An Study of Security Issues & Challenges in Cloud Computing

Mili Patel[1] Rakesh Patel[2]
[1,2]Lecturer
[1,2]Department of Information Technology
[1,2]Kirodimal Institute of Technology Raigarh (C.G.), India

Abstract— "Cloud Computing" is a term, which involves virtualization, distributed computing, networking and web-services. It is a way of offering services to users by allowing them to tap into a massive pool of shared computing resources such as servers, storage and network. User can use services by simply plug into the cloud and pay only for what he uses. All these features made a cloud computing very advantageous and demanding. But the data privacy is a key security problem in cloud computing which comprises of data integrity, data confidentiality and user privacy specific concerns. Most of the persons do not prefer cloud to store their data as they are having a fear of losing the privacy of their confidential data. This paper introduces some cloud computing data security problem and its strategy to solve them which also satisfies the user regarding their data security.

Key words: cloud computing, cloud data security, strategy

I. INTRODUCTION

A. *What Is Cloud Computing?*

Cloud computing ('cloud') is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption. From an architectural perspective; there is much confusion surrounding how cloud is both similar to and different from existing models of computing; and how these similarities and differences impact the organizational, operational, and technological approaches to network and information security practices.

II. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches:

A. *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 a service provider.

B. *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) as well as other traditional or cloud based software services.

C. *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 degree 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. Even private clouds tend to pool resources between different parts of the same organization.

D. *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.

E. *Measured service*

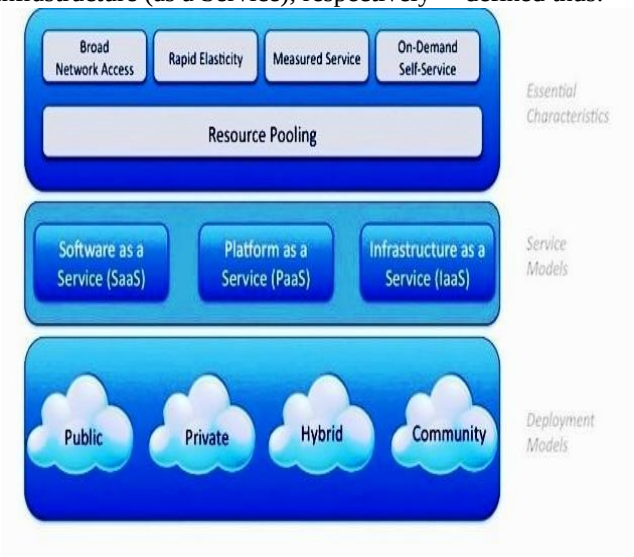
Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported — providing transparency for both the provider and consumer of the service. It is important to recognize that cloud services are often but not always utilized in conjunction with, and enabled by, virtualization technologies. There is no requirement, however, that ties the abstraction of resources to virtualization technologies and in many offerings virtualization by hypervisor or operating system container is not utilized. Further, it should be noted that multi-tenancy is not called out as an essential cloud characteristic by NIST but is often discussed as such. Please refer to the section on multi-tenancy featured after the cloud deployment model description below for further details.

III. CLOUD SERVICE MODELS

Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the "SPI Model," where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively —defined thus:

A. Cloud Software as a Service (SaaS)

Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the "SPI Model," where 'SPI'refers to Software, Platform or Infrastructure (as a Service), respectively —defined thus:



B. Cloud Platform as a Service (PaaS)

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.

C. Cloud Infrastructure as a Service (IaaS)

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).

IV. CLOUD DEPLOYMENT MODELS

Regardless of the service model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud services, with derivative variations that address specific requirements:

A. 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.

B. Private Cloud

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

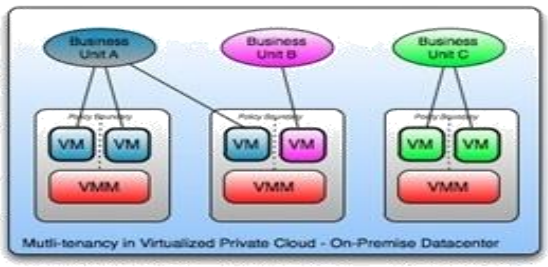
C. Community Cloud

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

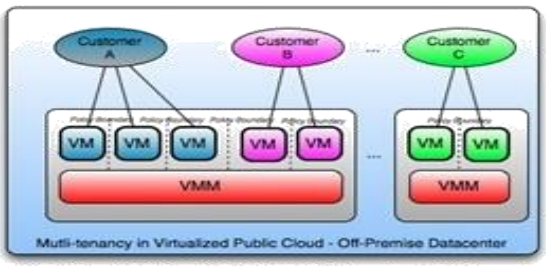
D. Hybrid Cloud

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).

It is important to note that there are derivative cloud deployment models emerging due to the maturation of market offerings and customer demand. An example of such is virtual private clouds —a way of utilizing public cloud infrastructure in a private or semi-private manner and interconnecting these resources to the internal resources of a consumers' datacenter, usually via virtual private network (VPN) connectivity. The architectural mindset used when designing "solutions have clear implications on the future flexibility, security, and mobility of the resultant solution, as well as its collaborative capabilities. As a rule of thumb, parameterized solutions are less effective than de-perimeterized solutions in each of the four areas. Careful consideration should also be given to the choice between proprietary and open solutions for similar reasons.



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure

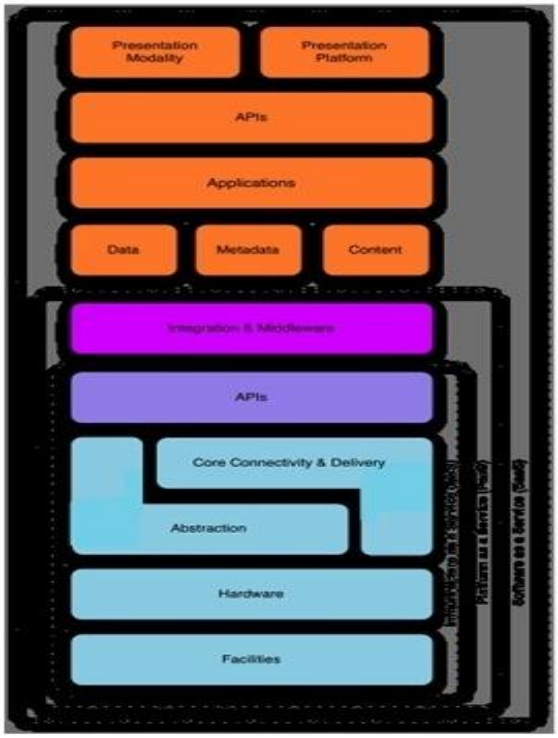


Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

V. MULTI-TENANCY

CSA has identified multi-tenancy as an important element of cloud. Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure. From a provider's perspective, multi-tenancy suggests an architectural and design approach to enable economies of scale, availability, management,

segmentation, isolation, and operational efficiency; leveraging shared infrastructure, data, metadata, services, and applications across many different consumers. Multi-tenancy can also take on different definitions depending upon the cloud service model of the provider; in as much as it may entail enabling the capabilities described above at the infrastructure, database, or application levels. An example would be the difference between an IaaS and SaaS multi-tenant implementation. Cloud deployment models place different importance on multi-tenancy. However, even in the case of a private cloud, a single organization may have a multitude of third party consultants and contractors, as well as a desire for a high degree of logical separation between business units. Thus multi-tenancy concerns should always be considered.



VI. CLOUD REFERENCE MODEL

Understanding the relationships and dependencies between Cloud Computing models is critical to understanding Cloud Computing security risks. IaaS is the foundation of all cloud services, with PaaS building upon IaaS, and SaaS in turn building upon PaaS as described in the Cloud Reference Model diagram. In this way, just as capabilities are inherited, so are information security issues and risk. It is important to note that commercial cloud providers may not neatly fit into the layered service models. Nevertheless, the reference model is important for relating real-world services to an architectural framework and understanding the resources and services requiring security analysis. IaaS includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the capability to abstract resources (or not), as well as deliver physical and logical connectivity to those resources. Ultimately, IaaS provides a set of APIs which allow management and other forms of interaction with the infrastructure by consumers. PaaS sits atop IaaS and adds an additional layer of integration with application development frameworks; middleware capabilities; and functions such as database, messaging, and queuing; which allow developers to build applications upon to the platform; and whose programming languages and tools are supported by the stack. SaaS in turn is built upon the underlying IaaS and PaaS stacks; and provides a self-contained operating environment used to deliver the entire user experience including the content, its presentation, the application(s), and management capabilities. It should therefore be clear that there are significant trade-offs to each model in terms of integrated features, complexity vs. openness (extensibility), and security.

For an excellent overview of the many cloud computing use cases, the Cloud Computing Use Case Group produced a collaborative work to describe and define common cases and demonstrate the benefits of cloud, with their goal being to "...bring together cloud consumers and cloud vendors to define common use cases for cloud computing...and highlight the capabilities and requirements that need to be standardized in a cloud environment to ensure interoperability, ease of integration, and portability."

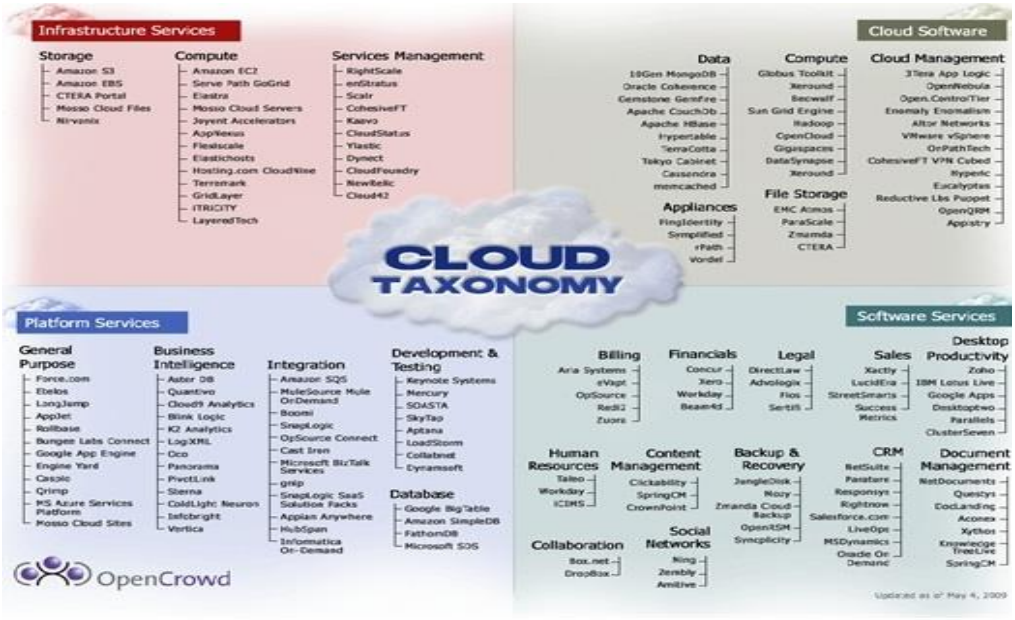


Fig 4: Open Cloud Taxonomy

VII. CLOUD SECURITY REFERENCE MODEL

The cloud security reference model addresses the relationships of these classes and places them in context with their relevant security controls and concerns. For organizations and individuals grappling with cloud computing for the first time, it is important to note the following to avoid potential pitfalls and confusion:

- The notion of how cloud services are deployed is often used interchangeably with where they are provided, which can lead to confusion. For example, public or private clouds may be described as external or internal clouds, which may or may not be accurate in all situations.
- The manner in which cloud services are consumed is often described relative to the location of an organization's management or security perimeter (usually defined by the presence of a firewall). While it is important to understand where security boundaries lie in terms of cloud computing, the notion of a well-demarcated perimeter is an anachronistic concept.
- The re-parameterization and the erosion of trust boundaries already happening in the enterprise is amplified and accelerated by cloud computing. Ubiquitous connectivity, the amorphous nature of information interchange, and the ineffectiveness of traditional static security controls which cannot deal with the dynamic nature of cloud services, all require new thinking with regard to cloud computing. The Jericho Forum has produced a considerable amount of material on the re-parameterizations of enterprise networks, including many case studies. The deployment and consumption modalities of cloud should be thought of not only within the context of 'internal' vs. 'external' as they relate to the physical location of assets, resources, and information; but also by whom they are being consumed by; and who is responsible for their governance, security, and compliance with policies and standards. This is not to suggest that the on-or off-premise location of an asset, a resource, or information does not affect the security and risk posture of an organization because they do —but to underscore that risk also depends upon:

1) The types of assets, resources, and information being managed
2) Who manages them and how
3) Which controls are selected and how they are integrated

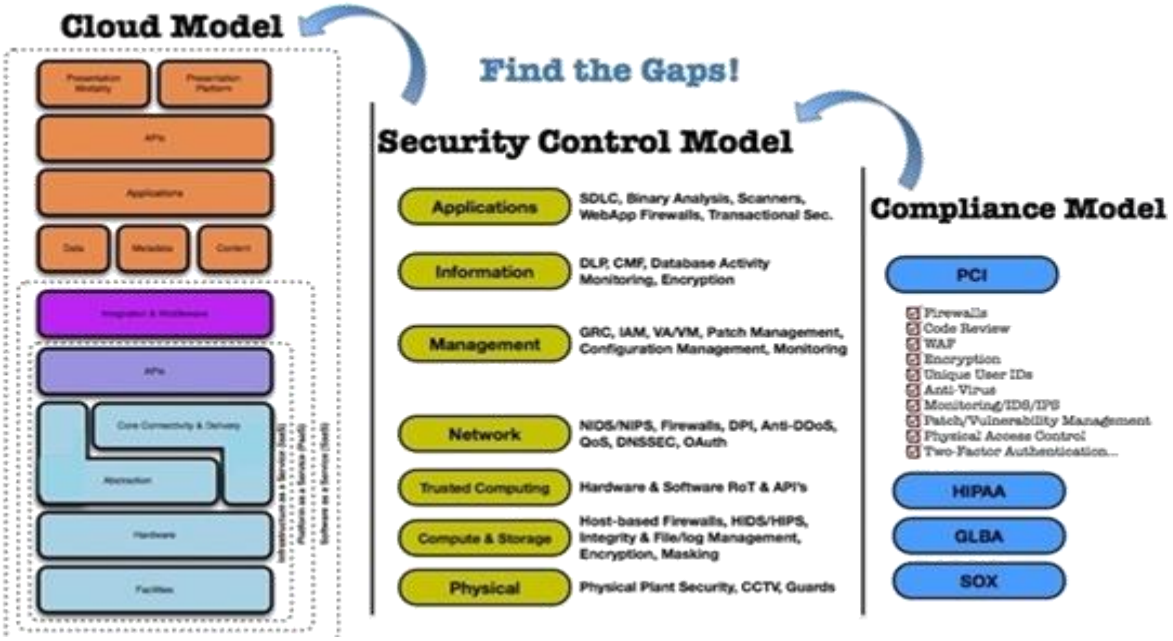


Fig: Mapping the Cloud Model to the Security Control & Compliance Model

VIII. What Is Security for Cloud Computing?

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions. Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties.

An organization's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure de (network security), to the IT systems (system security), all the way to the information and applications (application security). Additionally controls are implemented at the people and process levels, such as separation of duties and change management, respectively. As described earlier in this document, the security responsibilities of both the provider and the consumer greatly differ between cloud service models. Amazon's AWS EC2 infrastructure as a service offering, as an example, includes vendor responsibility for security up to the hypervisor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. The consumer, in turn, is responsible for security controls that relate to the IT system (instance) including the operating system, applications, and data. One of the attractions of cloud computing is the cost efficiencies afforded by economies of scale, reuse, and standardization. To bring these efficiencies to bear, cloud providers have to provide services that are flexible enough to serve the largest customer base possible, maximizing their addressable market. The figure below illustrates these issues: in SaaS environments the security controls and their scope are negotiated into the contracts for service; service levels, privacy, and compliance are all issues to be dealt with legally in contracts. In an IaaS offering, while the responsibility for securing the underlying infrastructure and abstraction layers belongs to the provider, the remainder of the stack is the consumer's responsibility. PaaS offers a balance somewhere in between, where securing the platform itself falls onto the provider, but securing the applications developed against the platform and developing them securely, both belong to the consumer. Understanding the impact of these differences between service models and how they are deployed is critical to managing the risk posture of an organization.

IX. Beyond Architecture: The Areas of Critical Focus

The twelve other domains which comprise the remainder of the CSA guidance highlight areas of concern for cloud computing and are tuned to address both the strategic and tactical security 'pain points' within a cloud environment, and can be applied to any combination of cloud service and deployment model. The domains are divided into two broad categories: governance and operations. The governance domains are broad and address strategic and policy issues within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture. Governance Domains Domain Guidance dealing with ...Governance and Enterprise Risk Management The ability of an organization to govern and measure enterprise risk introduced by Cloud Computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues, are some of the items discussed. Legal and Electronic Discovery Potential legal issues when using Cloud Computing Issues touched on in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc. Compliance and Audit Maintaining and proving

compliance when using Cloud Computing Issues dealing with evaluating how Cloud Computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit.

X. INFORMATION LIFECYCLE MANAGEMENT

Managing data that is placed in the cloud Items surrounding the identification and control of data in the cloud, as well as compensating controls which can be used to deal with the loss of physical control when moving data to the cloud, are discussed here. Other items, such as who is responsible for data confidentiality, integrity, and availability are mentioned. Portability and Interoperability The ability to move data/services from one provider to another, or bring it entirely back in house. Issues surrounding interoperability between providers are also discussed. Operational Domains Traditional Security, Business Continuity and Disaster Recovery How Cloud Computing affects the operational processes and procedures currently use to implement security, business continuity, and disaster recovery. The focus is to discuss and examine possible risks of Cloud Computing, in hopes of increasing dialogue and debate on the overwhelming demand for better enterprise risk management models. Further, the section touches on helping people to identify where Cloud Computing may assist in diminishing certain security risks, or entails increases in other areas.

XI. DATA CENTER OPERATIONS

How to evaluate a provider's data center architecture and operations this is primarily focused on helping users identify common data center characteristics that could be detrimental to ongoing services, as well as characteristics that are fundamental to long-term stability. Incident Response, Notification and Remediation Proper and adequate incident detection, response, notification, and remediation This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident handling program. Application Security Securing application software that is running on or being developed in the cloud

XII. CONCLUSION

This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS). Some specific security issues related to the cloud are also discussed. Encryption and Key Management Identifying proper encryption usage and scalable key management This section is not prescriptive, but is more informational is discussing why they are needed and identifying issues that arise in use, both for protecting access to resources as well as for protecting data. Identity and Access Management Managing identities and leveraging directory services to provide access control. The focus is on issues encountered when extending an organization's identity into the cloud. This section provides sin sight into assessing an organization's readiness to conduct cloud-based Identity and Access Management (IAM). Virtualization The use of virtualization technology in Cloud Computing. The domain addresses items such as risks associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. This domain focuses on the security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization.

REFRENCES

[1] Cloud Computing Issues and Benefits Modern Education By D.Kasi Viswanath, S.Kusuma & Saroj Kumar Gupta Madanapalle Institute of Technology and Science Madanapalle, Chittoor India
[2] Data Security Issues and Strategy on Cloud Computing by Sonam Singh , Department of Computer Science and Engineering, I.F.T.M University , Moradabad Province 244001, India
[3] An Overview and Study of Security Issues & Challenges in Cloud Computing Rajesh Piplode* by Umesh Kumar Singh Department of Computer Science Institute Of Computer Science Govt. Holkar Science College Indore-India Vikram University Ujjain-India
[4] Security Threats and Countermeasures in Cloud Computing Vahid Ashktorab, Seyed Reza Taghizadeh Department of Computer Engineering, Islamic Azad University of NajafAbaad, Isfahan, Iran Department of Information Technology, Kahje-Nassir-Toosi University of Technology, Tehran, Iran
[5] Cloud Computing Security Issues, Challenges and Solution Pradeep Kumar Tiwari1, Dr. Bharat Mishra M.phil (CSE)student, Reader in department of physical Science, at Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya Chitrakoot - Satna (M.P.)

