I.J. Wireless and Microwave Technologies, **2024, 1, 14-28**
Published Online on February 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.01.02

An Analytical Study of Cloud Security Enhancements

Imran Khan*
Assistant Professor, Harcourt Butler Technical University, Kanpur, UP, India
Email: imran.k@hbtu.ac.in
*Corresponding Author

Tanya Garg
Assistant Professor, BVICAM, New Delhi, India
Email: tanya.pathak@gmail.com

Received: 25 January, 2023; Revised: 09 March, 2023; Accepted: 18 April, 2023; Published: 08 February, 2024

Abstract: Enhancements and extensions in pervasive computing have enabled penetration of cloud computing enabled services into almost all walks of human life. The expansion of computational capabilities into everyday objects and processes optimizes end users requirement to directly interact with computing systems. However, the amalgamation of technologies like Cloud Computing, Internet of Things (IoT), Deep Learning etc are further giving way to creation of smart ecosystem for smart human living. This transformation in the whole pattern of living as well as working in enterprises is generating high expectations as well as performance load on existing cloud implementation as well as cloud services. In this complete scenario, there are simultaneous efforts on optimizing as well as securing cloud services as well as the data available on the cloud.

This manuscript is an attempt at introducing how cloud computing has become pivotal in the current enterprise setting due to its pay-as -you -use character. However, the allurement of using services without having to procure and retain involved hardware and software also has certain risks involved. The main risk involved in choosing cloud is compromising security concerns. Many potential customers avoid migrating towards cloud due to security concerns. Security concerns for the cloud implementations in the recent times have grown exponentially for all the varied stakeholders involved. The aim of this manuscript is to analyze the current security challenges in the existing cloud implementations. We provide a detailed analysis of existing cloud security taxonomies enabling the reader to make an informed decision on what combination of services and technologies could be used or hired to secure their data available on the cloud.

Index Terms: Cloud Computing, Cloud Security, Cloud Security Taxonomies, Authentication, Vulnerabilities, Threats, Countermeasures.

1. Introduction

The growing pace of modern day businesses accelerates the need for faster access to resources at negligible costs and no infrastructure maintenance[1]. In the current scenario, many commercial enterprises as well as academic institutions have migrated to the cloud. As per Gartner estimates, Cloud Computing is one amongst the top ten most significant skills that have a superior prospect of adoption among companies and organizations[2]. The basic idea of this cloud computing was envisioned way back in 1960’s when John McCathy predicted that utility based allocation of services will be provided to the customer[3]. Cloud computing marks the third generation evolution in the history of IT, mainly transitioning from hardware to software, software to services and distributed services to centralized services[4]. It is one skill that facilitates omnipresent, opportune, on-demand network admittance to a collective group of configurable computing assets like networks, servers, storage, application and services that can be swiftly processed and provisioned with minimal service provider interface or effort[5]. In the words of National Institute of Standards and Technology (NIST), U.S Department of Commerce “Cloud computing is the model for enabling ubiquitous, 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”[6]. Figure I below gives a NIST graphical view of this definition of the cloud. We shall abide by this definition of cloud computing for the rest of this chapter.

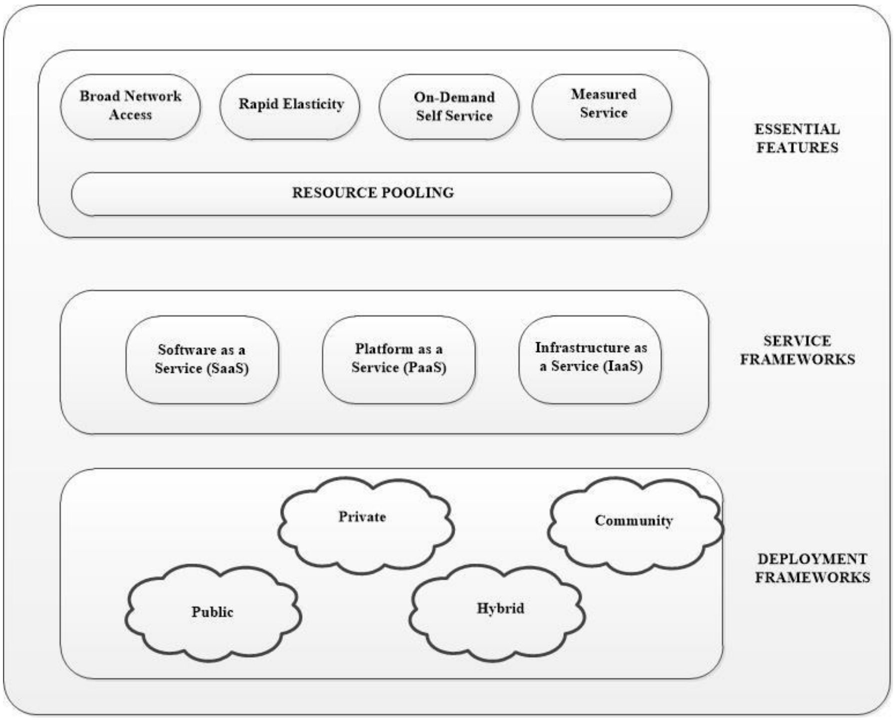

Fig. 1. Visual Representation of Cloud Computing (NIST View)

Cloud computing is the effective amalgamation of Utility Computing, Grid Computing, SaaS using external deployment of computational power, storage and business applications as a service[7].Cloud enables users to use a rapid on-demand network admittance to a collective group of resources eliminating need for service provider interaction[8]. Cloud has reduced client side complexity and leveraged users from hardware requirements to services[9]. Cloud scenario identifies diverse groups of participants such as services/service instances, service users and cloud provider[10]. The cloud model encompasses applications delivered as services as well as data centres comprising of system software and hardware that deliver those services[11]. These *software-as-a-service* model along with *data centres* are what comprise of the ‘Cloud’[11]. The term ‘Cloud’ has originated from the world of telecommunication networks where the concept of virtualization first set in through VPN services[12]. The cloud paradigm promises reliable service delivery through high performance data centres that are calibrated by virtualized compute and store technologies[13].

Broadly classified cloud computing is a computational idea as well as a service-allocation style that aims at enabling rapid, secure, convenient net computing as well as data storage facilities with all required computing services delivered over the Internet[14, 15]. Thus, the cloud can be visualized as a mechanism for enabling cooperation, dexterity, scalability and ability to adapt to dynamically fluctuating demands in a cost-effective and optimized fashion[16, 17]. To realize this aim cloud computing amalgamates varied computing notions as well as technologies like virtualization, Web 2.0, Service Oriented Architecture (SOA), Internet etc[17]. Through a proper and secure collaboration of these technologies any type of cloud implementation actually enables dexterous services to its users while their data and software is secured on the servers[17]. Hence, an attractive term cloud computing is generally projected as a low-cost, low-manpower solution to ever growing computing needs of varied organizations of varied sizes[18]. This has resulted in the enterprise trend drifting away from localized data storages to centralized data centres[19].

Recently cloud computing has garnered increased interest from policy makers, regulatory authorities as well as users like academic giants, business conglomerates and enterprises[20]. The prime reason for this interest is not just migration or adoption of some available cloud service but also a growing concern where numerous challenges and risks are posed in terms of cloud security involving compliance, legal issues and privacy[21]. These issues need to be carefully handled to increase user trust on cloud implementations leading to effective attainment of broader policy objectives[22].

As cloud computing is still a relatively novel computing framework, there lies a great deal of apprehensions as well security issues at all levels of its implementation be it network, host, application or data[23]. These apprehensions have in turn made security the number one risk as well as concern with cloud computing. Security concerns may recount to a number of domains including secure external data storage, secure access to public internet, internal security measures etc[5]. Notably the cloud itself characterizes to be a large scale framework with distributed resources that are inherently heterogeneous and completely virtual. Thus conventional security mechanisms like authentication and authorization are ineffective for the cloud[24]. Hence, cloud computing calls for more minute and integrated security measures.

This chapter aims to analyze the technical, operative as well as the authorized minutiae of cloud computing taking into consideration the security interests of all the stakeholders (individual user, organizations, cloud service providers, regulatory authorities) involved. We aim at highlighting the various security measures being implemented at all levels of real-time cloud deployments while bringing out the issues and challenges still haunting the complete security of the cloud. We try to present a detailed classification of the security issues allied to the diverse cloud service delivery models while identifying the key vulnerabilities and threats existing in the cloud ecosystem. For clarification, we specify that vulnerability may be defined as the flaw in a system that makes possible a successful attack. While a threat may be defined as, a potential attack resulting into unauthorized use of data as well as resources. In the course of this chapter while listing the vulnerabilities and threats we shall also try to uncover the inter-relationship among them while uncovering the possible countermeasures that can be used to overcome them.

The rest of this chapter is detailed as follows: Section II elaborates the varied cloud implementation models. Section III discusses the security risks and issues posed by different cloud implementations. Section IV delves into the various the various cloud migration issues enterprises, as well as customers face before adopting a cloud implementation. Section V details the varied cloud security frameworks and techniques being utilized with real-time cloud implementations. Section VI concludes the chapter while Section VII lays the future research directions. The chapter is aimed at serving as an advisory on policy and other interferences to be considered to ensure that clients of the cloud are appropriately protected and lay down a supportive as well as competitive cloud ecosystem.

2. Cloud Implementation Models

We first start with understanding the basic idea that goes behind a successful cloud implementation. Varied available cloud implementation models can be broadly classified either in terms of scope or in terms of service delivery. We detail these as cloud deployment and cloud service delivery models outlined below:

A. Cloud Deployment Model

The cloud computing model comprises of three main deployment models in terms of scope. Presently the deployment models in cloud are described as below[25]. These are further detailed diagrammatically in Figure 2 below[26]:-

1. Private Cloud- The cloud resources are provided to be used by a single organization and multiple authenticated users[27]. An organization’s private cloud is deployed within the organization’s private data centre[28]. Specific organizations and their authorized personnel have access to operate the organization’s private cloud[29]. Services are granted to reliable clients via a single-tenant operational atmosphere like the Intranet. In essence, an organisation’s data centre distributes cloud computing services to clients who may be physically present in the premises. For Example: SAM CloudBox etc
2. Public Cloud- Mainstream cloud implementation where off-site third party providers access resources and *pay-per-use*[25]. Services are available to human clients and organisations who desire to preserve flexibility and liability without engrossing the complete expenses of in-house infrastructures[26]. Public cloud users are considered unreliable by default. These implementations suffer in security, quality of service, etc. as there is a constant threat of malicious attack. For Example: Amazon web services (AWS), Microsoft Azure, Google Cloud etc.
3. Community Cloud- Cloud infrastructure is common between multiple businesses of a common communal concern, policies, values and requirements[27]. Such communities function in an economic equilibrium through a common degree of economic scalability[30]. Management of such cloud maybe organization central or through a third party vendor. For Example: FountainHead, SalesForce Community Cloud.
4. Hybrid Cloud- This combines service implementations of two or more composite infrastructures within a secured framework[27]. The composite cloud architectures can be of private, public or community cloud implementations. The open architecture of hybrid cloud has interfaces for interaction with other systems. For Example: Nanyang Technological University, SunCorp Bank etc.

Fig. 2 above details the basic components of the cloud deployment model. As can be observed, each cloud implementation whether public or private is assembled on the top of the SPI framework as detailed in the next section. However, what differentiates these different clouds are their user set.

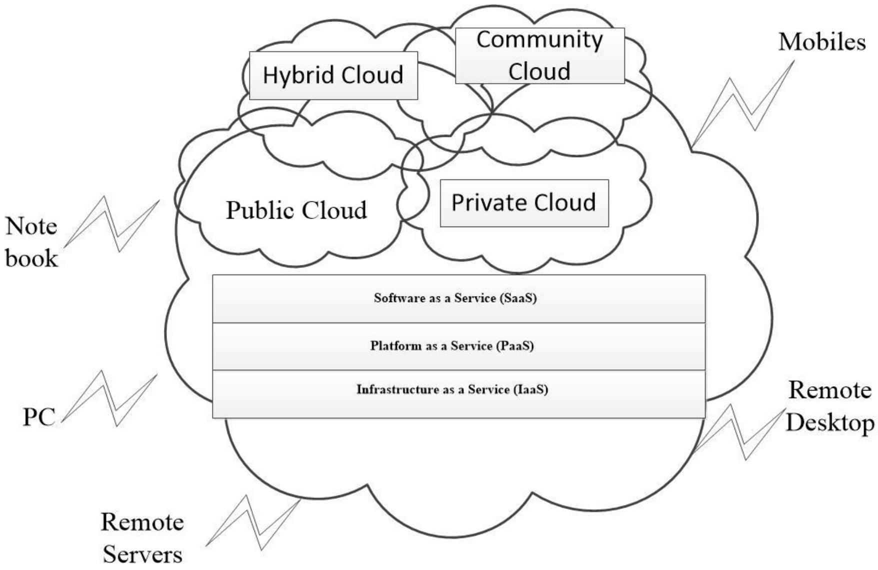

Fig. 2. Cloud Deployemnt Models

B. Cloud Service Delivery Models- The Spi Framework

Cloud computing caters for scalability, virtualization, interoperability and quality of service through cloud delivery models[31]. A *cloud client* is a software/hardware relying on the cloud model for delivery of services[32]. The cloud model has also been accepted as the Software Platform Infrastructure or SPI Model[33]. This acronym list the three services rendered by Cloud i.e. Software as a Service, Platform as a Service and Infrastructure as a Service. Literature identifies four main broad service delivery/SPI models in cloud architecture that are described below[34]:-

1. Software as a Service (SaaS)–Software as a service allows *pay-per-use* admission to services and software in the cloud. It is a network based access to commercial software coupled with the ease of access from any geographical location through the internet[32]. SaaS provides software applications to be accessible to the client by a thin client interface such as Gmail, Hotmail, Google Docs, etc. Most popular vendors for SaaS are- Google Docs, Apple’s MobileMe and Zoho Suite[33].
2. Platform as a Service (PaaS)–Platform as a service offers programming languages, APIs, development middleware, etc. NIST describes the PaaS as “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”[33]. Customers can use deployment platforms and application hosting systems environments for the lifecycle of development over the network such as Salesforce.com, Microsoft Azure, Google’s Apps Engine, etc[35].
3. Infrastructure as a Service (IaaS)-Infrastructural facility such as networks, virtual machines, computing nodes, servers, etc when provided for use as a service forms the IaaS service model. The NIST definition for Cloud Infrastructure as a Service is -“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)”[33]. Users are free from the responsibility of maintaining infrastructure but still retain control over operating it. Customers need to pay only for the time duration in which they use the service. IaaS enables consumers to cloud resources for running their applications such as Amazon’s EC2, Flexiscale[9].
4. Hardware as a Service (HaaS)- Here the cloud enables admittance to committed firmware through the Internet. In the words of Nicholas Carr[36] “Purchasing entire IT hardware or data centre for an enterprise comes into scalability as you opt for a *pay-as-you-go* service model. But in the era of IT automation and virtualization, the idea of *hardware-as-a-service* has its prime time approaching”. The entire cost of managing and purchasing a data centre is let off the enterprise. Examples of dedicated HaaS firmware over the internet are VMWare and XEN[37].

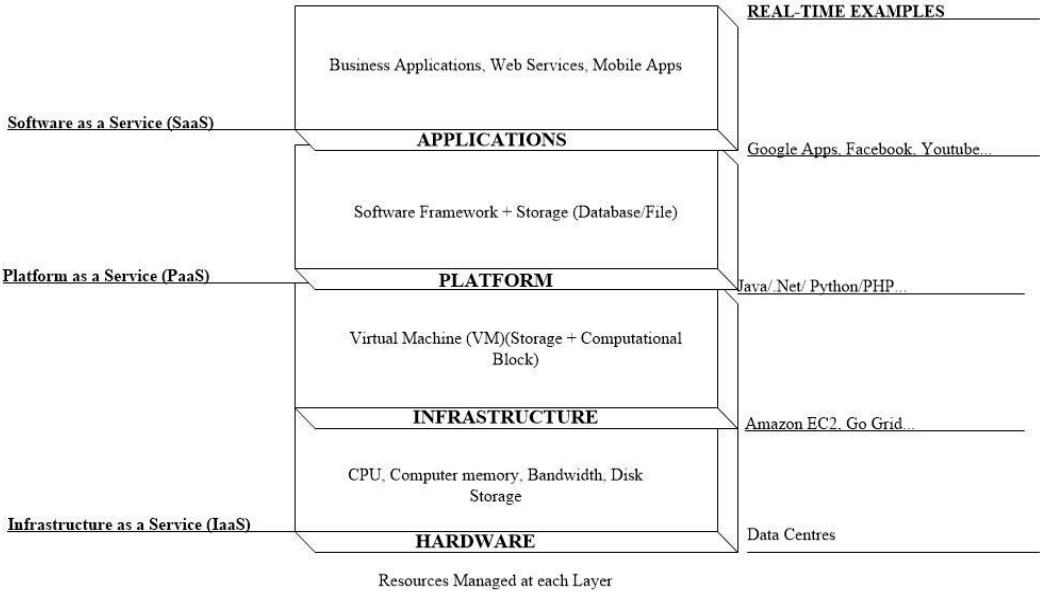
REAL-TIME EXAMPLES
Business Applications, Web Services, Mobile Apps
Software as a Service (SaaS)
APPLICATIONS
Google Apps, Facebook, Youtube...
Software Framework + Storage (Database/File)
Platform as a Service (PaaS)
PLATFORM
Java/.Net/ Python/PHP...
Virtual Machine (VM)(Storage + Computational Block)
INFRASTRUCTURE
Amazon EC2, Go Grid...
CPU, Computer memory, Bandwidth, Disk Storage
Infrastructure as a Service (IaaS)
HARDWARE
Data Centres
Resources Managed at each Layer

Fig. 3. Basic Cloud Computing SPI Framework

Figure 3 above visualizes the basic cloud computing SPI framework that forms the underlying basis of all cloud implementations. We also depict many real-time service providers available at each layer for enabling different services. The key services enabled at different layers are also detailed in table I below [38, 39]:

Table 1.Cloud computing technology stack pertaining to each cloud feature set

Cloud Feature	**SPI Layer Implementation**	**Feature Elaboration**	**Component Technology**	**Advantages**
Virtualization[40]	HaaS, IaaS Layer	Method of deploying computing resources.	Servers, network systems, storage systems, services, network devices.	Dynamic and centralized utilization of virtual resources, flexibility in implementation, cost reduction, reduced risk of management.
Mass Distributed Storage[41]	PaaS Layer	Distributed storage to save data enabling economical and realistic mass distributed storage and computing system	Hadoop Distributed File System (HDFS), Google File System (GFS)	Economic and credible distributed storage, fault tolerance, high throughput on large scale dataset
Parallel Programming Model[42]	IaaS Layer	Parallel execution of cloud computing programming model	MapReduce programming model by Google, Dryad and DryadLINQ	Parallelism and fault tolerance, data distribution, mass data processing, load balancing, network overhead reduction, performance improvement
Data Management[43]	PaaS layer	Analyzing and processing mass distributed data	HBase developed by Hadoop team, BigTable of Google, GFS, Scheduler, Lock Service	Efficiently managing mass distributed data, granularity based access authority, scalability, hierarchical data storage.
Open Source Software[44]	Saas Layer	Open source license free software without implementation environment management	Eucalyptus, Nimbus, Xen Hypervisor	Accessibility to computing power, no licensing cost overhead, large scale data intensive applications computation
Cloud Infrastructure Services[45]	IaaS Layer	Commercial cloud infrastructure for services	Amazon EC2/S3, GoGrid	Easy cluster computation, *pay-per-use* service model, cost effectiveness, service centralization

Table 1 above elaborates upon the varied technologies that amalgamate together to realize the complete cloud ecosystem. Security concerns of each of these technologies may also affect the robustness of real-time cloud implementations. Having understood the basic framework underlying any cloud deployment, we now look at the underlying risks and challenges involved from next section onwards.

3. Cloud Security Risks & Challenges

From our systematic review of existing literature we can state that Safety, Privacy and Reliance in the cloud are all interlinked. Before evaluating the security risks and challenges posed we first understand the meaning of the keywords security, privacy and trust in relation to the cloud by defining them[46]:

- **Security** is defined in terms of secrecy, accessibility and reliability of data or information. Security may also embrace validation and non-repudiation[46]. Security is said to be established in a transaction where all possible risks are either eliminated or bought to a nominal value[47].
- **Privacy** relates to obedience to diverse authorized and unauthorized norms relating to the right to concealed life[46]. The context may vary from nation to nation and may be understood as compliance to a nation's data protection regulations.
- **Trust** circles around 'assurance' that citizens, facts, things, information or courses will perform in accepted ways[48]. Trust may vary from human to human, machine to machine (for eg, handshake protocols settled within some protocols), human to machine (eg, when a client reassesses a digital signature advisory notice on a website) or machine to human (eg, when a system relies on client input and instructions without broad authentication)[46]. The Trusted Computer System Evaluation Criteria coined in 1970's and early 80's laid the basis of trust in convincing customers for the viability of a software[49]. Trust in IT is based on knowledge, calculus and social grounds[50]. At a deeper level, trust might be considered as an outcome of progress towards security or privacy objectives.

Taking the above definition of security, privacy and trust we shall now elaborate upon the various security risks posed by varied cloud deployments. For ease of understanding we have classified them into four broad categories namely: risks in service provisioning models, technological risks, operational risks as well as legal challenges as highlighted in the figure 4 and the sub-sections below:

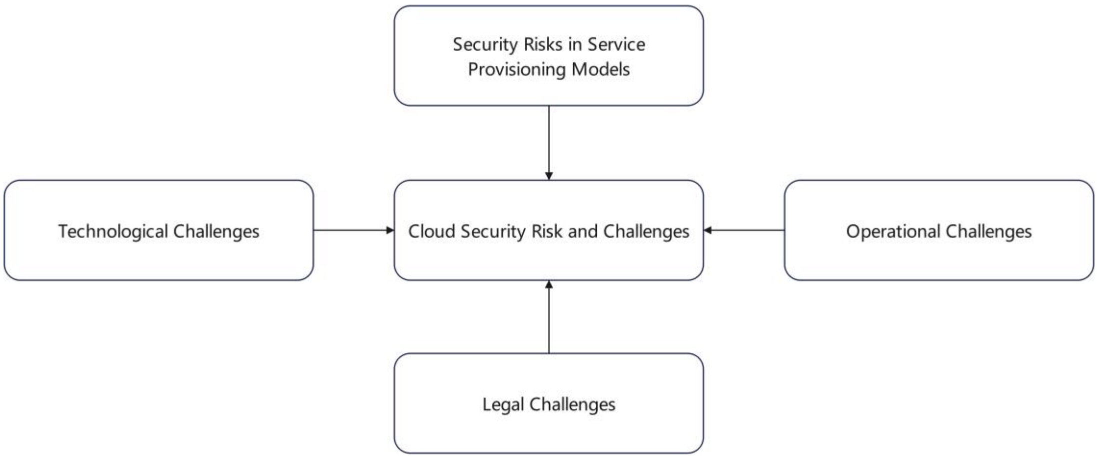
Security Risks in Service Provisioning Models
Technological Challenges
Cloud Security Risk and Challenges
Operational Challenges
Legal Challenges

Fig. 4. Cloud Security Risks and Challenges

A. Security Risks In Service Provisioning Models

Key hurdles in embracing the cloud are the real and superficial security risks. This section provides a holistic view of real-time cloud implementations protection to assess security preparedness for a business application to be migrated to cloud. By 2009, 70% of the CTOs in the IT sector believed the major apprehension in cloud transition were security and privacy concerns[51]. Gartner, surveyed and identified seven major cloud security risks in 2008 namely privileged user access, regulatory compliance, data location, recovery, data segregation, investigative support and long term viability[52].With the best demand fitting model and added advantages, cloud computing also comes out with some serious security concerns. A brief overview of these SPI (SaaS, PaaS and IaaS) security concerns at each service model is listed as follows-

1. Software as a Service (SaaS) Security Issues- The ability presented to the end user is to exploit the provider's application operating on a cloud infrastructure. The applications can be accessed from varied client devices through a thin client interface like a web browser (e.g., web-based email). Insecure end point usage of services is a security fear of SaaS. Hence, protection of enterprise data over SaaS necessitates close scrutiny. Here the security burden is completely onto the cloud provider due to the degree of abstraction. Hence, customer control or interference is minimal. Cloud service providers for SaaS are- LiveOps, Reval, Antenna Software, Cloud9 Analytics, CVM Solutions, Exoprise Systems, Gageln, Host Analytics, Knowledge Tree, Taleo, NetSuite, Google Apps, Microsoft 365, Salesforce.com, Rackspace, IBM, and Joyent[53].
2. Platform as a Service (PaaS) Security Issues- PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services. Compatibility of supported language and API types is a PaaS concern. Proprietary source platforms provide lesser control over security control than open source platforms. Here greater customer control is allowed as compared to SaaS due to reduced abstraction as compared to SaaS. Cloud service providers for PaaS are- Amazon AWS, Netsuite, IBM, Google Apps, Microsoft Azure, SAP, SalesForce, Intuit, WorkXpress, and Joyent[53].
3. Infrastructure as a Service (IaaS) Security Issues- 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. Security is the most critical concern of this layer as all other service models run on top of IaaS. Access privilege breach at hypervisors can lead to server content leak. Strong data encryption is a safeguard to third party access to data. This model offers the highest degree of customer control as compared to SaaS or PaaS. Cloud service providers for IaaS are- Amazon Elastic Compute Cloud, Rackspace, Citrix, Joyent, Bluelock, CSC, GoGrid, IBM, OpenStack, Rackspace, Savvis, VMware, Terremark, and BluePoint[53].

The security concerns and threats at varied SPI layers detailed above have been tabularized in Table 2 below:

Table 2. Security concerns and threats at varied cloud implementation levels [9]

Implementation Level	SPI Architecture Component	Users	Security Concern	Security Threats
Virtual Level[9]	Infrastructure-as-a-Service, Platform-as-a-service	Person deploying software on a cloud infrastructure.	Application security, data security, access control, image security, virtual cloud and communication security	Software interruption and modification, impersonization, DDOS, session hijack, exposing the network and disrupted communications, defacement
Application Level[9]	Software-as-a-service	Service subscribers to a cloud service provider	Multi-tenancy environment safeguard, communication protection, secure software and availability of service	Service level data modification, breach of privacy, data interruption, impersonization, session hijacking, network exposure.
Physical Level[9]	Data Centres	Owner/organization owning cloud deployment infrastructure	Legal and authentic use of cloud data centre. Hardware reliability and security maintenance. Network and resource protection from external threats.	DDOS attack, Connection flooding, hardware theft, modification and interruption, infrastructure misuse and natural disasters.

As observed from Table II above, it may be notable here to mention the interdependencies of these three cloud service models. SaaS and PaaS are hosted on top of the IaaS. Hence any attack on IaaS will definitely impact both SaaS as well as PaaS services[54]. This might be true the other way round too. Further we may also note that PaaS provides a platform to build and deploy SaaS applications[55]. Hence, increasing the interdependence between them. Thus an attack at any three of these service models will eventually effect the complete cloud deployment[56]. Further this interdependency may also generate confusion in case of an attack while fixing service provider responsibility. This immature and exploratory nature of cloud computing deployments; necessitates that cloud service users should be versed in risk tolerance prior to migrating to the cloud[57]. Issues like how to balance business benefits of cloud computing with the desirable levels of security and privacy should be clarified; proper integration of cloud security into conventional security measures need to be effectively dealt with. Sufficient and customised cloud security implementations can be achieved only once the cloud user has proper knowledge of the risks involved and bearable. Having identified the various security concerns as well as threats on the cloud we now elaborate how these concerns and threats can be transformed into attacks. A brief of such actual attacks is given in Table 3 below:

Table 3. A descriptive summary of different Attacks on Cloud [53], [58]

S.No	Attack Name	Nature of Attack	Attack Description	Attacking Methodology	Prevention Methodology
1	Malicious Insider[59]	Data Breach	Internal organization personnel abusing organization's data over the cloud	Corporate information misuse, private data exposure, worms, viruses and malicious code, theft of proprietary information or sensitive data.	Safeguarding internal firewall mechanism can be one optimal solution to the problem of malicious insider intrusions.
2	Online Cyber Theft[60]	Data Breach	Stealing an external organization's data over the cloud that is using external cloud computing platforms	LinkedIn stolen passwords, Dropbox spam attack, EC2 service virtual server scam	Autonomous security systems can be held in place to counter measure this situation.
3	Malware Injection Attack[61]	Cloud Security Attacks	Exploiting vulnerabilities of web applications by injecting malicious code for execution	Cross site scripting attacks, SQL injection attack, remote execution of system commands	File Allocation Table Utilization that will give an insight of user worthy apps.
4	Wrapping Attack[62]	Cloud Security Attacks	Using XML signature wrapping to exploit web servers validating authorized requests	SOAP message security breach, account hijacking attack on AWS, unauthorized access to EC2 instance	Digital Certificate based authentication for each XML document is a solution to Wrapping Attacks.
5	Denial of Service Attack[63]	Service Unavailability	Illegitimate users preventing legitimate users from accessing services warranted to them	Server request flooding, SYN Flood	Intrusion Detection Systems are a way to figure out and resolve DoS attacks.

B. Technological Challenges

With the evolving underpinnings in cloud technological advancements, there can be a vast range of challenges that come up for this technology[45]. These challenges can include:

a. Virtualization- Virtualization permits users to create, share, copy, and migrate and rollback virtual machines onto which they can run a varied set of applications. This creates loopholes for attackers so that they can draw advantage of the vulnerability of the extra layer introduced. Virtual machines need to be secured in the same way as physical machines as the two are inter-related and may affect each other as well. But in case of virtual machines, security guidance is much tougher on-ground implementation as this may lead to extrapolated entry points and increase interconnection complexity[45]. VMs need to be safeguarded in physical as well as virtual boundaries.
b. Interoperability of grid computing models at different levels of implementation.
c. Identity management implementation on cloud through mere web services.
d. Establishment and safeguard of trust in web application frameworks and service oriented architectures. Test of current technical encryption methodology and its ability to safeguard confidentiality.
e. Isolated virtual machines are managed by a hypervisor or the Virtual Machine Monitor (VMM). VMM is the main guardian of all isolated VMs in connections. If security at this level is compromised, the overall VM architecture security can be jeopardised. The low level software of VMM controls and manages traditional VMs and reports security flaws if any. The VMM implementation size is directly proportional to its vulnerability. Smaller and simpler VMMs have a lesser chance to be compromised on grounds of security.
f. Virtualization facilitates migration of VMs between physical servers for the purpose of load balancing, maintenance and fault tolerance. This can act as a security loophole and can transfer a VMM to a malicious server. If VM content is exposed on the network, data confidentiality and integrity is also at stake.
g. VMs located in the same server share resources like I/O, memory, CPU, etc. Resource sharing also leads to security compromise amongst VMs. VMs in the same server can breach information about each other without having to compromise the hypervisor. A malicious VM can monitor resources being shared amongst other VMs without being detected by VMM.

C. Legal Challenges

Numerous challenges are also posed by varied legal and regulatory frameworks relevant to cloud computing across nations[46]. These concerns may range from:

a. The viability of legal regimes imposing obligations based on the location of data;
b. The ex-ante definition of different entities (such as distinguishing between data controllers and processors);
c. Establishing consent of the data subject; the effectiveness of breach notification rules;
d. The effectiveness of cyber-crime legislation in deterring and sanctioning cyber-crime in the cloud and finally difficulties in determining applicable law and jurisdiction.

D. Operational Challenges

From operational perception, there are concerns relating to the efficacy of conventional risk governance frameworks[46]:

a. Whether cloud customers can meet their legal obligations when data or applications are hosted overseas,
b. How to be compliant and accountable when incidents occur;
c. Whether data will be locked into specific providers; the complexities in performing audit and investigations;
d. How to establish the appropriate level of transparency and finally measuring security of cloud service provision.

E. Cloud Migration

Cloud technology is penetrating in Small to Medium sized business ventures, compelling the service providers to migrate their operations and data on cloud[20].

1. Cloud Migration Advantages

This approach comes with many higher ups as mentioned below[64]:-

1. Humungous Data Analysis- Cloud computing is capable of detecting redundancy and discrepancy of humungous data volumes generated over the web. This scale of data manipulation and analysis gets difficult to manage in any offline data storage.
2. Location Independent Data Platform- Cloud is a global, language agnostic data platform for data transfer under the umbrella of efficient and fast computing. This model allows the user to access and manipulate his data from any geography independently[65].
3. Cost Efficient Model- Intensive business analytics are available to small and medium sized businesses at a very cost effective model[65]. Many third world countries that have faced backslash in the IT revolution are now pacing up with the advent of cloud computing.
4. Scalability- Enterprises can now service their delivery models to clients on an *as-on-need* basis. As soon as the requirements arise, computing resources can be deployed on the cloud. The software as a service API does cater to client load with as minimal of service provider interaction as possible[66].
5. Virtualization- Cloud provides a reliable mechanism for data backup and restoring using virtualization techniques.

2. Cloud Migration Issues

Migration of existing businesses and application domains over the cloud network poses some migration concerns that are detailed as below[67]-

1. Security and Privacy- Cloud computing is a new and shareable model that deals with great levels of uncertainty on security grounds at all implementation platforms. Security compromise is the prime concern of apprehension in cloud implementations today. The key to security and privacy is creating boundaries between unrelated entities, those who cannot be trusted in inter-communicative access[68]. With the best demand fitting model and added advantages, cloud computing also comes out with some serious security concerns. Placing faith on external reliance for data and services is a task for businesses[69]. Each business model deals with different users requirements and protecting each over the cloud is a separate concern[70].
2. Confidentiality- Confidentiality refers to only authorized access to data and protecting it from unintended usage[9]. Data confidentiality is hampered when there are multiple unwarranted accesses to data. Tremendous research has gone in into dealing with issues of data privacy, confidentiality and security over the cloud[71].
3. Data Integrity and Leakage- While migrating from client machines to cloud, data will face 2 major scenarios[72]. One is migration from local machine to cloud and second is change from single tenant to multi tenant environment. These changes compromise on data integrity and there is a high risk of data leakage. Applications are now designed in a Data leakage Prevention framework. The inter-operation of DLP agents with SaaS or PaaS services has technical implementation issues and still is a topic of research[73].
4. Compliance-Norms and regulation pertaining to storage and use of data vary across geographies. Customer need to comply with regular audit trails and reporting for managing compliance and security over the cloud[74].
5. Availability- The ultimate goal of cloud computing is that users should be able to use services, anytime, anywhere[75]. Availability is a system aspect of being available for use upon demand by a legal access[9]. System availability must pertain by alternate mechanisms even in the advent of security breach. Cloud owner has to take up the guarantee that the services will be available to authorized persons under all circumstances[9].

4. Cloud Security: Frameworks and Techniques

Cloud security has a set of implementable frameworks and techniques that ensure safeguarding privacy, confidentiality and integrity of data over the cloud. Few of these techniques are detailed at length below [67].

1. Cryptographic data separation- The success of the cloud security models implementation and deployment primarily depends on the factor as to how secure and protected is sensitive data within the framework[9]. One workaround of implementing such privacy is by cryptographically securing information and making it seem as a black box to the outside entities[76]. Encryption decryption techniques help in safeguarding integrity, confidentiality and data privacy[77]. Cryptography techniques are symmetric and asymmetric in nature. Symmetric cryptography provides high efficiency whereas asymmetric cryptography offers security, combining and using the two is the most efficient proven approach[77].
2. Client Server Authentication-The strongest authentication process in distributed computing environment functions in the combination of Ldap and SSO[9]. Outsourced services raise the need for adoption of a Single-Sign on solution for authentication purposes. Earlier concepts revolved around intra-organization identity based authentication that has now transitioned to application security within organizational cloud environments[36]. An open source middleware called Shibboleth provides inter and intra organizational Web Single Sign On[78], [79].
3. Security Domain Creation- Establishing trust between related entities in a secure domain can be done by collaborating federation groups along with Ldap[67]. A federation in essence is a legal body that enforces a common set of rules and policies for online resource sharing[80]. Cloud infrastructures can be distinguished into multiple security domains based on their implementations. The basis of this domain classification lies in the fact that few infrastructures share common authentication, authorization, session maintenance, etc[9]. Clouds grouped under different federations are commonly referred to as '*federated clouds*'. Federated clouds implementations interact and exchange data with each other under a common framework. Individual cloud implementations in a federated framework remain isolated in existence but are interoperable through standard interfaces[81]. Such interactions are authenticated and validated by security norms of the federation.
4. Certificate Based Authorization- Cloud provides a cohesive set of resources individual in nature that are dynamically accessible to the users[9]. The resources and users of cloud don not hail from the same security domain hence user identification is primarily based attributes and characteristics and not on conventional network identity check mechanism[67]. This enhancement calls for newer access control models based on attributes and characteristics[82]. PKI facility issued certificates like X.509 certificates can enforce access control in web setups[9]. The process of certificate issuance is to be centred with a certification authority as a global trusted centre[83]. Person specific attribute-value pairs contain attribute-value pairs for authentication. Attribute-based authentication adds up greatly to scaling distributed large-scale applications to the cloud.

5. Future Research Directions

Cloud Computing is a large umbrella business model, that may cover a whole organization, a country or the complete globe[84]. Hence, there need to be properly laid varied strategies that can secure a cloud from unauthorized access at various levels of deployment[85]. However, to completely secure a cloud deployment from any sort of misuse or attack proper regulatory laws and law enforcing agencies are also desired[86]. Thus, cloud computing as a research frontier shall always be open to finding novel ways and means to alleviate existing and new security concerns in the ever-expanding cloud ecosystem[87].

Notably, public cloud computing and virtualization of existing IT infrastructure shall be two scenarios more susceptible to new threats. Researchers from Xerox's PARC and Fujitsu Laboratories of America have warned that these 'new threats require new mechanisms to maintain and improve security' and highlight the need to design 'tools to control and understand privacy leaks, perform authentication, and guarantee availability in the face of cloud denial-of-service attacks'[88]. For example, encrypting stored data ensures data confidentiality. This, however, prevents cloud service providers from executing services on this data—'searching and indexing data is impossible to do with traditional, randomized encryption schemes'[89].

Here, it is also notable to mention that a lot of research issues need to be addressed before Cloud computing can attain its full potential[90]. Most importantly Scalability, high availability, Virtualization, Energy efficiency and power management along with automated service provisioning require to be closely monitored for potential security threats and attacks[91].

Worldwide cloud computing adoption in increasing very rapidly. India is not an exception for this. "In India, cloud services revenue is projected to have a five-year projected compound annual growth rate (CAGR) of 33.2 percent from 2012 through 2017 across all segments of the cloud computing market. Segments such as software as a service (SaaS) and infrastructure as a service (IaaS) have even higher projected CAGR growth rates of 34.4 percent and 39.8 percent," said Ed Anderson, research director at Gartner[92].However, it is important to understand the opportunities and threats for cloud computing in the current Indian ecosystem. We first try to lay down the bright opportunities for widespread cloud adoption:

i. The Digital India project of the Indian Government unleashes tremendous potential for widespread cloud adoption in all its e-governance initiatives[93].
ii. The ‘Make in India’ initiative of the Government is further boosting the manufacturing sector with considerably 24.1% contributions to the total cloud ERP market in India[94]. Ernest & Young India news release on cloud adoption mentions that more than 60% cloud implementations focus on infrastructure consolidation by adopting IaaS[95]. The manufacturing industry is rapidly virtualizing their servers and desktops along with SaaS platform for enterprise application deployments by many manufacturing firms[96]. The Indian manufacturing scenario offers big potential for cloud adoption in 2016 and beyond. Government initiatives like Digital India and Make in India are expected to foster cloud adoption among manufacturing SMEs and large enterprises[94].
iii. Government of India has embarked upon an ambitious initiative called GI Cloud also named MeghRaj[97]. This decision has been taken to utilize and harness the benefits of cloud computing. The focus of this initiative is to accelerate delivery of e-services in the country while optimizing ICT spending of the government[98].
iv. Microsoft to invest Rs 1,400crore in India cloud data centres[98]. Microsoft Launches Cloud Accelerator Program for Indian Enterprises & Government[99]. TCS involved in putting data centers in India.
v. Increased number of IT companies and ISPs in India.
vi. The key drivers for IT growth in India is highlighted by the growing acceptance of cloud based solutions, embracing merging technologies like Internet of Things (IoT), Big Data, mobile technologies (3G, 4G) and fuelled by Indian government’s initiatives for a digital India[100].

However the complete Indian ecosystem is not welcoming as it has its share of threats too. We list some notable ones below:

- India is a diverse country with wide diversity in terms of its population, land as well as the availability of resources throughout the country. In such a situation, data transfer bottlenecks and therefore the available network bandwidth constraint issue may arise.
- Poor connectivity in rigid terrain areas may further degrade the quality of service.
- Although the government of India has initiated the movement of using the cloud for e-governance applications, absence of strict legal laws, policies and their appropriate implementers may further play a spoilsport for effective cloud services implementation.
- India is not yet economically strong therefore direct service cost and hidden cost (backup, system recovery and problem solving may affect the adoption of cloud.

The above opportunities and threats are a brief into how cloud computing scenario is evolving in India[101]. The authors may not be de-motivated as the above discussion simply implies that India as a diverse nation has already embarked upon its journey for cloud adoption and is evolving with time in the same[100]. However, exploring the complete potential of cloud technology for the improvement of services, processes and life in India as a particular case poses a number of potential challenges that are being researched and viable solutions being prepared.

6. Conclusion

Cloud computing has changed the face of technological advancements in the present era. The crux of the innovation focuses on leveraging commercial attributes to the likes of reliability, cost, maintenance and acquiring technological systems through cloud driven data centres. This chapter analyzes and forecasts the long run of cloud computing industry in a developing economy like India where cloud strengths, opportunities, weaknesses and threats can be converted as developmental tools. Cloud enhances the enterprise business model by increasing industrial throughput in aspects of reduction of time and efforts and enhancing cost effectiveness. Along with the long list of higher ups come a few limitations in cloud adaption globally in terms of security, privacy, interoperability and compatibility. Modern research trends are indicative of the fact that a lot of active research goes into managing threats and weaknesses arising from cloud technical implementation scenarios. Statistics are indicative that even more efforts are required to overcome issues from the perspective of licensing issues, service level agreements, billing and pricing issues, adoption framework, etc. The upsurge of cloud model acceptance comes from hardware and software giants, government agencies, customers and research community. Our research is indicative that this trend will continue to rise in the upcoming years. The market competition and demands are imposing new evolutions in cloud computing. The near future shall witness a metamorphosis into cloud client/server architecture, personal cloud, hybrid cloud and IT. Many techniques and frameworks are evolving to counter measure data security, privacy breach and trust over cloud. The penetration of cloud in every private and public sector endeavours such as e-governance frameworks is the onset of a new transitional change in sectors like education, finance, healthcare, energy, etc.

References

[1] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in *2012 International Conference on Computer Science and Electronics Engineering*, 2012, pp. 647–651.

[2] "Top 10 Strategic Technology Trends for 2018: Cloud to the Edge." [Online]. Available: https://www.gartner.com/doc/3865403?ref=mrktg-srch. [Accessed: 31-Jan-2019].

[3] D. Parkhill, "Challenge of the computer utility," 1966.

[4] J. Yang, Z. C.-C. intelligence and software, and undefined 2010, "Cloud computing research and security issues," *ieeexplore.ieee.org*.

[5] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 1, p. 5, 2013.

[6] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology."

[7] K. Stanoevska, T. Wozniak, and S. Ristol, *Grid and cloud computing: a business perspective on technology and applications*. 2009.

[8] G. Christina Oliver, "NIST SP 800-145, The NIST Definition of Cloud Computing."

[9] D. Zissis, D. L.-F. G. computer systems, and undefined 2012, "Addressing cloud computing security issues," *Elsevier*.

[10] N. Gruschka, M. J.-2010 I. 3rd international conference on, and undefined 2010, "Attack surfaces: A taxonomy for attacks on cloud services," *computer.org*.

[11] A. Fox, R. Katz, A. Konwinski, and G. Lee, "Above the Clouds: A Berkeley View of Cloud Computing," 2009.

[12] L. K.-I. S. & Privacy and undefined 2009, "Data security in the world of cloud computing," *ieeexplore.ieee.org*.

[13] A. W.- networker and undefined 2007, "Computing in the clouds," *computing.dcu.ie*.

[14] S. Zhang, S. Zhang, X. Chen, … X. H.-S. international conference, and undefined 2010, "Cloud computing research and development trend," *computer.org*.

[15] G. Zhao *et al.*, "Cloud Computing: A Statistics Aspect of Users," 2009, pp. 347–358.

[16] A. K.-S. A. and Processing, 2010. ICSAP'10, and undefined 2010, "Cloud computing: Applying issues in small business," *ieeexplore.ieee.org*.

[17] M. G. Jaatun, G. Zhao, and C. Rong, *Cloud computing : first international conference, CloudCom 2009, Beijing, China, December 1-4, 2009 : proceedings*. Springer, 2009.

[18] "Home | Public Website," 2010. [Online]. Available: https://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf. [Accessed: 31-Jan-2019].

[19] M. Dikaiakos, D. Katsaros, … P. M.-I. I., and undefined 2009, "Cloud computing: Distributed internet computing for IT and scientific research," *ieeexplore.ieee.org*.

[20] S. Subashini, V. K.-J. of network and computer applications, and undefined 2011, "A survey on security issues in service delivery models of cloud computing," *Elsevier*.

[21] "How to Gain Comfort in Losing Control to the Cloud Randolph Barr CSO - Qualys, Inc SourceBoston, 23. April ppt download." [Online]. Available: https://slideplayer.com/slide/7248774/. [Accessed: 29-Jan-2019].

[22] J. Rittinghouse and J. Ransome, *Cloud computing: implementation, management, and security*. 2016.

[23] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud security and privacy: an enterprise perspective on risks and compliance*. 2009.

[24] W. Li, L. P.-I. I. C. on C. Computing, and undefined 2009, "Trust model to enhance security and interoperability of cloud environment," *Springer*.

[25] S. Ramgovind, M. Eloff, … E. S.-S. for S. A., and undefined 2010, "The management of security in cloud computing," *ieeexplore.ieee.org*.

[26] K. S.-I. J. of C. Networks and undefined 2011, "Cloud computing security issues and challenges," *researchgate.net*.

[27] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology."

[28] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 2010, pp. 27–33.

[29] P. Biljanović and E. and M.-M. Croatian Society for Information and Communication Technology, *MIPRO 2010 : 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics : May 24-28, 2010, Opatija, Croatia*. Croatian Society for Information and Communication Technology, Electronics and Microelectronics, 2010.

[30] J. Yang, Z. C.-C. intelligence and software, and undefined 2010, "Cloud computing research and security issues," *ieeexplore.ieee.org*.

[31] Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," in *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, 2012, pp. 877–880.

[32] P. Mathur, N. N. G. C. (PDGC), 2010 1st, and undefined 2010, "Cloud computing: New challenge to the entire computer industry," *ieeexplore.ieee.org*.

[33] L. Savu, "Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges," in *2011 International Conference on Computer and Management (CAMAN)*, 2011, pp. 1–4.

[34] J. Gibson, R. Rondeau, D. Eveleigh, and Q. Tan, "Benefits and challenges of three cloud computing service models," in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, 2012, pp. 198–205.

[35] I. Hashem, I. Yaqoob, N. Anuar, S. Mokhtar, A. G.-I. systems, and undefined 2015, "The rise of 'big data' on cloud computing: Review and open research issues," *Elsevier*.

[36] "ROUGH TYPE | Nicholas Carr's blog." [Online]. Available: http://www.roughtype.com/. [Accessed: 30-Jan-2019].

[37] A. Stanik, M. Hovestadt, and O. Kao, "Hardware as a Service (HaaS): Physical and virtual hardware on demand," in *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, 2012, pp. 149–154.

[38] S. Zhang, H. Yan, and X. Chen, "peer-review under responsibility of [name organizer]," *Phys. Procedia*, vol. 33, pp. 1791–1797, 2012.

[39] J. Ekanayake and G. Fox, “High Performance Parallel Computing with Clouds and Cloud Technologies,” Springer, Berlin, Heidelberg, 2010, pp. 20–38.

[40] F. Lombardi and R. Di Pietro, “Secure virtualization for cloud computing,” *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1113–1122, Jul. 2011.

[41] K. Gai, M. Qiu, and H. Zhao, “Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data,” in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 2016, pp. 140–145.

[42] R. L. Grossman, “The Case for Cloud Computing,” *IT Prof.*, vol. 11, no. 2, pp. 23–27, Mar. 2009.

[43] S. Sakr, A. Liu, D. M. Batista, and M. Alomari, “A Survey of Large Scale Data Management Approaches in Cloud Environments,” *IEEE Commun. Surv. Tutorials*, vol. 13, no. 3, pp. 311–336, 2011.

[44] D. Nurmi *et al.*, “The Eucalyptus Open-Source Cloud-Computing System,” in *2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, 2009, pp. 124–131.

[45] M. Armbrust *et al.*, “A view of cloud computing,” *Commun. ACM*, vol. 53, no. 4, p. 50, Apr. 2010.

[46] N. Robinson *et al.*, “The Cloud: Understanding the Security, Privacy and Trust Challenges,” *SSRN Electron. J.*, Nov. 2010.

[47] J. Falkheimer, “Anthony Giddens and public relations: A third way perspective,” *Public Relat. Rev.*, vol. 33, no. 3, pp. 287–293, Sep. 2007.

[48] D. Artz, Y. G.-W. S. Science, S. and A. on the, and undefined 2007, “A survey of trust in computer science and the semantic web,” *Elsevier*.

[49] A. Nagarajan and V. Varadharajan, “Dynamic trust enhanced security model for trusted platform based services,” *Futur. Gener. Comput. Syst.*, vol. 27, no. 5, pp. 564–573, May 2011.

[50] D. L.-C. Communications and undefined 2003, “Establishing and managing trust within the Public Key Infrastructure,” *Elsevier*.

[51] D. Chen, H. Z.-C. S. and Electronics, and undefined 2012, “Data security and privacy protection issues in cloud computing,” *ieeexplore.ieee.org*.

[52] J. B.- Infoworld and undefined 2008, “Gartner: Seven cloud-computing security risks,” *idi.ntnu.no*.

[53] T.-S. Chou, “Security Threats on Cloud Computing Vulnerabilities,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, pp. 79–88, Jun. 2013.

[54] S. Subashini, V. K.-J. of network and computer applications, and undefined 2011, “A survey on security issues in service delivery models of cloud computing,” *Elsevier*.

[55] W. Bin, H. Yuan, L. Xi, X. M.-B. Engineering, undefined 2009, and undefined 2009, “Open identity management framework for SaaS ecosystem,” *ieeexplore.ieee.org*.

[56] E. Fong and V. Okun, “Web Application Scanners: Definitions and Functions,” in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)*, 2007, p. 280b–280b.

[57] H. Demirkan and D. Delen, “Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud,” *Decis. Support Syst.*, vol. 55, no. 1, pp. 412–421, Apr. 2013.

[58] B. Prabadevi and N. Jeyanthi, “Distributed Denial of service attacks and its effects on Cloud environment- a survey,” in *The 2014 International Symposium on Networks, Computers and Communications*, 2014, pp. 1–5.

[59] D. Catteddu, “Cloud Computing: Benefits, Risks and Recommendations for Information Security,” 2010, pp. 17–17.

[60] A. Alqahtani and H. Gull, “Cloud Computing and Security Issues-A Review of Amazon Web Services,” 2018.

[61] A. Choudhary, M. D.-I. J. of Computer, and undefined 2012, “CIDT: Detection of malicious code injection attacks on web application,” *researchgate.net*.

[62] M. McIntosh, P. A.-P. of the 2005 workshop on Secure, and undefined 2005, “XML signature element wrapping attacks and countermeasures,” *dl.acm.org*.

[63] N. Gruschka, L. I.-W. Services, 2009. ICWS 2009. IEEE, and undefined 2009, “Vulnerable cloud: Soap message security validation revisited,” *ieeexplore.ieee.org*.

[64] A. Gupta, P. Dhyani, O. R.-I. J. of, and undefined 2013, “Cloud based e-voting: one step ahead for good governance in India,” *pdfs.semanticscholar.org*.

[65] A. Bisong, S. S. M. Rahman, and M. Rahman, “An Overview Of The Security Concerns In Enterprise Cloud Computing,” *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 1, pp. 30–45, Jan. 2011.

[66] A. Dubey, D. W.-T. M. Quarterly, and undefined 2007, “Delivering software as a service,” *pocsolutions.net*.

[67] D. Zissis, D. L.-F. G. computer systems, and undefined 2012, “Addressing cloud computing security issues,” *Elsevier*.

[68] R. S.-C. & Security and undefined 1992, “Distributed systems security,” *Elsevier*.

[69] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, “On Technical Security Issues in Cloud Computing,” in *2009 IEEE International Conference on Cloud Computing*, 2009, pp. 109–116.

[70] W. Voorsluys, J. Broberg, and R. Buyya, “Introduction to Cloud Computing,” in *Cloud Computing*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2011, pp. 1–41.

[71] J. Heiser, M. N.-G. Report, and undefined 2008, “Assessing the security risks of cloud computing,” *academia.edu*.

[72] F. S.-S. and N. (ICCSN), 2011 IEEE 3rd, and undefined 2011, “Cloud computing security threats and responses,” *ieeexplore.ieee.org*.

[73] “About Us | Trend Micro.” [Online]. Available: https://www.trendmicro.com/en_us/about.html. [Accessed: 30-Jan-2019].

[74] A. Kumar Gupta and S. Prakash, “SERVICE ENHANCEMENT USING CLOUD COMPUTING.”

[75] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, “On Technical Security Issues in Cloud Computing,” in *2009 IEEE International Conference on Cloud Computing*, 2009, pp. 109–116.

[76] C. Pfleeger and S. Pfleeger, *Security in computing*. 2002.

[77] D. Zissis, D. L.-F. G. computer systems, and undefined 2012, “Addressing cloud computing security issues,” *Elsevier*.

[78] C. Uikey and D. S. Bhilare, “Security and trust life cycle of multi-domain cloud environment,” in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2017, pp. 2670–2678.

[79] “Shibboleth | Internet2.” [Online]. Available: https://www.internet2.edu/products-services/trust-identity/shibboleth/. [Accessed: 07-Feb-2019].
[80] “UK federation information centre | Documents / AvailableServices browse.” [Online]. Available: https://www.ukfederation.org.uk/content/Documents/AvailableServices. [Accessed: 07-Feb-2019].
[81] K. Stanoevska, T. Wozniak, and S. Ristol, *Grid and cloud computing: a business perspective on technology and applications*. 2009.
[82] B. Lang, I. Foster, F. Siebenlist, R. Ananthakrishnan, and T. Freeman, “A Flexible Attribute Based Access Control Method for Grid Computing,” *J. Grid Comput.*, vol. 7, no. 2, pp. 169–180, Jun. 2009.
[83] “Security models for web-based applications,” *dl.acm.org*.
[84] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, “Security and Privacy in Cloud Computing: A Survey,” in *2010 Sixth International Conference on Semantics, Knowledge and Grids*, 2010, pp. 105–112.
[85] *International journal of engineering and computer science IJECS.* .
[86] M. Al Morsy, J. Grundy, and I. Müller, “An Analysis of the Cloud Computing Security Problem.”
[87] R. E.-G.-I. W. C. on T. and and undefined 2014, “A literature review on cloud computing adoption issues in enterprises,” *Springer*.
[88] S. Yoshikawa and S. Sasaki, “R&amp;D Strategy of Fujitsu Laboratories-Toward a Human-Centric Networked Society,” 2010.
[89] R. Chow *et al.*, “Controlling data in the cloud,” in *Proceedings of the 2009 ACM workshop on Cloud computing security - CCSW ’09*, 2009, p. 85.
[90] G. Christina Oliver, “NIST SP 800-145, The NIST Definition of Cloud Computing.”
[91] A. Beloglazov and R. Buyya, “Energy Efficient Resource Management in Virtualized Cloud Data Centers,” in *2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing*, 2010, pp. 826–831.
[92] P. Chatterjee and N. De, “CLOUD COMPUTING IS GENERATING ECONOMIC GROWTH AND EMPLOYMENT OPPORTUNITIES IN INDIA.”
[93] S. H. Patil, A. C. Adamuthe, V. D. Salunkhe, and G. T. Thampi, “Cloud Computing-A market Perspective and Research Directions,” *Inf. Technol. Comput. Sci.*, vol. 10, pp. 42–53, 2015.
[94] D. G. Chandra and R. S. Bhadoria, “Cloud Computing Model for National E-governance Plan (NeGP),” in *2012 Fourth International Conference on Computational Intelligence and Communication Networks*, 2012, pp. 520–524.
[95] G. F. Knolmayer and P. Asprion, “Assuring Compliance in IT Subcontracting and Cloud Computing,” Springer, Berlin, Heidelberg, 2011, pp. 21–45.
[96] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, “Cloud computing — The business perspective,” *Decis. Support Syst.*, vol. 51, no. 1, pp. 176–189, Apr. 2011.
[97] A. Lele, “Cloud Computing,” Springer, Singapore, 2019, pp. 167–185.
[98] D. Evans and D. C. Yen, “E-Government: Evolving relationship of citizens and government, domestic, and international development,” *Gov. Inf. Q.*, vol. 23, no. 2, pp. 207–235, Jan. 2006.
[99] N. Kshetri, T. Torbjörn Fredriksson, D. C. Rojas Torres, T. Fredriksson, and D. C. R. Torres, *Big Data and Cloud Computing for Development*. New York, NY : Routledge, 2017.: Routledge, 2017.
[100] L. A. Tawalbeh, W. Bakheder, and H. Song, “A Mobile Cloud Computing Model Using the Cloudlet Scheme for Big Data Applications,” in *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, 2016, pp. 73–77.
[101] A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, “Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS,” in *2010 IEEE 3rd International Conference on Cloud Computing*, 2010, pp. 450–457.

Authors’ Profiles

Dr. Imran Khan is currently working as an Assistant Professor at Harcourt Butler Technical University Kanpur, U.P. India. He completed his Ph.D> from Jamia Millia Islamia, New Delhi, India. He awarded his MCA from Aligarh Muslim University. He worked as an Assistant Professor at BVICAM, New Delhi and has more than 8 years of teaching and research experience. His area of research is Big Data, Cloud Computing and Data Science.

Ms. Tanya Garg is a Research Scholar at Faculty of Computer Applications, Bharati Vidyapeeth’s Institute of Management and Research, Bharati Vidyapeeth (deemed to be University), New Delhi, India. She is currently working as an Assistant Professor, Bharati Vidyapeeth’s Institute of Computer Applications and Management, New Delhi, India for the past 7 years. She has an additional 3 years of corporate work experience. She completed her BCA, MCA from Guru Gobind Singh Indraprastha University, New Delhi and is a University Gold Medalist for her MCA, Class of 2014. Her research interests include Machine Learning and Data Science.

How to cite this paper: Imran Khan, Tanya Garg, "An Analytical Study of Cloud Security Enhancements", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.1, pp. 14-28, 2024. DOI:10.5815/ijwmt.2024.01.02