Security Based Model for Cloud Computing

Shivlal Mewada
Dept. of Computer Science,
Govt. Holkar Science College
Indore-INDIA

Umesh kumar Singh
Institute of Computer Science,
Vikram University
Ujjian-INDIA

Pradeep Sharma
Dept. of Computer Science,
Govt. Holkar Science College
Indore-INDIA

Abstract— ABSTRACT: The cloud computing is the best way to save money and achieve efficiency which satisfies organizations requirement. But without security embedded into innovative technology that supports cloud computing, businesses are setting themselves up for a fall. The trend of frequently adopting this technology by the organizations automatically introduced new risk on top of existing risk. Obviously putting everything into a single box i.e. into the cloud will only make it easier for hacker. In this paper, we presents an overview of the cloud computing. Also include the several security and challenging issues, emerging application and proposed security model.

Keywords: Cloud computing, Security, Secure Key Management Model.

I. INTRODUCTION

Distributed computing is suffering from high scalability because it affects the performance of the resources. The volume of data quadruples in every 18 month while available processor speed doubles during same time period which does not allow centralized storage of data [1]. So we need some highly decentralized storage systems called "cloud" developed by major Internet based companies hence cloud computing supports distributed computing so that performance can be maintained by resource utilization in highly scalable environment.

The industry is moving towards the cloud computing, it will completely change the way we use the computer and the Internet. Cloud computing concerns with feasible ways to storing information and running applications. Instead of running application and data on an individual desktop computer, everything is kept in the cloud, a large pool of computers and servers accessed by the Internet [2].Cloud computing allows us to access all the documents and applications from anywhere in the world, i.e. it frees users from the limitations of the desktop and makes it easier for group members in different locations to communicate with each other.

Cloud computing is the computing analogous to the electricity revolution of a century ago. Before the advent of electrical utilities, stand alone generators were the medium of generation of electricity required for every farm and business. After the creation of electrical grid, farms and businesses switch off their generators and bought electricity from the utilities, because the price was much lower and the system was more reliable than the production of their own capabilities [2]. Same type of revolution is making cloud computing so much popular that's why the industries are looking it as a future scope but major concern is security, putting everything in the cloud makes highly unsecured environment The desktop-based concept of computing that we are using today is not as much capable as we could expect the universal access, 24x7 reliability, and ubiquitous collaboration promised by cloud computing.

II. CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) Information Technology Laboratory, cloud computing is defined as follows:

"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 [3].

Essential Characteristics

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

- Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

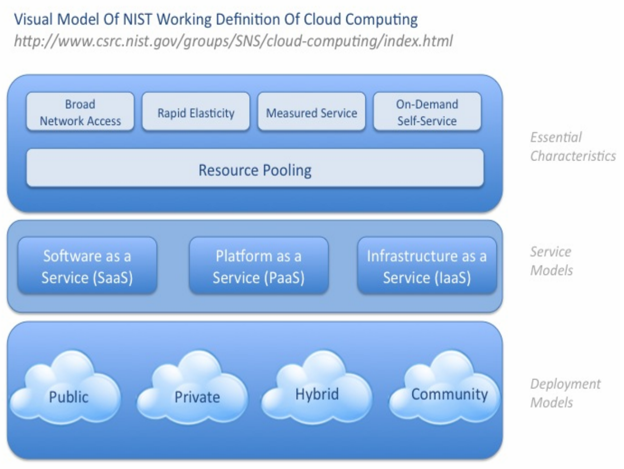
Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Fig. 1 Cloud Computing Framework

Service Models:

- Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- Cloud Platform as a Service . The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

- Cloud Infrastructure as a Service. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

- Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

- Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

- Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

III. Open Security Architecture Of Cloud Computing

Figure 1 shows the open secure architecture of cloud computing [4]. The Open Security Architecture cloud computing pattern is an attempt to illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations, and the controls that require additional emphasis.

The various controls in this architecture are [5]

- SA-1/4/5 System and Services Acquisition: ensure that acquisition of services is managed correctly.
- CP-1 (contingency planning): ensure a clear understanding of how to respond in the event of interruptions to service delivery.
- Risk Assessments controls: helps to understand the risks associated with services in a business context. The pattern also provides a view into activities that are shared by security architects, security managers, and business managers. They should:
- Agree on the control baseline applicable to this cloud sourcing activity/service.
- Confirm how this translates into the control framework of the cloud provider.
- Decide on additional risk mitigating controls.

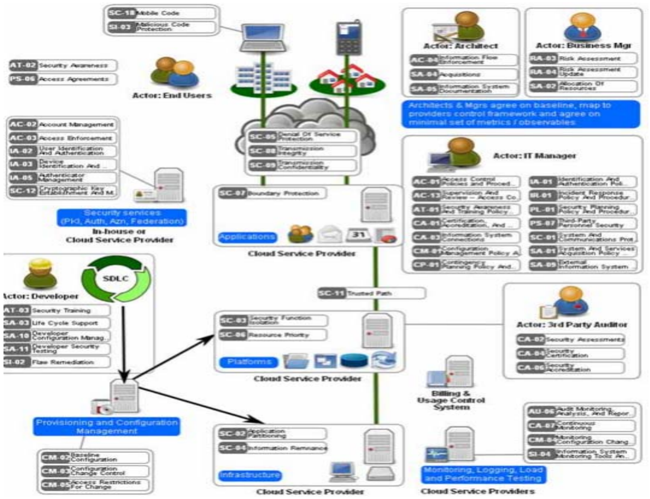
SC-18 Mobile Code
SI-03 Malicious Code Protection
AT-02 Security Awareness
PS-06 Access Agreements
Actor: End Users
AC-02 Account Management
AC-03 Access Enforcement
IA-02 User Identification And Authentication
IA-03 Device Identification And ...
IA-05 Authenticator Management
SC-12 Cryptographic Key Establishment And M..
Security services (PKI, Auth, Azn, Federation)
In-house or Cloud Service Provider
SC-05 Denial Of Service Protection
SC-08 Transmission Integrity
SC-09 Transmission Confidentiality
SC-07 Boundary Protection
Applications
Cloud Service Provider
Actor: Architect
AC-04 Information Flow Enforcement
SA-04 Acquisitions
SA-05 Information System Documentation
Actor: Business Mgr
RA-03 Risk Assessment
RA-04 Risk Assessment Update
SA-02 Allocation Of Resources
Architects & Mgrs agree on baseline, map to providers control framework and agree on minimal set of metrics / observables
Actor: IT Manager
AC-01 Access Control Policies and Proced..
AC-13 Supervision And Review – Access Co..
AT-01 Security Awareness And Training Policy..
CA-01 Certification, Accreditation, And ...
CA-03 Information System Connections
CM-01 Configuration Management Policy A..
CP-01 Contingency Planning Policy And..
IA-01 Identification And Authentication Pol..
IR-01 Incident Response Policy And Procedur..
PL-01 Security Planning Policy And Procedur..
PS-07 Third-Party Personnel Security
SC-01 System And Communications Prot..
SA-01 System And Services Acquisition Policy ...
SA-09 External Information System ..
Actor: Developer
SDLC
AT-03 Security Training
SA-03 Life Cycle Support
SA-10 Developer Configuration Manag..
SA-11 Developer Security Testing
SI-02 Flaw Remediation
SC-11 Trusted Path
SC-03 Security Function Isolation
SC-06 Resource Priority
Platforms
Cloud Service Provider
Actor: 3rd Party Auditor
CA-02 Security Assessments
CA-04 Security Certification
CA-06 Security Accreditation
Billing & Usage Control System
Provisioning and Configuration Management
CM-02 Baseline Configuration
CM-03 Configuration Change Control
CM-05 Access Restrictions For Change
SC-02 Application Partitioning
SC-04 Information Remnance
Infrastructure
Cloud Service Provider
AU-06 Audit Monitoring, Analysis, And Repor..
CA-07 Continuous Monitoring
CM-04 Monitoring Configuration Chang..
SI-04 Information System Monitoring Tools An..
Monitoring, Logging, Load and Performance Testing
Cloud Service Providers

Figure 2: Cloud Computing Model Open Source Architecture

There are a number of key control areas that should be considered carefully before moving the computing operations to cloud services: Contractual agreements, Certification and third-party audits, Compliance requirements, Availability, reliability, and resilience, Backup and recovery, Service levels and performance, Decommissioning. If the process is comprised of a number of cloud services, then supporting services such as security, load monitoring & testing and provisioning and configuration management are required.

IV. Important Issues In Cloud Computing

Security is the most important issue in cloud computing. We are residing everything in providers premises which makes the information highly unsecured [6]. It's a main obstacle in adoption of cloud computing. According to the IDC's survey on the cloud services, security concerns are number one issue facing cloud computing [7, 8]. IDC's findings in the survey of 224 IT executives are shown in fig.2.

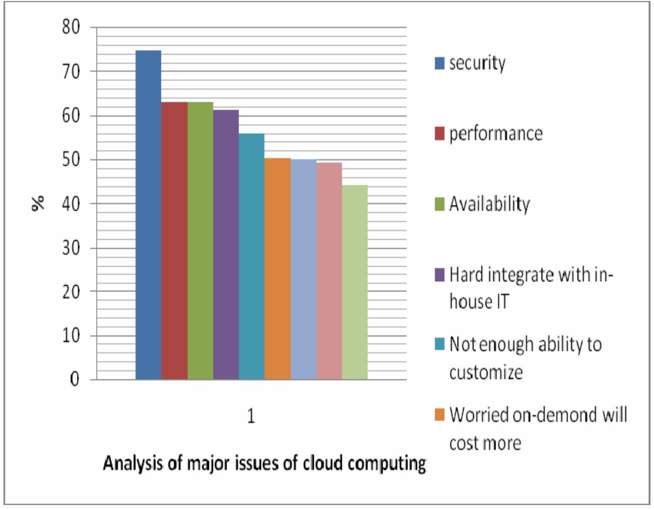

Figure 3. Analysis of major issues of cloud computing

Difficulties or overheads in front of cloud computing are the danger of-Disrupts Services, Theft of Information, Loss of Privacy, Damage of information. These problems prevent the organizations to adopt the cloud computing services. These can be removed by applying highly trusted security protocols.

V. Security Idea

Security involves a set of investments that are adequately funded. In Cloud, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a cloud network is very challenging. The goals to evaluate if cloud network is secure or not are as follows:

1) ***Availability:*** Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

2) ***Confidentiality:*** Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.

3) ***Integrity:*** Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

4) ***Authentication****:* Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

5) ***Non repudiation:*** Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

6) ***Anonymity:*** Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

7) ***Authorization****:* This property assigns different access rights to different types of users. For example a network management can be performed
by network administrator only.

VI. Security Solution Overcome to Security Issues

Following approaches can be helpful for secure cloud computing-

Backup: Natural disaster may damage the physical devices that may cause of data loss. To avoid this problem backup of information is the key of assurance of service provided by vendor.

- Network Security: A user can deny the access of any Internet based service by using IP Spoofing which can be a cause of security harm [6]. To solve this we can use Digital Signature technique. SSL (Secure Socket Layer) Protocol is used for managing security of message transmission on The Internet. Which also avoid resource hacking.

  Encryption Algorithm: Obviously cloud service providers encrypt the user's information using strong encryption algorithm. But problem is that encryption accident can make data totally unusable and encryption also complicates the availability [6]. To solve this problem the cloud provider must provide evidence that encryption scheme were designed and tested by experienced specialists.
- Investigation Support: Audit tools provided to the users to determine how their data is stored, protected, used, and verify policy enforcement. But investigation of illegal activity is quite difficult because data for multiple customers may be collocated and may also be geographically spread across set of hosts and datacenters. To solve this audit tools must be contractually committed along with the evidence.
- Customer satisfaction: Very hard for the customer to actually verify the currently implemented security practices and initiatives of a cloud computing provided by the service provider because the customer generally has no access to the provider's facility which can be comprised of multiple facilities spread around the globe [8]. Solution for this Provider should get some standard certificate from some governing or standardized institution that ensures users that provider has established adequate internal control and these control are operating efficiently.

VII. Proposed Secure Key Management Model

This section describes twenty recommended security management models and their requirements for cloud computing that cloud service providers should definitely consider as they develop or refine their compliance programs [9].

1) ***Software-as-a-Service (SaaS) security:*** SaaS is the dominant cloud service model for the foreseeable future and the area where the most critical need for security practices and oversight will reside. Just as with a managed service provider, corporations or end users will need to research vendors' policies on data security before using vendor services to avoid losing or not being able to access their data. The technology analyst and consulting firm Gartner lists [10] seven security risks which one should discuss with a cloud-computing vendor:

- *Privileged user access:* Get as much information as you can about the people who manage your data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.
- *Regulatory compliance:* Make sure that the vendor is willing to undergo external audits and/or security certifications.
- *Data location:* When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.
- *Data segregation:* Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
- *Recovery:* Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."
- *Investigative support:* Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then only safe assumption is that investigation and discovery requests will be impossible.
- *Long-term viability:* Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application. To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves.

2) ***Security management (People):*** One of the most important actions for a security team is to develop a formal charter for the security organization and program. The charter should be aligned with the strategic plan of the organization or company the security team works for. Lack of clearly defined roles and responsibilities, and agreement on expectations, can result in a general feeling of loss and confusion among the security team about what is expected of them, how their skills and experienced can be leveraged, and meeting their performance goals.

3) ***Security governance:*** A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. This committee must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions.

4) ***Risk management:*** Risk management entails identification of technology assets [11]; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls.

5) ***Risk assessment:*** Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets [12, 13]. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as -needed basis. More detailed and technical security risk assessments in the form of threat modeling should also be applied to applications and infrastructure.

6) ***Security awareness:*** People are the weakest link for security. Knowledge and culture are among the few effective tools to manage risks related to people. Not providing proper awareness and training to the people who may need them can expose the company to a variety of security risks for which people, rather than system or application vulnerabilities, are the threats and points of entry. Social engineering attacks, lower reporting of and slower responses to potential security incidents, and inadvertent customer data leaks are all possible and probable risks that may be triggered by lack of an effective security awareness program.

7) ***Education and training:*** Programs should be developed that provide a baseline for providing fundamental security team and their internal partners. This entails a formal process to assess and align skill sets to the needs of the security team and to provide adequate training and mentorship-providing a broad base of fundamental security, inclusive of data privacy, and risk management knowledge.

8) ***Policies and standards:*** Many resources and templates are available to aid in the development of information security policies and standards. A cloud computing security team should first identify the information security and business requirements unique to cloud computing, SaaS, and collaborative software application security. Policies should be developed, documented, and implemented, along with documentation for supporting standards and guidelines. To maintain relevancy, these policies, standards, and guidelines should be reviewed at regular intervals or when significant changes occur in the business or IT environment.

9) ***Third party risk management:*** Lack of a third-party risk management program may result in damage to the provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

10) ***Vulnerability assessment:*** Classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading.

11) ***Security image testing:*** Virtualization-based cloud computing provides the ability to create "Test image" VM secure builds and to clone multiple copies. Gold image VMs also provide the ability to keep security up to date and reduce exposure by patching offline. Offline VMs can be patched off-network, providing an easier, more cost-effective, and less production-threatening way to test the impact of security changes.

12) ***Data governance:*** This framework should describe who can take what actions with what information, and when, under what circumstances, and using what methods.

13) ***Data security:*** Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the European Union. It can also force encryption of certain types of data, and permit only specified users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCI DSS).

14) ***Application security:*** This is where the security features and requirements are defined and application security test results are reviewed. Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development teams. Although product engineering will likely focus on the application layer, the security design of the application itself, and the infrastructure layers interacting with the application, the security team should provide the security requirements for the product development engineers to implement.

15) ***Virtual machine security:*** In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

16) ***Identity Access Management:*** *I*dentity and access management is a critical function for every organization, and a fundamental expectation of SaaS customers is that the "principle of least privilege" is granted to their data. The principle of least privilege states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary.

17) ***Change management:*** The security team can create security guidelines for standards and minor changes, to provide self-service capabilities for these changes and to prioritize the security team's time and resources on more complex and important changes to production.

18) ***Physical security [9]:*** Since customers lose control over physical assets, security model may need to be reevaluated. The concept of the cloud can be misleading at times, and people forget that everything is somewhere actually tied to a physical location. The massive investment required to build the level of security required for physical data centers is the prime reason that companies don't build their own data centers, and one of several reasons why they are moving to cloud services in the first place. Some samples of controls mechanisms:

- 24/7/365 onsite security.

- Biometric hand geometry readers.
- Security cameras should monitor activity throughout the facility.
- Heat, temperature, air flow, and humidity should all be kept within optimum ranges for the computer equipment.
- Policies, processes, and procedures are critical elements of successful physical security that can protect the equipment and data housed in the hosting center.

19) ***Disaster recovery [9]:*** In the SaaS environment, customers rely heavily on 24/7/365 access to their services and any interruption in access can be catastrophic. Using the virtualization software virtual server can be copied, backed up, and moved just like a file (live migration). Benefits are:

- Quickly reallocating computing resources without any downtime
- Ability to deliver on service-level agreements and provide high-quality service

20) ***Data privacy:*** A privacy steering committee should also be created to help make decisions related to data privacy. The security compliance team, if one even exists, will not have formalized training on data privacy. The answer is to hire a consultant in this area, hire a privacy expert, or have one of your existing team members trained properly. This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators.

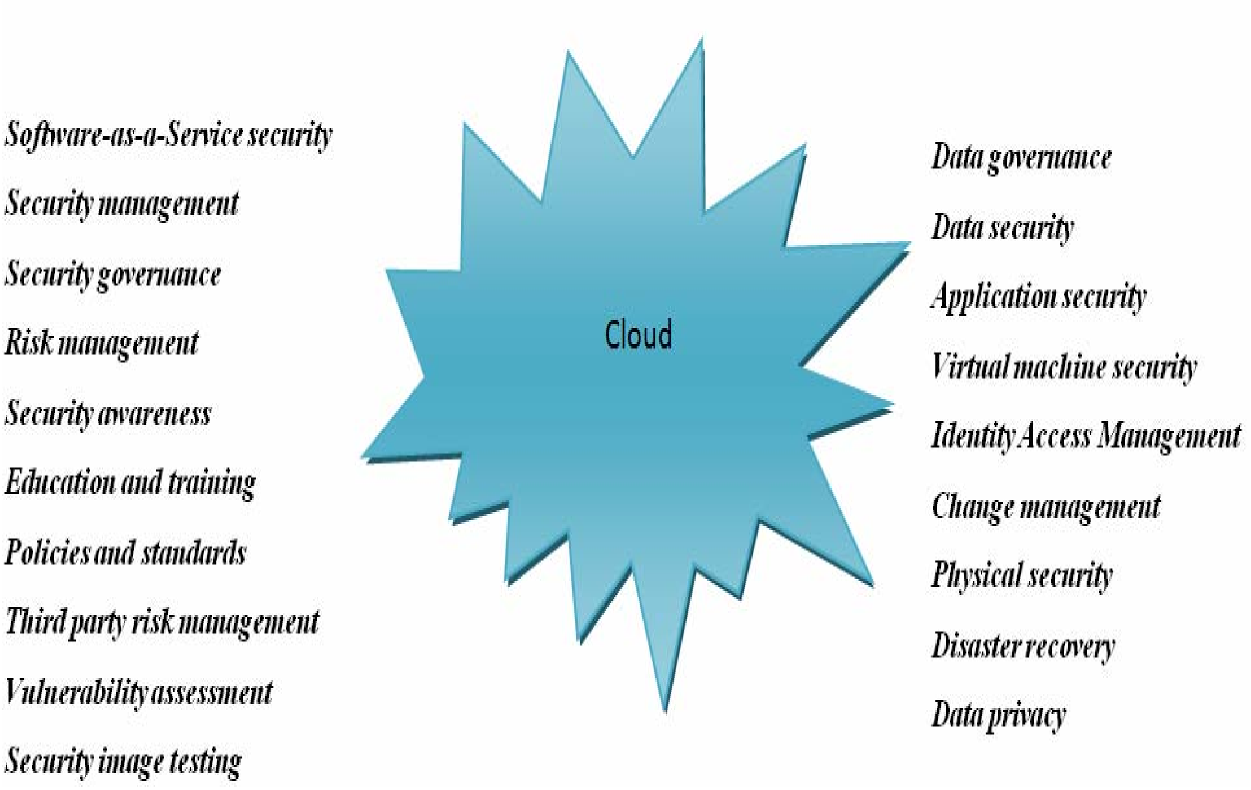

Figure 4: Secure Key Management Model

VIII. RECOMMENDATION

Security is a very important consideration as the network cannot be reliable if data transmission is not secure. There are many security risks to information as hackers are always looking ways to steal critical information.

A network will get a better performance if these factors are considered accurately. All the recommendations mentioned above would help improve performance of the cloud computing system.

IX. CONCLUSION

Cloud computing is the future of IT industries. It helps the industries to get efficient use of their IT Hardware and Software resources at low cost. This paper totally discuss about the cloud computing secure key management model. In this paper, we also analyze cloud computing vulnerabilities, security threats, cloud computing faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of Cloud computing require high degree of security and on the other hand, cloud computing are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt the demanding requirements of these networks.

The future of cloud computing is really appealing, giving the vision of cheap communications. At present, the general trend in cloud computing is toward mesh architecture at large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Large scale cloud computing is another challenging issue in the near future. As the involvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in ad-hoc networks will be smaller, cheaper, more capable, and come in all forms. In all, although the widespread deployment of cloud computing still year away, the research in this field will continue being very active and imaginative.

X. REFRENCES

[1] Ricardo vilaca, Rui oliveira 2009. Clouder: A Flexible Large Scale Decentralized Object Store. Architecture Overview. Proceeding of WDDDM '09

[2] Michael Miller. 2009. Cloud Computing-Web Based Application that change the way you collaborate online. Publishing of QUE, 2nd print.

[3] National Institute Of Standard and technology. csrc.nist.gov/groups/ SNS/cloud-computing/cloud-def-v15.doc, 2009

[4] Open Security Architecture http://www.opensecurityarchitecture.org/

[5] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks

[6] GregBoss, Padma Malladi, Dennis Quan, Linda Legregni and Harold hall 2007. Cloud Computing. Available from www.ibm.com/developerworks/websphere/zones/hipods/

[7] Anthony T.Velte, Toby J.Velte and Robert Elsenpeter 2010. Cloud Computing- A Practical Approach. Publishing of Tata McGRAW Hil.

[8] Saurabh Kumar. Security Issues In Cloud Computing. Available fromserl.iiit.ac.in/cs6600/saurabh.ppt.

[9] Krešimir Popović, Željko Hocenski," Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia

[10] Gartner: Seven cloud-computing security risks, 02 July 2008, http://www.infoworld.com/d/security-central/gartnerseven-cloud-computing-security-risks-853?page=0,0

[11] Wikipedia, 6 February 2010, http://en.wikipedia.org/wiki/Risk_management

[12] Wikipedia, 27 January 2010, http://en.wikipedia.org/wiki/Risk_assessment

[13] D. Catteddu, Giles Hogben: European Network and Information Security Agency, November 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessmen

AUTHORS PROFILE

Shivlal Mewada has received his Master of Philosophy in Computer Science (M.Phil.-CS) from Institute of Computer Science, Vikram University, Ujjain. He is currently pursuing Ph.D. in Computer Science from Institute of Computer Science, Vikram University, Ujjain - INDIA. He is presently working as Guest lecturer in Department of Computer Science, Govt. Holkar (Autonomous) Science Collage, Indore - India. He has published various research papers in international journals. His research interest includes Security in-Mobile Ad-hoc Networks (MANET), Wireless Mesh Network (WMN), Cloud Computing, Data Mining and Information Technology based education.

Dr. Umesh Kumar Singh obtained his Ph.D. in Computer Science from Devi Ahilya University, Indore-INDIA. He is currently Reader (Director) in Institute of Computer Science, Vikram University, Ujjain-INDIA. He served as professor in Computer Science and Principal in Mahakal Institute of Computer Sciences (MICS-MIT), Ujjain. He is formally Director I/C of Institute of Computer Science, Vikram University Ujjain. He has served as Engineer (E&T) in education and training division of CMC Ltd., New Delhi in initial years of his career. He has authored a book on "Internet and Web technology "and his various research papers are published in national and international journals of repute. Dr. Singh is reviewer of International Journal of Network Security (IJNS), IJCSIS, ECKM Conferences and various Journals of Computer Science. His research interest includes network security, secure electronic commerce, client-server computing and IT based education.

Dr. Pradeep Sharma obtained his Ph.D. in Physics from Devi Ahilya University, Indore-INDIA. He is currently Professor and Head of department, (HOD) in Department of Computer Science, Govt. Holkar (Aotonomous) Science College-INDIA. He has 28 year teaching excepience in college level. His various research papers are published in national and international journals of repute. His various paperr published in national and international conferencess His research interest includes X-ray spectroscopy,Networking.