An Approach to Enhance Security of Cloud Computing Services using Software Engineering Model

Manu A.R.
PESIT, Bangalore

Dinesha H.A.
PESIT Bangalore

Manoj Kumar M.
NMIT, Bangalore

V.K. Agrawal, PhD
CORI, PESIT, Bangalore

K.N. Balasubramanya Murthy, PhD
Vice-chancellor, PES University, Bangalore

ABSTRACT

Cloud computing has great prospective of benefitting rigorous computational supremacy to the civilization society at reduced price. It facilitates consumers amid restricted computational assets to subcontract their bulky computational work assignments to the cloud, and cost-effectively have the benefit of the immense computational supremacy, bandwidth, storage, and even suitable software that can be pooled in a pay-per-use manner.

Regardless of the tremendous acceptance, security and privacy is the primary and major hindrance that stops the broad acceptance of this endowed computing sculpt, particularly for consumers whilst their private data or information are possessed and produced during the computation.

Delighting the cloud since an inherently timid insecure computing stage from the perspective of the cloud consumers, in this work we devise cloud computing life cycle model to facilitate not only to defend confidential information by permitting computations with encrypted records, but also shield consumers from malevolent performances by permitting the validation of the computational outcome. Such a scheme of broad-spectrum of protected computational subcontracting lately shown to be viable in hypothesis, but to devise method to facilitate practically efficient also remains as an extremely challenging task. Focusing on engineering and computing approach for minimization tasks, this paper proposes widely applicable method through proper design of the secure model for implementing the security measures in the cloud life cycle model using the software engineering approach.

Keywords
Cloud computing, Security, Privacy, Cloud life cycle, Services.

1. INTRODUCTION

Cloud computing is online Internet-centric computing based model for enabling convenient, pool of shared resources, software and information services are offered to computers and erstwhile devices on - demand, like an unrestricted utility [1] [2]. The term cloud is coined as a simile/metaphor for the Internet, supported on the cloud blueprint used previously to represent the communication networks and later to portray the Internet, as a notion of the core infrastructure, it symbolizes.

Cloud computing vendors deliver universal trade functions online which are accessed and obtained via web browser, whilst the software and information/records are accumulated on servers. It is the initiative of accessing the records, files, data, software applications and other computing services over the Internet, instead of own personal computer, notepads or mainframe computers. In general, cloud computing consumers do not possess/own the corporal assets, instead evading the investment costs, hire the service by lease the usage from a third-party service provider. They crunch through the resources as a facility services and pay only for resources they consume, using the pay as they use (go) model.

Cloud computing provides computation, software, information, network and storage space that do not involve customer acquaintance of the physical locality and configuration of the system that delivers the services [3] [4]. Cloud computing services benefits in i) reducing hardware installation cost. ii) reducing cost of infrastructure maintenance iii) e-waste minimization iv) on demand, anywhere, from any devices v) efficient usage of electrical power vi) flexibility and highly automated virtual business setup, which is easier to replace, upgrade and easier to maintain and manage.

Cloud service activities are upgraded or improved by the cloud service provider based on the customer needs. This work identifies the security issues of the cloud services and proposes engineering approach to ensure effective and secured use of cloud services over insecure internet.

The paper is organized as follows: Section 2 depicts different Cloud Computing services. Section 3 provides information about cloud computing deployment models. Section 4 addresses cloud computing security issues. Section 5 describes, design of Cloud Computing life cycle security model using engineering approach. Section 6 presents concluding remarks and future work.

2. CLOUD COMPUTING SERVICES

Cloud computing is an maturing fashion of computing where applications, information and resources are provided to users as a services over the network and these services are accessed over the web, personal computers, notepads, tablets, main frame computers and mobile apps connected to communication network, while the business related application software and customer data are stored on servers at a isolated geographical location different from customers location, where the control is vested with the service provider. Cloud Computing services are categorized as SaaS, DSaaS, IaaS and PaaS[1] .

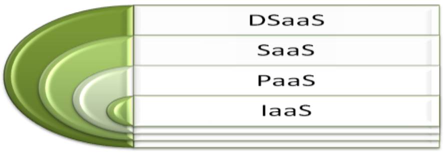

Fig. 1: Cloud Computing Services

Cloud SaaS (Software as a Service) SaaS costs by removing the effort of procuring the software application, developing the application, maintenance and delivery of the software totally eliminating the software licensing and infrastructure costs; and reducing capital expenditure (capex) for management, support and administration. SaaS solutions deliver software applications over web, where the service vendor deploys the software to the end user on demand normally through the licensing model. SaaS consists of application, data, runtime, middleware, operating system, virtualization hypervisor manager, server storage, and network [5 6].

Cloud PaaS (Platform as a Service) In PaaS public cloud service providers are actually offering an entire Platform as a Service. They provide the base to build highly scalable, flexible nature, measured and robust web base apps in the same way as traditional operating system done in the past for software developers. In PaaS an entire application development environment, not just the use of an application, PaaS solutions provide a cloud hosted virtual development platform, accessible via a web browser. This relinquishes application development and execution time platforms as a service. These may include programming languages, run-time construction of abstract, database catalogue services and more. It saves investment by reducing capex software licensing and infrastructure costs, and by reducing ongoing opex for development, testing and hosting environments. PaaS consists of set of connections, storage space, server virtualization, operating-system, middleware, execution-time forecast etc [5 6 7].

Cloud DSaaS (Data Storage as Services) Cloud computing provides internet - based on demand replicate copy of the back-up storage tune-up to consumer. Cloud DSaaS vendors are responsible for customer data to keep confidentially as per Service Level Agreements[7]. The ability to leverage storage that physically exists remotely but logically a local storage resource to any application that requires storage of data or information.

Cloud IaaS (Infrastructure as a Service) is on demand infrastructure set up service. It consists of infrastructure virtualization, server, storage, and network. It helps in massive provision of infrastructure resource requirement handle peak in demand; resources can be dynamically scaled up and down based on need, reducing capex and ongoing opex for support, maintenance, management and administration, organization – end user consuming infrastructure from the service vendor, and access the service over web. Organization can massively increase their datacenter resources without significantly increasing the human resource staff needed to support it [5 6 7].

Cloud Information as a service: This refers to the ability to consume any type of remotely hosted information – stock price information, address validation, credit reporting etc.

Cloud Security as s service: It is the ability to deliver security services remotely over the internet.

3. CLOUD COMPUTING DEPLOYMENT MODELS

Cloud computing delivery model can be categorized in to four types of deployment models as per NIST [1] namely: Private, Public, Community and Hybrid. Brief descriptions of these models are given below.

3.1 Private Cloud

In private clouds a business essentially turns its IT environment into a cloud and uses it to deliver services to their users [5]. Private cloud (also called domestic cloud or corporate cloud) consists of registered computing structural design and pattern that provides in house hosted group or individual services to a restricted number of people which is behind the firewall. Private Clouds vie with cloud computing on concealed networks. These (using virtualization automation) artifacts tender the facility to mass applications or virtual machines in an organization’s own group. It may be managed by the organization or a third party and may exist on premise or off premise.

3.2 Public Cloud

These are the clouds which are open for use by general customers who wanted to opt the service from the vendors who provide service on usage and requirement basis by signing the SLA’s which exist outside the firewall of an organization, completely serviced and administered by service supplier and they make available the services, like infrastructure resources, applications and storage, to the common public over the web Internet. They strictly adapt “pay as you go” model on rental basis which helps small and medium level companies to start small and go big devoid of spending greatly in the IT infrastructure. Here a customer does not encompass command of the management of the resources and infrastructure. The whole thing is administered by the third party and it’s their liability to concern software update installations, security patches etc. This means that IT organization are pooled by diverse clients to a very high extent, and ever since the groups are not separated, the consumer in actuality doesn‘t know the location, where exactly his data and records of information is stored [5 6 7 8].

3.3 Community cloud

A cloud which is controlled and used by a group of organizations that have a common vision mission, objectives, the members of the community group share access to the information and application in the cloud connected to web [5]. According to NIST [1] The cloud infrastructure is shared by several organization and support a specific community those have share concerns for example security requirements, policy, and compliance concern, it might be administered by the group or a third party and may exist on premise or off premise.

3.4 Hybrid cloud

The hybrid cloud infrastructure created with any permutation with combination of or either two or all types of public, private and community cloud services. Cloud service consisting of several domestic and/or exterior service providers. Consequently they employ the remuneration benefits and core characteristics of both/all the public, community and private clouds and leaving out the various pitfalls. This assists in realize all the allied goals of the end consumer with least investment. Thus the information and appliance that desires to be in the community scope and the records/information safety and protection is not a concern, here they use public clouds so that data and applications that is of high importance [5 6 7]. Value, defence and security are key factors that are set in the private clouds. The genuine prospective of amalgam clouds will be realized when institutes are able to switch dispensation between domestic and peripheral resources, where applications are spread across those borders.

4 Cloud Computing Service Security Issues

In brief let's present some of the security concerns that should be considered for the cloud deployments [5].

1. Multi-tenancy: As long as the cloud provider builds its higher-risk client, the entire lower risk client gets better security than they would have normally [5].

2. Security Assessment- The cloud service provider should perform regular security assessment by third party who is certified security auditor, able to identify issues and fix it [5].

3. Shared threat: Sometimes a cloud service provider may not be the cloud operator, but may provide the value added service on top of another cloud provider's service [5].

4. Staff security screening: Many organization employ contractors as part of their workforce. As with regular employees, the contractors should go through a full background investigation on par to the cloud user's own employees [5].

5. Distributed Datacenters: Disasters are a fact of life, and include natural and manmade disasters like hurricanes, landslides, earthquakes, and even fiber cuts. Cloud providers can provide an environment that is geographically distributed, henceforth the provider to have working and regularly tested disaster recovery plan, which includes SLA's

6. Physical Security: Physical threats should be analyzed carefully when choosing a cloud security provider. Should have the minimum facilities a mantrap, card or biometric access, surveillance, an onsite guard, and all guests be escorted and all non guarded egress points be equipped with automatic alarms [5].

7. Policies: Cloud providers should have incident response policies and they should have procedures and guidelines for every client that they feed into overall incident response plan [5].

8. Coding: Cloud providers still use in-house software, which may contain application bugs, so every organization should make sure that their cloud provider follows secure coding practices. Also codes written using standard methodology, documented and demonstrated to the customer.

9. Data Leakage: Every government worldwide has regulations that mandate the protections for certain data type, at a minimum that data that falls under legislative mandates or contractual obligation should be encrypted while in flight and at rest-also vendor should have a policy into the security incident policy to deal with any data leakages that might happen [5].

10. A public cloud is shared cloud computing infrastructure that anyone can access. It provides hardware and virtualization layers that are owned by the vendor and shared by all customers which are connected to public internet [5].

11. In PaaS there is a challenge for tight binding of the applications with the platform which makes portability across vendor's extremely difficult, PaaS offerings lack the functionality needed for converting legacy applications into full fledged cloud services [5].

12. Applications that require extensive customization are not good candidates for SaaS e.g. most complex core business applications that will not be the best suit for SaaS. Moving applications to the internet cloud might require upgrades to the local network infrastructure to handle an increased network bandwidth usage. Businesses are obliged to upgrade to the one latest version of software on the vendor's schedule introducing the compatibility problem between different vendor's offerings [5].

13. Lacking to follow open architectures, restricted standards, unknown risks and compliance controls, governance and control, identity and access management, access and intrusion management.

14. Benefits of Cloud include Cost, network, Innovative Expandability, Speed to implementation, it's green. Drawbacks include Security, control, cost, openness, compliance, service level agreements etc…

5. PROPOSED WORK

Creating new approach of coalition sustained by information technology can only be achieved by concentrating on the human facet. Further explicitly, we require tackling several of the fears and hindrances public face using this cloud technology. The most important concerns are: Trust: It is a stipulation for societal communication. Citizens will only work with citizens spread across the system, corporations, associated tools and data which can be trusted. Trust means the identity of the peoples associated. Shared culture: it includes shared leadership, shared goals and policy or norms, administration of cloud services from on demand to retirement. Cloud computing has the prospective to radically renovate IT, growing IT receptiveness to industry needs, whilst concurrently motivating downward the cost of investment infrastructure, platforms, and applications, virtual machines, dynamically changing management requirements etc…. now being replaced by a new delivery model where trade purchase IT components including software, hardware components or network bandwidth, storage as services from providers located at different geographical locations in the world.

IT institute must formulate major resolution regarding supporting platforms, flexibility, and scalability, deploying a single, integrated platform that administer whole cloud lifecycle diagonally both in-house and externally fabricated cloud assets — beginning from appeal for the service, commissioning and fabrication of the demanded service, self-service provisioning, to continuance, resiliency, asset management , cloud governance, high availability and disaster recovery, charging models, usage reporting, billing and metering, decommissioning, component services are virtualized and multiple service orchestrations etc. benefits easier costuming, fine tuning the business, better utilization and greater responsiveness The lifecycle should be tailored as per business needs, flexibility to deliver end user –oriented, multi-tiered, multitenant, multiplatform, from request to retirement [6 7 8].

5.1 Cloud Life Cycle

Under the metaphor of physical security – millennia of experience with keeping physical assets safe would serve us in keeping digital assets safe [5]. The main characteristics of cloud services is agility, goal to reduce time to sell, boost the velocity and rate of recurrence of software release, computerized and automated workflows across tool chains and reduce defects in production e.g. configuration errors, governance and configuration of underlying infrastructure. For incorporating security into the cloud service life cycle, an engineering approach is followed in different stages. Three important aspects of modeling cloud life cycle- include the actors, assets and their associated responsibilities. In first stage we start defining the problem and gathering the requirements, Configuration of the required components and resources, and define their responsibilities and roles. **Actor: Service provider**: roles include they should, define what need to be connected and offered as a service to the customer who demanded the service for their business needs, and to manage the services, using private, public, or hybrid model. Vendor should analyze the request for proposal, and request for service utilization using service discovery engine, using the orchestration and perform service certification related auditing, accounting, provide authorization, list the service, define service levels and cost of the services provided, define and sign SLA and Contract between the customer, provide the bundled and fabricated service which is packaged and delivered at one time or periodically as and when needed, define service termination based on ontology with joint responsibilities, cloud usage reporting and provisioning. **Resources**- define the component network, storage, resource requirements, **Service Governor**: Intellectually place things based on configured policies, regulations defined in SLA. **Tenants or end users:** Define the usage who wants to use the service provisioned to them, should set up different levels of monitoring, auditing and security zones for each role, enable auto scaling and setting physical security, monitoring policies, intrusion detection systems, biometric security usage, Identity access management etc., setting well secured policies, SLA's administering process and workflows, resources, service compliance, service quality etc. Also before moving to cloud deployment tenant should analyze the strengths, opportunities, weakness, threats, security and privacy of cloud deployment, and perform service discovery, setting requirements, managements, security blueprints, standardization of work flows, services, methodology, and lifecycle, identify requirements, constraints and capabilities, responsibilities needed for each phase of life cycle, capture ontology based quality services, consumer should also perform few responsibilities, he should identify the functional, technical, non technical, constraints and specifications, determine service and business related policies, and ways to implement the same and place request of proposal and sign the service level agreement between the consumer and service vendor and also sign quality of service (QOS) contracts, between the dependent services consumed, perform service monitoring, make service payments to the vendor for the rendered service, identify SLA metrics, monitoring includes synchronous or asynchronous, real time sharing, distributed, batch mode, module or component or block mode etc.. **Service Architecture**: architect and design the services available in the cloud. **Service Catalog**: defines who can all see the services defined to those concerned [8]. In second phase, we begin with secure design, in third phase we implement secure coding, computer security – concerned with controlling access to IT, pc network era, how to ensure the security of data on a personal computer, safe place with allowed access threats might appear from everyplace including inside our own organization, any number of physical ills, designed and developed, to increase the drama of security theft, nature of data is viral attack, data security needs to understand as something new, requiring new and innovative solution instead of traditional and existing solutions, virtualization and agility, over an attempt to control the risks, email, instant messaging and web browsing implementing appropriate controls usually works for better and a good solution then instead of simply stop the initiatives, to generate innovation in the concepts of data security and integrity, we need tools and process that recognize the ephemeral nature of data and the reality [5]. In fourth phase we perform security testing, wide availability of bulk amount of integrated and sanitized data is a tremendous benefit to academics researchers and industrial branching and end users, full potential of cloud can be achieved and realized by knowing the space and time tradeoffs, vulnerabilities and tradeoffs. With bucket full of benefits of cloud computing also brings with it concerns about security, privacy of information, concerns involve leakage and unauthorized access of data among virtual machines running on the same server, failure of cloud vendor to properly handle, defend and maintain confidentiality of data, releasing or exposing, authorizing critical, confidential and sensitive data to law enforcement or government – law framing agencies, The vision, hype, mission, objective of cloud computing is for the people, from the people, of the people, by the people, to the people. Cloud computing is the delivering the good quality service with quantity, right product at right time is the motto. Hackers breaking into client applications hosted on the cloud acquiring and distributing sensitive information, robustness of security protection instituted by the cloud provider, avoidance of lock-in and extent and degree of interoperability available, continued availability of the clients data [5]. In the fifth phase we move to the secure deployment to real time production environment, and provide security maintenance. Figure 1a shows the cloud development life cycle and various models for incorporating security for various cloud services, figure 2 shows the traditional water fall model with fabricated suitable security measures for cloud service life cycle with, in orbit commissioning of security to the time bound projects. Figure 3 depicts the hybrid model of cloud computing with resident/remote monitoring and metering the various activities carried out in the various stages of the cloud services, in addition designing the prototype. Incorporating and fabricating suitable security measures for cloud life cycle using iterative and spiral model.

Figure 4 shows stages of implementation of cloud cycle. It involves requirement analysis, planning, feasibility study, design, acquisition, deployment, testing, and maintenance, retirement from the opted service, historical architectural characteristics, security fundamental, cloud computing risks and threats, steps in implementing secure cloud services with historical architectural, technical, and operational influences, software security, cloud security services, cloud security principles, secure software requirements, addressing cloud business continuity planning, disaster recovery, redundancy and secure remote access, compliance regulation, traditional concepts of data, identity access managements, risks and threats identification addressing the data ownerships, privacy protections, data mobility, quality of service, service labels, bandwidth costs, data protection and support.

In summary the stages involved in Cloud life cycle includes [International Standards Organization-27001] and emphasizes iterative Plan-Do-Check-Act (PDCA) Cycle. 1. Plan: establish scope, design information security management systems (ISMS), perform risk assessment, develop and design risk treatment plan, determine control objectives and controls, statement of applicability 2.Do: Operate the controls, detect and document to incident recovery plan, provide security awareness training, mange. 3.Check: Intrusion detection operation, incident handling operation, conduct ISMS audit, conduct management review, 4.Act: improvements, corrective actions, preventive actions, apart from the stated requirements it also includes the virtualization of resources, which need to be developed, deployed, executed, managed, migrated and retired, identify and cataloging of the deployed virtual machines, scoping and plan, initializing using the cloud requirement engineering, requirement elicitation for user needs, domain information, existing system information, requirement analysis and negotiation, requirement documentation, design format specification, requirement validation etc. designing disaster recovery models, exception handling, threat analysis, risk assessment, developing the abstraction for the cloud services [5].

Requirement should be specific, unambiguous, direct, handy, clean, consistent, simple, flexible for changes, measurable to ensure that needs has been met, attainable, realizable, attenuated, traceable track-able, thru design, appropriate-derived from real need, or demand, consistency, correctness, reasonable, meeting the requirement in physically possible with likely project, time and space constraint., buildable, goal oriented, reliable, performance, security, accuracy, cost maintainable, confidentiality, integrity, availability, privacy, authentication, authorization, creditable, non repudiation, price-able, accountable, predictable, functional, valuable, allowable, modifiable, easily built and deployable, operable, usable, performance specific, quantifiable, maintainable, comparable, addressable to legal regulations and policy issues, bench makeable, properly decomposable, conduct-able, assumable, locatable, flexible for changes, assure-able, communicable, simulated, integral, inferable, conformable, tangible, recoverable, follow standards, guidelines, and best practices, procedures, policies, security control, committable, delivery oriented, requirement constraints, subject to store transmit, create, modify, delete, given data type object, performable, identifiable, defendable organizable, justifiable, reviewable, legitimate, auditable, informational, administrable, reliable, responsible, monitor-able, manageable, implementable, trainable, acquirable, passable, establish able, separable, foundational, qualify-able, designable, quantifiable, securable, coverable, unique, interoperable installable, referential, suitable, tunable, mature-able, documentable, fault tolerable, GU-interface-able, methodological, sustainable, addressable, programmable, recoverable, attributable, usable, movable, understandable, shift-able, learnable, certifiable, efficient, analyzable, testable, changeable, suitable, stable, format-able, protectable, adaptable, methodological, portable, acceptable, replaceable, quantifiable, conformable, recommendable, abstract-able, interchangeable, assertion-able, penetrate-able, qualify-able, standardized, mitigated, validated, harvested, enumerated, reversible, enforceable, encrypt-able, generable, pacify-able, automated, invent-able, documentable, innovate-able, ensure-able, logical, satisfy-able, transactional, correctable, compose-able, flow-able, detectable, generate-able, predictable, restrict-able, applicable, locatable, protectable, contextual, behavioral, unique, periodical, coverable, interoperable, characterize-able, comparable, purchasable, deterministic, informational, procedural, conduct-able, voluminous, referential, specifiable, measurable, simplistic, ideological, process-able, continual, executable, deployable, satisfy-able, interpretable, code-able, obscure-able, deter-able, desirable, analyzable, reverse engineering, synthesized, configurable, perspective, dynamic, detrimental, enhance-able, professional, ethical, projectable, visible, recoverable, summarize-able, reasonable, procedural, capable, process-able, least complex, rational, amendable, plan-able, projectable, supportable, establish-able, retire-able, restorable, returnable, reliable, revisable.

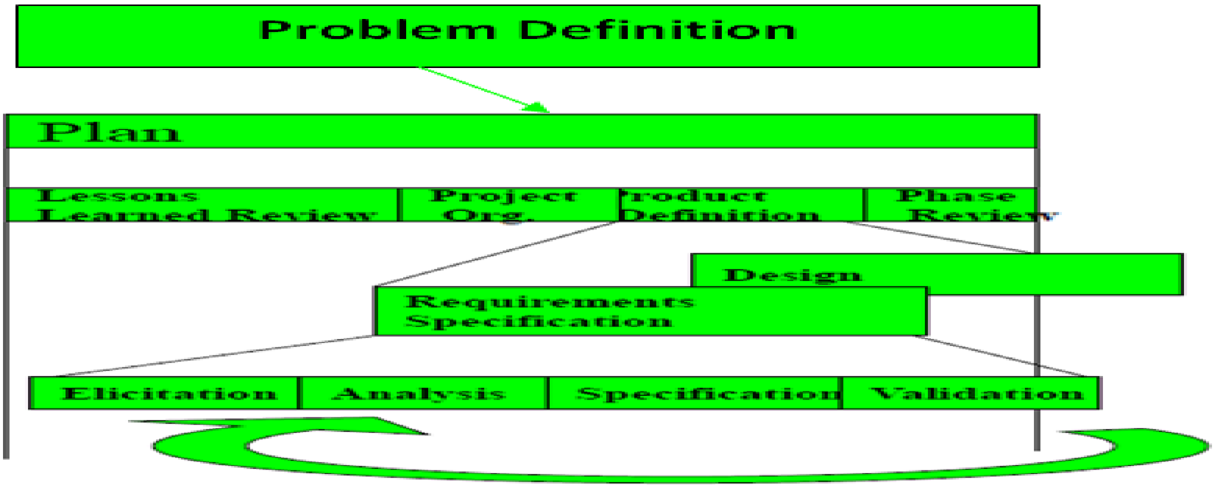

Figure 1a. Cloud Service Devlopment Life Cycle stages

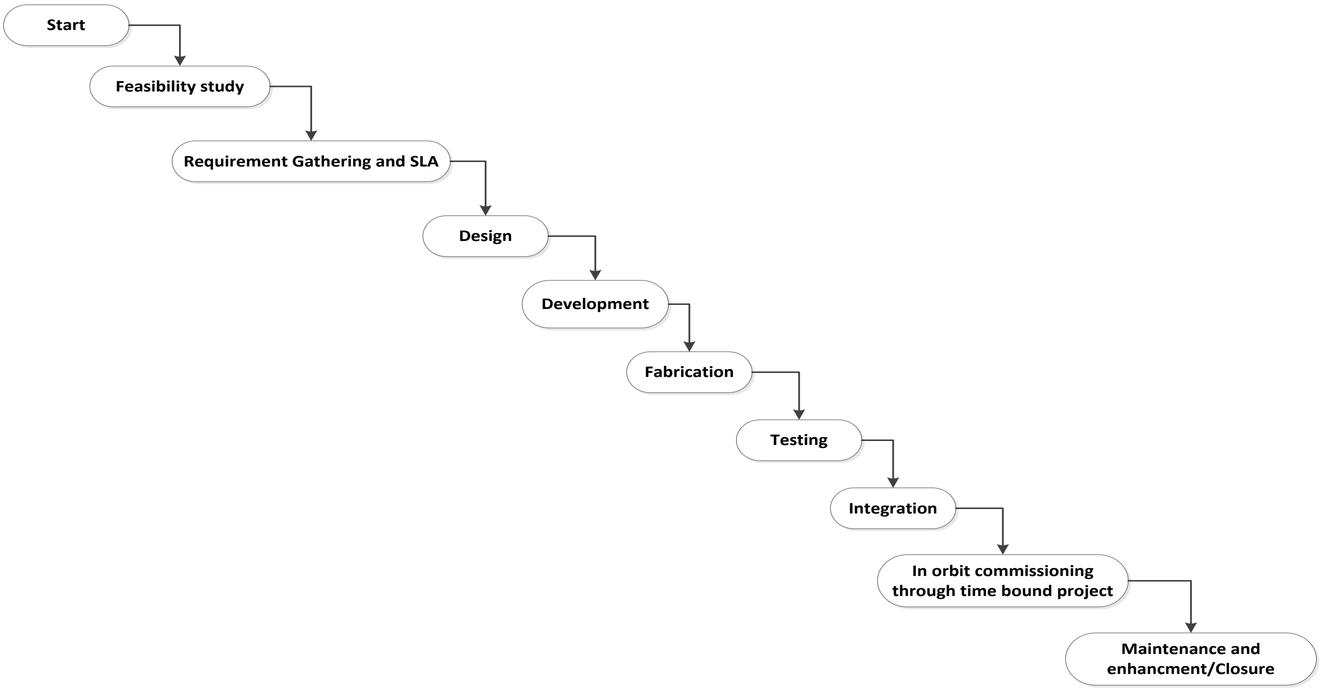
Start
Feasibility study
Requirement Gathering and SLA
Design
Development
Fabrication
Testing
Integration
In orbit commissioning through time bound project
Maintenance and enhancment/Closure

Figure 2: Water fall model for Cloud Services

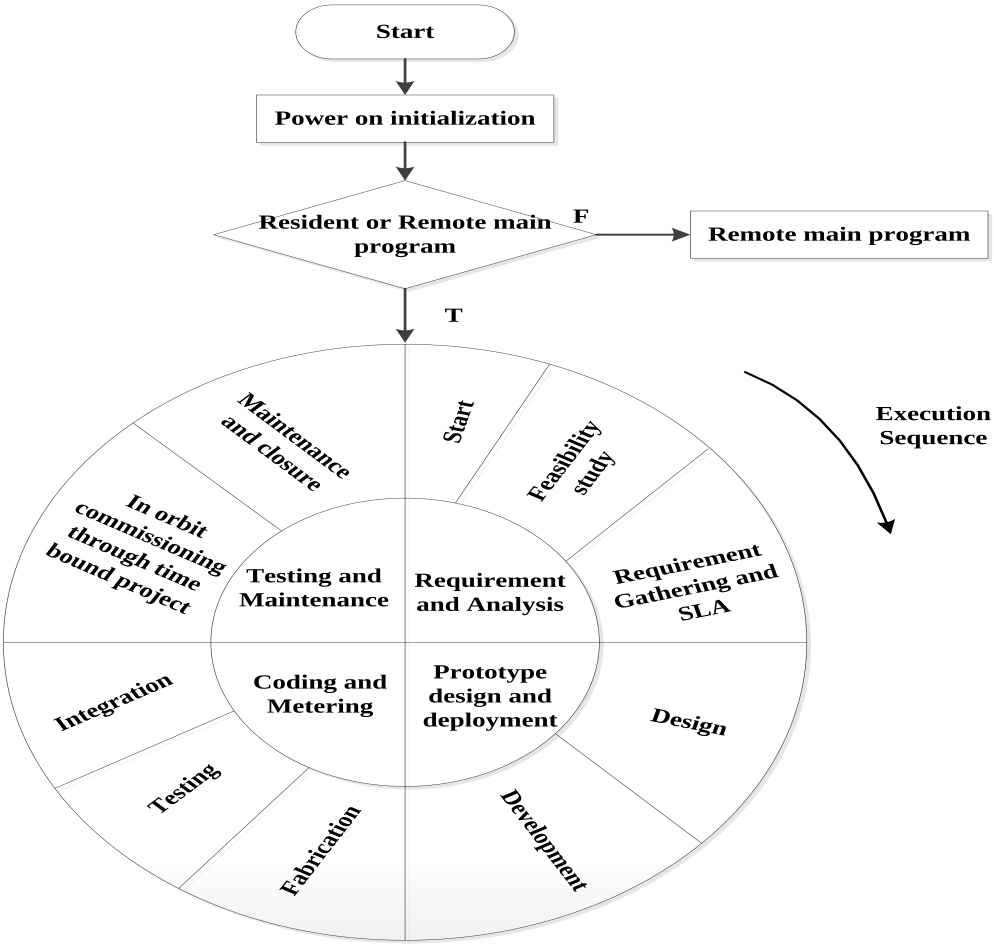

Figure 3 Hybrid Model- Deployment/fabrication strategy for security in Cloud computing

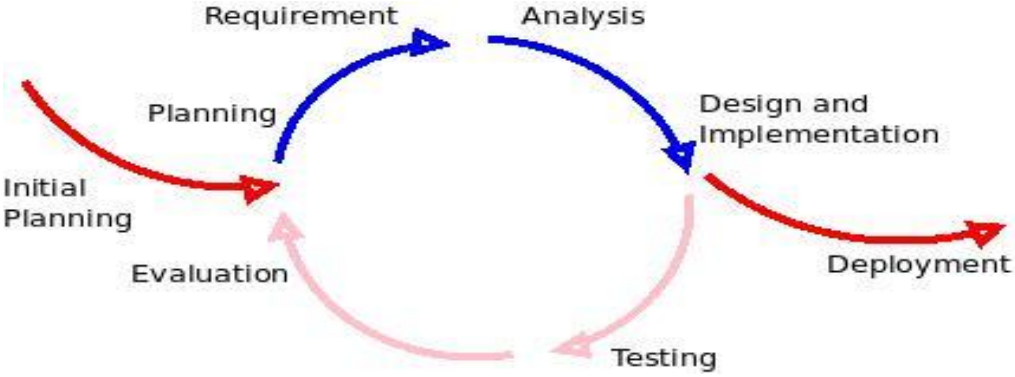

Figure 4 stages of implementation of cloud cycle

Classification of various existing security solutions for cloud computing can be categorized into **1. Collection and listing** of various identified security and privacy threats. **2. Detection** of the issues prevailing of identified threats and analyzing the root cause analysis for the occurrence of the threats. **3.** Setting up of **preventive** methods and measures to the detected threats. **4.** Implementing **protection** strategies for identified threats. **5.** Document the **response** for the protective strategy implemented, and **analyzes** the behavior of the system for the measure. The step by step representation and grouping of various Security solutions is shown in the Figure 5.

.

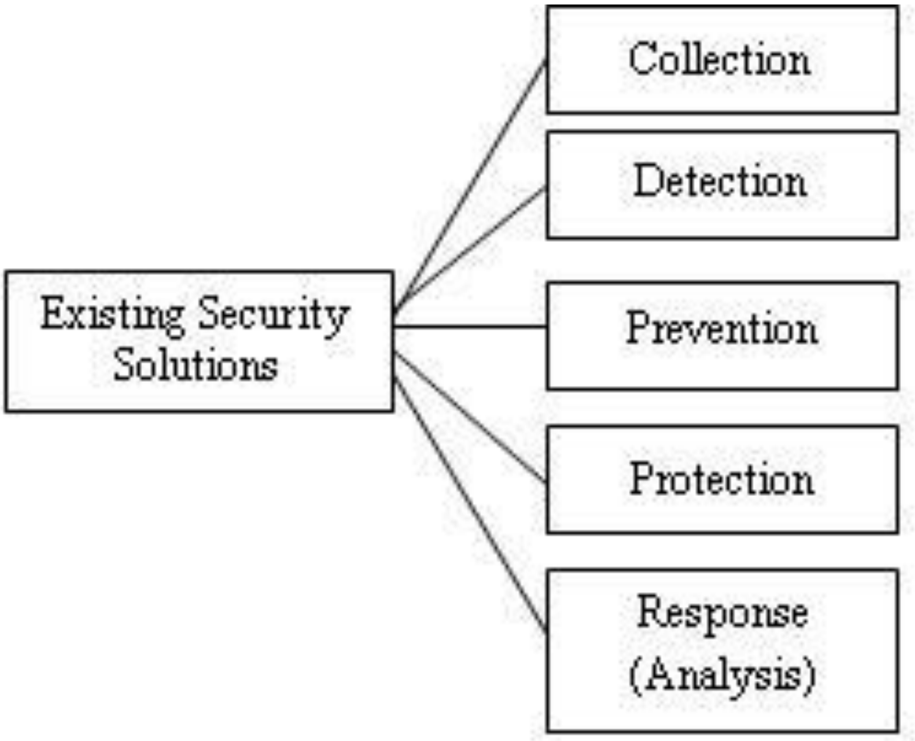

Figure 5: Classification of various Security solutions

6. CONCLUSION AND FUTURE WORK

This paper presents the concept of cloud computing along with its services and deployment models. It presents the cloud challenges and the cloud service security issues/concerns and solution using the software engineering design of cloud computing life cycle. Cloud use cases have to be explored comprehensively in order to evolve detailed security architecture, how much security is required for a Cloud? Deployment model, type of application – available budget and resource constraints, to come out with a unique architecture for cloud services involving security and privacy issues and improved design of security algorithms. A new set of efficient algorithms shall be designed using various cryptographic approaches (encryption and decryption) for cloud computing services. There is still a lot of research work going on to completely nullify the issues related to outsourcing the services to Cloud computing. In future work it is planned to investigate some interesting method to devise robust algorithms to achieve stability and confidence in the customers to use the cloud service, investigate the sparsely structure of predicament for further competence improvement. Establish strict security framework.

7. REFERENCES

[1] CSA- Reference Doc

[2] NIST definition of cloud computing.

[3] Hyper Text Transmission Protocol: Communication Technology Proceedings-2003. by Xiaoli Yu; Jianping Wu; Xia Yin; Dept. of Computer Tsinghua Univ., Beijing, China

[4] Hyper text transmission protocol with security: A Performance Analysis of Secure HTTP Protocol by Xubin He, Member, IEEE.

[5] ”Cloud Security a comprehensive guide to secure cloud computing”, Ronald L Krutz and Russell Dean Vines, Wiley India.

[6] Cloud computing second edition Dr.Kumar Saurabh Wiley India.

[7] Wikipedia “Secure_Hypertext_Transfer_Protocol”.

[8] [Cloud Computing] BMC Cloud Lifecycle Management: Managing Cloud Services from Request to Retirement | BMC Communities Blog.

[9] Man in the middle attack Moxie Marlinspike (2009).

[10] Cloud Computing Challenges and Related Security Issues: a survey project report on Cloud Computing Challenges and Related Security Issues by Prof. Raj Jain

[11] Protocols for Secure Cloud Computing IBM Research – Zurich Christian Cachin April 2011

[12] Datamation “Ten-Challenges-Facing-Cloud-Computing” -3869466-2.

[13] blogs.sap-“innovation/cloud-computing/top-9-challenges-in-cloud-computing-that-are-slowing-its-adoption-011918”.

[14] “Wireless Sensor-Cloud Integration Using Ant Colony Routing Algorithm”, R. Monica, Dinesha H A, Dr. V.K Agrawal, International Conference on cloud computing and service engineering (CLUSE2012), held at Raja Rajeshwari College of Engineering & KINGSTON, UK, 11-13 April 2012, 294-298.

[15] “Multi-level Authentication Technique for Accessing Cloud Services”, Dinesha H A, Dr. V.K. Agrawal, IEEE International Conference on Computing, Communication and Applications (ICCCA-2012), Dindigul, Tamilnadu, India, 978-1-4673-0270-8, 1 – 4.

[16] “Cloud Computing Technologies in Indian Rural Schools and Engineering College Education“, Abhishek A, Dinesha H A, Dr. V. K Agrawal, ICICS’s2012, Jan, 2012, 67-70.

[17] “Virtualization Technologies and Techniques in Education Learning Applications “, Dinesha H A, Dr. V. K Agrawal, International Conference on e-Education and e-Learning ICEEEL, held at World Academy of Science, Engineering and Technology, PARIS-FRANCE on November 14-16, 2011, 984-991.

[18] “Multi-dimensional Password Generation Technique for accessing cloud services”, Dinesha H A, Dr. V. K Agrawal, Special Issue on: "Cloud Computing and Web Services", IJCCSA, Vol.2, No.3, June 2012, 31-39.

[19] “Formal Modeling for Multi-Level Authentication in Sensor-Cloud Integration System”. Dinesha H A, R Monica and V.K. Agrawal. IJAIS, Published by Foundation of Computer Science, New York, USA, May 2012, 16-21.

[20] “Advanced Technologies and Tools for Indian Rural School Education System”, Dinesha H A, Dr. V. K Agrawal, International Journal of Computer Applications (IJCA) (0975 – 8887) Volume 36– No.10, December 2011, 54-60.

[21] wikipedia , “Cloud_computing_security”.