Object Oriented Techniques for Cloud Computing Security

Madhuri R. Dhange
Dept. of Computer Science and Engg.
VVP Institute of Engg. and Technology
Solapur , Maharashtra, India
e-mail id: madhuri.dhange@gmail.com

S.P.Deshmukh
Dept. of Computer Science and Engg.
VVP Institute of Engg. and Technology
Solapur , Maharashtra, India.

***Abstract* — cloud computing is a upcoming computing model which is new technology The based on distributed computing, virtualization technology, grid computing, parallel computing, utility computing and other computer technologies. It has characters such as large scale computation and data storage, virtualization, high reliability, high expansibility, and low price service. Cloud computing is becoming popular enterprise model in computer world in which computing resources are made available on-demand to the user as their requirements. Cloud computing use the internet technologies for delivery of IT-Enabled services to any needed users i.e. through cloud computing we can access anything from anywhere to any computer without worrying about their storage, structure, cost, management etc. So as we use internet, it is prone to several types of security risks. Therefore a systematic strategies and processes are essential to analyze security needs. The Security policies should be implemented for cloud computing systems at multiple levels to threats, risk and weakness. Here this paper introduce a high order object oriented techniques and methods for construction of vigorous security policy to build cloud system more reliable.**

Keywords— Cloud Computing, Cloud computing Models, General Security Policies, Security Requirements, Use case, Misuse case, Swim lane diagrams

I. INTRODUCTION

The "cloud" can be scalable to multiple data centers and server farms. Actually in the cloud system, the end user is not aware where exactly his request is executed. Within the cloud, according to user requirements, it grows and shrinks dynamically by acquiring exactly as much resources as needed to fulfill. The cloud can be considered as a new kind of middleware that enables entirely new business models. All topmost IT leaders of the market promises it as a economic model to consume IT resources, and cloud is a new technological business model which is based on existing technologies which are gaining maturity. Cloud Computing allows development of highly reliable, highly scalable and highly flexible, high performance applications. Security and Privacy are main issues related to IT and for business challenges, with consideration of more secured and reliable services, security policies must be implemented as a part of the application. The cloud computing resources providers are not paying attention on security in the cloud. Rather, their main concern is delivering low cost solutions with fast deployment that improves needs of the customer services and increases the competence of the IT function. Non functional part of cloud environment such as security, safety and reliability should be measured and integrated in the system along with the functional requirements throughout its development process. Security cannot be achieved with the integration of system architecture and prevention methods to threats at each stages of the system. Therefore, it is required to integrate overviews of user-oriented security threats and mitigations with system architecture, because security threats and architecture considerations are linked.

II. RELATED WORK IN CLOUD COMPUTING SECURITY

A. *Current Model of Cloud Computing Security*

In order to lay up security in cloud computing system, some technologies have been used to build the security mechanism for cloud computing. The cloud computing security can be provided as security services. Security messages and secured messages can be transported, understood, and manipulated by standard Web services tools and software. This mechanism is a good choice because the web service technology has been well established in the network-computing environment. Even the mechanism for the cloud computing security has many advantages now, but there are still some disadvantages. The performance is reduced apparently when the cryptographic computing are processed. There are also lack of some mechanisms to register and classify the participants carefully, such as the tracing and monitoring for them. In the following section, we will analyze the challenge for the cloud computing security in deep.

B. *The challenge in cloud computing Security*

In cloud computing environment, many users join in the CLOUD and they leave CLOUD dynamically. Other resources in the cloud computing environments are the same too. Users, resources, and the CLOUD should establish the trustful bond among themselves. And they will be able to deal with the changing dynamically. The CLOUD includes distributed users and resource from distributed local systems or organizes, which have different security policies. According to this reason, how to build a suitable and secure relationship among them is a challenge. In fact, the requirements for the security in cloud computing environment have some aspects, including confidentiality, multiple security policy, dynamic of the services, the trust among the entities, dynamically building trust domains etc.

III. USED CONCEPTS

A. *Use Case Diadgram:*

A use case is defined as a description of steps or actions between a user and a software system. Use cases are helpful in capturing functional requirements. The use case is obtained by a set of possible order of interactions between systems and users in a particular environment and related to a particular goal [7]. The use case should contain all system activities that have significance to the users. The use case map notation was introduced in 1992 by Buhr and his team at Carleton University [2,3] and quickly gained popularity.

B. *Misuse Cases (MUC) Diagram:*

Misuse cases (MUC) [1] have become popular for security requirements elicitation and threat modeling. They complement use cases for security purposes by extending them with misusers, misuse cases and mitigation use cases, as well as new relations like threatens and mitigates. A misuse case is the contrary of a use case. MUC diagrams use an inverted notation and are combined with regular use case diagrams [4]. They represent security issues from the view of an attacker. MUCs allow an early focus on security in the development process and facilitate discussion among stakeholders including regular developers with no special security training. However, they are not equally fit for all cases, for example they do not provide an integrated view of attacks and of system architecture.

C. *Swim Lane Diagram:*

A swim lane diagram, also called a cross-functional diagram, is a process flowchart that provides information on who does what [5]. It can also be expanded to show times, when tasks are done and how long they take. A swim lane is a visual element which is used in process flow diagrams. Swim lanes may be arranged either horizontally or vertically. Parallel lines divide the chart into lanes, with one lane for each person, group or sub process. Each lane has a label which shows how the chart is organized. The vertical direction represents the sequence of events in the overall process, while the horizontal divisions represent what sub process is performing that step. Arrows between the lanes represents flow of information between the sub processes. Many process modeling methodologies make use of the concept of swim lanes as a mechanism to organize activities into separate visual categories in order to demonstrate different functional capabilities or responsibilities. Swim lanes are used in Business Process Modeling Notation and Unified Modeling language (UML) activity diagram modeling methodologies

IV. CLOUD COMPUTING

A first definition, proposed by the consulting firm Gartner [6] is:" A style of computing where scalable and elastic IT-related capabilities provided "as-a-service" is using internet technologies to multiple external customers. " Another one, submitted by the National Institute of Standards and Technology [8], has been largely referred to by all the actors:"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources e.g., networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

A. *Hierarchical Architecture of Cloud*

This section presents information on various architectural essentials that form the foundation for cloud computing. Fig.1 shows a hierarchical design of cloud computing architecture.

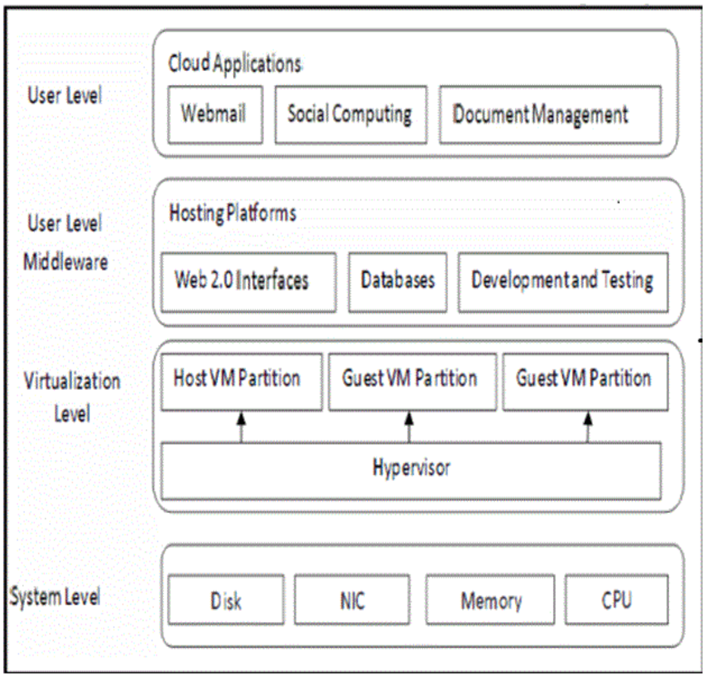


Fig. 1 Hierarchical Architecture of Cloud

At the bottom is the system level, which serves as a basis and the strength of the cloud. It consists of a compilation of data centers that make available the computing power in the cloud surroundings. At this level, there exist massive physical resources such as storage disks, CPUs, and memories. On moving just higher than this level, the system level is the virtualization level. Virtualization can be viewed as the factor that facilitates cloud computing. It is a concept of applications and services from the fundamental physical services. It is achieved with the help of a middleware named as hypervisor, a software or hardware that serves as a bridge between physical devices and virtual applications. In this concept it is required that no application or service is attached directly on the hardware resources. This level manages the physical resources and allows sharing of their capacity among virtual instances of servers, which can be enabled or destroyed on demand. The physical cloud resources and their virtualization capabilities form the foundation for delivering IAAS. The user-level middleware includes software-hosting platforms such as Web 2.0 Interfaces that authorize developers to create affluent, cost-effective user interfaces for web based applications. It also provides the programming environments and tools that simplify the creation, deployment and execution of applications in clouds. The main purpose of this level is that it should provide PAAS capabilities.

B. Cloud Computing Service Models

Cloud computing is a delivery of computing where massively scalable IT-related capabilities are provided — as a service across the internet to numerous external clients. This term effectively reflects the different facets of the Cloud Computing paradigm which can be found at different infrastructure levels. Cloud Computing is broadly classified into three services: —"IaaS", "PaaS" and "SaaS".

1. *IaaS (Infrastructure as a service) model*:

The main concept behind this model is virtualization where user have virtual desktop and consumes the resources like network, storage, virtualized servers, routers and so on, supplied by cloud service provider. Usage fees are calculated per CPU hour, data GB stored per hour, network bandwidth consumed, network infrastructure used per hour, value added services used, e.g., monitoring, auto-scaling etc. Examples: Storage services provided by AmazonS3, Amazon EBS. Computation services: AmazonEC2, Layered tech and so on.

2. *PaaS (Platform as a service) model:*

It refers to the environment that provides the runtime environment, software deployment framework and component on pay to enable the direct deployment of application level assets or web applications. PaaS is a platform where software can be developed, tested and deployed. It means the entire life cycle of software can be operated on a PaaS. This service model is dedicated to application developers, testers, deployers and administrators. Examples: Google App Engine (GAE), Microsoft Azure, IBM SmartCloud, Amazon EC2, salesforce.com and jelastic.com and so on.

3. *SaaS (Software as a service) model:*

Through this service delivery model end users consume the software application services directly over network according to on-demand basis. For example, Gmail is a SaaS where Google is the provider and we are consumers. Other well known examples of PaaS include billing services provided by Arial system, op source. Financial services: Concur, workday, Beam4d. Backup and recovery services: Jungle Disk, Zmanda cloud back up and so on.

C. Cloud Computing Deployment Models

There are four primary cloud computing deployment models which are available to service consumer as shown in Fig. 2

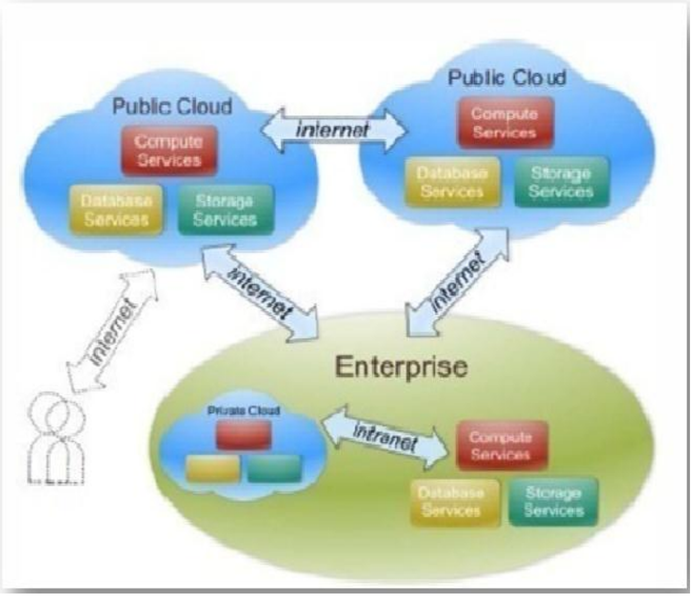


Fig. 2 Types of Cloud Deployment Models

1. *Public Cloud:*

It has no proprietorship to an organization. It works as a "Pay-as-you-go" model. Consumer accesses this virtualized infrastructure and cloud service provider updates all information through a portal. Customer can request to a provider according to his need. It includes all security elements, services and a secure VPN connection to their own networks. Amazon Web Services EC2 (Elastic Compute Cloud) is the first public cloud that offers various services, such as Amazon Simple Storage. It also enables the use of existing security and management policies.

2. *Private Cloud:*

Private Cloud has proprietorship to an organization. It describes traditional mainstream sense, whereby resources are used on a fine grained self service basis over internet. It is a pool of resources which can be used within a company. Private cloud works inside the data centers and uses some of the public cloud characteristics like virtualization and dynamic provisioning. Basically, private clouds are companies who only want to use services that are hosted in-house and do not want to share their infrastructure. They do not provide much flexibility as public cloud offers. IBM is one of the manufacturers that put forward services for companies who want to create an Internal Private Cloud.

3. *Hybrid Cloud:*

Hybrid cloud allows for transitive information exchange. It's a combination of different clouds i.e. Public and Private Clouds. A cloud service provider utilizes standard or proprietary methodologies regardless of their ownership or location. They provide application compatibility and portability across disparate Cloud service offerings. It consist multiple internal and external providers. Many organizations have started implementation in hybrid cloud such as Amazons, Google, and Microsoft etc

V. CLOUD SECURITY PROBLEMS

The cloud system runs on the internet and the security problems related to the internet also can be found in the cloud system. The biggest concerns about cloud computing are security and privacy. The traditional security problems such as security vulnerabilities, virus and hacking can also make threats to the cloud system and can produce more serious results because of property of cloud computing. Hackers and malicious intruder may hack into cloud accounts and steal sensitive data stored in cloud systems. The cloud system can make the application in different place or different hardware. The cloud system must provide reliability server for the user and the data in the cloud center also must be protected. The cloud scale in the cloud system can be extended dynamically and can meet the growth of application and number of users. The application in the cloud also can be extended according to the number of user. The user can't control the progress or deal with the data and the user can't make sure the data security by themselves. The data resource storage and operation and network transform also deals with the cloud system. The key data resource and privacy data are very import for the user. The cloud must provide data control system for the user. The data security audit also can be deployed in the cloud system. The data security audit also can be deployed in the cloud system. Data moving to any authorized place you need it, in a form that any authorized application can use it, by any authorized user, on any authorized device. Data integrity requires that only authorized users can change the data and Confidentiality means that only authorized users can read data. Cloud computing should provide strong user access control to strengthen the licensing, certification, quarantine and other aspects of data management. In the cloud computing, the cloud provider system has many users in a dynamic response to changing service needs. The users do not know what position the data and do not know which servers are processing the data. The user do not know what network are transmitting the data because the flexibility and scalability of cloud system. The user can't make sure data privacy operated by the cloud in a confidential way. The cloud system can deploy the cloud center in different area and the data can be stored in different cloud node. The different area has different law so the security management can meet the law risk. Cloud computing service must be improved in legal protection.

VI. STRATEGY

Any security architecture framework should include all the operations for providing protection to data such as authorization, authentication, control on accessing of data, integrity, confidentiality and non repudiation as well as operational procedures, technology specifications, people, organizational management, and security program compliance and reporting. A security architecture document should meet all the objectives by using security and privacy principles. This task can be achieved by integrating formal system development life cycle with business case, requirements definition, design, and implementation plans.

A. *Framework of the Structured Development of Cloud:*

Security Policies:

The approach which is used to make security policies should involve two phases.

- Cloud security requirements are analyzed.
- Cloud security policies are developed, and measures are put in place to communicate and enforce them.

1. *Security policies at System level:*

There are security requirements, which must be fulfilled at system level to make a robust security policy.

i. The System must provide the physical protection to all physical hardware.
ii. The System must employ multi factor authentication.
iii. The System must monitor network requests so that any kind of distributed denial of attack can be detected.
iv. The System must audit and log cloud end user.
v. The System must encrypt data.

2. *Security policy at user level:*

The security policy should include the following points for providing security at user level.

i. The computing environment should be divided into multiple security domains in the cloud. Each domain should specify different security operation such as mutual authentication, digital signature verification, access of data etc. at each level.

ii. The user's connection and interactions should be ensured. Security should be checked with the SSL,VPN and PPTP, etc. Multiple authorizations among user should be tartan by using license and after proper authorization the service owner and agents should be allowed for access to data securely.

iii. The third-party monitoring mechanism should be ensured so that operation of cloud computing environment is in safe hands and steady.

iv. Using a series of measure to solve the user dynamic requirements, including a complete single sign-on authentication, proxy, collaborative certification, and certification between security domains.

v. The different user's requirements should be identified and according to requirement different data storage protection should be provided. At the same time, the efficiency of data storage should be improved. In this way, user gets data security assurance.

vi. Various safety tests should be applied on computing requested by service requester so that it can check whether they contain malicious requests to weaken the security rules.

B. High OrderObject Oriented modeling Technique (HOOMT):

The HOOMT, which is used here as a key approach for the analysis of cloud security policies, it provides a structured object-oriented design methodology based on hierarchical model development. This technique allows every object in the cloud to be modeled widely. In addition to, it provide a systematic verification for completeness. The analysis process should combines use cases, misuse cases, and malactivity swim lane diagrams with the HOOMT. Each misuse case should be analyzed and decomposed for malactivity swim lane diagrams, which reveals the activities of misusers in every aspect. It helps to prevent or mitigate all malactivity. This technique serves as a countermeasure for identified threats. Furthermore, this technique makes possible the development of comprehensive cloud security policies and the result, which it's, provide a more resourceful way to discover threats posed to cloud computing systems, both internally and externally. The structured development of the cloud security policies together with the use cases, misuse cases and swimlane diagram provides the proficient way to make secure system.

C. . Cloud Security Requirements Analysis:

The Requirements Analysis process uses high order object for development of a context object diagram in the cloud computing environment. The context object diagram (COD) provides the most abstract information of entire cloud system. It shows requests for services to cloud either internally or externally. The COD also serves as the initial point for the analysis process. Subsequently, it specifies use cases, which describes the response of each request in cloud computing environment. These cases determine the behavioral requirements of the cloud computing system which is derived

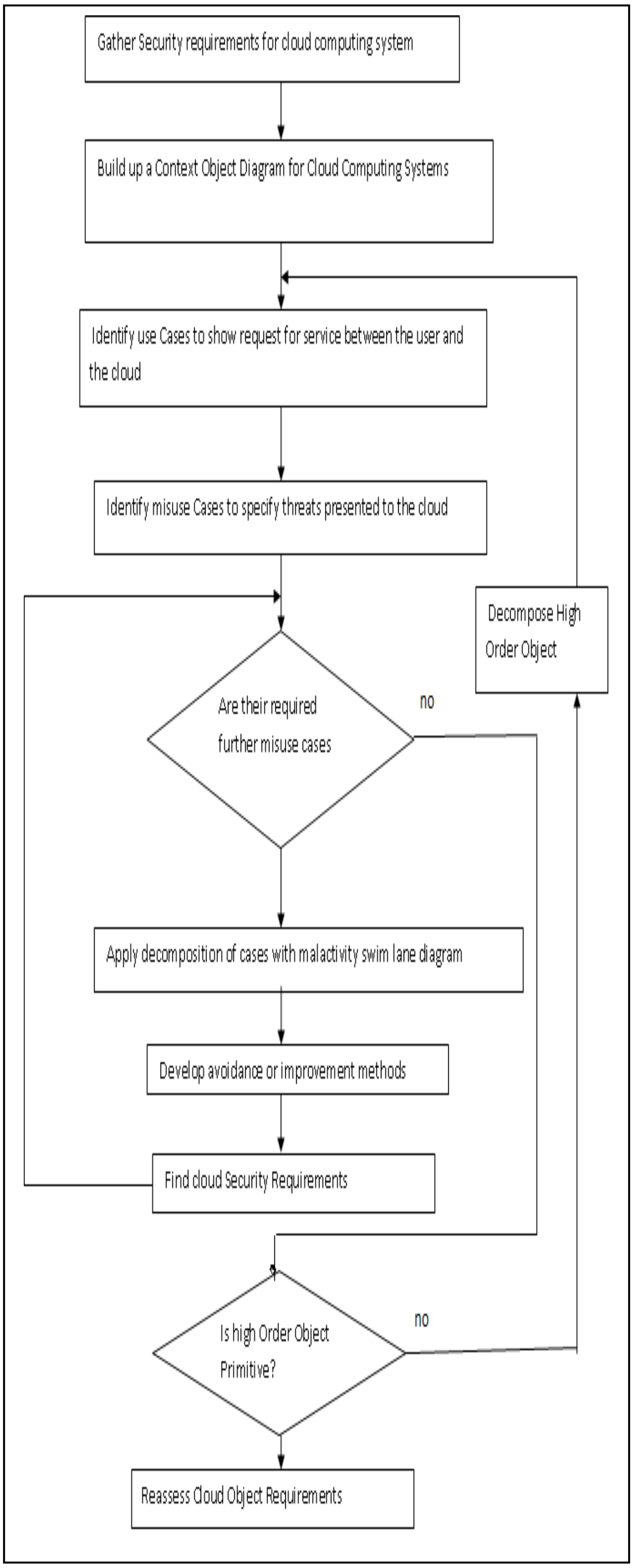

Gather Security requirements for cloud computing system
Build up a Context Object Diagram for Cloud Computing Systems
Identify use Cases to show request for service between the user and the cloud
Identify misuse Cases to specify threats presented to the cloud
Decompose High Order Object
Are their required further misuse cases
no
Apply decomposition of cases with malactivity swim lane diagram
Develop avoidance or improvement methods
Find cloud Security Requirements
Is high Order Object Primitive?
no
Reassess Cloud Object Requirements

Fig. 3. Cloud security Requirement Process

from the cloud's functionalities. In next step, each use case is analyzed comprehensively to determine how it could be undermined. This analysis specifies misuse cases and misusers, either internal or external. The misuse cases also expose an assortment of threats posed to the cloud at each level of the hierarchical model. The details of misuse events can be found by further decomposition of misuse cases with malactivity swim lane diagrams. Thus identification of more threats can be done with the help of these diagrams, which can serve as countermeasures to misuse cases, to identify security requirements. It specifies the actions taken by the misusers in fact and the inclusion of both hostile and legitimate activities. So that the point can be determined at which prevention, avoidance and mitigation options can be added. This information is used for identifying security requirements. In next step, the Cod can be further decomposed which specifies the decomposition of cloud object at lower level. This process generates the cloud security requirements at the end of every cycle, it continues until a point is reached at which the cloud objects are primitive and corresponding use and misuse cases are fully explored. At that point, the cloud security requirements are distinguished by inspection for inconsistencies and ambiguities. They serve as a deliverable at the end of the first phase of the approach.

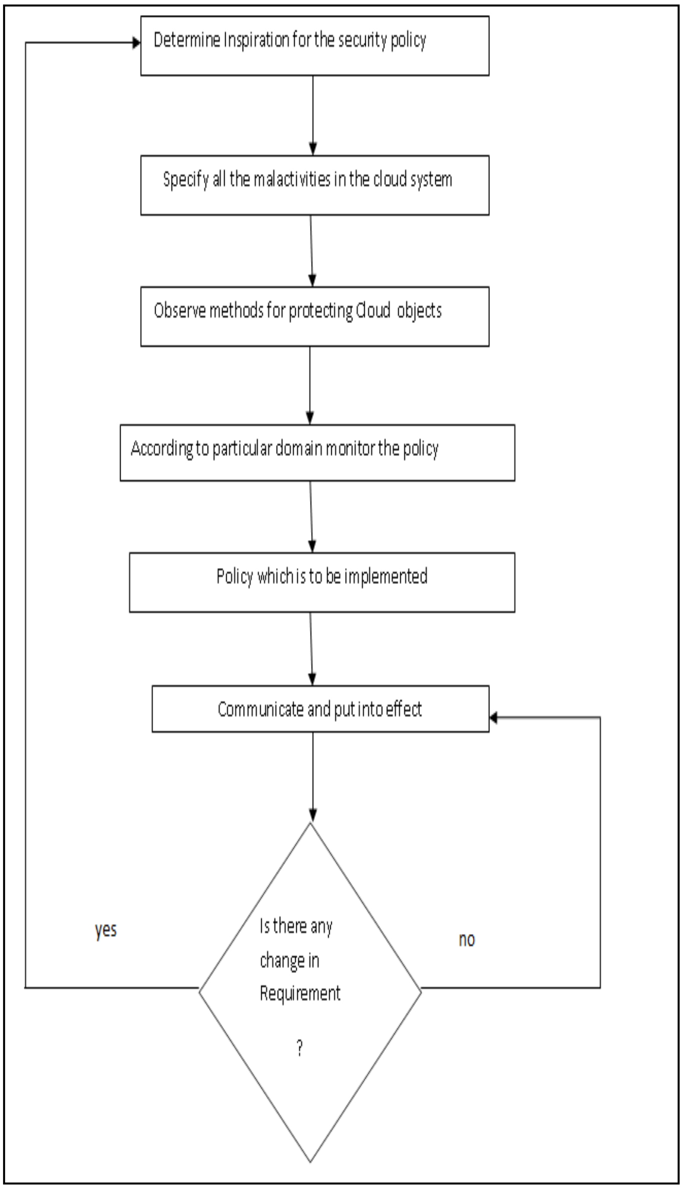
D. Cloud Security Policy Development, Communication and Enforcement:

The robust security policy is quite important for any system, the security policies for cloud computing systems are based on the cloud security requirements through the security and requirements are not necessarily mapped one-to one. Usually, one requirement can be satisfied by a set of security policies. These requirements are high-level statements of countermeasures that will adequately prevent or mitigate identified misuse cases and are dependent on rigorous analysis of threats to the cloud at each level. Consequently, security policies are developed and integrated into the development of the cloud computing system. This approach provides a framework of best practices for Cloud Service Providers and makes security policies acceptable. The policies ensure that risk is minimized and that any security incidents are met with an effective response. Then process of developing these policies allows authorized security workforce to monitor and probe security breaches and other issues pertaining to cloud security. The process which is illustrated in the fig. 4 can be summarized in these steps.

a) The process starts with a statement enunciating the inspiration for the development of security policy. It describes the regulator of mal activities and lists the cloud data, which is to be protected. The problem the policy is designed to resolve is articulated.

b) The methods are observed for protecting cloud objects in each domain. Any exceptions to this policy are also noted. At this stage, the policy itself is expressive. It gives a clear vision that, what points are covered by the policy. The farm duties of the various domains or groups and the technical requirements that each individual or device requires, are comprehensible. They act in accordance through the policy.

c) At the end, when cloud security policies have been developed then they must be dispersed to users, vendors, staff and support workforce. The cloud computing environment is complex, it demands that all the policies should not be communicated to the users or consumers, it is also necessary from the security point of view. The implementation of security policies is also a vital part of the process. This can be done with the documentation of policies which should be provided to user, so that they read, understood and agreed to abide by the policies. It should discuss how violations will be handled.


Determine Inspiration for the security policy
Specify all the malactivities in the cloud system
Observe methods for protecting Cloud objects
According to particular domain monitor the policy
Policy which is to be implemented
Communicate and put into effect
Is there any change in Requirement ?
yes
no

sFig. 4. Policy Development Process

VII. CONCLUSION AND FUTURE SCOPE

It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. This concern is immediately followed by the robust security policy which can be analyzed by the security requirements. Security processes are noticeable on layers of cloud computing system. The lack of visibility in layers can create a number of security and compliance issues. The systematic way to follow the security policies provides threat management capabilities like intrusion prevention, Web application protection and network policy enforcement. Cloud providers can support SaaS and IaaS within and across clouds. The provider should bind to implementation best practices and provide clients with maximum visibility into the security and compliance posture of cloud services. The entities should know which security limitations have been applied on the cloud computing system at each level. This can be broadened by adding the analysis of operational and management security controls.

VIII. REFERENCES

[1] G. Sindre, A. L. Opdahl, "Eliciting Security Requirements with Misuse Cases, Requirements Engineering", Springer-Verlag London Limited,pg 34-44,2004.

[2] R. J. A. Buhr, R. S. Casselman, "Use Case Maps for Oject Oriented Systems", Prentice Hall, 1995. ICCCNT'12 26th_28th July 2012, Coimbatore, India IEEE-201S0

[3] R. J. A. Buhr, " Use case maps for attributing behavior to system architecture", Proceedings of the 4th International Workshop on Parallel and Distributed Real-Time Systems, p.3, 1996.

[4] Peter Karpati, Andreas L. Opdahl, GuttormSindre, "Experimental Comparison of Misuse Case Maps with Misuse Cases and System Architecture Diagrams for Eliciting Security Vulnerabilities and Mitigations", Sixth International Conference on Availability, ReI iabil ity and Security, 2011.

[5] Swim Lane Diagrams, Available at www.niatx. netlPDF/PIToolbox/swimlane.pdf

[6] Gartner, "Cloud Computing will be as influential as ebusiness" Available at http://www.gartner.comlitlpage.jsp?id=707508. 2008

[7] Architecture resources Bredemeyer Consulting, Available at http://www.bredemeyer.com.pdf

[8] National Institute of Standards and Technology, "Cloud Computing", Available at http://csrc.nist.gov/groups/SNS/cloudcomputing/inx. html, October 2009.

[9] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", Special Publication 800-145,2009.

[10] SojanMarkose, Xiaoqing (Frank) Liu, and Bruce McMillin, "A Systematic Framework for Structured Object-Oriented Security Requirements Analysis in Embedded Systems",TEEE,20 Jan 2009

[11] ZhidongShen and Qiang Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems (ICSPS), 2010

[12] White Paper, "Cloud Computing Use Cases Cloud Computing Use", Open Cloud Manifesto, Version 2.0, 30 October 2009

[13] Research Report, "Security of Cloud Computing Providers study" Ponemon Institute, April 2011.