International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 5 – No. 5, April 2013 – www.ijais.org

A Study on Security and Privacy Issues of Cloud Eco-System

Manu A R
PESIT, Bangalore

V K Agrawal, Ph.D.
PESIT, Bangalore.

K N Bala Subramanya Murthy, Ph.D.
PESIT, Bangalore,

ABSTRACT
Cloud computing is an Internet-based model for enabling appropriate on - demand network gateway to the pooled setup of computing resources and related infrastructure on sharing basis. Cloud computing offers four broad categories of services namely, IaaS, PaaS, DSaaS and SaaS. In these cloud services, individuals and organizations usually face security, privacy and trust challenges. Most of the R & D centers and researchers across the world are working towards resolving these security issues and achieving the trust among each other. In this paper we present a framework for unified security design which may help to resolve privacy, trust and security challenges that are faced in cloud- based networks. We also expect that this would help us to understand existing security challenges, while trying to achieve common standards for secure cloud services, design secure cloud transmission protocol, and devise an algorithm in this regard.

Keywords
Cloud Computing, Challenges, Security and Privacy Issues.

1. INTRODUCTION
If we look at the history of the evolution of computing system, in the initial stages end users accessed the computing resources and its utilities using the standalone desktop terminals and accessories. These were in turn connected to centralized mainframe systems. Later, after entering in to the era of networking and revolutionizing the telecommunication systems, resources started getting accessed using the web-based systems connected via the internet. This has resulted in the growth of parallel processing-computing, distributed computing, grid computing, and led to the development of cloud computing services. However, cloud computing is emerging form of distributed computing which is still in its infancy.
Cloud computing technology is an open standard service. It is Internet-centric, data storage and network- related computing services [1]. This cloud-based service can be randomly provisioned and discharged with least management effort. Cloud computing can be considered as a new computing paradigm with implications for larger flexibility, elasticity, accessibility and availability of resources and necessary infrastructure at a reduced price [1].
The Cloud computing facilitates a software deployment model, using **pay as you go model, standard subscription model, premium pricing model and various hybrid pricing models.** This allows the customer to acquire the basic computing setup of servers, software, necessary infrastructure and resources which are outsourced on demand. Using this model may help customers to reduce the cost of ownership, setting up and managing the computing infrastructure components individually or as an organization. This enables to use the cloud infrastructure for the required duration of time and pay an amount as a rental fee to the service provider based on the measured usage and consumption of resources.

As the market tends to expand it leads to the exponential growth of the business. This in turn would increase pressure on businesses in terms of not only competition but also additional capital expenditure - CAPEX and operational expenditure - OPEX for servicing the increased demand. Due to more capital investment and pressure, entrepreneurs face shortage of time, resources and capital investment to buy, acquire, deploy and manage the infrastructure to run their business and provide quality services at appropriate cost. The cloud computing utilities may support the future businesses with faster return on investments (ROI), faster to market and even gain productivity.
Summarizing, the benefits of cloud computing include the reduction in the requirement of the dynamically changing resource consumption, and promoting user- friendly greener environment. Further, cloud computing could potentially reduce the energy consumption by the various computing resources, storage setup and cooling resources.

Cloud computing technology provides various internet- based services. According to NIST-USA [1], these are categorized into four major categories of services namely:

- Data Storage as a service (DsaaS),
- Software as a service (SaaS),
- Platform as a service (PaaS) and
- Infrastructure as a service (IaaS).

Figure 1 represents these basic cloud computing services.

Figure1: Cloud Computing Technology services.

Cloud Computing Technique provides four types of deployment models that a customer can establish namely:

- Private cloud service setup,
- Public cloud service setup,
- Community cloud service setup and
- Hybrid cloud service set up [1].

An organization can make use of any one or more deployment model for their business persistence purposes.
With outsourcing of any IT (Information Technology) services to the third party, there exist concerns about the implications of IT security and privacy of confidential data. Particularly, for moving vital applications or data from one organization's computing centre to another. While reducing cost is a primary motivation for moving towards a cloud

service provider, security and privacy issues are of real concern.
To overcome the security and privacy drawbacks of internet protocols, as discussed in Section 2, our paper may show a way to devise the secured unified design of cloud services. This is an amalgamation of security measures as outlined by various organizations, like National Institute of science and technology [1] [2], and Cloud Security Alliance, International Standards Organization.

This paper is organized in the following manner: Section 2, describes the existing security challenges, Section 3 emphasizes the design to depict cloud security and privacy issues. Section 4 tells about conclusion of the work carried out and possible future enhancements.

2. CLOUD SECURITY AND PRIVACY ISSUES

This section enumerates and discusses various existing security challenges and issues that are involved in cloud computing services**.**

2.1 General Cloud Security Issues

As mentioned above, the cloud computing technology is based on internet services, and in the Internet services, secrecy and prudence of the information, unity and availability of the data and resources are the key issues. The way to access any services over Internet is through web browser. Web browsers typically use protocols such as http, https and s-http. In general, http is used in sending and receiving information between web server and web browser which happens without encryption. However, for sensitive trading, such as online e-commerce or cyber access to financial accounts, the web browser and server encode this information, referred as https. The https has been designed to withstand data hacking and also provides data confidentiality, whereas s-http allows encapsulation of messages like encryption, signing or MAC- based authentication. In literature we find many cloud computing security and privacy issues, and in this direction we have tried to present these security and privacy issues in consolidated form.

General Security issues associated with the cloud can be categorized into two broad categories:

i. Security issues faced by cloud service providers/vendors (organizations providing IaaS, PaaS, SaaS).

ii. Security issues faced by cloud service end users.

2.1.1 Security and privacy issues faced by cloud service providers

Security and privacy issues faced by cloud service are categorized under various domains such as, Governance Domain, Operational Domain and computer network Domain related issues. These are described below:

2.1.1.1 Governance Domain

In this domain the cloud service provider specific security and privacy threats involves the following issues in practice:

- Cloud computing design and framework, supremacy and governance, enterprise threat management.
- Legal and electronic detection, conformity and assessment planning, information system regulatory mapping, contract / authority maintenance, intellectual property.
- Data ownership, data classification, information – handling, labeling, security policy, data retention policy, secure disposal of data, risk assessments.
- Information life cycle administration and management, portability and inter-operability, infrastructure and asset administration.
- Employee recruitment, employment agreements and violation /termination from job (HR management), employee's background screening etc.
- Information Management- security management, support and involvement from management, framing and reviewing, and enforcement of the policy, law and baseline requirements.
- User access - restriction, revocation, authorization and reviews.
- Scheduling and organizing training and awareness, providing the real time industrial production knowledge and benchmarking over the same.
- Defining the roles and responsibilities, segregation of duties, management decision for providing the workspace etc.

2.1.1.2 Operational Domain

The operational domain issues are:

- Customer guarantee, business transaction endurance.
- Disaster recovery, data centre transactions, event feedback, announcement and rectification.
- Product protection, encoding and quintessential controlling, uniqueness and admittance management, virtualization [3].

2.1.1.3 Computer Network

In this domain the security threats may involve any one or more of the forms of following threats –
Denial of service attacks (Smurf, fragile, ping of death, SYN flood), Land – Exploits TCP/IP stacks using spoofed SYNs, teardrop, bonk, Back door- (Net Bus, Back Orifice).
Intrusion attacks, illicit/illegal content, Router/switch operating system attacks, viruses, worms, Trojans, Unlawful capture of content (spyware, redirects, phishing, Domain Name System (DNS) poisoning, Remote attacks on corporate networks, wireless intrusions, inside attacks, zombies.
SQL injection, exchange attacks etc... Existing features for security deployment using - spyware, antivirus, IPS VPN. End point security management using antivirus, desktop firewall, device control, hosts IDS etc… Spoofing, man-in-middle-attack, replay or rerun attack, TCP/IP hijacking.
Mathematical attacks (includes key guessing method), Password- secret code guessing, using brute force method, lexicon (dictionary word-searching) attacks, estimating logons and keys, Malevolent code- (bugs and Viruses – Infecting systems and multiply copies of themselves- self replicating), Trojan horse – camouflage malevolent code within apparently useful appliances, Logic Bombs, Worms – Self replicating forms of other types of malicious code, Java and Active X control – Automatically executes when sent via email, Societal Engineering operating people – the most vulnerable point in a network are the types of attacks based on network security.

2.1.2 Security issues faced by cloud service consumers

The security and privacy issues faced by the cloud service consumers include the following:
Governance, Compliance–law and regulations, Data location –electronic discovery, Trust–insider access, data ownership, composite services, visibility, ancillary data and risk

management, Architecture–attack surface, virtual network protection, virtual machine images and client-side protection. Identity and Access administration– verification and access control, Software isolation–hypervisor complexity and attack vectors, Data protection –value concentration, data isolation and data sanitization, data loss or leakage, Availability– temporary outages, prolonged and permanent outages and denial of service, Incident response–Data availability, incident analysis and resolution, authentication, use of unsafe API's (Application Programming Interface), shared technological flaws, storage flaws, privacy breaches, data retention, destruction, auditing and monitoring, perils of platform lock-ins, policies, system portability, violation of law and policies, jurisdictional/ location legal issues, lack of knowledge of the cloud platforms/services/applications supported, mismanaged performance guarantees, underestimating the cloud sprawl and agility, physical security, incompatibility of platform, lacking to follow standards and implementing the same, lacking up to date information to protect the data, hypervisor security, multi-tenancy, implementing the policies related to networking security, even-ting and reporting, reliability, lacking to follow open standards, compliance [4], lack of freedom to store and retrieve the data, long-term viability, following the weak cloud standards, secrecy, accessing data everywhere - substantially increases convenience, but also increases the associated risk , lack of the knowledge and don't always know where user data is, use of weak credentials, insecure protocols and web-based application flaws, lacking business continuity planning, budgeting and disaster recovery plans, lack of secure software development process cycle, vendor lock in, lack of adequate provisions in SLA and termination of service level agreements, unauthorized or inappropriate use of data.

Termination of user accounts without the knowledge of the customer, ownership of the data [5], publicity, disclaimer warranty service, and modification of the contract, automatic renewal, indemnification by both customer and vendors.
The consolidated view representing the vendor specific related issues is shown in Figure 2.

Figure 2: The consolidated view representing cloud service provider related issues.

2.2 Cloud Security Alliance-CSA Security Issues

This sub-section enumerates security and privacy issues, according to Cloud Security Alliance as shown in the figure 3 represents the consolidated view of issues/components as per Cloud security Alliance.

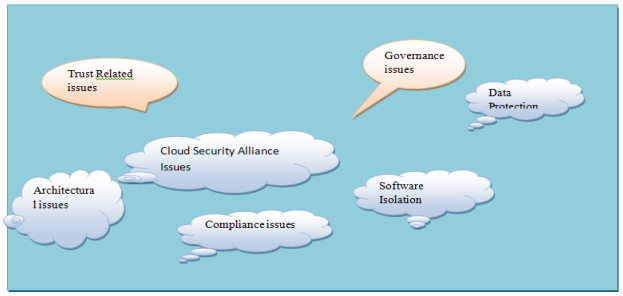

Figure 3: Consolidated view of Issues/Components – as per the Cloud Security Alliance

2.3 Cloud service specific issues

Here we summarize the various security threats and privacy issues for various cloud services. In the case of **SaaS**, issues like privileged access, authenticated access user types, it needs to ensure user authentication with correct privileges checking before using any appliance. For **PaaS**, before providing platform to launch customer application, ensure bug-free, vulnerability of platforms, multi-tenanted application remoteness, validation rights to meticulous user, is to be considered [6] [7]. In the case of **DSaaS**, before using storage service, it needs to ensure information defense, reliability, susceptibility and defense from intruder [7]. In the case of **IaaS**, before taking infrastructure, it needs to ensure the cases of physical security, privileged access rights, control and monitoring infrastructure, maintaining infrastructure, communication channel security, intruder detection, privileges to access the infrastructure, auditing techniques, etc. Table 2.1 presents an overview of the security and privacy issues of various cloud services [7].

Name	On demand service for	Consumer Control	Ensure security challenge
SaaS	Application, Just as with managed service supplier, corporation or consumers will require to investigate vendors policies on data security before using vendor services to avoid losing or not being able to access their data	No control on Operating system, Hardware, Network infrastructure.	Privileged access, authenticated access user types.
PaaS	Platforms (hosting environment). The consumer uses a hosting environment for their applications	Can control hosting environment not on Operating system, hardware, and network infrastructure on which they are running.	Bug, vulnerability of platforms, multi-tenanted appliance remoteness, and validation rights to scrupulous user. , PaaS service providers are responsible for the security of the platform software stack.
DSaaS	When securing and storing sensitive data, small-midsized businesses (SMBs) should look Storage area	No control	Data protection, integrity, vulnerability and security from intruder.
IaaS	Infrastructure computing resources, processing power storage,	Consumer Can manage Operating system, storage space deployed	Physical security, privileged access rights, control and monitoring infrastructure, maintaining infrastructure, communication channel security,

	network or middleware, demand fundamental computing resources	applications and possibly networking apparatus such as firewalls and load balancers, but not the cloud infrastructure underneath them	intruder detection, privileges to access the infrastructure, auditing techniques. Many of the potential issues arise because of the IT infrastructure is under the control of a third party. This includes conventional outsourcing/contracting, the outcome of a physical safety infringe which can have an impact on multiple customers (organizations)

Table 2.1: Cloud services security issues [7].

Figure 4 is the consolidated representing the security issues specific to Cloud services (PaaS,IaaS,SaaS, DSaas).

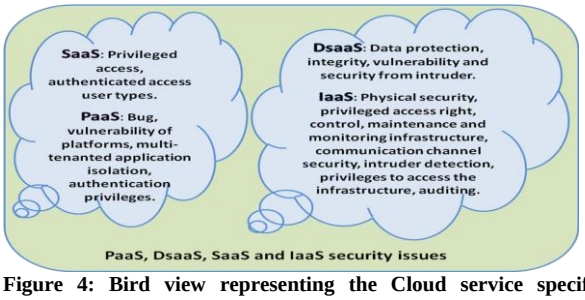

Figure 4: Bird view representing the Cloud service specific security issues

2.4 Issues Related to Virtualization and its Vulnerabilities

In the cloud computing environment, decisions about the allocation of Virtual Machines (VMs) to physical hosts are made entirely by the data center staff. The migration of data can occur between the physical hosts in the same or between the other datacenters. Other types of issues include Hypervisor security and other virtualization vulnerabilities. Customer depends totally on data center staff - this could be a concern to confidential data security of customer.

2.5 Legal Issues

Legal issues include authority, compliance, judicial and jurisdiction- related aspects [8] [9]. It is important to identify the technical and legal challenges that are faced by the cloud providers. Table 2.2 presents various legal issues specific to vendor and customer which we considered while designing framework.

Types of Legal issues	**Associations and applicability of legal issues**
Clientele related issues	Location and jurisdiction: Ownership of servers-Privacy laws, -accessibility to services includes-open ordeals, trade endurance, functioning, Post cessation of the agreement-Retention of data – security related to data are- Physical, Operational , Programmatic, –Privacy: Compliance with privacy laws, Privileged information (lawyer-client, doctor-patient), Court mandated disclosures, –Intellectual property: Trade secrets, Third party IP associated asserts,–restriction of liabilities, – tax assessment: custody of tax records –8 years in India, –Exclusion of warranties: –termination clause: Negotiate on the termination clause- "material breach" must be defined, –pretrial discovery: Presumption that all documents are in the possession, custody and control of a litigating party, –bankruptcy of the vendor: Customer must have permission to gain access to data, possession of data, reappearance of data etc…
Service Provider/Vendor Related Issues includes	Privacy laws: -Access/Transfer of data: –EU Data Protection Directive, –US has sector specific laws – e.g. HIPPA (business associate agreement), GLB, PATRIOT Act etc.,–Service Tax Liabilities: Services provided within India or imported into India is taxable, –Objectionable Content: Information Technology Act, 2000, –PRICING: Differential pricing based on types of services provided.
Data in Transit	Confidentiality as well as integrity needs to be taken care for data on transit, e.g.: FTP over SSL, HTTPS, and Secure Copy Program (SCP).
Data at rest	i) Encryption is ok with IaaS and is strongly suggested ii) Encrypting data at rest for PaaS, SaaS cloud applications is not always feasible, generally not encrypted, as it would prevent processing, indexing or searching of the data. However on-going research on homomorphism encryption scheme allows data to be processed without decrypting (requires immense computational effort) where and when the data is specifically located within the cloud? iii) Following path of Data is data lineage and is important for auditing and compliance purposes.
Data Provenance	i) Means not only that the data has veracity, but also that it is reckoning precise. ii) Financial and scientific calculations need Data Provenance.
Data Remanance	It is the residual representation of data that has been in some way nominally cleared or detached. These lees may be due to information existence left integral by a nominal erase operation, or by means of corporeal characteristics of the storage medium. The risk posed by data remnance in cloud services is that an organization's data can be inadvertently exposed to an unauthorized party-regardless of which cloud service you are using (SaaS, PaaS, or IaaS). Many CSP's rather refer to defiance with United States Department of Defense (DOD) 5220.22-M (the National Industrial Security Program Operating Manual).
Legal, E-Discovery	i) Functional: which functions and services in the Cloud have legal implications for both parties? ii) Jurisdictional: which governments administer laws and regulations impacting services, stakeholders, data assets? iii) Contractual: terms and conditions, iv) parties must understand each other's roles – trial hold, innovation hunts, – connoisseur testament, v) Provider must save primary and secondary (logs) data, vi) Where is the data stored? –laws for cross border data flows, vii) Plan for unexpected contract termination and orderly return or secure disposal of assets, viii) you should ensure you retain ownership of your data in its original form ix) Nondisclosure Agreements x) Third Party Agreements.

Table 2.2 Presents Legality Issue

3. DESIGN

In this section we envisage the design and frame work depicting to incorporate security and privacy design parameters which are enlisted in section 2. The main objective of designing the cloud security framework is to ensure security and privacy for customers using cloud services over the insecure Internet. Thus, this frame work may serve as a roadmap for IT organizations to understand, select, design and/or deploy cloud services. We begin our discussion of the cloud security architecture/framework and to illustrate industry oriented best practices and standards.

In this context to design our framework we try listing complete parameters of cloud ecosystem based on existing literature.

3.1 Few essential Cloud Characteristics:
We envisage few **essential Cloud characteristics [1][3] :**Broader network access, rapid elasticity, measured service, on-demand self service, resource pooling , simple and flexibility, billing, queues, web front end, provisioning, coupled security, client security, Internet web-browser features, online storage network systems, unified and federated, computer data reliability, information agility, reliability task, information access, business application cluster, device cluster, programming performance, user interface, web architecture, large scalability, powerful application, computing sites, software scalability,

maintenance, coupled resources, interface security, server architecture, reliable task, agility, application program interface, cost, device and location independence, virtualization – virtualized infrastructure, multi-tenancy – centralization peak-load capacity, utilization, and efficiency, security automation, automated life cycle management, data center centric, bring your own stack (BYOS), developer centric fully managed models, automated operations.

3.2Cloud service models

We find various **cloud service models** [Wikipedia]: **NaaS**- Network as a service, **SaaS**- web-based service, **DSaaS, PaaS, IaaS**- virtualized infrastructure as a service- infrastructure includes facilities, compute, and network and storage equipment, **SECaaS**- Security as a Service, **DaaS**- Data as a Service, **TEaaS**- Test environment as a Service , **APIaaS**- API as a Service, BaaS- Backend as a Service, **IDEaaS**-Integrated Development environment as a service, **DaaS:** Desktop as a service.

3.3 Evolution Stages of Cloud Computing

- **Cloud Computing:** IaaS, PaaS, SaaS, DSaaS
- **Federal Computing:** It provides a high-level overview of the key functional components for cloud computing services for the Government
- **Ubiquitous Computing:** It is a post-desktop model of human-computer interaction, vision of tiny, low-priced, robust networked routing devices, circulated at all scales
- **Grid Computing:** Distributed processing commoditize hardware, massive parallel processing, super computing
- **Centralized Computing:** Mainframe computers dumb terminals, Real time, time sharing

3.4 Existing Cloud Deployment Models [3]:

Private: own organization, on-premise, trusted.

Public: Third party managed and owned, off-premise, un-trusted.

Hybrid: own organization and third party owned and managed, both on premise and off-premise, both type trusted and trusted, community.

Managed: By third party, on-premise, trusted and un-trusted.

Community Clouds: Controlled and used by a group of organization those have shared interests, specific requirements of common mission, objective, vision and hype.

Shared Private Cloud: Shared compute capacity with variable usage based pricing to business units, undertaken by internal profit care centre.

Dedicated Private Cloud: IT Service Catalogue with dynamic provisioning that can be broadly deployed shared and dedicated into new and existing accounts and is a lower cost model.

3.5: MULTI –TENANCY

Multi-tenancy characteristics includes: Multi-tenancy in virtualized private cloud-on premise datacenter, multi-tenancy in virtualized public cloud off- premise data center.

3.6 Cloud Reference Model

Based on Cloud Cube model various cloud offerings/ properties can be viewed as: external, internal, proprietary, open, perimeterized, deperimeterised, in sourced, outsourced. Cloud Meta-model consists of following components: Concepts and packages, business, specifications, implementation, deployment, service. Various stages of cloud life cycle include the following stages: Planned, Specified, Provisioned, Certified, Deployed, Operational, and Retired. Figure 5 shows cloud references model as per CSA.

Presentation Modality | Presentation Platform
API – (Application program Interface)
Application
Information | Meta-data | Content
Assimilation & Middleware
Application Program Interface's
Generalization | Connectivity and Deliverance
Hardware
Competences

Figure 5: Cloud Reference Model [3]

3.7 Levels of control

Governance/Managerial control, Operational domain -related control and Technical control between people and cloud technology, Figure 6 depicts the various controlling parameters in cloud eco system. The following paragraph describes the parameters respectively:

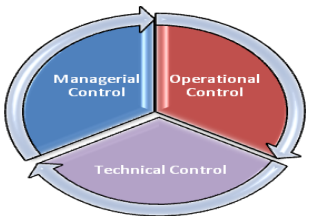

Figure 6: Cyclic representation of control

3.7.1 Governance Domain /Managerial control [10]

Listing and monitoring, policy, strategy, roles and responsibility includes: remote office employees, customer, partner, metrics and performance management, risk management: enterprise. Legal & regulatory: electronic discovery, education and awareness, conformity and assessment, (ILCM) data-life-cycle-management, portability and interoperability, document management, IT service tune-up administration, trade management, selling management, employee management, HR management, finance management, customer management: establishing trust, video collaboration .

3.7.2 Operational Domain

Conventional security, commerce continuity and DR, data center actions, event reaction warning and remediation, appliance defense, encryption key administering, uniqueness and admission management, virtualization, storage, awareness and guiding, pattern management, eventuality forecast, maintenance, media protection, corporal and ecological shielding, scheduling, private defense, system and data security, private defense, safeguard of production inputs and outputs.

3.7.3 Technical Domain Control

It includes strategic, technological implementations, accomplishments of security in the organization, system, communication protection, developing and integrating the controls into the business functions. It includes logical access controls- identification validation, consent, assessment and liability (including audit trials), cryptography, classification of assets and users, partner management, establishing enterprise collaboration, certificate accreditations, security assessment, system and services acquisitions.

3.8 Roles and Responsibilities of Various Actors in Cloud Eco System [Open Security Alliance]

Actor 1: Architect: Information flow enforcement, acquisitions, information security documentation.

Actor 2: IT Manager: Access controls, policies and procedure implementation, supervision and review, access control, security awareness & training, policy and procedures, certification accreditations, information system connection, configuration management policy and procedures, contingency planning, policy and procedures, identification and authentication policy and procedures, incident response policy and procedures, security planning policy and procedures, third party planning policy and procedures, system and communication protection policy and procedures, system and service acquisitions planning policy and procedures, external information systems, architects and management agree on baseline map to provide control framework and agree on minimal set of metrics observables.

Actor 3: Cloud Broker: Service intermediation, service aggregation, service arbitrage.

Actor 4: Third party Auditor: Security assessments audit, security certifications, security accreditations, privacy impact audit, performance audit.

Actor 5: End Users: Security awareness, access agreements, service level agreements.

Actor 6: In house Cloud Service Provider: Security services (PKI, Auth, Azn, and federation), account management, access enforcement, user identification and authentication, device identification and authentication, authentication management, cryptographic key establishment and management.

Actor 7: Developer: SDLC, security training, life cycle support, developer configuration management, developer security testing, flaws remediation.

Actor 8: Cloud service provider: Boundary protection: Across applications, across platforms: Security function isolation, resource priority, across infrastructure: application partitioning. Trust path, across provisioning and configuration management: baseline configuration, configuration change control, access restrictions for change, billing and usage control system. Across monitoring, logging, load and performance testing: audit monitoring analysis and reporting, continuous monitoring, monitoring configuration change, information system monitoring tool and techniques. Service orchestration, resource abstraction and control layer, physical resource layer cloud service management: business support, provisioning / configuration, handy/interoperability, user customized security objects, cloud personal work bench services, cloud ecommerce services, cloud data management services, cloud development platform services, cloud operating system services.

Actor 9: Administrator [IBM]: a)Workload resource administration and managing patterns : include virtual application, system applications, database patterns, managing catalog, deployment, system resources, b) Cloud group administration: managing cloud resources, access reports, c) Hardware administration: managing hardware resources, mapping, managing system resources, reports, d) Auditing: managing auditing resources-internal auditing log utilization, configuring external auditing, log storage server, security administration managing users-groups, managing security configuration, granting system resources, granting system access rights monitoring reports.

3.9 Core Fundamental Competences of Cloud Computing for Designing Framework.

3.9.1 Service management and provisioning

Service provisioning, SLA management, utilization monitoring and measuring, DR/backup, operation management , data management, utilization of resources & reduce cost, performance of infrastructure & assure service quality, scale and accelerate deployment of infrastructure & services, ensure continued business operations, resiliency & security, accelerate and optimize the release & deployment of applications, visibility, control, automation, cloud bursting, better computer acquisition decisions, operational efficiency, systems virtualization, storage space virtualization, Input / Output virtualization, appliance virtualization, verify policy and procedure to handle certain workload and script them automatically build up and teardown the environment to meet workloads SLA's, partition in scale up create resource pools in scale out, file/print services, mail services, web services, balanced systems designs include performance, availability, memory capacity, integrated systems/storage/network and database management. Access points, managing underlying systems/storage/networking functions will need to be monitored and controlled, intelligent orchestration (and coupled libraries), programmed policy-based proviso, job-flow management, SLA (service-level-agreement) and management, energy monitoring and management, and real-time workload handling responsiveness, transparently to handle unexpected workloads, integration, on security software site licenses to cover hundreds or thousands of distributed nodes, ramifications on server availability, superior systems and application management, rapidly deliver quality service.

3.9.2 Security and data privacy

Data network security, data privacy, certification accreditation and regulatory compliance. Authentication & authorization, auditing and accounting, complexity of risk assessment, legal rules for data processing, data replicated, expected level of security and privacy, protecting consumer privacy e.g.: profiling, online behavioral advertising. Breaches can, result in punishment, lawful action, business failure and societal damage. Protect the stored personal data against unauthorized, access, copy, leakage or processing, deletion of data so that it cannot be recreated. Transmission and login, no information has been provided about what data are logged or how long the log is stored, data protection principles and rules for police and judicial cooperation in criminal matters.

3.9.3 Data center infrastructure

Routers / firewalls, Local Area Network / Wide Area Network, internet admittance, hosting hub, devoted servers for elevated concert needs, high fault tolerance, dedicated CPU, disk, RAM, and networks, load balancing, utilizing RAID 10 storage, IT racks, clustering of servers, pooled arrays of servers, closed-coupled cooling to enable hardware to perform at peak levels, security from unauthorized access, video, surveillance, fire and safety, provisioning including camera, key cards. Onsite guards or biometric authentication, physical infrastructure monitoring over the intranet, clear visibility of all datacenter assets, dynamic data center solutions, virtualization and convergence, greening as bi-product of broader industry transformation towards consolidation , virtualization of the cloud, optimize their facility through the increased energy efficiency and innovative data center trends, usage of new renewal energy forms that are available for the datacenter, Co-location facilities, convergence and optimized

infrastructure virtualization, agility and flexibility, power and cooling, green retrofits, quality control, resiliency, orchestration, scalable multitier infrastructure, ability to alter capacity as needed to optimize CAPEX, and OPEX. Scalable space, geographic diversity, network links, fiber links dedicated generators and battery backup, reliability and interoperability, new generation, outdoor datacenter for SME with high integration facility, rapid deployment and provisioning on demand.

3.10 Various Skeptics of Cloud Services

3.10.1 SaaS:
i) Societal Engagement: Social networking, collaboration and participatory tools.
ii) Government Productivity: Email/ IM, virtual desktop, office automation [12].
iii) Government enterprise apps: Business service apps, core commission apps, legacy apps (mainframe), packaged application, custom application, and native cloud applications developed specifically to be working under the cloud paradigm, ported cloud applications, where the applications which were originally deployed in the traditional license model are ported to the cloud environment. Merchandise re-designing is vital in several cases to support multi-tenancy and implementation of new security models.

3.10.2 PaaS
Database, developer tools, DBMS directory services, multi tenancy, cache, workflow, message services and data services, client libraries, cache, data services, validation / approval, job-flood (procedure, policy and rationales), multi-tenancy support, messaging services, etc., provides various development tools in the form of components and supports multiple client programming language libraries, data mapping, to and fro data transfer procedures, design and development of multi tenant business application providing dynamic dashboards and reports for sales performance and customer satisfaction.

3.10.3 IaaS
Storage, virtual machines, web hosting, app servers, content distribution network, failover backup, VM provisioning, database, storage, application server, it provides the complete infrastructure requirements for the development and execution of the cloud solution including the sustaining hard-ware, software, and the supplementary allied infrastructure. This stratum should be at slightest as potent, protected, vigorous, trustworthy, and accessible as any physical infrastructure within some of the most sophisticated goods of the ISV. The infrastructure stratum typically comprises a combination of one or more components: physical, compute (CPU's), network and storage and is required to immediately provide additional virtual machines as and when the customer apps insist it, to guarantee flexibility-an vital attribute of cloud computing.

3.11 User Tools Used Throughout Cloud Eco System

- Application integration: API's, work flow engine, mobile device integration, data migration tools [11].
- User /admin portals: User profile management, order management, trouble management, billing/ invoice tracking, product catalog.
- Reporting and analytics: Analytic tools and reporting.
- Security devices: Sensors and connected devices, embedded devices, sensors, digital cameras, measuring meters.

3.12 Cloud Decision Strategy by Cloud Consumer to Select the Cloud Vendor and Identify the Cloud Services [Gatrner 2012].
Step 1: Pre-work: Create cloud computing core team, formulate business operations, scope the effort and requirements, formulate cloud adoption principle, and make feasibility study.
Step 2: Business and application assessment: Instigate the business intelligent survey, establish an internal const models, evaluate the changes to organization procedure before and after the adoption of cloud, identify and classify application requirements and dependencies, application external cloud ready, keep the application internal.
Step 3: Vendor selection procedure: Create and submit the RFT, review vendor response, select suitable vendor, revaluate the app, send RFO and kickoff migration planning.
Step 4: Mitigate risk and liability: Devise an exit strategy, explore other risk mitigation option, identify the risk acceptable, and add the app to the cloud road map.
Step 5: Steady state: Manage vendor, govern internally, and review regularly.

3.13 Blueprint or strategy for cloud migration [3]

- Shifting from infrastructure to service management,
- Prioritizing services that are best suited for migration,
- Selecting the best cloud provider.

3.14 Identifying the Technology Economy and Business in the cloud services

3.14.1 Technology
Centralized compute and storage, thin clients, PC's and server for distributed computer storage etc. larger DC's, commodity hardware, scale out devices.

3.14.2 Economic
Optimize for efficiency due to high cost, optimized for agility due to low cost, order of magnitude better efficiency agility.

3.14.3 Business
High upfront costs for hardware and software, perpetual license for OS and application software, pay as you go and only for what you use.

3.15 Various Service Measurement Index SMI [29]

3.15.1 Agility
a) Capacity/Elasticity b) Adaptability c) Flexibility: Portability, replace-ability d) Awareness/Visibility.

3.15.2 Risk
a) Provider: Business stability, certification, contract/SLA verification, supply chain, ethically, b)Compliance: Audit-ability c) HR d) Risk communication, context establishment, risk assessment, risk treatment.

3.15.3 Security
a) Physical and environmental b) Communications and Operations c) Access control d) Data- i) Policy: Retention/Disposition ii) Accountability iii) Geographical/Political iv) Ownership v)Privacy and Data loss vi)Integrity.

3.15.4 Cost
a) Acquisition b) On-going

3.15.5 Quality
a) Serviceability: i) Maintainability ii) Supportability iii) Service Continuity b) availability: i) Reliability ii) Stability iii) Resiliency/Fault Tolerance iv) Root Cause

Analysis/Analyzability v) Recoverability c) Function ability: i) Suitability ii) Accuracy iii) Testability iv)Interoperability v)Transparency d)Effectiveness i) Value, ii)Efficiency : service response time, sustainability iii) Usability : Install-ability, learn-ability, operability, understandability iv)Contracting experience

3.15.6 Capability:

3.16 Cloud computing ecosystem and its related characteristics

3.16.1 Projects
a) Cloud decision, b) Procurement: vendor selection, budgeting, c) Planning: legacy versus green-field, time lines, architecture, d) Development: prototyping, testing, e) Production: operation, data recovery/ BCP.

3.16.2 Cloud stack
a. Virtualization, b. Storage, c. Cloud OS: API, metering, virtualization abstraction, storage abstraction, d. DC management, e. Cloud management: provisioning, configuration management, hybrid cloud integration, operation, automation: auto-scaling, auto-recover, backups, governance: data integrity, monitoring, key management, audit, inventory, identity, financial constraint

3.16.3 Types of cloud
SaaS, PaaS, IaaS (storage, compute).

3.16.4 Deployment models
Private -(internal, external), public- multitenant, hybrid.

3.16.5 Characteristics
Calculated service, speed flexibility, appliance pooling, and broader network access, and on - demand.

3.16.6 Benefits
Security, flexibility: auto-scaling, rapid provisioning, auto recovery, R & D, training, sales demos, time to market, financial: no CAPEX, lower costs, greater automation, geography: fault tolerance, automated DR, regulatory flexibility.

3.16.7 Barrier
Security: encryption, transparency, key management, identity management, access controls, audit controls, intrusion detection, control, maturity. 8. Governance: data integrity, monitoring, audit, inventory, identity & access, financial controls, jobs, compliance, vendor.

3.17 CSA Security Control Model

- **Application:** SDLC, Binary Analysis, Scanners, Web App, firewalls, transactional security
- **Information:** DLP, Database Monitoring and Encryption., CMF
- **Management :** GRC,IAM,VA/VM, Patch and Configuration managing, watching
- **Network:** NIDPS, firewalls, DPI, Anti DDOS, QOS, DNSSEC, O Auth
- **Trusted Computing:** Hardware and Software, ROT & API's
- **Compute and Storage:** Host-based firewalls, HIDS/HIPS, Integrity and file / Event and Logs management, Encoding, facading
- **Physical :** Physical Plant security, digital cameras and security guards

3.18 Existing Compliance Model [3]

- **PCI**
  - Firewall
  - Code Review
  - WAF
  - Encryption
  - Unique User ID's
  - Antivirus
  - Monitoring/IDS/IPS
  - Path/ Vulnerability Management
  - Physical Access control
  - Multifactor Authentication
- **HIPAA**
- **GLBA**
- **SOX**

3.19 Various Security components and parameters: to be implemented at different layers include: a) physical security, b) logical network security, c) host security, d) transmission level security, and e) database security. These measures need to be implemented at various layers as shown in Figure 7.

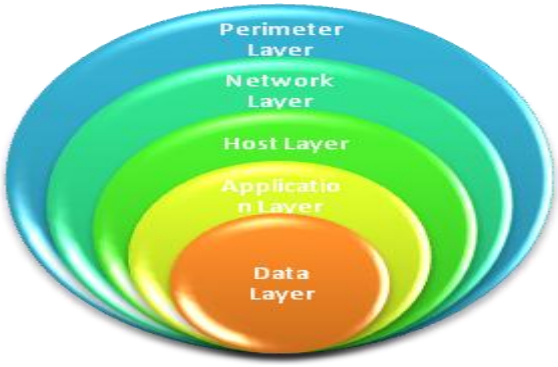

Figure 7: View of the layers to which security has to be incorporated.

For designing the framework one has to consider different parameters like policy, standards, baselines, guidelines, procedures etc. As shown in Figure 8.

Figure 8: Hierarchy of the parameters / components to be followed for framework design

Figure 9 depicts the security and privacy issues, aspects highlighted in Section 2, which is to be considered while designing the framework. This design involves all the issues presented in section 2, related to the cloud issues faced by cloud service provider, cloud consumers, general network issues and various deployment issues involving the guidelines as per NIST, CSA, and various other standard consortiums.

Figure 9: Generalized views for security and privacy issues.

The CSA security architecture to be defined from various perspectives is presented below figure 10:

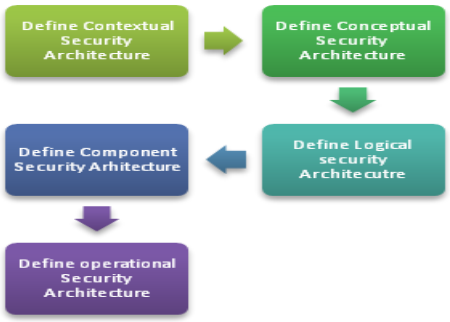

Figure 10: Steps to define the security architecture

3.20 Security Layer Model [3]

GRC, business continuity, SIEM, identity access, cryptography, data security, application layer security : business application, platform security: execution runtime, application server, web server, database development tool infrastructure layer security: cloud groups, virtual machines, networking, virtual network, disk storage, OS, firewall, host security, network security, physical security.

3.19 Overview of existing cloud services level layer

3.19.1 User Security & Monitoring

Identity Services – Auth N/Z, federation, delegation, provisioning information security – data supporting services: auditing, super user, privilege management.

3.19.2 Application Security

Business oriented application stack, service connectors, database, and storage.

3.19.3 Platform Layer Security

Execution runtime, application server, web server, data base server, development tool, PaaS services- no SQL, API, message queue, storage, blob services, guest OS – level (firewall, hardening, and security monitoring. hypervisor / host level (firewall, security monitoring), network layer (BGP, weight balancers, firewalls, defense monitoring).

3.19.4 Infrastructure Security

Cloud groups, virtual machines, networking, virtual networks, disk storage, OS firewall, encryption (transit, rest, processing), key management, ACL, logging, testing apps & API's for vulnerabilities, hardening virtual image, security controls: multifactor authentication, fine granular authorization, logging, security automation: automatic provisioning of firewall guidelines, licensed accounts, DNS, appliance uniqueness. Figure 11 presents the components of cloud security.

Figure 11: representing the components of cloud security.

3.19.5 Cloud Data Stages includes

Data isolation, data deletion, data encryption, data location, data portability, data integrity, data backup, data recovery, secure data migration, data security, and data platform independent.

3.20 Security Management

Visibility – Access control, event correlation centralized. authentication, identification, authorization, identity + key management, audit trials, backup redundancy recovery, forensics + investigation, cryptography, auditing and monitoring, unified computing system, port security, authentication, QOS features, data-ONTAP, security features, authentication, access control infrastructure security features are enabled to defend gadget, traffic jet and manage jet, implicit Access, VM ware shield, virtual firewall, real time monitoring, firewall rules, NAT services, virtual switch monitoring, service node (data center service security), IDS/IPS: provide traffic analysis and criminal identification, network investigation – offer passage supervising and data analysis, application firewall: mitigates XSS, HTTP, SQL,XML- based attacks, initial filter for DC ingress and ex-gress traffic, virtual context used to split policies for server-to-server filtering, server load balancing masks servers and application, ACL's, port security, VN Tag, net flow, ERSPAN,QOS, COPP, DHCP, SNOOPING.

4. CONCLUSIONS AND FUTURE ENHANCEMENT

Cloud computing is a technology that uses the internet and central remote servers to maintain data, platforms, infrastructure and services. Cloud computing allows customers and corporate members, to use appliance, platforms, infrastructure without installation and access their personal files at any computer with internet access [20]. However, there are internet security issues that need to be addressed. We have proposed the cloud security framework design and cloud security architecture for secure cloud transmission. It is expected to create such secure channel over insecure internet. It is important to adopt the existing security solutions at various layers for deployment in cloud environment. It is proposed with strict authentication techniques and cryptographic approaches. Framework design and cloud security architecture, which are presented in this paper may help to fix the major security challenges which are identified in http and related protocols for cloud computing services. Our future plan is to carry out the unified

architecture and detailed design along with its security proof implementation strategy.

5. ACKNOWLEDGMENTS

The successful endeavor of any task ends only after acknowledging the help received from all quarters for the completion of the task. We express our sincere gratitude to **Dr. Shylaja. S** Prof and Head of Department of Information Science and Engineering for providing us with all necessary facilities.

6. REFERENCES

[1] National Institute of Standards & Technology, Definition and standards, on cloud computing.

[2] N. Sarat Chandra Babu, "Cloud Security", CSI. Proceedings of the international conference on advances in cloud computing, ACC-2012, July 26-28.

[3] Security Guidance for Critical Areas of Focus in Cloud Computing - *CSA.*

[4] Whitehall drives open standards compliance regime

[5] David Bicknell Published 01 November 2012.

[6] "The-Emergence-of-As-A-Service-Offerings-That-Are-Not-Cloud-Services", Business & Technology Sourcing Review - Issue 18, 19 Dec 2012.

[7] White paper "The Seven Standards of Cloud Computing Service Delivery" - Salesforce

[8] Dinesha H A, V.K Agrawal "Framework Design of Secure Cloud Transmission Protocol", IJCSI, Vol. 10, Issue 1, No 1, January 2013

[9] Government of Saskatchewan Reference document – Plan and annual Report, Comprehensive guidelines

[10] CONCURRENT JURISDICTION PLANNING, GUIDELINES,AND APPLICATION - MICHIGAN SUPREME COURT, State Court Administrative Office

[11] N. Sarat Chandra Babu, Cloud Computing Overview National Workshop on Cloud Computing, 21st May 2011 C-DAC, KP, Bengaluru

[12] Slidesharenet "Cloud computing vision and strategy feb - 2010, GSA draft.

[13] Scribd- doc-48631944-1-Cloud-Computing.

[14] Principles of practices of information security – Michael E. Whitman, Herbert J. Mattord. Cengage learing, India edition.

[15] "Planning Guide Cloud Security", Seven Steps for Building Security in the Cloud from the Ground Up, Intel

[16] Planning for Security – VTU elearning Dr. Nalini N. Prof. & Head, Dept of CSE,NMIT,Bangalore

[17] HTTP: Communication Technology Proceedings-2003. ICCT 2003. International Conference on Study on conformance testing of hypertext transfer protocol by Xiaoli Yu; Jianping Wu; Xia Yin; Dept. of Computer. Sci., Tsinghua Univ., Beijing, China.

[18] Microsoft -licensing-options and enrollments.

[19] Security Challenges with Virtualization – *Thesis by Hans Peter Reiser*

[20] Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra, Diego Zamboni, "Cloud Security Is Not (Just) Virtualization Security", CSE-PSU, IBM T.J. Watson Research

[21] "Security in Inter Cloud",

[22] Wikipedia – "Cloud_computing_security".

[23] Ibm developer works-websphere-techjourna--0904_amrhein.