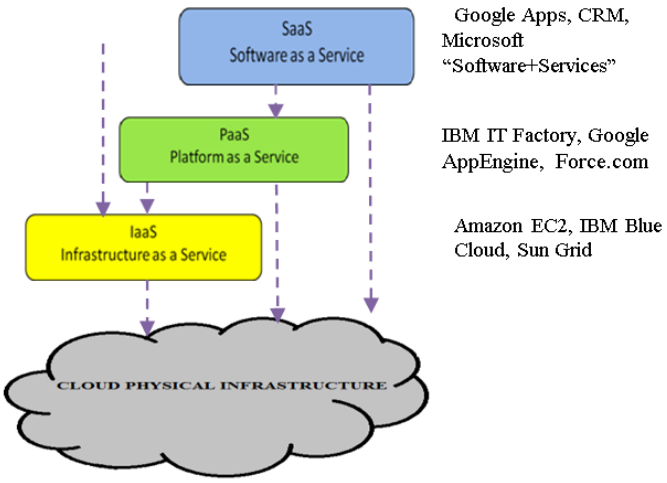

Figure 1: Cloud service delivery models

Irrespective of the above mentioned service models, cloud services can be deployed in four ways depending upon the customers' requirements:

A. Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party [6]. Multiple enterprises can work on the infrastructure provided, at the same time. Users can dynamically provision resources through the internet from an off-site service provider. Wastage of resources is checked as the user pays for whatever they use.

B. Private Cloud: Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider [6]. This uses the concept of virtualization of machines, and is a proprietary network

C. Community cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider.

D. Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other [7].

1. Cloud Computing Architecture

Cloud computing can be divided into two sections, the user and the cloud. In most scenarios, the user is connected to the cloud via the internet. It is also possible for an organization to have a private cloud in which a user is connected via a intranet. However, both scenarios are identical other than the use of a private and public network or cloud [8]. The user sends requests to the cloud and the cloud provides the service. See Figure 2.

Within the cloud, a central server is responsible for administering the system and in many ways functions as the operating system of the specific cloud network. Another name for this is called "middleware" which is the central server for a particular cloud. Examples include Google App Engine and Amazon EC2 [5].

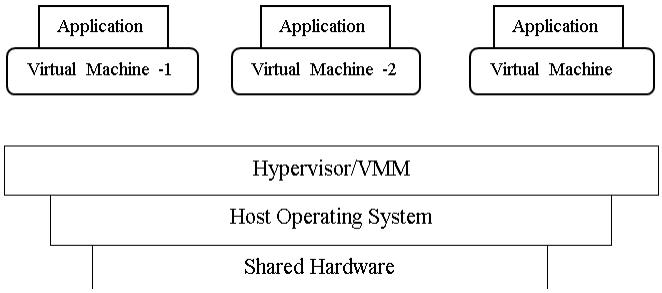

Figure 2: Cloud Computing Architecture

With an avalanche rise towards the deployment of Cloud Computing, the ever consistent security and privacy issues have become more sophisticated, more distributed in the sense that the user section for such services is growing by leaps and bounds [9]. With the increase of on-demand application usage, the potential of cyber-attacks also increases. Individual users have to frequently provide online information about their identification, and these could be used by attackers for identity theft. In order to maintain various security and privacy issues like: confidentiality, operational integrity, disaster recovery and identity management, following schemes should be deployed at least to ensure data security [10] to some extent like:

- An encryption scheme to ensure data security in a highly interfering environment maintaining security standards against popular threats and data storage security.
- The Service Providers should be given limited access to the data, just to manage it without being able to see what exactly the data is.
- Stringent access controls to prevent unauthorized and illegal access to the servers controlling the network.
- Data backup and redundant data storage to make data retrieval easy due to any type of loss unlike the recent breakdown issues with the Amazon cloud.
- Distributed identity management and user security is to be maintained by using either Lightweight Directory Access Protocol (LDAP), or published APIs (Application Programming Interfaces) to connect into identity systems.
- An important aspect of cloud computing is that it does give rise to a number of security threats from the perspective of data security for a couple of reasons.

Firstly, the traditional techniques cannot be adopted as these have become quite obsolete with respect to the ever evolving security threats and also to avoid data loss in a cloud computing environment. The second issue is that the data stored in the cloud is accessed a large number of times and is often subject to different types of changes. This may comprise of bank accounts, passwords and highly confidential files not to be read by someone else apart from the owner. Hence, even a small slip may result in loss of data security [7].

The organization of this paper is as follows: Section 2 includes literature survey on cloud computing. We will discuss cloud security and its issues in Section 3. In addition, a list of security issues that all users should be aware of is given and suggestions are made for users to minimize security risks if they choose to use cloud security issues in Section 4. Section 5 we discuss about the traditional and cloud computing with unmanageable risks. In Section 6, the conclusion summarizes all of the security concepts and Section 7, suggests future areas of research based on the on the material discussed in this paper.

II. METHODS AND MATERIAL

1. Literature Review

Cloud Computing distinguishes itself from other computing paradigms like grid computing, global computing, and internet computing in various aspects of on demand service provision, user centric interfaces, guaranteed QoS (Quality of Service), and autonomous system [11] etc. A few state of the art techniques that contribute to cloud computing are:

•Virtualization: It has been the underlying concept towards such a huge rise of cloud computing in the modern era. The term refers to providing an environment that is able to render all the services, supported by a hardware that can be observed on a personal computer, to the end users [12]. The three existing forms of virtualization categorized as: Server virtualization, Storage virtualization and Network

virtualization, have inexorably led to the evolution of Cloud computing. For example, a number of underutilized physical servers may be consolidated within a smaller number of better utilized severs [13].

•Web Service and SOA: Web services provided services over the web using technologies like XML, Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI). The service organization inside a cloud is managed in the form of Service Oriented Architecture (SOA) and hence we can define SOA as something that makes use of multiple services to perform a specific task [14].

•Application Programming Interface (API): Without APIs it is hard to imagine the existence of cloud computing. The whole bunch of cloud services depend on APIs and allow deployment and configuration through them. Based on the API category used viz. control, data and application, different functions of APIs are invoked and services are rendered to the users accordingly.

These were the few technological advances that led to the emergence of Cloud Computing and enabled a lot of service providers to provide the customers a hassle free world of virtualization fulfilling all their demands. The prominent ones are: Amazon-EC2 (Elastic Compute Cloud), S3 (Simple Storage Service), SQS (Simple Queue Service), CF (Cloud Front), SimpleDB, Google, Microsoft Windows-Azure , ProofPoint, RightScale, Salesforce.com, Workday, Sun Microsystems etc. and each of them are categorised either as one of the three main classifications based on the cloud structure they provide: private, public and hybrid cloud. Each of the above mentioned cloud structure has its own limitations and benefits.

The fundamental factor defining the success of any new computing technology is the level of security it provides [15]. Whether the data residing in the cloud is secure to a level so as to avoid any sort of security breach or is it more secure to store the data away from cloud in our own personal computers or hard drives?

The cloud service providers insist that their servers and the data stored in them is sufficiently protected from any sort of invasion and theft. Such companies argue that the data on their servers is inherently more secure than data residing on a myriad of personal computers and laptops. However, it is also a part of cloud architecture, that the client data will be distributed over these individual computers regardless of where the base repository of data is ultimately located. There have been instances when their security has been invaded and the whole system has been down for hours. At-least half a dozen of security breaches occurred last year bringing out the fundamental limitations of the security model of major Cloud Service Providers (CSP). With respect to cloud computing environment, privacy is defined as "the ability of an entity to control what information it reveals about itself to the cloud/cloud SP, and the ability to control who can access that information". R. Gellman discusses the standards for collection, maintenance and disclosure of personality identifiable information in . Information requiring privacy and the various privacy challenges need the specific steps to be taken in order to ensure privacy in the cloud as discussed in.

In case of a public-cloud computing scenario, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario. A public cloud acts as a host of a number of virtual machines, virtual machine monitors, and supporting middleware etc. The security of the cloud depends on the behaviour of these objects as well as on the interactions between them. Moreover, in a public cloud enabling a shared multi-tenant environment, as the number of users increase, security risks get more intensified and diverse. It is necessary to identify the attack surfaces which are prone to security attacks and mechanisms ensuring successful client-side and server-side protection. Because of the multifarious security issues in a public cloud, adopting a private cloud solution is more secure with an option to move to a public cloud in future, if needed. Also, privacy needs to be maintained as there are high chances of an eavesdropper to be able to sneak in Cloud computing security challenges and issues discussed various researchers. The Cloud Computing Use Cases group discusses the different use case scenarios and related requirements that may exist in the cloud computing model. They consider use cases from different perspectives including customers, developers and security engineers. ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in cloud computing that may lead to such risks. Similar efforts discussed in "Threats to Cloud

Computing" by CSA [10]. Balachandra et al discuss the security SLA's specifications and objectives related to data locations, segregation and data recovery Kresimir et al discuss high level security concerns in the cloud computing model such as data integrity, payment, and privacy of sensitive information. Kresimir discussed different security management standards such as ITIL ISO/IEC 27001 and Open Virtualization Format (OVF). Meiko et al discuss the technical security issues arising from adopting the cloud computing model such as XML-attacks, Browsers related attacks, and flooding attacks. Bernd et al discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology related, cloud characteristics related, security controls-related Subashini et al discuss the security challenges of the cloud service delivery model, focusing on the SaaS model. CSA discusses critical areas of cloud computing. They deliver a set of best practices for the cloud provider, consumers and security vendors to follow in each domain.

In our paper we did a deep investigation in the cloud model to identify the root causes and key participating dimensions in such security issues/problems. This will help better to understand the problem and delivery solutions.

2. Cloud Security And its Issues:

A. Cloud Security:

Security remains the biggest barrier preventing companies from entering into the cloud. Security is a continuous consideration in IT-related projects. Unlike many other traits in technological contexts, security is notoriously hard to quantify or even compare qualitatively. For this reason, security evaluation of cloud offerings will mostly hinge on company reputation and, eventually, real-world track records but even real world track records are difficult to compare between companies, because security breaches may not be publicly disclosed unless compelled by regulation. Like SLAs, companies might specify contractual compensation for certain kinds of provider negligence leading to security failures, but such provisions may be worth very little since security failures are not as easily observable as service availability failures.

Businesses using cloud services want to ensure that their data is secure from both external attackers as well as internal snoopers (employees of the cloud provider). Although data theft and snooping is mitigated by properly encrypting data to be stored within the cloud , encryption cannot prevent denial-of-service attacks such as data deletion or corruption. Some early research users of Amazon S3 suggest, "users should employ some kind of data authentication technology to assure themselves that data returned by S3 is the same as the data that was stored there. Technology such as an HMAC or a digital signature would protect users from both accidental data modification by Amazon and from malicious modification by third parties who managed to crack a password or intercept a password reset email message" . Service integrity is another security issue: businesses want to ensure their running services are not subject to denial-of-service attacks or hijacked. The latter can be very insidious, as a third party might (for example) gain control of a business's e-commerce site and besmirch its reputation. This situation is the digital equivalent of identity theft. Isolation is a related concern – cloud providers serve many customers and they all share common hardware and infrastructure. Although resource virtualization prevents customers from having to explicitly coordinate resource sharing, the cloud provider must ensure that multiple customers do not interfere with each other, maliciously or otherwise.

B. Parameters affecting cloud security

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

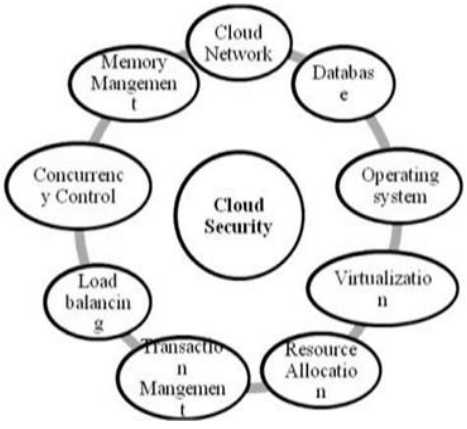

Figure 3: Parameters that affects cloud security

Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

C. Security Issues faced by Cloud computing

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud.

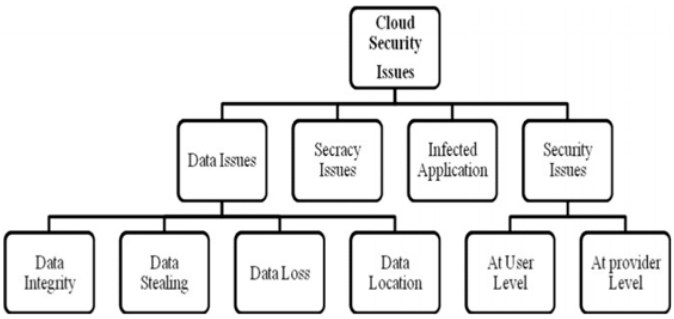

Figure 4: Cloud Security Issues

There are four types of issues raise while discussing security of a cloud Fig. 2.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues

Data Issues: sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing. Secondly, data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server. Thirdly, Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accessesable to users. Fourthly, data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial.

It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

Secrecy Issues: The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.
Infected Application: cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

Security issues: cloud computing security must be done on two levels. One is on provider level and another is on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or

stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

The Open Web Application Security Project (OWASP) maintains a "top 10" list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes. Cloud computing shares in common with other network-based application, storage and communication platforms certain vulnerabilities in several broad areas:

1. **Web Application Vulnerabilities,** such as cross-site scripting and sql injection which are symptomatic of poor field input validation, buffer overflow; as well as default configurations or mis-configured applications.
2. **Accessibility Vulnerabilities,** which are vulnerabilities inherent to the TCP/IP stack and the operating systems, such as denial of service and distributed denial of services.
3. **Authentication** of the respondent device or devices, IP spoofing, RIP attacks, ARP poisoning (spoofing), and DNS poisoning are all too common on the Internet. TCP/IP has some "unfixable flaws" such as "trusted machine" status of machines that have been in contact with each other, and tacit assumption routing tables on routers will not be maliciously altered.
4. **Data Verification,** tampering, loss and theft, while on a local machine, while in transit, while at rest at the unknown third-party device, or devices, and during remote back-ups.
5. **Physical Access Issues,** both the issue of an organization's staff not having physical access to the machines storing and processing a data, and the issue of unknown third parties having physical access to the machines.
6. **Privacy and Control Issues,** stemming from third parties having physical control of a data is an issue for all outsourced networked applications and storage, but cloud architectures have some specific issues that are distinct from the usual issues. Christodorescu, et al. show a significant gap between what is assumed and what is reality, i.e., all virtual machines are brought into existence clean, when in reality a compromised hypervisor can spawn compromised VMs, or all VM operating systems are known and available for audit, when in reality the Windows source-code, among others, is not available for audit.
7. **Data Confidentiality,** clients must have a mechanism to ensure that their data is secure and private in an untrusted cloud.
8. **Trust Computation**, a client can encrypt data stored on a cloud to ensure privacy, but this is not possible when compute services are requested, as the unencrypted data must reside in the memory of the host running the computation. Amazon's EC2, and other IaaS (Infrastructure as a Service) cloud services typically host virtual machines (VMs) where a client's computation can be executed. In these systems, anyone with privileged access to the host can read and manipulate client data. Given this security whole, cloud service providers are going to great lengths to secure their systems against insider attacks.
9. **Accountability**

   In addition to the security challenges we have described, there remains the issue of accountability in the face of incorrect behaviour. If data leaks to a competitor, or a computation returns incorrect results, it can be difficult to determine whether the client or the service provider is at fault. Haeberlen argues that the cloud should be made accountable to both the client and the provider, and in the event of a dispute, there should be a way to prove the presence of the problem to a third party (i.e. a judge).

III. RESULTS AND DISCUSSION

1. Solutions And TIPS To Cloud Security Issues

There are several groups interested in developing standards and security for clouds and cloud security. The Cloud Security Alliance (CSA) is gathering solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud (Cloud Security Alliance (CSA) – security best practices for cloud computing, 2009). The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups (Clouds Standards, 2010).

There is need for advanced and extended technologies, concepts and methods that provide secure server which leads to a secure cloud. For this a layered framework is available that assured security in cloud computing

environment. It consists of four layers as shown in Fig. 3.

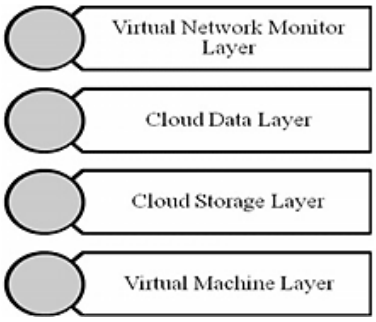

Figure 5 : Layered Framework for Cloud Security

First layer is secure virtual machine layer. Second layer is cloud storage layer. This layer has a storage infrastructure which integrates resources from multiple cloud service providers to build a massive virtual storage system. Fourth layer is virtual network monitor layer. This layer combining both hardware and software solutions in virtual machines to handle problems such as key logger examining XEN.

However, there are several groups working and interested in developing standards and security for clouds. The Cloud Standards web site is collecting and coordinating information about cloud-related standards under development by other groups. The Cloud Security Alliance (CSA) is one of them. CSA gathers solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. Another group is Open Web Application Security Project (OWASP). OWASP maintains a list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes. The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers.

There are some tips and tricks that cloud security solution providers should kept in mind when they delivers their service to cloud service consumer in a public cloud solution.

Verify the access controls: Set up data access control with rights and then verify these access controls by the cloud service provider whenever data is being used by cloud service consumer.

To implement access control methods for consumer side, the cloud service provider must describe and ensure that the only authorized users can access the user or consumer's data. Control the consumer access devices: Be sure the consumer's access devices or points such as Personal Computers, virtual terminals, gazettes, pamphlets and mobile phones are secure enough. The loss of an endpoint access device or access to the device by an unauthorized user can cancel even the best security protocols in the cloud. Be sure the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features. Monitor the Data Access: cloud service providers have to assure about whom, when and what data is being accessed for what purpose. For example many website or server had a security complaint regarding snooping activities by many people such as listening to voice calls, reading emails and personal data etc.

Share demanded records and Verify the data deletion: If the user or consumer needs to report its compliance, then the cloud service provider will share diagrams or any other information or provide audit records to the consumer or user. Also verify the proper deletion of data from shared or reused devices. Many providers do not provide for the proper degaussing of data from drives each time the drive space is abandoned. Insist on a secure deletion process and have that process written into the contract.

Security check events: Ensure that the cloud service provider gives enough details about fulfillment of promises, break remediation and reporting contingency. These security events will describe responsibility, promises and actions of the cloud computing service provider.

Web Application Solutions: The best security solution for web applications is to develop a development framework that shows and teaches a respect for security. Tsai, W. et al. put forth a four-tier framework for web-based development that though interesting, only implies a security facet in the process.

"Towards best practices in designing for the cloud" by Berre, Roman, Landre, Heuvel, Skår, Udnæs, Lennon, & Zeid (2009) is a road map toward cloud-centric

development, and the X10 language is one way to achieve better use of the cloud capabilities of massive parallel processing and concurrency (Saraswat, Vijay, 2010).

Accessibility Solutions: Krügel, C., Toth, T., & Kirda, E. (2002) point out the value of filtering a packet-sniffer output to specific services as an effective way to address security issues shown by anomalous packets directed to specific ports or services.

An often-ignored solution to accessibility vulnerabilities is to shut down unused services, keep patches updated, and reduce permissions and access rights of applications and users.

Authentication Solutions: Halton and Basta , suggest one way to avoid IP spoofing by using encrypted protocols wherever possible. They also suggest avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables are logged . Data Verification, Tampering, Loss and Theft Solutions: Raj, Nathuji, Singh and England (2009) suggest resource isolation to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache. Hayes points out that there is no way to know if the cloud providers properly deleted a client's purged data, or whether they saved it for some unknown reason. Would cloud-providers and clients have custody battles over client data?

Privacy and Control Solutions: Hayes (2008) points out an interesting wrinkle here, "Allowing a third-party service to take custody of personal documents raises awkward questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to a document if you fail to pay a bill?"

The issues of privacy and control cannot be solved, but merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private.

Physical Access solutions: One simple solution, which Milne (2010) states to be a widely used solution for UK businesses is to simply use in-house "private clouds".

Nurmi et. al, show a preview of one of the available home-grown clouds in their (2009) presentation. "The Eucalyptus Open-Source Cloud-Computing System" . Data confidentiability: This can be realized through cryptographic methods, where a client can verify the integrity of his remote data by storing a hash in local memory and authenticating server responses by re-calculating the hash of the received data and comparing it to the locally stored value. When dealing with large datasets, this method is implemented using hash trees, where the leaves of the tree are hashes of data blocks, and internal nodes are hashes of their children. A user verifies a given data block by storing the root hash of the tree; this results in a logarithmic number of cryptographic operations in the number of blocks.

Recent research has focused on efficiency of cryptographic methods, in particular Papamanthou et.al propose a mechanism to verify the correctness of server responses to queries, as well as integrity of stored data. They augment a hash table with a secure digest, a "fingerprint" of the entire stored dataset, which serves as a secure set description to which the answer to a query will be verified at the client, using a corresponding proof provided by the server. They meet their efficiency goals, as their method is the first which authenticates a hash table with constant query cost and sub linear update cost Trusting Computation:

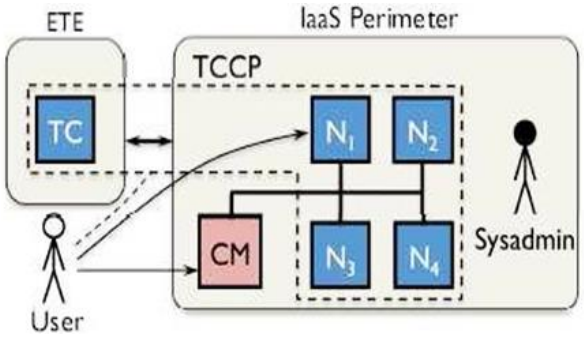

Figure 6. Trusted cloud computing platform (TCCP)

Trusted cloud computing platform includes a set of trusted nodes (N) and a trusted coordinator (TC). Users talk to the cloud manager (CM) to request services. The TC is maintained by an external trusted entity (ETE) in order to provide isolation from the IaaS perimeter. They restrict access to hardware facilities , adopt stringent accountability and auditing procedures, and minimize access to critical components of the infrastructure.

Despite these efforts, customers VMs are still susceptible to insiders, and clients need a solution that guarantees the confidentiality and integrity of their computations in a way that is verifiable. Santos et.al. propose a trusted cloud computing platform (TCCP) which enables IaaS providers to serve a closed box execution environment that guarantees confidential execution of guest VMs[44]. This system allows a customer to verify if its computation will run securely, before requesting the service to launch a VM. TCCP is based off a trusted computing platform called Terra, which uses a trusted virtual machine monitor (TVMM) to partition a single platform into multiple isolated VMs. The TVMM allows an application in a VM to authenticate itself to remote parties in a process called attestation. Attestation must identify each component of the software stack; this is achieved by building a certificate chain, starting from tamper-resistant hardware all the way up to a VM. Terra uses private, permanent keys embedded in a tamper-resistant chip to certify the system firmware (i.e. the BIOS). This firmware certifies the system boot loader, which then certifies the TVMM, which can finally certify the VMs that are loaded.

TCCP follows a similar method, using the trusted platform module (TPM) chip which is bundled with commodity hardware. Attestation is performed using simple public key cryptography to authenticate between a remote party and a platform running on an untrusted host.

Cloud providers house datacenters with many machines, and a client VM is dynamically scheduled to run on any machine. This means that the attestation procedure described above must be implemented on each node in the cloud. A sysadmin, however, can divert clients VM to a node not running the platform, either when the VM is launched, or during execution (using migration, which is supported by Xen). Although Terra was successful in a single host environment, we require a platform with stronger guarantees in the face of an untrusted cloud. TCCP provides these stronger guarantees by combining a TVMM with a trusted coordinator (TC). Fig 3 outlines the components of this platform. The TC manages the set of "trusted nodes" - the nodes that can run a client VM securely. A node is trusted if it is both running the TVMM, and it resides inside the security perimeter (i.e. it is physically inaccessible to attackers). The TC needs to record the nodes located in the security perimeter, and attest to the node's platform to ensure that the node is running a trusted platform implementation. A client can then verify whether the IaaS secures its computation by attesting to the TC. The key to preventing insider attacks is the fact that the TC is hosted by an external trusted entity (ETE), which securely updates the information provided, to the TC about the nodes in the perimeter. Admins with privileged access to the servers do not have access to the ETE, and they therefore cannot tamper with the TC. Although TCCP provides an execution environment that guarantees confidential execution of guest VM's, we note that moving the TC onto an external server poses other risks. We must be assured that the TC is running on a trusted server, and also that communication between the TC and IaaS perimeter is secure. We also note that while there is a working version of the Terra system, TCCP does not yet have a working prototype.

Accountability: Traditionally, a client maintains a server farm on their premises, where the client has physical access to the machines, and can directly oversee the maintenance and management of the machines. When this job is outsourced, management of these machines is delegated to the service provider, and the client has relinquised control over her computation and data. When an issue does arise, it is difficult to agree on who is responsible - the provider will blame the clients software, while the client will place blame on the provider. The lack of reliable fault detection and attribution not only deters potential customers, but it may also prevent certain applications from being hosted on the cloud, when strict laws regulate the release of sensitive data (for example, personal health information). Heaberlen proposes the notion of accountability: "a distributed system is accountable if a) faults can be reliably detected, and b) each fault can be undeniably linked to at least one faulty node". They do not have a prototype of this system, but their goal is to implement a primitive called AUDIT(A, S, t1, t2) that can be invoked by a client to verify whether the cloud has fulfilled agreement A for service S in the time interval t1, t2. AUDIT either returns OK, or some evidence that S has failed to meet agreement A. At first it may seem as though accountability only benefits the client, and places a greater burden on the provider. However the provider has incentives to adopt this system as well: aside from the obvious reason, that it may attract previously reluctant customers, the provider

can now proactively detect and diagnose problems. Some of the necessary steps in reaching this goal including building a system which supports tamper-evident logs, virtualization-based replay, trusted time stamping, and sampling using checkpoints. Due to lack of space we refer the reader to for more details. The accountable cloud is still being designed, and questions remain about whether such a system can be put in place with acceptable performance.

Virtualization in general increases the security of a cloud environment. With virtualization, a single machine can be divided into many virtual machines, thus providing better data isolation and safety against denial of service attacks. The VMs provide a security test-bed for execution of untested code from un-trusted users. A hierarchical reputation system has been proposed in the paper for managing trust in a cloud environment.

2. List Everyone Should Know

There are arguably an infinite number of items that users should be aware of and consider before choosing to use cloud computing or cloud operating systems. We attempt to list several of these items and do not in any way suggest that this list is complete.

Also, anyone viewing this list should be aware that security especially for something as dynamic as cloud computing is constantly evolving and growing and he or she should seek additional items.

1. Social Engineering is probably the easiest method for hackers to gain access to confidential material. Always review the authenticity of any form, email, or phone call when an individual is asking you for login information, passwords, or confidential information. If in question, go directly to the website of the organization and login, never login through a third-party source.
2. Cloud computing has security flaws but so does traditional computing. There are security flaws in every form of computing. The main determinant is how hard someone is willing to take advantage of the security flaws to get your information. Every user should be aware that no form of computing is safe, however measures can be taken to lower the chances of exposure.
3. Cloud computing is arguably more secure than traditional PC computing for most users. Within the cloud experts are responsible for maintaining the security of information and date being handled by the servers. Most individuals do not have the expertise or are not willing to implement the most up-to-date security features on their home PC. For this reason, many argue that cloud computing and cloud operating are actually safer than traditional computing.
4. Be aware of how confidential your data should be and act accordingly. No amount of security features will protect someone that blatantly posts confidential information in non-secure or public areas within the internet. A large portion of security is in the hands of the user. Similarly, a user should be aware of the level of required confidentiality of the data being used to determine what services should be used. For example, a user planning to create a blog will not want to keep their posts secure and hidden from the public because the author wants people to read the post. In contrast, an organization responsible for maintaining a list of social security number must be sure that the social security numbers are not available to the public and are protected from malicious attacks. The majority of the services made available on the cloud are more or less social instruments that are not typically secure sensitive. If you are planning to only use cloud computing for social instances and not post anything that should be kept from the public then you should not fear using the cloud computing. However, if the data is secure sensitive then further evaluation of the security offered by the cloud service should be evaluated.

Finally, the last item is to use reputable companies within the cloud and do research on companies that you are not familiar with to reduce your chance of falling victim to a phishing scam or false entity.

IV. CONCLUSION

Cloud, is prone to manifold security threats varying from network level threats to application level threats. In order to keep the cloud secure, these security threats need to be controlled. Moreover data residing in the cloud is also prone to a number of threats and various issues like security issues, accessibility issues,

confidentiality, integrity of data.Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider.In addition to this, cloud service providers must ensure that all the SLA's are met and human errors on their part should be minimized, enabling smooth functioning. In this paper various security concerns related to the three basic services provided by a Cloud computing environment are considered and the solutions to prevent them have been discussed.

V. FUTURE WORK

In this survey, we studied several key security concerns for Cloud computing environment from multiple perspective and the solutions were discussed that all users and organizations should be aware of, when deciding whether to use the cloud or not and this paper helps to find out the solution for the drawbacks found in other methods and come up with new solution or method to secure the cloud.

VI. REFERENCES

[1] L. Wang, G. Laszewski, M. Kunze and J. Tao, "Cloud computing: a perspective study", J New Generation Computing, 2010, pp 1-11.

[2] Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[3] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing,"2009, http://www.wheresmyserver.co.nz/storage/media /faq-files/clouddef- v15.pdf, Accessed April 2010.

[4] R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.

[5] Ertaul, L. and Singhal, S. 2009. Security Challenges in Cloud Computing. California State University, East Bay.

[6] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[7] Rohit Bhadauria et. al. paper on "A Survey on Security Issues in Cloud Computing".

[8] Joachim Schaper, 2010, "Cloud Services", 4th IEEE International

[9] Conference on DEST, Germany. R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing," The World Privacy Forum, 2009. http://www.worldprivacy forum.org/pdf/WPF_Cloud_Privacy_Report. pdf.

[10] Lori M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy Journal, vol. 7, issue. 4, pp. 61-64, July- Aug 2009, ISSN: 1540-7993.

[11] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience", 10th IEEE Int.Conference on High Performance Computing andCommunications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[12] Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, "Cloud Computing Research and Development Trend", Intl. Conference on Future Networks, pp. 93-97, China, 2010.DOI: 10.1109/ICFN.2010.58

[13] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine", ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264 2010, IEEE Computer Society, USA, 2010.ISBN:978-0-7695-3961-4.

[14] Youseff, L; Butrico, M; Da Silva, D., "Toward a Unified Ontology of Cloud Computing", Grid Computing Environments Workshop, pp. 1-10, Nov,2008, Austin, Texas. DOI: 10.1109/GCE .2008. 4738443.

[15] Julisch, K., & Hall, M., "Security and control in the cloud", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309, 2010.