Privacy and Security Breaches in Cloud Computing

Arun Balaji Buduru[1] and Rashmi Nagpal[2]

Abstract— **Cloud computing is an evolving paradigm with tremendous potential to significantly reduce costs through optimization and by sharing computing and storage resources. It offers powerful abstraction that provides agility, scalability and infrastructure as a service, thereby, enabling end-user to exploit supercomputing power on demand. Without investing in privacy and security solutions for cloud, this revolutionary paradigm could become a huge failure. In this survey paper, we revisit the debate on privacy and security breaches in cloud computing and explores the roadblocks to providing trustworthy cloud computing environment.**

Keywords: Privacy, Cloud Computing, Virtualization, Security, Vulnerabilities

I. INTRODUCTION

With the tremendous development of processing and storage resource computational resources have become far cheaper. This trend has enabled the realization of a new computing model called as cloud computing which uses pay-per-use business model. A study by Gartner[1] considered Cloud Computing as topmost important technologies and with a better prospect in successive years by organizations. Cloud computing enables on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity which are geared toward using clouds seamlessly and transparently.Its main objective is to provide secure, quick, convenient data storage, with all computing resources visualized as services and delivered over the Internet[2,3]. Further, it leverages the cost reduction through optimized and efficient computing[4,7]. Many companies such as Amazon, Google, Microsoft and others accelerate their paces in developing Cloud computing systems and enhancing its services to a larger amount of users.It seems impotant to start to setup applications in Cloud computing system or to adopt the services provided by it. As Cloud computing has advantages for both providers and users, it is increasing its base at exponential rate and is predicted to grow further and adopted by a large number of users in near future.[8] Although, there are many benefits to adopting Cloud computing, there are also some significant barriers to adoption.Most significant of all, is security, followed by issues regarding compliance, privacy and legal matters [9]. Since, cloud computing represents a new computing model, so there exists a great deal of uncertainty about how security and privacy at all levels can be achieved be it network, host, applications and data levels and how these are moved to Cloud computing[10].This uncertainty has led information executives to state that security and privacy are a major concern with Cloud computing. Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations which are moving beyond their data centers' concerns, a cloud solution provider must ensure that their data centers' network is under their control.

II. OVERVIEW OF CLOUD COMPUTING

This section presents a general overview of cloud computing, including its definition and a comparison with related concepts.

A. Definition

In this paper, we adopt the definition of Cloud computing provided by National Institute of Standards and Technology(NIST)[12], as it covers, all the essential aspects of Cloud computing:
Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg.,networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
In nutshell, cloud computing leverages existing technologies such as virtualization and utility-based pricing to meet the technological and economic requirements of existing technologies.

*This work was not supported by any organization

[1] Arun Balaji Buduru is with Faculty of Computer Science Engineering, Indraprastha Institute of Information Technology-Delhi,India arunb@iiitd.ac.in

[2] Rashmi Nagpal is an undergrad at Indraprastha Institute of Information Technology-Delhi,India rashmi14085@iiitd.ac.in

B. Related technologies

Cloud computing services are many-a-times compared with each of below mentioned technologies:

- **Grid Computing:** Grid computing belongs to distributed computing paradigm which provides dependable, consistent, pervasive & inexpensive access to computational capabilities.However, Cloud computing leverages virtualization technologies at multiple levels to leverage resource sharing and dynamic resource provisioning.

- **Utility Computing:** Utility computing represents service provisioning model in which a service provider makes computing resources and infrastructure management resources freely available to the customers as and when needed and charges them for specific usage rather than at a flat rate. While Cloud computing follows pay-per-use pricing business model. Hence, with on-demand resource provisioning and utility based pricing, service providers can truly maximize resource utilization and minimize operation costs.

- **Cluster Computing:** Cluster computing too belongs to distributed computing paradigm which comprises of a set of loosely or tightly connected computers which work together so that they can be viewed as a single system.More systems can be added to the clusters to improve its performance, redundancy and fault tolerance.

- **Virtualization:** Virtualization is a technology which abstracts away from the details of physical hardware and provides virtualized resources for high-level applications. Virtualization plays a vital role in Cloud computing as it bridges the gap between third party and software applications provided by cloud service providers.

III. CLOUD COMPUTING ARCHITECTURE

This section describes the architectural, business and various operational models of cloud computing.

A. layered model of cloud computing

: The architecture of a cloud computing environment can be divided into 5 layers: the cloud application layer, cloud software environment layer, cloud infrastructure layer, software kernel and the hardware layer.We describe each of them in detail:

- **Cloud Application Layer:** Instead of traditional applications, cloud applications leverage automatic-scaling feature to achieve better performance, availability and lower operational cost.

- **Cloud Software Environment Layer:** The second layer in our proposed cloud ontology is beneficial for cloud applications developers, for deploying and implementing applications on cloud.

- **Cloud Infrastructure Layer:** Cloud services offered in this layer can be categorized into: computational resources, data storage and communications.

- **Software Kernel:** This cloud layer provides the basic software management for physical servers which can be implemented as an OS kernel, hypervisor and virtual machine monitor.

- **Hardware Layer:** The bottom-most layer in cloud computing ontology, is responsible for managing the physical resources of the cloud including physical servers, routers, switches, power and cooling systems. Typical issues at hardware layer include hardware configuration, fault-tolerance, traffic management & cooling resource management.

B. Business Model

Cloud computing employs a service-driven business model i.e. hardware and platform-level resources are provided as services on an on-demand basis.However, services provided by clouds are grouped into three categories: software as a service(SaaS), platform as a service(PaaS) and infrastructure as a service (IaaS).

- **Software as a Service(SaaS):**SaaS ensures that complete applications are hosted on the internet and users use them. It eliminates the need to install and run the application on the customer's local machine hence, reduces the burden for software maintenance.

- **Platform as a Service(PaaS):**PaaS model aims to protect data, especially important in case of storage as a service. This model offers greater extensibility and greater customer control.

- **Infrastructure as a Service(IaaS)):** It refers to the sharing of hardware resources for executing services, using virtualization technology. With IaaS approach, multiple users use available resources which can be scaled up on the demand from the user and can be charged on a pay-per-use basis.
  .

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

- **Public Cloud** A cloud in which service providers offer their resources as services to the general public. Public clouds offer service key benefits to service providers.

- **Private Cloud** It is also, known as internal or enterprise cloud designed for exclusive use by a single organization. A private cloud may be built and managed by the organization or by external providers. It offers highest degree of control over performance, reliability and security.

- **Virtual Private Cloud** An alternative to addressing the limitations of both public and private clouds is called Virtual Private Cloud(VPC). A VPC is essentially a platform running on top of public clouds.

- **Hybrid Cloud** A composition of two or more cloud deployment models which are linked in a way that data transfer takes place between them without affecting each other. In a hybrid cloud, part of the service infrastructure runs in private clouds while remaining parts runs in public clouds.

For most service providers, selecting the right cloud model is dependent on the business scenario. For example, high scientific computation-incentive applications are best deployed on public clouds for cost-effectiveness. In particular, it was predicted that hybrid clouds will be the dominant type for most organizations.

IV. CLOUD COMPUTING CHARACTERISTICS

In this section, we have summarized several features showcased by Cloud computing which differs from traditional computing models:

- **Multi-tenancy** With respect to traditional applications, cloud applications leverage automatic-scaling feature to achieve better performance, availability and lower operating cost.

- **Shared resource pooling** The second layer in our proposed cloud ontology is beneficial for cloud applications developers, for deploying and implementing applications on cloud.

- **Elasticity**Such dynamic resource assignment capability provides much flexibility to infrastructure providers for managing their resource usage and operating costs. This characteristic, enables scaling up and down resources alloted to a service based on the current service demands. It helps in resource utilization, cost and service availability.

- **Ubiquitous network access** Clouds are accessible through the use of Internet as a service delivery network. To achieve high network performance and localization, many cloud centers are located at various parts around the globe.

- **On demand self service** User can provision cloud resources such as server time and network storage, without requiring any human intervention with service provider.This is one of the key features of cloud computing which can be obtained and released on the fly.
  The cloud model has motivated industry and academia to adopt cloud computing to host a plethora of applications randing from high computationally intensive models to light weight services.These models are well-suited for small and medium businesses because it helps in adopting IT without upfront investments in infrastructure,software licenses and other requirements.

V. CLOUD COMPUTING: STATE-OF-THE-ART

Cloud computing distinguishes itself from other computing paradigm, as discussed in introduction section in various demand service provision, user-centric interfaces, guaranteed QoS(Quality of Service) and autonomous system[10] etc. A few state-of-the art techniques which contribute to cloud computing services are :

- **Application Programming Interface(API)**:The whole bunch of cloud computing services are dependent on APIs as they allow configuration and deployment through them.Based on these APIs various functions like control, data and application are invoked and services are rendered to the users accordingly.So, its hard to imagine existence of cloud computing without APIs.

- **Web 2.0**: It refers to World Wide Web websites that empathize user-generated content, usability and interoperability for end users.It allows the users to interact and collaborate as creators of user generated content in a virtual community[11,12].

- **Service Oriented Architecture**: The service organization inside cloud interface is managed in the form of Service Oriented Architecture(SOA).SOA makes use of multiple services to perform a specific task.

- **Distributed application framework over clouds**: HTTP-based applications usually conform to some web-application framework such as Java EE.In modern data center environments, clusters of servers are used for computation and data-intensive jobs such as financial trend analysis. MapReduce[16] is one such software introduced by Google to support distributed computing on large data sets on clusters of computers.The open source Hadoop MapReduce project[17] is inspired by Google's work.At present, many organizations are using Hadoop MapReduce to run large data-intensive computations.

- **Distributed file system over clouds**: Google File System(GFS)[15] is a prominent file system developed by Google to provide efficient, reliable access to data using large clusters of commodity servers.Compared with traditional file systems, GFS is designed and optimized to run on varied data centers to provide high data throughputs, low latency and survive against individual server failures.

These technological advances has led to the emergence of Cloud Computing and has enabled a lot of service providers to provide hassle free virtualization services to the customers, fulfilling their demands.Most prominent ones are: Amazon-EC2(Elastic Compute Cloud), SQS(Simple Queue Service), SimpleDB,Google,Microsoft Windows-Azure,Salesforce.com,Sun Microsystems and top of all, S3(Simple Storage Service) amongst others.

With substantial rise in number of cloud computing deployments, issues related to security and privacy have become more sophisticated and distributed in the sense that the user-section for such services is growing by leaps and bounds[13,14].

With an increase in on-demand of cloud computing applications usage, the possibility of cyber attacks has also increased.The amount of significant information available with these applications is acting as a catalyst for distributed attacks on confidential information. Attackers could use information available to these applications for identity theft.In order to maintain, various security and privacy issues like confidentiality, integrity, authentication, authorization and mitigation from any disaster, following sections will describe in detail to mitigate from privacy and security breaches.

The most vital aspect of cloud computing is that it does give a number of security and privacy threats from the perspective of attacker for a couple of reasons.First and foremost, the traditional queries cannot be adopted as they have become quite obsolete, to the ever evolving cloud applications.Secondly, data stored in these applications is often subjected to different types of changes which may comprises of bank accounts, transactions history or any other confidential files, hence a small error may result in loss of data security.

VI. Security Aspects

Though cloud computing provides better utilization of resources using virtualization techniques but it is fraught with security risks[13].The complexity of security risks in a complete cloud environment is illustrated in Fig.1 below.

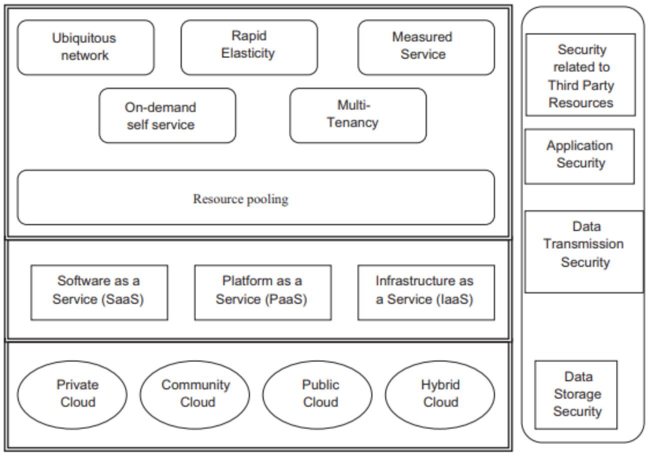

Fig. 1. Complexity of security in cloud environment.

In Fig.1, the lower layer represents the different deployment models of the cloud that are, private, community, public and hybrid cloud deployment layer which represents different delivery models that are utilized within a particular deployment models.These delivery models are SaaS(Software as a Service),PaaS(Platform as a Service) and IaaS(Infrastructure as a Service) delivery models.These models exhibit certain characteristics like on-demand self-service, multi-tenancy, ubiquitous network and rapid elasticity which are represented in top-layer. There are various security issues in the cloud : confidentiality, integrity, availability.These issues are as follows:

- **Confidentiality**:Confidentiality, refers to preventing the information from unauthorized access by any user.In cloud, confidentiality comes in the area such as intellectual property rights, covert channels,traffic flow analysis over the network, encryption techniques which is used to store the information and the inference mechanisms.

- **Integrity**: To maintain the consistency and correctness of the data is known as integrity.The cloud provider should ensure that unauthorized modifications are not made up on the stored data.

- **Availability**:Cloud Systems should be available for functioning properly when needed i.e. users should be able to use the cloud resources and systems when needed hence, they should be 24/7 available.For example, Ddos(Dynamic Denial of Service attack) hampers the availability of networks, service models and applications.
  In nutshell, to overcome these security issues efficient security applications must be incorporated by the cloud systems.Research should be carried out to make the cloud more secure and reliable.

VII. SECURITY THREATS AND CHALLENGES

In spite of ”Cloud computing” being a buzzword, there are certain aspects associated with Cloud Computing as a result of which many organizations are still in dilemma of shifting their database into cloud. Certain loopholes in architecture design of varied Cloud computing makes it vulnerable to security and privacy breaches.
Atleast half a dozen security breaches occurred last year bringing out the fundamental limitations of the security model of major Cloud Service Providers(CSP).
With respect to public-cloud computing scenario, we have multiple security issues which needs to be addressed.Since,in a public cloud enabling a shared multi-tenant environment,the number of users increases, security risks gets more intensified and diverse.Henceforth, it is necessary to identify the attack surface which are vulnerable to security attacks and mechanisms.[18]

A. Security Issues in the cloud deployment models

From security perspective, each of cloud services has its own advantages and limitations which needs to be addressed with a specific strategy to avoid them.

Security Issues in public cloud: In public cloud, there exist many customers on a shared platform and infrastructure platform.A few of the security issues in public cloud include:

- In case a Cloud Service Provider uses a third party vendor to provide its cloud services, it should be ensured what service level agreements they have in between as well as the contingency plans.
- Proper SLA’s should be adopted[19] such as what level of encryption data should undergo, when it is sent over the Internet and what are the penalties in case the service provider fails to do so.
- In case of public cloud, the same infrastructure is shared between multiple tenants and the chances of data leakage between these tenants are very high.However, most service providers run a multi-tenant infrastructure.
- Data must be protected during various stages of creation, sharing, archiving and processing.However, in case of a public cloud where we do not have any control over the service provider’s security practices.

Security Issues in private cloud:

- Virtualization techniques are popular in private clouds.In virtual environment it may happen that virtual machines are able to communicate with other VMs.To ensure that they communicate with the ones they are supposed to, proper authentication and encryption techniques need to be implemented.
- In private cloud, users are facilitated with an option to be able to manage portions of the cloud and access to the infrastructure is provided through web interface or HTTP end-point.
- The host operating system should be free from any sort of malware threat and should be monitored to avoid any sort of risk.Guest operating system should be able to communicate well with the host operating system directly.

Though, private cloud model is safer in comparison to public clouds, still they have multiple issues which if unattended may lead to major security loopholes.

The chief concern in cloud applications is to provide security around multi-tenancy and isolation, giving customers comfort besides ”trust us” idea of clouds[20].Service delivery models as discussed above, is one of many aspects which have to be considered to provide comprehensive evaluation over security issues.While security at different levels such as Network level, Host level, Application level is necessary to keep clouds up and running continuously.Various security breaches which may occur have been classified into below section:

1) Basic Security: :

- **Cross Site Scripting(XSS) attacks**: It injects malicious scripts into Web contents either by using Stored XSS or by Reflected XSS[21].In Stored XSS, the malicious code is permanently stored into resource managed by the web application and attack is carried out when the victim requests a dynamic page which is constructed from the contents of this resource.While in Reflected XSS, the attack script is not permanently stored: it is reflected back to the user.
- **Man-in-the-middle attacks**: In such an attack, an entity tries to include in an ongoing conversation between a sender and a client to inject false information and also, need to have that information transferable to the other end.Various tools helps to incorporate strong encryption technologies like Dsniff, Ettercap, Airjack have been developed.
- **SQL Injection attacks**: Here, the authors gain unauthorized access to a database and are able to access sensitive information.Various techniques like : avoiding the usage of dynamically generated SQL in the code, using filtering techniques to sanitize the user input etc are used to check the SQL injection attacks.

2) Network Level Security: :

Networks are categorized as shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats, which they have to deal with. There is less vulnerability in a private cloud than in public cloud.However, in case of public cloud implementation, network topology should be changed in order to implement security features and following have been addressed as a part of public cloud implementation:

- Ensure proper access controls within the cloud.
  - Security policies inside cloud should be upto date so that other parties within the cloud should be able to access information at any given point.
  - Since, the data is hosted over the cloud system, so it increases the chances of data leakage or a security breach.
- Encryption techniques and models should be changed to improvise security in a public cloud.
- Confidentiality and Integrity of the data-in-transit needs to be ensured in public cloud architecture.

  Other security issues which are associated with network level security consists of Distributed Denial of Service Attacks(DDoS), Sniffer attacks, DNS Attacks.

Distributed Denial of Service Attacks: : DDoS attack is an advanced version of DoS, in terms of denying the availability of services running on a server by flooding the destination server with tons of packets such that the target server is not able to handle such requests.In DDoS, attackers have the power to control the flow of information by allowing the amount and type of information which are available for public usage for a given interval of time. Basically, in DDoS attack which is run by three functional units: A Master, A Slave and A Victim.Master which is an attack launcher is behind all these attacks cause DDoS, Slave is the network which acts like a launch pad for Master as it provides a platform to the Master to launch the attack.

Sniffer Attacks: : These attacks are launched by applications which can capture packets flowing through the network and if the data transferred through these packets is not encrypted, it can lead to privacy breach.There are chances that vital information flowing across the network can be traced or captured.Using malicious sniffing tools like ARP(Address resolution protocol) and RTT(Round trip time)can be used to detect a sniffing system running on the network.

DNS Attacks: : Domain Name Server(DNS) performs the translation of a domain name to an IP address since, domain names are easier to remember.But in cases, when having server by name, the user is redirected to some other malicious cloud services instead of destination IP address.Also, it may happen that even after taking security measures, the route selected between the sender and receiver could cause security issues.

Human Errors: : Major cause of security breaches could be due to human errors.Human errors occurs when the cloud user fail to follow the instructions and guidelines and general carelessness.Such kind of data breaches are called as accidental data breaches.These errors include : wrong delivery of sensitive information to the unauthorized user either through email or messages or by innocently publishing information on social media.

Employee Misuse: : If it is an insider attack of the cloud services.The employees who are working in the cloud environment may involve in data breach activity as these employees have access as well rights over sensitive information stored in cloud.

VIII. SECURITY APPROACHES

In order to secure cloud computing applications against various types of security threats as mentioned above, various techniques supplied to cloud service providers must be adopted.A comparative analysis of some of the security schemes has been done in Tabular Chart 1.

Moreover, the need to have a generic security framework is much needed.Web security cloud's architecture rests upon two major components:

- **Multi layer security**: It helps to build multiple layers of security and hence, a better and stronger security platform.
- **URL filtering**: To ensure data security filtering the various web pages such that content from malicious can be blocked. Many biggest cloud service providers like Amazon Web Services, provides multi-factor authentication technique thus ensuring enhanced control over AWS account settings and management of AWS services and resources.

Comparative Analysis of various Security Schemes		
Security Scheme	Approach	Limitation
Data Storage Security	Use homomorphic token with distributed verification which supports dynamic operations on data blocks such as update, delete and append with any loss of data and data corruption.	Security in case of dynamic data storage should be considered.
Trust Model for interoperability	Trust strategies should be built up for service providers and customers which helps the customers to avoid malicious suppliers.	This scheme will only be able to handle only a limited number of security schemes in a fairly small environment.
Secure Virtualization	Advance Cloud Protection system should be incorporated as it ensures the security of guest virtual machines such that the behaviour of cloud components be monitored.	If adversary is able to pinpoint the location of other VMs, then ot may try to attack them.

TABLE I
VARIOUS SECURITY SCHEMES AND THEIR LIMITATIONS

Every cloud service provider has installed various security measures depending on its cloud offering and architecture.These models depends upon the user being served,type of cloud service they provide and the deployment models[22]. It is very important to secure the data-in-transit and security of transmitted data which can be achieved through various encryptiona and decryption schemes.An ideal security model will be one which has a dedicated portal for monitoring data coming in and out of a virtual machine on a hypervisor.So, when there is any suspicious activity observed, the corresponding virtual machine may be blocked or de-blocked so as to maintain security.

A. ***Server aided secure computation***

This security mechanism offers a server and users to perform computation on the cipher-text without revealing the contents of the original data.

B. ***Structured encryption***

It is a service level agreement between CSPs and its clients.It ensures the data to be stored in the CSPs servers would never be used by CSP without clients permission[28].

C. ***High-assurance remote server attestation***

Due to lack of transparency, many organizations are keeping form moving their information to the cloud.Information proprietors wish to perceive at how their information is being abused or used.So, this issue depends on trusted computing i.e. a trusted screen should be introduced at the cloud server to screen the activities of the cloud server.

D. ***Homomorphic encryption***

This encryption technique provides a mechanism to perform a specific type of computation on cipher-text which won't be possible with any other encryption technique.With this technique, data can be stored in the cloud as cipher-text format.

IX. PRIVACY ASPECTS

Privacy is an indispensable issue for cloud computing, both in terms of legal compliance and user trust; so needs to be considered at every crucial step of design funnel.Top database vendors are adding cloud support for their databases like Oracle is using Amazon's cloud service platform EC2, so more data is loading into the cloud, which leads to growth of privacy concerns as these databases often contain sensitive and personal information.Hence, certain steps should be executed by the cloud customer to add privacy enforcement structures to the software and data before transferring them to the computing cloud.

X. PRIVACY THREATS AND CHALLENGES

Several efforts have been established to conceptualize privacy - for example Westin[23] defined privacy as follows:

”Privacy is the claim of individuals,groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others”.

Over the span of time, organizations have been collecting information of individuals or events which may comprise of sensitive data, personally identifiable information,usage data or so.However, during collection, several tools and protocols for anonymization or encryption of data for confidentiality purposes should be followed.The authors[23] defined the concept of ”outsourcing privacy” where a database owner updates the database over time privately.In[24] authors discussed several privacy issues which are associated with genomic data sequencing and proposed a privacy-preserving model for genomic data processing using homomorphic encryption on genome-wide association studies. ”Anonymity” is another termed coined to ensure privacy of sensitive data.It is important to allay user's fears about usage of cloud services.Dilemma occurs when costumer are dubious and aren't aware of how their information will be used or passed onto other parties.

Lack of User Control: : When SaaS environment is used, service provider becomes responsible for storage of data,as it becomes storage and control limited.In cloud services, consumers' data is processed and stored in ”the cloud” on machines which they do not own or control hence, this lead to threat of theft,misuse or unauthorized resale.It can also, be difficult to get data back from clouds and to avoid vendor lock-in.

Lack of Customer Trust: : When it is not clear to costumers why their personal information is requested, or how and by whom it will be processed and what will be inferred from that information, this lack of control and visibility will lead to suspicion and ultimately distrust. This leads to security-related threats concerns whether data in the cloud services will be adequately protected or not[25]. Below table2, gives description of certain vulnerabilities in cloud computing.

Vulnerabilities in cloud computing	
Vulnerability	Description
Data-related vulnerabilities	• Data is often stored,processed and transferred in clear plain text. • Incomplete data deletion. • Information about the location of the data is usually unavailable or can't be disclosed.
Insecure interfaces and APIs	• Cloud service providers offer services which can be accessed through APIs(SOAP,REST or HTTP).The security of cloud depends on the security of those interfaces. Some problems include : Weak credential, Insufficient authorization checks etc. • Cloud APIs need to be updated regularly.
Vulnerabilities in Virtual Machines	• Unrestricted allocation and deallocation of resources with VMs. • Incomplete data deletion. • VMs have IP addresses which are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud.
Unlimited access of resources	Inaccurate allocation of resource usage can lead to inconsistent provisioning of resources.

TABLE II

VULNERABILITIES VS DESCRIPTION

Below table3, will depict certain privacy and security threats and their countermeasures.

Relationship between threats and their countermeasures	
Security Scheme	Approach
Zero-day exploit in the HyperVM virtualization application which hampered	Use HyperSafe
An attacker can gain insights of the victim's account to get access to the target's resources.	Trusted cloud computing platform should be executed.
Sniffing and spoofing virtual networks	Virtual network framework network modes: "bridged" and "routed"
Insecure virtual machine migration	A security framework which customizes security policies for each virtual machinie, hence provides continuous protection through virtual machine live migration.
Customer data manipulation	Web application is a program which scans web applications through the web front-end to identify vulnerabilities.
Data Leakage	Digital signatures proposes secure data with RSA algorithm while data is being transferred over the Internet.
An attacker can request for more computational resources,so that other legitimate users should not be able to access resources like in DDoS attacks.	Cloud Service Providers should force policies to offer limited computational resources.

TABLE III

THREATS VS COUNTERMEASURES

XI. PRIVACY APPROACHES

Since clouds can outsource processing, storage or maintenance of data seamlessly.

Data Handling Mechanisms

In order to help protect sensitive information, be it customer data or corporate data an organization using cloud services must take below measures:

- classify information assets to segregate which ones are confidential.

- before selecting a cloud service provider, determine data protection and business continuity capabilities.
- clarify ownership of data collected and what will happen when the agreement ends.
- clarify what will happen if data is lost.
- define policies for data retention and destruction.

Data Security Mitigation

To a large extent, privacy issues arise if data is not disclosed transparently within the cloud. Encrypting personal data is feasible, if using IaaS cloud service for simple storage. However, data-at-rest in cloud systems is not encrypted as encryption would prevent indexing or searching the data.So, in general customers will still need to pay close attention to the security of their data in the cloud.Another approach is to use, Google Secure Data Connector[26], which allows programs to access information behind its firewall.

Design for Privacy

Certain privacy concepts like Fair Information Principles[27] are applicable to cloud computing scenarios and can mitigate the risks.An initial approach is being provided in [27],building upon that generic approach of design for privacy is much needed.

Privacy Protocols

Cloud customer can add certain privacy enforcement structures to the software and data before transferring them to the computing cloud.For example, adding software execution and data processing protocol or privacy feedback protocol should be considered as it helps in designing privacy-aware cloud services.These protocols helps in informing users of different privacy mechanisms which are applicable to their data and make them aware of any data leaks or risks which may jeopardize the confidentiality of sensitive information.In data processing protocol, steps are executed by crypto co processor and the main server hosting the co processor to safely execute the customer cloud software.It presents the privacy enforcement mechanisms which ensure the privacy of customer sensitive data when processed in the computing cloud.

In summary, as the evolution of cloud can necessitate more fluid design specifications, and challenges traditional thinking about jurisdiction related to data protection[28].In particular, as users requirements change, functionality and privacy needs to be reassessed at regular intervals.Furthermore,data governance models needs to be re framed to take account of these changing infrastructures, and as a result legal as well as regulatory privacy requirements should significantly change over time.

XII. CONCLUSIONS

Cloud computing leverages many technologies but it also inherits their security issues.Traditional web applications, data hosting and virtualization have been looked over, but some of their solutions are immature or inexistent.We have presented various security issues for cloud models: IaaS, PaaS and IaaS, and types of cloud : private, public and hybrid..We have presented in this paper, various security and privacy concerns in Cloud Computing.We have shadowed upon the fact that ”Enumeration of security issues is not enough”, so we have to build a relationship between threats and vulnerabilities so that we can identify what vulnerabilities contribute to the execution of threats and helps to make system robust.Also, we have listed present solutions in order to mitigate these threats since traditional privacy and security components does not gel out well with cloud computing architecture.An integrated privacy and security model targeting different levels of security of data for a typical cloud infrastructure is under research.Though cloud computing is a disruptive technology[29] with profound implications not only for Internet services but also for IT sector as a whole.Still, several outstanding issues exist, particularly related to service-level agreements(SLA), security and privacy & power efficiency.Until a proper module is not in place, potential users will not be able to leverage the advantages of this technology.

REFERENCES

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

[2] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347358

[3] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 9397.

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

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

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

[7] Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP10), pp 278281

[8] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., Above the clouds: A Berkeley view of cloud computing, University of California, Berkeley, Tech. Rep, 2009.

[9] KPMG (2010) From hype to future: KPMGs 2010 Cloud Computing survey.. Available: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs-2010-cloud-computing-survey/2384291

[10] 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 and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[11] James Governor, Web 2.0 Architectures: What Entrepreneurs and Information Architects Need to Know by James Governor, May 15, 2009; OReilly; ISBN-13: 978-0596514433.

[12] Amy Shuen, Web 2.0: A Strategy Guide: Business thinking and strategies behind successful Web 2.0 implementations, O'Reilly Media; 1st edition; Apr 30, 2008; ISBN-13: 978-0596529963.

[13] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice), OReilly Media, Sep. 2009; ISBN: 978-0596802769. http://oreilly.com/catalog/9780596802776.

[14] R. Gellman, Privacy in the clouds: Risks to privacy and confidentiality from cloud computing, The World Privacy Forum, 2009.http://www.worldprivacyforum.org/pdf/WPF Cloud Privacy Report.pdf.

[15] Ghemawat S, Gobioff H, Leung S-T (2003) The Google file system. In: Proc of SOSP, October 2003

[16] Dean J, Ghemawat S (2004) MapReduce: simplified data processing on large clusters. In: Proc of OSDI

[17] Hadoop MapReduce, hadoop.apache.org/mapreduce

[18] Wayne Jansen, Timothy Grance, NIST Guidelines on Security and Privacy in Public Cloud Computing, Draft Special Publication 800-144, 2011. http://csrc.nist.gov/publications/drafts/800-144/DraftSP-800-144_cloud-computing.pdf.

[19] A. Verma and S. Kaushal, Cloud Computing Security Issues and Challenges: A Survey, Proceedings of Advances in Computing and Communications, Vol. 193, pp. 445-454, 2011. DOI: 10.1007/978-3-642-22726-4_46

[20] Ryan K.L.Ko, Bu Sung Lee and Siani Pearson, Towards Achieving Accountability, Auditability and Trust in Cloud Computing, Communications in Computer and Information Science, Vol. 193(4), pp. 432-444, 2011. DOI: 10.1007/978-3-642-22726-4_45

[21] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis, Proceedings of the Network and Distributed System Security Symposium (NDSS07), February, 2007.

[22] Amitav Chakravartty, Serena Software, Serena Service Manager Security in the Cloud.

http://www.serena.com/docs/repository/products/servi ce-manager/Serena-Service-Manager-Security-in-theCloud.pdf

[23] Y. Huang and I. Goldberg, Outsourced private information retrieval, in Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society, WPES 13, (New York, NY, USA), pp. 119130, ACM, 2013.

[24] K. Lauter, A. Lopez-Alt, and M. Naehrig, Private computation on encrypted genomic data, Tech. Rep. MSR-TR-2014-93, June 2014

[25] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing. 2009.

[26] http://code.google.com/securedataconnector/docs/1.0/overview

[27] Pearson, S. Taking Account of Privacy when Designing Cloud Computing Services. ICSE-Cloud09, Vancouver, IEEE. Also available as HP Labs Technical Report, HPL-2009-54, http://www.hpl.hp.com/techreports/2009/HPL-2009-54.html, 2009.

[28] Barona, R., and E. A. Mary Anita. A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats. 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT), 2017, doi:10.1109/iccpct.2017.8074287.

[29] Siani Pearson, Taking Account of Privacy When Designing Cloud Computing Services, International Conference on Software Engineering (ICSE) Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, May 23, 2009.

[30] Anna University Tirunelveli, Tirunelveli, TN 627007, India,S.SubashiniV.Kavitha ”a survey on security issues in service delivery models of cloud computing”, Computing, 201